IoT security a layered Approach for Attacks and Defenses

Ankit R. Patel[1], Jigneshkumar A. Chauhan[2]
[1]*Research Scholar, Ganpat University*
[2]*Assistant Professor, Ganpat University*

Abstract **- Internet of things(IoT) are everywhere in our daily life. Internet of things is the connection of embedded technologies that contained physical objects and is used to communicate and intellect or interact with the inner states or external surroundings rather than people to people communication. Internet of Things(IoT) includes millions of connected devices that can sense ,compute, and communicate data. Recent advancements in wireless technology have created an exponential rise in the number of connected devices leading to the internet of things(IoT) revolution [7]. Large amount of data is captured, processed, and transmitted through the network by IoT devices. Security of the transmitted data is a major area of concern in IoT networks. security is a big challenge in IoT numerous encryption algorithms have been proposed to ensure security of transmitted data through the IoT network[7]. we analyzed the various challenges and security requirements and various light weight cryptographic algorithms.**

Index Terms **- IoT, Security, Privacy, Radiofrequency Identification, Lightweight Security.**

INTRODUCTION

Internet of things (IoT) is a collection of things embedded with electronics, software, sensors, actuator, and connected via the internet to collect and exchange data with each other. The IoT devices are equipped with sensors and processing power that enable them to be deployed in many environment[3].the fast growth of the number of IoT devices utilized is predicted to reach 41 billion in 2020 as stated in the 2013 report of the international Data Corporation(IDC). The IoT device can create information about individual's behaviours, analyze it, and take action. Services provided by IoT applications offer a great benefit for human's life.

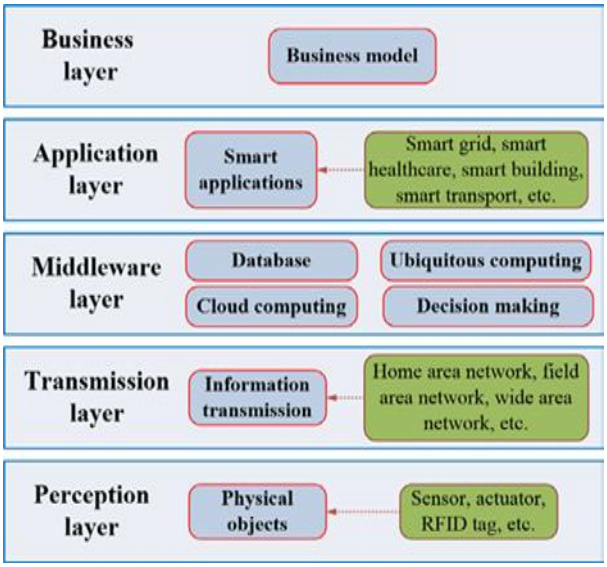
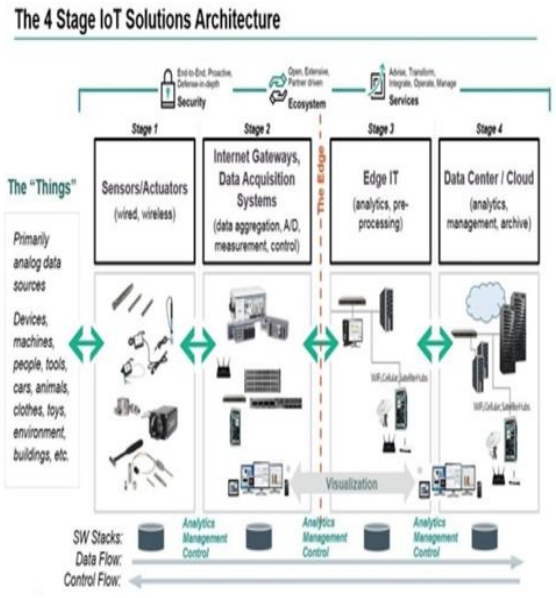


Fig.1 Different Layer of IoT
Sources : https://www.researchgate.net/figure/The-five-layer-IoT-architecture- 114_fig7_309606980

Security and privacy remain huge issues for IoT devices, which introduce a whole new degree of online privacy concerns for consumers. That's because these devices not only collect personal information like user's name and telephone number's but can also monitor user's activity[3] To address these challenges when many smart devices are connected in an IoT environment, the increasing demand for the use of appropriate cryptographic solution into the embedded applications. However, these smart devices generally have constrained resources, or they can be called low-resource devices in regard to their low computation power, limited battery life, small size, small memory, and limited power supply. Hence, the conventional cryptographic primitives might not be suited for low-resource smart devices. For example, the 1204-bit RSA algorithm [12]

HOW IOT WORK?



Sources: https://easybusinessfinance.net/business-process-development-steps/

INTERNET OF THINGS (IOT) SECURITY CHALLENGES

A. Lightweight computation

W. Trappe, R. Howard[1] mentioned that conventional cryptography cannot work on IoT systems, since the devices have limited memory space which can't handle the computing and storage requirements of advanced cryptography algorithms. To support security mechanisms for the constrained devices, the authors suggested reusing existing functions. An example is to use physical layer authentication by applying signal processing at the receiver side to verify whether a transmission came from the expected transmitter in the expected location.

Lee et al. [7] Presents the lightweight authentication protocol by enhancing the original RFID system security base on IoT .In the existing RFID protocol authentication is done without encryption which is security flaw. To overcome this problem light weight cryptographic protocol based on XOR method is proposed by which encrypted passwords are used for authentication.

B. IoT Authentication Scheme

Internet of things security being a sizzling topic for researcher today, there is a myriad of publication indicating security and privacy issues in IoT. Due to huge number of IoT devices and machine to machine communication feature of IoT, legacy authentication and authorization techniques are not viable for it. Devices must authenticate each other before exchanging any information between them (M2M communication) which is a challenge for researcher due to massive number of devices. Some of the work related to device authentication and access control in IoT are discussed here.

Chen et al. [6] proposed Capability-based access control model for distributed IoT environment. It supports group access by using single token and guarantee end to end security using IPsec. A requester can use a single token for group access (Group of devices that offer common services) to communicate with any device in the group. Network prefix of unique local identifier (ULA) is used as access group identifier. Each device in the group is identified by a ULA. In a group access token the requester puts its ULA and the network prefix of access group. Hence the devices in the group can verify the token using its ULA and prefix in the token. It can also provide access control based on requester ULA in the token.

C. IoT Perception Layer Securities

The perception layer contains various types of collecting and controlling modules, such as the temperature sensors, sound sensors, vibration sensors, pressure sensors etc and technologies include wireless sensor networks (WSNs), implantable medical devices (IMDs), Radiofrequency Identification (RFID), Global Positioning System. One perception layer security issue is the detection of the abnormal sensor node. This could happen when the node is physically attacked (e.g. destroyed, disabled), or intruded/compromised by cyber-attacks like.

- Physical node attack
- Spoofing
- Fake node
- Node tempering
- Denial of Service(Dos)
- Timing Attack
- Reply Attack
- Heterogeneity in technologies
- Side Channel Attack

D. Network Layer Securities

Just like any other Network Layer Model this includes network interfaces ,communication channel, network management, information management and intelligent processing, and is mainly responsible for the communication and connectivity of all the devices in IoT system through the help of multiple communication protocols[5] For IoT devices in WSN context, it is desirable to extend IPv6 over Low power Wireless Personal Area Networks (6LowWPAN) to enable IPSec communication with IPv6 nodes. This is beneficial because the existing endpoints on the internet do not need to be modified to communicate securely with the WSN and the true end to end security is implemented without the need for trustworthy gateway.

- Mass node Authentication
- Heterogeneity Problem
- Network Congestion Problem
- RFIDs interference
- Node Jamming in WSN
- Eavesdropping Attack
- Denial of Service
- RFID Spoofing
- Routing Attacks
- Sybil Attacks
- Interoperability and Portability

E Transport layer Securities

Kothmayr et al. [10] presented the first fully implemented two-way authentication scheme for the IoT system, based on existing Internet standards, especially the DTLS protocol. The proposed security scheme is performed during a fully authenticated DTLS handshake and based on an exchange of X.509 certificates containing RSA keys. It can work over standard communication stacks that offer UDP/IPv6 networking for 6LoWPANs.

Raza et al. [9] proposed 6LoWPAN header compression for DTLS. They linked the compressed DTLS with the 6LoW-PAN standard using standardized mechanisms. The proposed DTLS compression significantly reduces the number of additional security bits. For example, only for the DTLS Record header that is added in every DTLS packet, the number of additional security bits can be reduced by 62%. In their follow-up work [10], an integration of DTLS and CoAP is proposed for the IoT, named Lithe. They also proposed a novel DTLS header compression scheme that aims to significantly reduce the energy consumption by leveraging the 6LoWPAN standard.

Brachmann et al. [8] pointed out that security protocols such as Transport Layer Security (TLS) or DTLS adopted on the Internet does not necessarily mean that the same security levels can be achieved in Low-power and Lossy Network (LLN), which is still vulnerable to resource exhaustion, flooding, replay and amplification attacks, since the 6LoWPAN Border Router typically does not perform any authentication.

F. Application layer Securities

The Application layer consists of widely different service domains such as smart homes, healthcare, connected cars, and smart grids, security threats for the Application layer heavily depend on the domain. Therefore, each application area should consider its own security threats and prepare countermeasures for each threat [11].

Most modern IoT device contain configurable embedded computer system. Some are even running complex software and resembling general – purpose computers ,when connected to the internet , they could get infected by computer virus like trojan[2]

- Attacks on the clouds
- Service interruption
- Third party attacks
- Encryption
- Data access and Authentication
- Phishing Attack
- Malicious Active X Scripts
- Malware Attacks
- Security Requirements of Application layer

LAYER WISE IOT SECURITY AND ATTACKS

Table 1[4]

S.#	Attacks	Perceptual Layer	Network Layer	Support Layer	Application Layer	Impact
01	Node Tempering	✓	×	×	×	High
02	Fake Node	✓	×	×	×	High
03	Side Channel Attack	✓	×	×	×	Medium
04	Physical damage	✓	×	×	×	Medium
05	Malicious Code Injection	✓	×	×	✓	High
06	Protecting Sensor Data	✓	×	×	×	Medium
07	Mass Node authentication	✓	✓	×	×	High
08	Heterogeneity Problem	×	✓	✓	×	High
09	Network Congestion Problems	×	✓	×	×	Medium
10	RFIDs interference	×	✓	×	×	Low
11	Node jamming in WSN	×	✓	×	×	Low
12	Eavesdropping Attack	×	✓	×	×	Low
13	Denial of service	×	✓	×	×	High
14	RFID Spoofing	×	✓	×	×	High
15	Routing attacks	×	✓	×	×	High
16	Sybil Attack	×	✓	×	×	High
17	Data Security	×	×	✓	×	High
18	Interoperability and Portability	×	✓	✓	×	Medium
19	Business continuity and Disaster Recovery	×	×	✓	×	Medium
20	Cloud Audit	×	×	✓	×	Medium
21	Tenants Security	×	×	✓	×	High
22	Virtualization Security	×	×	✓	×	Medium
23	Data Access and Authentication	×	×	×	✓	High
24	Phishing Attacks	×	×	×	✓	Medium
25	Malicious Active X Scripts	×	×	×	✓	High

CONCLUSION

In this survey, we have presented the security and privacy issue in IoT application and systems. We also studied existing classification approaches for IoT attacks and security mechanisms [3]. Then we reviewed the recently proposed IoT authentication schemes and architectures.in The last part of our work analyzed the security issues and solutions in four layers, including the perception layer, network layer, transport layer, and application layer [3].

Overall, the safety IoT lightweight cryptography algorithm is needed so here we discuss some lightweight cryptographic algorithm.

REFERENCES

[1] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities on the internet of things," IEEE Security Privacy, vol. 13, no. 1, pp. 14–21, Jan 2015.

[2] Anass Sedarthi, Abdellati Mezrioui, "A Survey of Security Challenges in Internet of Things", Astesj, ISSN : 2415-6698

[3] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250–1258. doi:10.1109/jiot. 2017.2694844'

[4] Inayat Ali, Sonia Sabir1, Zahid Ulla, "Internet of Things Security, Device Authentication and Access Control: A Review" IEEE INTERNET OF THINGS JOURNAL

[5] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015, pp. 180–187.

[6] B. Chen, Y L. Huang, M G. Unes, "S-CBAC: A secure access control model for supporting group access for internet of things." 2015 IEEE.

[7] Rajesh, S., Paul, V., Menon, V., & Khosravi, M. (2019). A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. Symmetry, 11(2),293.doi:10.3390/sym11020293

[8] J. Lee, W. Lin, Y. Huang, "A Lightweight Authentication Protocol for Internet of Things.", International Symposium on Next-Generation Electronics, ISNE 2014

[9] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-end transport security in the ip-based internet of things," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), July 2012, pp. 1–5.

[10] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure coap for the internet of things," IEEE Sensors Journal, vol. 13, no. 10, pp. 3711–3720, Oct 2013.

[11] T. Kothmayr, C. Schmitt, W. Hu, M. Bryunig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," Ad Hoc Netw., vol. 11, no. 8, pp. 2710–2723, Nov. 2013.

[12] Shin, H., Lee, H. K., Cha, H.-Y., Heo, S. W., & Kim, H. (2019). IoT Security Issues and Light Weight Block Cipher. 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). doi: 10.1109/icaiic.2019.8669029

[13] Padmavathi, M. P. M. (2013). A Study on the Biological activity of Hepatitis C Analogs Prediction by QSAR -An Insilco Approach. IOSR Journal of Pharmacy (IOSRPHR), 3(4), 28–32. doi: 10.9790/3013-034102832