Proposal of Research for Security in IoT

Han Sun
Yunning Gong
Hongzhi Fu

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction[1]. Since IoT requires data transferring all the time, high level security is necessary to keep data safe from unauthorized accesses.

IoT is deeply integrated with one of the top research fields, deep learning, in particular, face recognition. In recent years, this technique has been applied to lock/unlock vehicles right on their mobile devices, which brought great convenience for us[2]. However, many security issues also arise to threaten the system, e.g. thieves attempt to forge an image to fool the verification model[3].

Meanwhile, IoT is complemented by the application of artificial intelligence in the medical area, to learn user behavior patterns, gain knowledge of the context, define action rules for each scenario in relation with the user's behavior etc[2]. If patients' personal data are interfered or stolen, it may possibly cause health or even life risk for them.

For home IoT services, IoT devices have low power consumption and low security[5]. Attackers can often easily enter the home gateway. When an attacker gains unauthorized access to IoT devices, it may try to harm the users such as home burglaries[6].

This report examines current security approaches in different fields of IoT applications, as well as providing some evaluations on the effectiveness of these approaches. This report also discusses several challenges for security in IoT, and gives out some possible solutions for existing challenges.

1. Introduction

- Describe IoT
- Analyze how security work in IoT
- Discuss some inadequacies currently appearing in the field

2. Approaches

- Automobile
  Face recognition
- Medical
  Personal medical data
- Home
  Personal privacy

Big data analysis

3. Critical Evaluation

- Analyze how current security approaches work well and how they don’t work well.
- Provide possible solutions or alternatives.

4. Conclusion

Reference

[1] Rouse, Margaret (2019). "internet of things (IoT)". IOT Agenda. Retrieved 14 August 2019.
[2] Pawar, Mahesh & Rizvi, Imdad. (2018). IoT Based Embedded System for Vehicle Security and Driver Surveillance. 466-470. 10.1109/ICICCT.2018.8472984.
[3] Marbukhari, Norhaflyza & Mohamed, N.N. & Mat Isa, Mohd Anuar & Syed Adnan, Syed Farid & Hashim, Habibah. (2017). An automobile security protocol: side-channel security against timing and relay attacks. International Journal of Electronic Security and Digital Forensics. 9. 239. 10.1504/IJESDF.2017.10005632.
[4] A. J. J. Valera, M. A. Zamora and A. F. G. Skarmeta, "An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments," 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2010, pp. 1-5, doi: 10.1109/CCNC.2010.5421661.
[5] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[6] A. C. Jose and R. Malekian, "Improving smart home security: Integrating logical sensing into smart home", IEEE Sensors J., vol. 17, no. 13, pp. 4269-4286, Jul. 2017.

Appendix

Teamwork breakdown: Automobile(Hongzhi Fu), Medical(Han Sun), Home(Yunning Gong).