SECURITY AND PRIVACY BIG CHALLENGES IN INTERNET OF THINGS

[1]Ms Priyanka D. Raut, [2]Prof Sachin Vyawhare

[1]ME Scholer Sanmati Engineering College, Washim.
[2]Assistant Professor, Sanmati Engineering College Washim (MH)

Abstract - *Internet of Things systems has fastly growing in all over the world and major roles in daily life by providing new capabilities to streamline diverse tasks. IoT provide the new capabilities and creates opportunities for increased productivity and societal benefits. IoT also provide the broad area of functionality and components will result in important challenges of privacy and security should be addressed. Large-scale, pervasive networks that receive the data from the world. Used new predictive technologies and algorithms that enable IoT. Once the data collected from IoT devices and algorithms that process this data and afterword used for decision-making. IoT also presents new security and privacy challenges. Sometimes it is more difficult to deploy security and protection schemes for IOT devices because with less functionality, less processing power, minimum storage capacity etc. Such deployments may need new protocols and system designs that are better implemented to operate in resource-limited environments. Policy and technical approaches to show the IoT privacy and security challenges should continue to encourage innovation while ensuring that user trust in these devices and systems will maintain the strong privacy and security.*

Key Words: **Internet of Things, Network Security, Privacy & Security Protocol, Predictive Technology, Pervasive Network, etc**

1. INTRODUCTION

Day by day internet technology and communications technology are fastly growing; our life is gradually changed into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. To eliminate this impulsion, a new technology is required to sum-up the imaginary space and real-world on a same platform which is called as Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models.

There are several security and privacy concerns at different layers viz; Front end, Back end and Network. In this paper is to present the study of security and privacy issues in Internet of Things (IoTs) and by present some challenges.

2. LITURATURE REVIEW

J. Sathish Kumar et. al. [1] presents the Internet of Things with architecture and design goals. They show the security and privacy concerns at different layers in IoTs. In addition, they identified several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things. They also discussed applications of IoTs in real life.

Sivarama Subramanian et. al. [2] introducing security in the early life cycle of the IoT solution can make mitigation design much easier. Security and privacy challenges for any IoT solution can be addressed by following secure systems development life cycle (SDLC) practices, secure coding practices and periodic penetration testing activities.

Zejun Ren et. al. [3] analyze the privacy and security challenges in the IoT and survey on the corresponding solutions to enhance the security of IoT architecture and protocol. They should focus more on the security and privacy on IoT and help to promote the development of IoT.

Shervin Erfani et. al. [4] analyzes distinct IoT security and privacy features, including security requirements, threat models, and attacks from the smart home perspective. Further, this paper proposes an intelligent collaborative security management model to minimize security risk. The security challenges of the IoT for a smart home scenario are encountered, and a comprehensive IoT security management for smart homes has been proposed.

What is IoT?

Internet of Things is the system to connect the physical devices and operate or access through the internet. The 'thing' in IoT could be a person with a heart monitor with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to receive and transfer data over a network without manual assistance or intervention. The embedded technology in the objects helps them to interact with internal states or the external environment, which in turn affects the decisions taken..

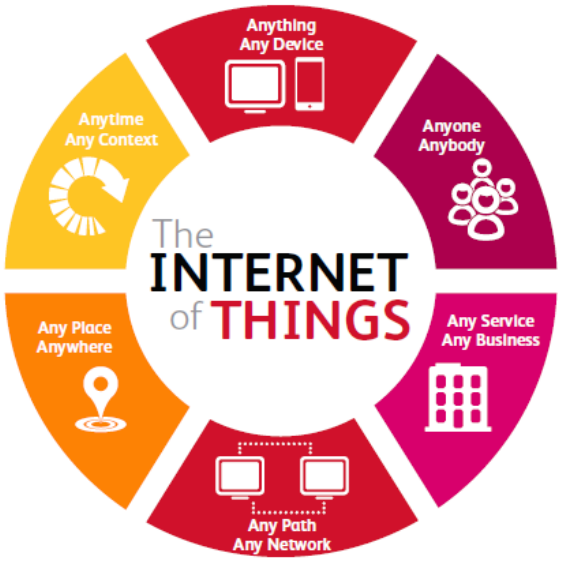


Fig -1: IoT

3. SECURITY AND PRIVACY CHALLENGES

IoT provide novel and universal access to the devices that make up everything from assembly lines, health and wellness devices, and transportation systems to weather sensors. Free access to that much data poses major security and privacy challenges, including:

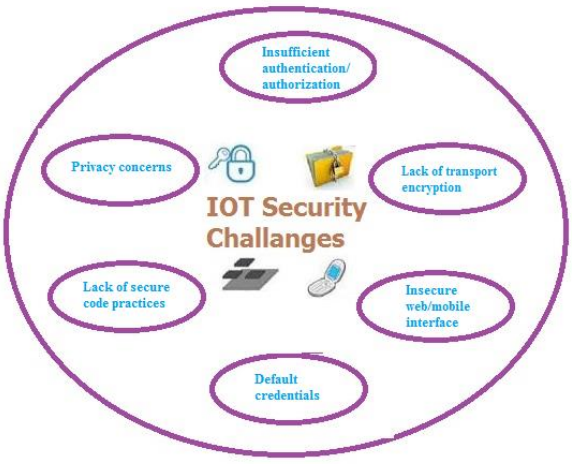


Fig -2: IoT Security challenges

Insufficient authentication/authorization: A huge number of users and devices rely on weak and simple passwords and authorizations. Many devices accept passwords such as ABCD or 1234.

Lack of transport encryption: Most of the devices fail to encrypt data that are being transferred, even when the devices are using the Internet.

Insecure web/mobile interface: IoT-based solutions have a web/mobile interface for device management or for consumption of aggregated data. This web interface is found to be prone to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities, such as poor session management, weak default credentials and cross-site scripting vulnerabilities.

Default credentials: Most devices and sensors are configured to use the default username/passwords.

Lack of secure code practices: Services and business logic would be developed without adhering to secure coding practices.

Privacy concerns: Devices used in the health care domain receives at least one piece of personal information; the vast majority of devices collect details such as username and date of birth. However, the fact that many devices transmit information across networks without encryption poses even more privacy risk. Privacy risk arises as the objects within the IoT receive and integrate fragments of data that relate to their service. For example, the regular purchase of different food types may divulge the religion or health information of the buyer.

4. MITIGATING SECURITY AND PRIVACY CHALLENGES

IoT products are manufactured only for security when security is embedded at the time of production. Each product should undergo security parameters to detect vulnerabilities.

Countermeasures, such as the following, can be taken to address the security challenges:

Base device platform analysis: Weak platform configuration might lead to compromises such as privilege increases. Base device platform operating system and its security properties, configurations and features should be verified against the base-lined information security requirements. Verification needs to be done to ensure that any test interfaces are removed from the hardware.

Network traffic verification: Network traffic (wired or wireless) should be analyzed for any in-disputable, unencrypted or versatile data. There is a compromise between performance and security when encryption is recommended. Lightweight encryption algorithms can be used to cater to performance requirements.

Verification of functional security requirements: To validate the high-level functional security requirement. The negative testing is important of software. IoT solutions can uses the cloud services such as Software as a Service which is based on identity management solutions for authorization and authentication requirements.

Trust boundary review and fault injection: All trust boundaries across the signal path should be reviewed and subject to fault injection using negative test cases. The trust boundaries can be verified using manual testing techniques. Mostly Periodic penetration testing is suggested.

Side channel attack defense verification: If side channel defenses are implemented, either in software or hardware, they should be verified using continuous penetration testing activities. Continuous penetration testing helps to minimize advanced persistent threats (APTs) for IoT solutions.

Secure code reviews: Early secure code reviews lead to early mitigation techniques. Sensitive and security impact areas such as boot process, security enforcement and encryption modules should go through secure code reviews. The cost of fixing a security defect is greatly reduced when the security vulnerability is discovered during the development cycle.

End-to-end penetration test: End-to-end penetration tests should be conducted across the signal path to identify any vulnerability in the web interface, mobile interface and cloud interface of the IoT solutions. The penetration testing give the more security of the IoT solution for each components.

Security Assessment of an IoT Solution

A US-based software company developed a Secure Travel product using IoT technology. The product provides real-time data about the speed of vehicles, location of the vehicles and people traveling on the vehicles.

The technology components involved included:

- Sensors in the vehicles
- Gateways
- Services
- Web interface
- Mobile interface

Threat modeling using the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS), Elevation of privilege (STRIDE) software approach was conducted to identify the attack scenarios and formulate mitigation plans for each of the components.

5. CONCLUSIONS

The Internet of Thing makes large development in everyone's everyday life. In the IoTs term, the short-range mobile transceivers will be implanted in variety of daily requirements. The connections between people and communications of people will grow and between objects to objects at anytime, in any location. The efficiency of information management and communications will arise to a new high level. The dynamic environment of IoTs introduces unseen opportunities for communication, which are going to change the perception of computing and networking. The privacy and security refer such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users has been identified as one of the key challenges in the IoT. In this paper is to present the study of security and privacy issues in Internet of Things (IoTs) and by present some challenges.

REFERENCES

[1] J. Sathish Kumar, Dhiren R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887), Volume 90 – No 11, March 2014.

[2] Sivarama Subramanian,Varadarajan Vellore Gopal,Marimuthu Muthusamy, "Security and Privacy Challenges of IoT-enabled Solutions", ISACA JOURNAL VOLUME 4, 2015.

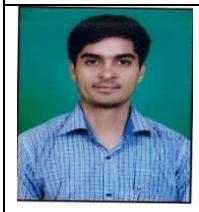
[3] Zejun Ren, Xiangang Liu, Runguo Ye, Tao Zhang, "Security and privacy on internet of things", 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017

[4] Shervin Erfani, Majid Ahmadi, Long Chen, "The Internet of Things for smart homes: An example", 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017.

[5] Elias Tabane, Tranos Zuva, "Is there a room for security and privacy in IoT?", International Conference on Advances in Computing and Communication Engineering (ICACCE), 2016

[6] Snehal Deshmukh, S. S. Sonavane, "Security protocols for Internet of Things: A survey", International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017.

BIOGRAPHIES

	Miss Priyanka D. Raut completed Bachelor of Engineering in computer science and engineering from MGI-COET, Shegaon and pursuing Master of Engineering in Computer Science and Information Technology from Sanmati Engineering College, Washim.
	Prof. Sachin Vyawhare is working as Asst. Professor and HOD of Computer Department at Sanmati Engineering College Washim (MH). He received BE degree and ME degree from S.G.B.A.U. Amaravati. His research interest includes networking, Operating System and Image Processing.