Security And Privacy Issues In IoT Smart Cities

IOT AND SMART CITIES

What is IoT?

Internet of things is a system of those devices, appliances or machines which has the ability to transfer the data over internet without the need of human to human interface.

What is a smart city?

Smart city is an area where internet of things sensor are used to collect data of citizens or devices that is processed or analyzed traffic management, power systems, water managements etc.

SECURITY AND PRIVACY

Security means protection of a data from unauthorized access where as privacy means protection of personal identification information. Security can be achieved without privacy but privacy cannot be achieved without security:

- Constrained devices.
- Weak encryption
- Botnet Activities Related Security Threats in IoT Smart Cities
- Leakage in Data Sensing
- Threats of AI in Smart Cities
- RFID Tags of Smart Cities Cause Data Privacy Issues

ADVANTAGES AND DISADVANTAGES

It is yet to be answered if a smart city has advantages or not.

After looking at many scholarly articles it will be too early to say if smart cities are successful or not. Looking at the privacy and security issues, a lot needs to be done in order to make smart cities secure.

SOLUTION

- Multitenancy, a serious problem, can be solved by creating a separate virtual LAN.
- No leakage of data
- Strict regulations required to protect cyber security
- Stop Artificial intelligence to access data
- Make it secure from DoS, Man In the Middle etc attacks

CONCLUSION

As this project suggests that IoT is playing an important role in order to make on city into smarter but there have been privacy and security issues. Some measures need to be taken in order to make smart city more secure and have more privacy. There is no doubt IoT smart city has many benefits but few disadvantages has make it questionable.

REFERENCES

1. Burhan, M., Rehman, R., Khan, B., & Kim, B.S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors, 18(9), p.2796.
2. Cherrier, S., Movahedi, Z., & Ghamri-Doudane,Y.M. (2015). Multi-tenancy in decentralised IoT. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 256-261). IEEE.
3. Cui, L., Xie, G., Qu,Y., Gao, L., & Yang,Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, pp.46134-46145.
4. Falco, G.,Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities. IEEE Access, 6, pp.48360-48373.
5. Ijaz, S., Shah, M.A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. International Journal of Advanced Computer Science and Applications, 7(2), pp.612-625.
6. IoT Analytics. (2015). The 10 most popular Internet of Things applications right now. Retrieved from https://iot-analytics.com/10-internet-of-things-applications/
7. IoT Analytics. (2018). The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects. Retrieved from https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/
8. Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2017). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In International Conference on Mobile Networks and Management (pp. 30-44). Springer, Cham