Digital Security in IoT devices

-Dr. Zulkharnain

CAIT, Jazan University, Saudi Arabia

zbadruzzama@jazanu.edu.sa

Abstract

The domain of Internet of Things is very challenging nowadays as these devices are growing at fast pace, particularly due to wearable and smart home applications. All these devices are interconnected through internet. Remote control is a simple process for this network. Commercial firmware and software used here is highly vulnerable. Hackers can easily get experience, by gaining knowledge from IoT vulnerabilities. Thus, there is an immense need of providing security to these Digital devices. If ignored, data breach can occur causing threat to personal information. It may also cause financial loss and also put life of people in Danger.

In this paper, a brief discussion is made regarding, some of the challenges faced in Digital security faced in such environment. A simple two-level approach is discussed here regarding that.

Keywords: *Digital Security, IoT devices, IoT vulnerabilities; IoT Security, Threats, security breach;*

1. Introduction of security system

Decision making process is an important task involving the use of IoT devices (1). The next important process here is Data acquisition (2). Last but not least, is Data exchange process (3). Thus, there is need of constant surveillance while using this system. A simple compromise in home automated system may initiate devices to switch on and off in intervals, thereby the Devices can burn off! Similarly Self driving car can crash due this problem.

We also need to consider here, IoT communication system. Ultra-reliability dependance can cause compromise situation, that leads to trouble here. Integrity, reliability and availability are interdependent process. Lack of information can also cause problems here. Thus, identity assurance, and protection aspects should be taken care.

IoT -Two level approach is a technique, that can provide security to IoT system. Here traffic of the network is studied, and taken care at the application level. Continuously monitor and establish Trust among the connections. The unexpected behavior of any of the device connected here, is isolated from the network. Initial trust is assigned to each of the device with each other to start with. History of interactions are stored here, for checking later.

Similarly Routing protocol (4) may be used to find lossy network. Thus, Network resilience can be established. Machine learning is also a better way to check the trust. Elastic side window method is useful in checking broken and malfunctioning device. Light weight authorization method uses quality of service, social relationship to give trust values.

2. Energy efficiency of IoT Devices

Energy efficiency is desirable in peer-to-peer network (5). Software agents can be used here, to check attitudes of each device. A system of smart contracts (6) may be used. Weighted averages can be used (7). Direct and regional trusts can be built (8). Simulations can be done to check power consumptions (9). Using information theory directional graph can be built (10). Entropy of capability of the device can be found out (11). Thus, malicious devices can be detected. For better reliability private key protection may also be used (12).

Here in all the above ways, we need to have information needed to establish trust. First receiver IoT is given an initial trust value. It then adjusts the trust in the transmitter IoT device. This trust is decreased as time passes. Every device should know which device it is supposed to communicate with. Identification of the device helps veracity. This avoids tampering and duplication process in the network. Encryption schemes are most suitable here. Private and public keys are thus generated. Public keys are generated using IP address. Numerous messages during authentication can be avoided here. This way all devices interconnected are energy efficient. Thus, less battery power is utilized and long life to the battery is ensured.

3. Private Key Generation

PKG is needed, because access to public information is done here. A random element is added to each private key before distribution. PKG should not be vulnerable. PKG is decentralized, and the trust is distributed. Full nodes are considered as those, who do administration of correction, and ensure trustful operation. They are basically not IoT devices here. They are resourceful edge devices. This does the verification process. Access to malicious devices can be done by this. By access management security can be provided. Consensus protocol is based on proof-of-stake. Information theory is used to model incoming throughput of device. Then respective relative entropy is found out. In this way traffic patterns of the device can be known. Temporal decay occurs when a device stops communicating.

'Trust approach' is a 3 tier security system. Cloud, Edge and Thing are the 3 levels here. Edge Tier is high level one and 'Thing' is low level. Edge tier has blockchain interconnections. Thing-tier has traffic analysis and temporal trust decay check.

Topology changes due to device battery draining, device entering and leaving, and connection disruptions are recorded. First of all.

Each IoT device makes a query, by checking identity. When initial trust is established, communication starts. Relative entropy of traffic is then computed and the trust value is varied. Misbehavior of device leads to disconnection. Disconnection is also done when communication completes. This process is repeated, and is in loop.

4. Challenges:

Here Trust is built based on information from other devices. Malicious history is irrelevant here, for trust. Transmission is based on high trust that is built here. Trust is asymmetric and context dependent. It is also dynamic. The system does still have any open issues, based on development of applications. IOT features of heterogeneity is still a challenge, in proving trust! Trust is also complicated due to scalability factor, with ever increasing connections. Similarly, integrity of data is also becoming challenging day by day. There exist no standards for solving these problems!

5. Conclusion:

The proposed 2 level approach for providing security is given above, with Trust building suggestion given. Issues still are open for further research and solution are required to the problems discussed above. An IoT device should build reputation based on traffic behavior. Fake traffic behavior may also lead to compromise! Trust decreases when device changes behavior, and due to any malicious act. The new behavior needs to be updated by other devices. This is an important requirement.

6. References

1. F. Piccialli, G. Casolla, S. Cuomo, F. Giampaolo and V. S. di Cola, "Decision Making in IoT Environment through Unsupervised Learning," in IEEE Intelligent Systems, vol. 35, no. 1, pp. 27-35, 1 Jan.-Feb. 2020, doi: 10.1109/MIS.2019.2944783.
2. N. Maleki, A. Musaddiq, D. Mozart, T. Olsson, M. Omareen and F. Ahlgren, "DeltaBin: An Efficient Binary Data Format for Low Power IoT Devices," 2023 International Conference on Computer, Information and Telecommunication Systems (CITS), Genoa, Italy, 2023, pp. 1-5, doi: 10.1109/CITS58301.2023.10188750.
3. "IEEE Approved Draft Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management," in IEEE P2144.1/D3, August 2020, vol., no., pp.1-20, 25 Jan. 2021.
4. C. Sharma and N. K. Gondhi, "Communication Protocol Stack for Constrained IoT Systems," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519904.
5. M. Ghorbani, M. R. Meybodi and A. Mohammad Saghiri, "An Architecture for Managing Internet of Things based on Cognitive Peer-to-peer Networks," 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 2019, pp. 111-116, doi: 10.1109/ICWR.2019.8765283.
6. Y. Xiang and Q. Yue, "Research on Trusted Service Assurance for IoT: A Blockchain Smart Contract-Based Method," 2023 8th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2023, pp. 1774-1777, doi: 10.1109/ICSP58490.2023.10248638.
7. P. Machaka, A. Bagula and F. Nelwamondo, "Using exponentially weighted moving average algorithm to defend against DDoS attacks," 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech), Stellenbosch, South Africa, 2016, pp. 1-6, doi: 10.1109/RoboMech.2016.7813157.
8. W. Najib, S. Sulistyo and Widyawan, "Trust Based Security Model in IoT Ecosystem," 2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2022, pp. 195-199, doi: 10.1109/ICITISEE57756.2022.10057930.
9. Q. Ren, J. Lu, S. Li, X. Yin, Z. Zhou and B. Jiang, "Simulation Research on Micro Distribution Interconnection System Based on Long-scale Power Flow Calculation," 2020 7th International Conference on Information Science and Control Engineering (ICISCE), Changsha, China, 2020, pp. 2181-2186, doi: 10.1109/ICISCE50968.2020.00427.
10. G. Astudillo, M. Kadoch and B. Abdulrazak, "Directional Graph-Based Energy Model for IoT Wireless Relay Systems," 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 2019, pp. 251-258, doi: 10.1109/FiCloud.2019.00042.
11. H. Lotfalizadeh and D. S. Kim, "Investigating Real-Time Entropy Features of DDoS Attack Based on Categorized Partial-Flows," 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), Taichung, Taiwan, 2020, pp. 1-6, doi: 10.1109/IMCOM48794.2020.9001690.
12. M. G. Z. Fernando, A. M. Sison and R. P. Medina, "Securing Private Key using New Transposition Cipher Technique," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2019, pp. 490-493, doi: 10.1109/ECICE47484.2019.8942798.