International Journal of Engineering & Technology, 7 (2.32) (2018) 341-344

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Review on Security Issues and Challenges of IoT

Dr. E. Suresh Babu[1], V. Bhargav Raj[2], M.Manogna Devi[3], K.Kirthana[4]

[1,2,3,4]Dept.CSE, KLEF, Guntur, India
**Corresponding author E-mail: sureshbabu.erukala@kluniversity.in*

Abstract

This papers reviews and surveys the security issues, mechanism of internet of things (IoT) proposed in the literature. As IoT is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The main advantages of IoT improve the resource utilization ratio and relationship between human and nature. In addition, it possesses various characteristics like sensing, heterogeneity, connectivity, dynamic nature and intelligence. However, it possesses several challenges like connectivity, compatibility, longevity, privacy and security. Specifically, Security and privacy are the crucial issues that need to be solved for successful deployment of IoT. Moreover, some of the data collected from the IoT are very sensitive and should not be revealed to third parties. Such data needs to be protected by some provided legislations. We reviewed some of the security challenges of IoT like secure communication, data privacy and integrity, authorizing and authenticating the devices.

Keywords:*Security issues in IoT, challenges in IoT, Review on IoT.*

1. Introduction

Internet of Things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The main advantages of IoT improve the resource utilization ratio and relationship between human and nature. Moreover, it is more flexible and accessible anywhere. In addition, it possesses various characteristics like sensing, heterogeneity, connectivity, dynamic nature and intelligence. These characteristics exhibits with various applications of IoT in real world like smart homes, smart cities, IoT in agriculture, smart retail, healthcare, smart technology. These applications are being developed in every sector to provide more service from this technology. However, it possesses several challenges like connectivity, compatibility, longevity, privacy and security. Specifically, Security and privacy are the crucial issues that need to be solved for successful deployment of IoT because of insufficient security features, ineffective authentication, insecure web interface, insecure cloud interface, insecure network services, insecure mobile interface, lack of transport encryption and insecure software. The basic security weakness of the IoT is that it increases the number of devices behind your network's firewall. Few years back, the issue was on securing our personal computers which later it came to securing our smartphones. Now our cars, home appliances, and many other IoT devices are also vulnerable to the security attacks. Moreover, some of the data collected from the IoT are very sensitive and should not be revealed to third parties. Such data needs to be protected by some provided legislations. Some of the security challenges of IoT like securing constrained devices, secure communication, ensure data privacy and integrity, ensure high availability, predict and pre-empt security issues managing device updates, detecting vulnerabilities and challenges and authorizing and authenticating devices. This papers review various issues, mechanism on security proposed by various researchers in the literature.

2. Security Issues

To develop an IoT application security framework has got a great importance. There are some security concerns (shown in Fig.1) while creating a secured and attack resistant IoT applications.

2.1 Data Encryption

Typical IoT applications gather huge amounts of data where data retrieval and processing is the core part of IoT. As the data is personal it should not be disclosed to anyone. So, it should not be encrypted using Secure Socket Layer when your data is present online. Websites in default use SSL certification to secure the user's data online. In a wireless protocol this is a part and the other part comes into picture during data transfer which should also be encrypted. As sensitive data should be available only to the concerned user and not to anyone else. So, make sure to use wireless protocol with default encryption.

2.2 Data Authentication

There is a chance of IoT device being hacked even after successful encryption of data. The security is compromised, if the device could not be provided authenticity where data is communicated to and from an IoT device. For example consider a temperature sensor in a smart home. Even after encrypting the data it transfers, authentication is not provided then someone can hack it give some wrong data which might insist your sensor to heat the room even though the room is hot. Authentication issues may not be noticed in small things but definitely be a security risk.

2.3 Side Channel Attacks

Encryption and authentication have chance for side channel attacks. These attacks focus more on how that information is being presented and less on the information. Suppose if someone is able to handle data like timing information, power consumption or electromagnetic leak, this data can be used for side channel attacks.

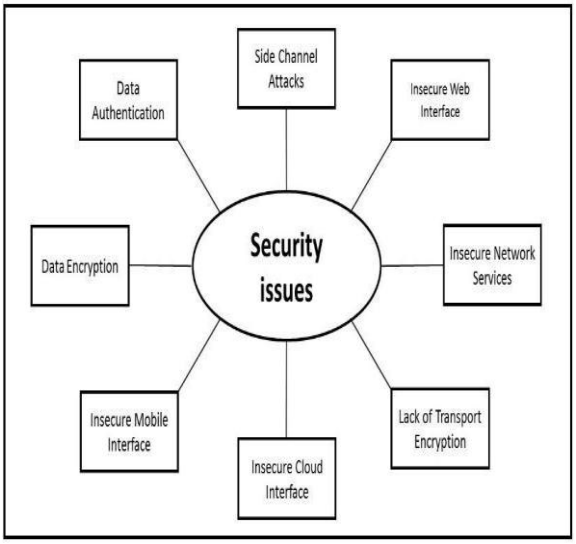

Fig.1. All Security issues in IoT

2.4 Manage Device Updates

For instance, when we apply updates the reliability crosswise over conveyed situations. When updates are applied to the devices they strengthen the down time and should be available across all generations.

2.5 Authorize and Authenticate Devices

The authorize and authenticate devices are for securing IoT systems. In authorize and authenticate the devices must identify before they can access. At some point these devices fall in authenticate like by using weak passwords. By adopting IoT platform we can resolve these issues. In this system each device will access throughout the system.

2.6 Secure Constrained Devices

Numerous IoT gadgets have restricted measures of capacity, memory, and preparing ability and they regularly should have the capacity to work on bring down power, for instance, when running on batteries. Security approaches that depend intensely on encryption are not a solid match for these obliged gadgets, since they are not fit for performing complex encryption and unscrambling rapidly enough to have the capacity to transmit information safely continuously. These gadgets are regularly defenceless against side channel assaults, for example, control investigation assaults, that can be utilized to figure out these calculations. Rather, obliged gadgets ordinarily just utilize quick, lightweight encryption calculations. IoT frameworks should make utilization of different layers of safeguard, for instance, isolating gadgets onto isolate systems and utilizing firewalls, to adjust for these gadget confinements.

3 Security Challenges in IoT

Due to the expanded utilization of IoT gadgets, the IoT systems are prone to different security attacks. The below mentioned are the various security challenges faced in IoT which are the root cause of security attacks.

3.1 Detect Vulnerabilities and Challenges

In spite of best endeavours, security vulnerabilities and breaks are unavoidable. How would you know whether your IoT framework has been traded off? In expansive scale IoT frameworks, the many-sided quality of the framework regarding the quantity of gadgets associated, and the assortment of gadgets, applications, administrations, and correspondence conventions included, can make it hard to distinguish when an occurrence has happened. Techniques for distinguishing vulnerabilities and ruptures incorporate checking system interchanges and action logs for irregularities, taking part in infiltration testing and moral hacking to uncover vulnerabilities, and applying security insight and investigation to recognize and advise when episodes happen.

4. Security Services

Apart from the challenges of security in IoT, there are various services provided to ensure security. The main motto of the services is to guarantee the accuracy and consistency of data.

4.1 Authentication

Authentication identifies legitimate users from unauthorized users. It ensures that the access is only provided to the actual users. It is the act of confirming the truth of an attribute of data claimed true by an entity which is necessary to validate the user's data in a system. There are different kinds of authentication types which can identify the real users of a system. Some of them are Kerberos authentication protocol, digest authentication, SSL/TLS, VPN and smart cards.

4.2 Integrity

The assurance of consistency and accuracy of the data can be termed as data integrity. Integrity is one of the security policy to ensure privacy of the data. Data integrity can be verified by mathematical algorithm called hash, in which SHA(secure hash algorithms) is more popular. A better approach for a data integrity check is with a shared private key which is called keyed-hash message authentication code. Integrity checks likewise should be utilized for information that is being handled to guarantee that the information and its flow can be trusted.

4.3 Confidentiality

When the data is shared publicly, it must be protected in order to avoid unwanted access of the information. The confidentiality attacks occur at the network layer while the data is routing through the medium and being exposed. An intended exposure attack happens when the routing element enables the data to be exposed to an outside element either because of misconfiguration or by some attack. To prevent this kind of attack, the communicating nodes must be authenticated.

4.4 Privacy

Some of the data collected by IoT are very sensitive and should not be revealed to third parties. Such data is protected by some provided legislations. Even then the required precautions are not taken while storing data or sharing it with others. In some cases, the single data might not be sensitive but when combined with other devices, the data pattern might be revealed which may cause damage. Hence individual privacy is more recommended

5. Various Mechanisms Proposed in Literature of IOT

5.1 Confidentiality

1. In [1] zhicaishi et.al have presented a protocol which utilizes CRC function not hash function to encrypt all sessions so as to ensure the confidentiality. For each authentication, different random numbers are assured. After each successful authentication, RFID system is update.

2. In [2] chih-Hsuehlin et.al have proposed the concept of random key pre distribution scheme to perform key agreement for wireless sensor network. In this process, the sensor nodes will implement embedded with a random subset of keys. The sensor nodes will implement a challenge and response process to explore the common key among the sensor nodes.

3. In [3] christoschatzigeorgiou et.al have presented a protocol which is a two-step privacy protection. In this process it consist of two step process. Each step involves a server with a unique role. In the first step, it conceals the user's identity and in the second step it supports the end to end encryption.

4. In [4] juhannes braun and Johannes buchmann et.al have proposed the quantum key distribution .This mechanism is used to securely transmit a key. That key can then be used as an OTP to encrypt the data. It inherit to point to point character.

5. In [5] parkand ji-yong et.al have proposed a secure key checksum ,an integrated secure mechanism suitable for network coding with encryption and checksum combining an encryption key and a checksum see. The secure key checksum provides confidentiality by using encryption of information with block cipher between source and destination

Table 1: Different mechanisms for providing Confidentiality

S.no	Title	Mechanism	Advantages	Disadvantages
1	A light weight RFID authentication protocol with confidentiality and anonymity	Radio Frequency Identification(RFID)	a)prevent eavesdropping b)prevents information leakage c)prevents replay attack d)needs less computation	a)storage resources are limited. b) easy attackable c)It reveals their privacy.
2	private–trust-confidentiality	Random secret key pre distribution	a)prevents forgery and replay attack. b)prevents masquerading attack. c)prevents sensing information.	a)Weakness of storing plain keys
3	Communication gateway architecture for ensuring privacy and confidentiality in incident reporting	Two step privacy protection	a)eavesdropping is not possible because of double encryption b) prevention of data supports anonymous reporting of incidents	a)anonymity b)can easily attack the encrypted data c)occurs correlation of time.
4.	Perfect Confidentiality Network	Quantum key distribution	a)detect the eavesdropper b)we can securely transmit the key	a)the data can be transmitted to limited kilometers b)equipment is expensive. c)quantum key distribution has an inherent point-to-point character
5.	Integrated Security Mechanism Network Coding Combining Confidentiality and Integrity	Integrated security mechanism.	a) flexible b)fast enough to check the integrity	a) Decoding the blocks b)intermediate node do not know the context of the transmitted data.

5.2 Privacy

1. In [6] Yuchen Yang et.al have proposed security issues in battery life and resources. Possible solutions were to extend the light weight computation. The presented scheme consist of authentication in RSA keys.

2. In [7] Sofia Zebboudj et.al have presented protocols namely Attribute based encryption, CHORD protocol and uTESLA. The ABE and uTESLA model works with the help of entities like public key generation, data generation and transmission, decryption and encryption and access control for the users. The ABE mechanism is used to generate keys based on the user attributes which identifies whether the user has the right to access the encrypted data or not.

3. In [8] Ana Nieto et.al have presented a scheme in the view of privacy.It defines privacy mechanism. This allows the anonymous witnessing.

4. In [9] Mohamed Abomhara et.al have presented a survey which consists of various challenges faced with privacy. The RFID(Radio Frequency Identification Techniques) make the concept of IoT feasible. The major IoT targets to create smart environment and self-conscious with the help of privacy.

5. In [10] Zhen Ling et.al have presented a view on security and privacy. The functionalities of the Edimax IP cameras were discussed. Real time experimenting has been done on the cameras and types of attacks were discovered. By performing experiments on the camera, the success rate of the device spoofing attack is up to 98%. The model needs to be served with secure and privacy preserving IoT system.

Table 2: Different mechanisms for providing Privacy

S.no	Title	Mechanism	Advantages	Disadvantages
1	A Survey on Security and Privacy Issues in Internet-of-Things	Two way authentication by DTLS protocol	a) life of battery is extended b) Light weight computation	a) No security policy b) Standards of IoT products are poor
2	Big Data source location privacy and access control in the framework of IoT	Attribute based encryption, CHORD protocol, uTESLA	a) ABE allows the encryption of data depending on the access policies defined by user attributes. b) uTESLA protocol is used to authenticate in real time.	a) Denial of service attack. b) More processing time for ABE.
3	Digital Witness and Privacy in IoT: Anonymous Witnessing Approach	Digital Anonymous Witnessing	a) privacy in network is ensured. b) Also ensures integrity of data.	a) It does not provide privacy in the devices.
4	Security and Privacy in the Internet of Things: Current Status and Open issues	RFID technology for dynamic system networks	a) RFID can reach long distances. b) It is a Lightweight mechanism. c) Privacy is ensured by cryptographic techniques.	a) It does not assure interoperability. b)Lack of complete Authentication and authorization.
5	A View on security and privacy.	Edimax IP Camera system	a)device gives live updates b)can be accessed from anywhere	a) scanning attack b) brute force attack

5.3 Integrity

1. In [11] Anderson Fongen et.al have presented a protocol which provides a combined control of authentication and integrity while providing service to the client. This is a protocol which is developed on simple hardware and simple cryptographic functions. It has got implementation for both symmetric and asymmetric keys which differ from the wired connection of hardware unit, providing safer key management in an asymmetric key implementation. By the combination of cryptographic functions, IdP and keys the integrity is provided.

2. In [12] Henrich C. P¨ohls et.al have presented a problem in the transport layer during the communication of sensors. This is used as the message's data structure. Elliptic curve based digital signature is used. To achieve this, it carries integration protection.

Table 3: Different mechanisms for providing Integrity

S.no	Title	Mechanism	Advantages	Disadvantages
1	Identity Management and Integrity Protection in the Internet of Things	Crypto functions.	a) Simple cryptographic operations and hardware	a) This methodology is a static view of memory which loads the necessary code files only on the demand.
2	JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application	Elliptic Curve based Digital Signature Algorithm	1) It provides origin authentication to which entity signed the data. 2) It is better than COSE (COBR Object Signing and Encryption), cause original JSON data is still present. But this data is lost when COSE is used. 3)It provides fast end to end integrity protection to even complex systems	a) The software prototype developed is not that secure, but is used as a performance indicator

5.4 Authentication

1. In [13] Alireza Esfahan et.al proposed a lightweight authentication mechanism for devices like smart sensors. In this process there is a authentication between sensor and router.

2. In [14] Bacemmbarek et.al have proposed a technique to reduce the authentication delay. This refers in the receivers buffer.

3. In [15] Shamini Emersonand Young-Kyu Choi OAuth proposed a protocol in which there will be third party restriction. They will access the data only when they provide credentials.

4. In [16] Padraig Floodand Michael Schukat proposed a technique which consist of fixed number of devices. Due to zero knowledge there will be no security and devices must compromise.

Table 4: Different mechanisms for providing Authentication

S.no	Title	Mechanism	Advantages	Disadvantages
1	Lightweight authentication mechanism Hash and XOR operations in M2M communications	Lightweight Authentication.	1)low cost 2)resistance against: 3)man-in-the-middle attack	It is only suitable for machine to machine communication it should be extended to sensor communication
2	Secure authentication mechanism for Resource Constrained devices	state of the art protocol µTESLA	1) aims to reduce the delay of forged packets in the receivers buffer, by efficiently computing the key disclosure delay 2) reduce the impact of Dos attacks leading a node to propagate malicious message until the battery is drained	In terms of energy consumption, we noticed that E-LEAP and E-LEAP++ consume more energy in the absence of attacks; while they consume less energy in the presence of attacks compared to LEAP and LEAP++.
3.	An OAuth based Authentication Mechanism for IoT Networks	OAuth 2.0 protocol.	1)flexibility in managing IoT networks 2)reduce the cost overhead to maintain secure database in IoT networks 3)it reduces the burden for users from registering to multiple networks or applications.	hybrid approach of periodic database update and database query to service provider during user login will be considered for research.
4.	Peer to Peer Authentication for Small Embedded Systems	zero knowledge proof it provides mutual authentication based on the GMW protocol	1)completeness 2)soundness 3)zero knowledge 4)protocol provides perfect forward secrecy 5)it avoids computational and management overheads created by alternative solutions that provide PFS, e.g. X.509 certificates and public key infrastructures.	1)does not scale well with large deployments 2)requires the distribution of credentials pre deployment 3)Cryptographically strong Diffie Hellman implementations require public keys in the order of 768 or 1024 bits, which result in combination with the protocol in either large graphs or an appropriate number of rounds for key exchange, therefore resulting in communication overheads.

6. Summary

Table6: Summary of all mechanisms above mentioned

SNo	Author	Mechanism	Confidentiality	Privacy	Authentication	Integrity	Attacks
1	Zhicaishi	RFID	✓				Eavesdropping attack
2	Bacem Mbarek	U TELSA			✓		E-LEAP attack
3	Chi-Hsueh Lin	Secret key distribution	✓				Masquerading attack
4	Padraig Flood And Michael Schukat	Zero knowledge proof			✓		Diffie Hellman attack
5	Christoscha tzigeorgiou s	Two step privacy	✓				Encrypted data attack
6	Shamini Emersonan d	O Auth 2.0			✓		Hybrid approach for database update
7	Juhannes	Quantum key distribution	✓				Distribution attack
8	Anderson Fongen	Symmetric rpto keys				✓	Memory insufficient
9	Parkand ji-Yong	Integrated security	✓				Decoding the blocks
10	Yuchen Yang	Two way by DTLS		✓			Security policy
11	Sofia Zebboudj	uTELSA		✓			Denial Service Attack
12	Ana Nieto	Digital Anonymous		✓			Privacy
13	Alireza Esfahani	Light weight authentication				✓	Machine to Machine attack
14	Mohamed Abomhara	RFID		✓			Interoperability
15	Henrich Pohls	Elliptic curve				✓	Software prototype
16	Zhen Ling	Edimax IP		✓			Scanning attack

7. Conclusion

This papers reviews and surveys the security issues, mechanism of internet of things (IoT) proposed in the literature. Specifically, Security and privacy are the crucial issues that need to be solved for successful deployment of IoT. Moreover, some of the data collected from the IoT are very sensitive and should not be revealed to third parties. Such data needs to be protected by some provided legislations. We reviewed some of the security challenges of IoT like secure communication, data privacy and integrity, authorizing and authenticating the devices.

References

[1] Zhicai Shi, Jiwei Chen, Shanshan Chen, "A lightweight RFID authentication protocol with confidentiality and anonymity", IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2017

[2] Chih-Hsueh Lin, Wen-Shyong Hsieh, Fu Mo, Ming-Hao Chang, "A PTC Scheme for Internet of Things: Private-Trust-Confidentiality", 30th International Conference, Advanced Infor-mation Networking and Applications Workshops (WAINA), 2016

[3] Christos Chatzigeorgiou, Lazaros Toumanidis, Dimitris Kogias, Charalampos Patrikakis, Eric Jacksch, "A Communication Gateway Architecture for Ensuring Privacy and Confidentiality in Incident Reporting", IEEE 15th International Conference, Software Engineering Research, Management and Applications (SERA), 2017

[4] Johannes Braun and Johannes Buchmann, "Perfect Confidenti-ality Network", 5th International Conference, New Technologies, Mobility and Security (NTMS), 2012

[5] Park Ji-yong, Mi-sun Ryu, Jung Eui suk, "An integrated securi-ty mechanism for network coding combining confidentiality and integrity", 11th International Conference, Advanced Communication Technology, 2009. ICACT 2009

[6] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li_, and Hongbin Zhao, "A Survey on Security and Privacy Issues in Inter-net-of-Things", IEEE Internet of Things Journal (Volume: 4, Issue: 5, Oct. 2017)

[7] Sofia Zebboudj, Rabah Brahami, Chahinas Mouzaia, Celia Ab-bas, Nabil Boussaid and Mawloud Omar, "Big Data Source Loca-tion Privacy and Access Control in the Framework of IoT", 5th International Confer-ence, Electrical Engineering - Boumerdes (ICEE-B), 2017

[8] Ana Nieto, Ruben Rios and Javier Lopez, "Digital Witness and Privacy in IoT: Anonymous Witnessing Approach", IEEE Trustcom/BigDataSE/ICESS

[9] Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things: Current Status and Open Issues", International Conference, Privacy and Security in Mobile Systems (PRISMS), 2014

[10] Zhen Ling, Kaizheng Liu, Yiling Xu, Yier Jin, Xinwen Fu, "An End-to-End View of IoT Security and Privacy", http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf

[11] Anders Fongen, "Identity Management and Integrity Protec-tion in the Internet of Things", Third International Confer-ence Emerging Security Technologies (EST), 2012

[12] Henrich C. Pohls, "JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Applica-tion", 9th International Conference, Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015

[13] Alireza Esfahani, Georgios Mantas, Rainer Matischek, Firooz B. Saghezchi, Jonathan Rodriguez, Ani Bicaku, Silia Maksuti, Markus Tauber, Christoph Schmittner, and Joaquim Bastos, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment", IEEE Internet of Things Jour-nal (Volume: PP, Issue: 99)

[14] Bacem Mbarek, Aref Meddebz, Wafa Ben Jaballahy, Mo-hamed Mosbah, "A Secure Authentication Mechanism for Re-source Constrained Devices", IEEE/ACS 12th International Conference, Computer Systems and Applications (AICCSA), 2015

[15] Shamini Emerson, Young-Kyu Choi, Dong Yeop Hwang, "An OAuth based authentication mechanism for IoT networks", International Conference, Information and Communication Tech-nology Convergence (ICTC), 2015

[16] Padraig Flood, Michael Schukat, "Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the Internet of Things", 10th International Confer-ence, Digital Technologies (DT), 2014.