How To Deal With IoT Security Threats

Mr.Vishwanath Chavan [1], Mr.Sandesh Pare [2]
[1, 2] Assistant Professor, Dept of Computer Science and Engineering
[1, 2] Walchand Institute of Technology, Solapur, MH, India.

Abstract- *This paper deals with security threats in IoT and how to deal with it. Five different cases have been dealt with respect to security threats like Mobile device management, Access limit to consumer data, Strong cryptography, Data loss prevention and Web filtering.*

Keywords- Mobile Device Management, Role Based Access Control, Data Loss Prevention, Web filtering.

I. INTRODUCTION

Today nearly all devices have ability to connect with internet. These devices are protected by different techniques, tools and strategies. IoT security can be implemented by different kind of methods. The devices can be tracked and monitor with the help of network access control. IoT devices which are connected to internet are segmented according to networks and they can face security challenges. Modern threats can be handled by cyber security teams. Security gateways have an ability to secure the devices from hackers. These gateways have more memory and processing power. IoT devices can be update by software's .New security challenges can be handled by teams to whom training is given. Different teams can be integrated like security and programming to ensure device security. Educating to consumers like updating of software's, use of high security devices etc. IoT security attacks include like attacks on the device software, physical attacks and communication attacks. Cryptography technology helps combat communication attacks. IoT technology stack layer consists of physical devices like sensors, transducer, actuators etc. An object may have few or thousands of sensors and transducers. IoT gateways can be software/hardware, it plays important role on interaction of devices. There are gateways for edge computing, industrial IoT, gateways for home automation etc. IoT platforms are an IoT application enablement platform. IoT device management is virtually present in IoT platform

II. MOBILE DEVICE MANAGEMENT (MDM)

Organizations started the use of mobile devices which leads more efficiency and adds burden on data security.MDM allows admin to secure the devices.

How Mobile Device Manager (MDM) deals with security?

Data security:

Mobile device management (software) manages the devices like laptops, tablets, smart phones and operating systems like iOS, android, windows etc

It secures, manage and monitor devices of employee. And it optimizes the functionality of mobile devices .Mobile device management deals with corporate data for isolation, securing emails, monitoring documents on mobile devices .It secures the access of app. It controls apps based on time, geoloaction and IP. Ensures privacy for BYOD.It keeps sensitive and confidential of data more secure. Mobile devices can be organized in symmetric manner. Automatic updation of apps when new version is available. It renders useful features backup .Enables the use of GPS or RFID to secure the data.

Device protection:

Admin can manage on boarding devices and secure the data. Unauthorized devices can be removed from accessing data. Operating systems ensures the devices are updated. Device location and history is also monitored. Issues of devices can be solved remotely.

App security:

Through mobile apps admin is able to provide data. Blocking the malicious apps, configuring the apps and giving essential permission can secure the app data. Locking the device apps and updating also secures the data. Enterprise apps can deploy to protect from critical bugs.

Protect corporate network access:

Corporate data can be protecting by restricting unknown devices and allowing enrolled devices to to connect. Device specific certificates can be create and distribute. Corporate resources and apps can be configuring through VPN. Web site access can be blacklist and allow list.

Secure email access:

Through trusted apps/document viewer users can access corporate emails and it can be enabled for conditional access.

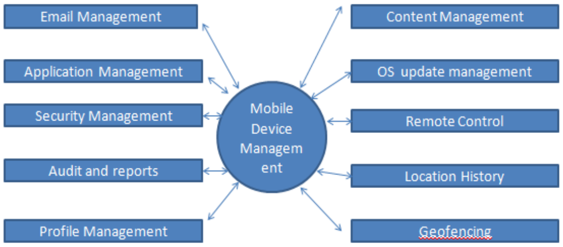

Fig 1: Mobile Device Management

III. ACCESS LIMIT TO CONSUMER DATA

According to employees jobs profile data can be restricted to their systems i.e. role based access control (RBAC). Role based access allows to access the data which is required for their data.

Role based access can be implemented more efficient and accurately. Access levels can be assigning according to need. Some time some accounts may need more access. Training should be given to employee to understand what level of access they have and what others have. Documenting the access right is a good practice. Document which employee has how much access. Update the documents whenever the employee added and taken out.

Role based access control system:

Business oriented organization should implement role based access control system. Payment Card Industry requires defined and up to date list of roles with access to card data.i.e. Organization needs to update the employees data as and when. Social engineering attacks can be limited be based on role based access. It prevents stealing of data by social engineering attacks. Remote access attacks can be secure by software’s. Implements unique usernames and password, limits log in attempts. It reduces data attacks by restricting access, segmentation of networks, antivirus software’s .Limitation of access to employees helps to give clarity of their responsibilities.Emplyoees roles will be cleared. Based on role based access, employee’s and employer responsibilities also clear. This prevents confusion and streamlines responsibilities.

IV. STRONG CRYPTOGRAPHY

Encryption and hashing are the techniques for payment card industry data security standard (PCI-DSS).Standard algorithms and key lengths are AES-128 bits.TDES/TDEA-Triple length kays,ECC-224 bits or Higher and DSA/D-H-2048/224 bits or higher,RSA-2018 bits or higher. Security services like confidentiality, data integrity, authentication, authorization,,non-repudiation,support services are implemented by strong cryptography.

V. DATA LOSS PREVENTION (DLP)

Based on policy, flow of outbound data can be monitored and it can be stop. Tools are used to ensure that sensitive data is not lost. Misused, access by unauthorized users.To protects personally identification information organizations use DLP. In large organization data visibility is achieved by secure mobile workforce and BYOD enforcement. The common causes of data leaks are insider, extrusion by attackers and negligent data exposure/unconditional. This can be secure by remote cloud systems.

Components of a Data Loss Solution:

Technology which is installed at network edge can analyze traffic/sensitive data [11].Endpoint agents controls information transfer between users, groups of users and external parties which secures end points

In real time some endpoint systems can block communication and provide user feedback. Data at rest can be secure by access control, encryption and data retention policies. Unauthorized or unintentionally/intentionally activities can be monitored by DLP system [11].Some time it should be known whether data need to be protected or not. Data can be sensitive by rules/metadata/machine learning.DLP solutions/security systems identify data whether it is anomalous or suspicious. Security systems like IDS, SIEM and IPS are used for this purpose [9].

VI. WEB FILTERING

Software based solutions identifies types of sites, visited sites etc. Content is grouped in to categories using keyword/commonalities between sites .Protect your organization by blocking access to malicious, hacked, or inappropriate websites. Improves security by blocking access to malicious and risky websites Prevents malware downloads from malicious or hacked websites Keeps your defense current with automatic intelligence tools, targeted threat analysis, and continuous updates

VII. CONCLUSION

This paper focuses on security threats in IoT and how to deal with it. How security can be achieved by mobile device management, access limit to consumer data, strong cryptography. data loss prevention and web filtering.

VIII. FUTURE WORK

Encryption and hashing are the techniques for payment card industry data security standard can be studied for more security.

REFERENCES

[1] Ang, K.L.M. and Seng, J.K.P., 2019. Application specific internet of things (ASIoTs): Taxonomy, applications, use case and future directions. IEEE Access, 7, pp.56577-56590.

[2] Zhong, X., Zhang, L. and Wei, Y., 2019. Dynamic load-balancing vertical control for a large-scale software-defined internet of things. IEEE Access, 7, pp.140769-140780.

[3] Xu, S., Wang, X., Yang, G., Ren, J. and Wang, S., 2020. Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint. Journal of Communications and Networks, 22(2), pp.145-158.

[4] Bouras, M.A., Farha, F. and Ning, H., 2020. Convergence of computing, communication, and caching in internet of things. Intelligent and Converged Networks, 1(1), pp.18-36.

[5] Tran-Dang, H. and Kim, D.S., 2018. An information framework for internet of things services in physical internet. IEEE Access, 6, pp.43967-43977.

[6] Eldrandaly, K.A., Abdel-Basset, M. and Shawky, L.A., 2019. Internet of spatial things: A new reference model with insight analysis. IEEE Access, 7, pp.19653-19669.

[7] Yan, Z., Li, H., Zeadally, S., Zeng, Y. and Geng, G., 2019. Is DNS ready for ubiquitous Internet of Things?. IEEE Access, 7, pp.28835-28846.

[8] Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M. and Jain, R., 2019. Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal, 6(4), pp.6822-6834.

[9] Xu, T., Gao, D., Dong, P., Zhang, H., Foh, C.H. and Chao, H.C., 2017. Defending against new-flow attack in sdn-based internet of things. IEEE Access, 5, pp.3431-3443.

[10] Li, A., Ye, X. and Ning, H., 2017. Thing relation modeling in the Internet of Things. IEEE Access, 5, pp.17117-17125.

[11] Siegel, J.E., Kumar, S. and Sarma, S.E., 2017. The future internet of things: Secure, efficient, and model-based. IEEE Internet of Things Journal, 5(4), pp.2386-2398.

[12] Xu, T. and Darwazeh, I., 2018. Non-orthogonal narrowband Internet of Things: A design for saving bandwidth and doubling the number of connected devices. IEEE Internet of Things Journal, 5(3), pp.2120-2129.