International Engineering Journal For Research & Development
Vol.4
Special Issue

E-ISSN NO:-2349-0721

Impact factor : 6.03

IOT SECURITY USING MACHINE LEARNING

Prof. Swapnil V. Deshmukh, Miss. Sonali S. Kathale, Miss. Bhavana B. Bande

Dept. of computer science and engg.
Prof. Ram Meghe Institute ofTechnology and Research, Badnera,
sonalikathale1998@gmail.com , bhavanabande1998@gmail.com

Abstract---

"IOT" is becoming the most popular amongst the world. The internet of things enables everyone to be connected anywhere and anytime. "The IOT Security using Machine Learning" for IOT devices helps in protecting and securing devices from various attacks. Machine learning techniques, which are able to provide embedded intelligence in the IoT devices, are provided with different security problems. This paper presents the review of the security solutions using machine learning. Machine learning is a field of study that allow computers learning from past experience to enhance future execution.

Keywords—security, methods

1. LITERATURE REVIEW

Machine learning is the operating power for artificial intelligence. The advantage of ML systems is that it uses heuristic learning, logical models, data purchasingan decision trees for essential administration. Each machine learning parable has a specific system of learning and based on the assessment of its parameters. The utilization of machine learning is used for human illness helps treatment devotees in light of the signs at a starting time, anyway of the way that a couple of richness show practically identical signs. Among these, it gives tractability, visibility and unsheltering quality to the system under administration. A machine learning model is made in outlook of the relationship between the marker property assessment of its parameters.

2. INTRODUCTION

Internet of Things speed up integration between the physical world and computer communication networks, and applications such as footing management and environmental observing make privacy and security techniques censorious for future IoT systems.

In many IoT devices, the security is become most important topic. Most of the devices are damaged due to various IoT attacks. So machine learning is very useful term for protecting IoT devices. Composing of radio frequency identification, wireless sensor networks, and cloud computing. Iot have to protect from such type of attacks and address security issues such as spoofing attacks, intrusions, denial of service attacks, distributed denial of service attacks, jamming eavesdropping, and malwares.

3. ML BASED IOT SECURITY METHODS

Basically there are two methods in the internet of things using machine learning. These two methods are used to protect IoT devices from various attacks. The methods are learning based authentication and learning based access control.

Authentication control using machine learning:- Conventional authentication procedure are not always applicable to IoT devices with restricted computation, battery and memory resources to detect identity-based attacks such as spoofing and Sybil attacks. Physical layer authentication techniques that utilize the altitudinal

decorrelation of the PHY-layer features of radio channels and transmitters such as the received signal strength indicators, received signal strength, the channel impulse response of the radio channels, the channel state information, the MAC address can provide light-weight security protection for IoT devices with low computation and communication overhead without draining user privacy information.

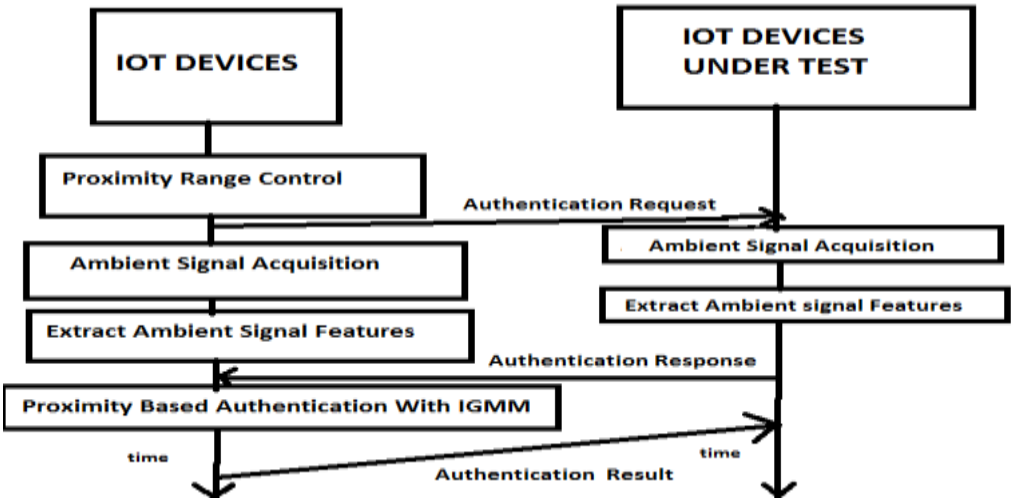

Fig 1: Authentication control using machine learning

Access control using machine learning: To design access control for IoT systems it is very challenging in critical networks with various types of nodes and multisource data. Machine learning methods such as SVM and neural network is being used for displacement detection. The DoS attack detection as put forward in uses multivariate correlation examination to insert the geometrical correlations between network traffic features.

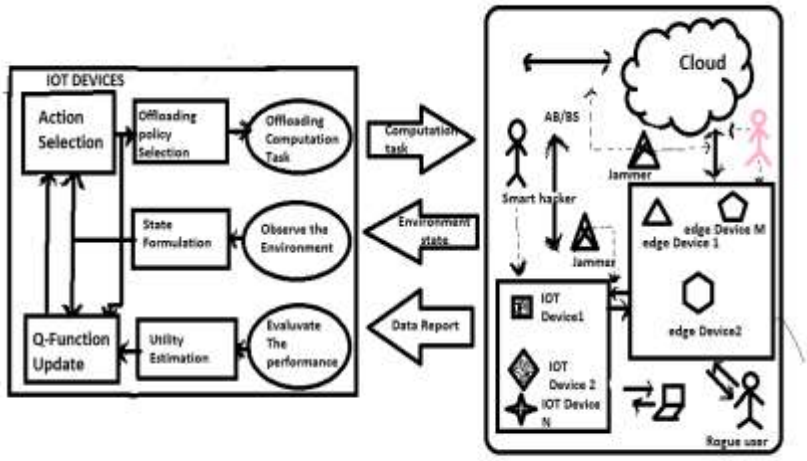

Fig 2: Access control using machine learning

4. CONCLUSION AND FUTURE SCOPE

IoT security and protecting IoT devices from various attacks are of paramount importance and plays an important role in the capitalization of the IoT technology. Long-established security and privacy solutions suffer from a lot of issues that are similar to the dynamic nature of the IoT networks. Machine learning techniques can be used to authorize the IoT devices to justify to their gingery environment. In this machine learning techniques there might be a problems regarding to partial state observation, computation and communication overhead and backup security solutions. So it can be overcome in future work by improving and additional techniques. The

security techniques that are already exist assure that the each learning representative knows the exact state and calculate the immediate reward for each action in time. Therefore, upcoming machine learning techniques with low measurement and communication upward have to be investigated to intensify security and privacy for IoT systems.

REFERENCES

[1] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. and Byers, A., Big data: The next frontier for innovation, competition, and productivity. Technical report, McKinsey Global Institute, 2011.

[2] Mitchell, T. M. Machine Learning, McGraw-Hill, New York, NY, 1997.

[3] Aldrich, A. and Auret, L., Unsupervised process monitoring and fault diagnosis with machine learning methods, Springer, 2013.

[4] Mandal, I., and Sairam, N., Accurate prediction of coronary artery disease using reliable diagnosis system, Journal of Medical Systems, 36(5), 3353-3373, 2012.

[5] Mandal, I. and Sairam, N., Enhanced classification performance using computational intelligence, Communications in Computer and Information Science, 204, 384-391, 2011.

[6] Mandal, I. and Sairam, N., New machinelearning algorithms for prediction of Parkinson's disease, International Journal of Systems Science, 45(3), 647-666, 2014.

[7] Feng, G., Qian, Z. and Zhang, X., Evolutionary selection extreme learning machine optimization for regression, Soft Computing, 16 (9), 1485-1491, 2012. DOI: 10.1007/s00500-012-0823-7