International Journal of Research in Advent Technology, Vol.7, No.6S, June 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Survey to Understand Data and Information Security Issues and Other Challenges for IoT

Manjunath S, Dr.Anitha T N, Kavana N, Arpitha S M

Abstract—At present day use of modern techniques and technology is an essential and required consideration for being smart for every person to make immediate and smart decisions. For which data and information is essential required parameter?. So one of the method that the users are adopting for daily requirement is IoT. By which needy data is made available at any time, user work is made simple and easier as objects/things are made intelligent such that they are capable to collect data, generate information, transmit information to any place, any time with use of access technologies. Authorized user can access data, information for concerned application, make immediate and smart decisions with that information. Hence such sensitive private data & information generated by such things/objects should be secured irrespective of time and place of access from any unauthorized user. In this paper effort is made to identify and understand issues related to IoT security and other challenges to consider for IoT adaptation in daily use. How these issues can be tackled by using security methods, algorithmic techniques considering for constrained devices. As objects in IoT which are constrained basically in design and its use.

IndexTerms— IoT, Privacy, Access technology, Machine Learning, Artificial Intelligence.

I. INTRODUCTION

With emergence of internet, accessing of any needy information by user is made at fingertips with globally connected. Today, objects/things and devices is less useful without information communication this barrier is overcoming with industrial revolution 4.0. Use of Internet of Things made its way make data and information available to user with electronic applications which is combined with hardware and software. Hence there exist a security issues for protecting user private data so no security breach should not occur either at hardware and software levels.

IoT introduces many opportunities in the areas of healthcare, business, transportation, and logistics. Developers face many challenges to ensure that IoT applications are secure because applications deal with sensitive information. Many security breaches have been encountered, so that the developers must secure the applications or devices at the time of implementation only. IoT devices are deployed in uncontrolled and complex manner. Securing these IoT systems presents a number of challenges of which Security is the main concern for IoT application development. [1].

Manuscript revised May 13, 2019 and published on June 5, 2019
***Manjunath S**, Asst Prof, CSE Dept, SJCIT, Chickballapur*
***Dr.Anitha** T N, Prof and HOD,CSE Dept, SJCIT, Chickballapur*
***Kavana N**, Student,CSE Dept, SJCIT, Chickballapur*
***Arpitha S M**, Student,CSE Dept, SJCIT, Chickballapur*

II. TOP SECURITY CHALLENGES FOR IOT DATA & INFORMATION

a. Constrained devices Security
b. Device identity via Authorize and Authentication
c. Secure Access Technology for Communication
d. Availability should be ensured all time
e. Manage device updates by proper Management
f. Secure Applications (web, mobile, and cloud)
g. Ensure high availability
h. Detect vulnerabilities and incidents
i. Manage vulnerabilities
j. Predict and pre-empt security issues

a. Constrained devices Security

Objects/things used by IoT applications are said to constrained means limitations in Processing, Memory used & Power consumed. Data generated by these devices may be at rest or mobile where device layer security is needed. But use of complex cryptography i.e., for encryption and decryption are not better suited.

So security concerned for these constrained devices is by use of Lightweight hardware and software method is preferred to overcome attacks by side channel where attacker try to get power usage analysis to collect data about device and applies reverse engineer.

Also possible to make use of Spheres of Security approach in depth so multi layer security is given with firewall & different network use [1] [2].

b. Device identity via Authorize and Authentication

Another critical for IoT data secure is at device layer concerned for device identity management and device authentication. As the attackers can easily get device information as the users are unaware of default device password used by manufacturer. To ensure this user must change default password given and user their own password for devices.

Before accessing the gateways and upstream services, a device must establish their identity. There are some devices which goes down when it comes to device authentication. IoT platform is adopted, so that there are no security problems and helps in solving those issues. Consider an example, the two factor authentication (2FA) is enabled by enforcing the usage of strong password certificates. Using IoT platforms, it is possible to access an device authorization

doi: 10.32622/ijrat.76S201928

service which is used to identify the services, resources, or apps that each of the device has to access all over the system [1] [2].

c. Secure Access Technology for Communication

Data gathered from objects must be securely communicated from one end device to another end, device at far place and cloud application which is made possible by use of various network access technology/ techniques for IoT application. Hence secure communication is of much importance as data propagates through various kinds of network to reach destination.

Due to constrained nature many IoT devices that does not encrypt the messages before sending the messages all over the network. So the best to practice the use of transport encryption and adopting the standard, for example, transport layer security (TLS).

It is possible to establish secure and private communication by using separate networks to isolate the devices, thus the data transmitted remains confidential. MQTT payload encryption is another method when TLS cannot be used but still the application data should not be sent in plain text [1] [2].

d. Ensure data privacy and integrity

Maintaining Data privacy and integrity is essentially followed to ensure accuracy, efficiency and decision making. Secure storing and processing of transmitted data over network is important to ensure data privacy and integrity.

By applying fundamental theories personal data processing has to carried, which as 6 data protection principles: The first and foremost theory is concerned with correctness, equality and transparency, second theory is purpose restriction, third theory is data minimization, fourth theory is Accuracy, fifth theory is storage limitation, and sixth theory is integrity and confidentiality [6].

Data privacy must be implemented which includes the redacting sensitive data before it is stored. Data which is not used long time, it should be disposed securely. Legal with regulatory frameworks is necessary for proper maintaining of stored data is also a challenging. As a common method for ensuring data integrity is by using digitally signed data and checksum so that no data modification be done.

Another present approach for IoT data integrity is blockchain which offers scalable, resilient, and decentralized distributed technique, in which blockchain is a record list called blocks which are linked using cryptography [1] [2].

e. Manage device updates

Updating or a new version is must and should for any software or devices to meet the requirements. To use IoT devices and gateways efficiently various challenges has to overcome including updates like security patches to software and firmware. Using heterogeneous devices in distributed environment applied updates should be consistently support as devices will use various networking protocols with wide range of frequency capabilities with low power transmission for sending data from the point of existence. Especially this leads to automation for industries if they already have IoT objects.

Devices need not be accessed physically or pulled temporarily from the production to adopt updates, as not all the devices support the air updates or updates without downtime. All devices need not be having the updates. Hence supporting for the older existing devices or the devices that are not used long time supported by manufacturer has to be taken care when new updates in software architectural changes are done. Even though updates are available the choice of user to sort it out for including the updates to the devices or to software. It is necessary for device management to follow with the versions changes with the devices used so that data specifications can be easily made available for enhanced application development [1][2].

f. Secure web, mobile, and cloud applications

As mobile, web and applications are used for organizing access and in processing of IOT devices and its information, it is necessary to maintain them so that they remain secured as the part of multilayered approach to the IOT security.

While developing IoT applications, vulnerabilities such as OWASP top 10 vulnerabilities should be avoided by Applying secure engineering practices. Due to non standardization of input/output leads to Web application vulnerabilities, which causes unauthorized access and able to source code manipulation. Web Application Firewall is used for protection from application security threats. So to block any attempts to attack by verifying traffic flow these solutions are designed.

As devices support authentication, apps should also design in such a way that it supports authentication, both for the application and the user of the applications, by enabling with the options like secure password recovery options and 2FA. To make safer application layer security for cloud applications Cloud Application Security is preferred [1] [2].

g. Availability should be ensured all time

As needed with IoT application data availability is the most important need for the user at all time irrespective of accessing place with the use of mobile and web applications using physical things which are managed by the IoT systems. As a result of device failures or connectivity out rages, or due to the arising result of attack like DoS Denial of service attack, the potential of disruption occurs. The lack of availability may result in loss of revenue, damage of equipments, or even loss of life.

Consider an example, an IoT device also has pacemakers and insulin pumps. To make sure high availability of IoT devices and IoT infrastructure which is responsible for the services such as traffic control, healthcare, in some connected cities. IoT devices must be protected against cyber attacks and physical tampering as well. IoT devices should include redundancy to eliminate single points of failure, and should be designed in such a way that it should be resilient and fault tolerant, so that it becomes easy to adapt and recover quickly when the problem arises [1].

doi: 10.32622/ijrat.76S201928

h. Detect vulnerabilities and incidents

Apart from the efforts to make IoT devices secure, there are security vulnerabilities and breaches which are unavoidable. Possible vulnerabilities and incidents are common staffs, no control on critical data, servers in local are not secured, precautions by automate for updates, place for critical data backup, use of default password given by manufacturer, not identifying internal security threats etc.,

Approaches for determining vulnerabilities and breaches involves supervising the network communication and logs of activities for anomalies, ethical hacking to expose vulnerabilities, engaging in penetration testing and applying security intelligence and analytics to detect and notify when incidents has occurred. The complexity of some IoT systems is determined by the number of devices connected, various kinds of devices, applications, services, and protocols for communication which are present, which is possible to make it to be composite so that it is becomes difficult to detect when an incident has taken place .

i. Manage vulnerabilities

Maintaining a register of devices is the responsible of Device managers to identify any weakness in the device also if any incident tried to access the system and extent of breach can be assess, so that affected devices are temporarily disabled/isolated till they are patched. The challenges to overcome are identify kind of data and services that are compromised by accessing which devices in the system, identify which devices, users are affected this makes IoT system more complex. Hence necessary to resolve immediately and to take suitable action so that such vulnerabilities never occur in the future.

Vulnerability scanner are used to discover and assess any vulnerabilities occurrences in computer, networks, and application by analyzing open ports, insecure software configuration, and susceptibility to malware infections. Hence Vulnerability Tracker is very essential security control to implement so that identifying any known weakness in Software and configuration setting can be known. For devices such as gateway this feature plays important role by which potential adverse effect or harm can be limited.

By including rules engines and mentioning rules based on vulnerability management policies so that essential action can be done automatically and immediately [1, 2, 5].

Flooding with data is one example with the compromised system.

j. Predict and pre-empt security issues

By applying new techniques like machine learning and Artificial Intelligence with the devices to predict by Thread modeling, detect and control the adverse affect due to security threats these techniques will helps to overcome IoT security challenges. Also by make efficient use of modern tools for monitoring and data analytics to evaluate corresponds with events and observe the timely changes for real time data helps for faster and efficient decision making [2]

III. Other Challenges To Be Considered For Iot

a. Standardization Lagging: Need to develop for hardware and software standards for global acceptance.
b. Support for mobility: Need for effective communication by consider moving objects/things along with fixed objects.
c. Address acquisition: Need for methods to build contact list for Ethernet over Internet
d. Scalability: Need for future number of object increase.
e. Handling new network traffic pattern: As variety of data gathered by IoT application with small data to large data at variable frequency affects traffic that need to handle.
f. Energy efficient protocols for low power communication: As objects/things are limitation with power as most objects are battery operated execution need to consume less power.
g. Non-lossy and high speed channel communication: Need to consider effect of loss while high speed transfer is preferred by application.
h. Low memory routing protocols: As Mesh topology is preferred by IoT interconnect, need to identify hybrid topology for dynamic routing.
i. Make use of Machine learning, Artificial Intelligence and Advanced Analytics for faster analysis [3, 4].

IV. Conclusion

To conclude with this survey for IoT Data & Information security use of Lightweight hardware, software design, techniques and use of ML and AI protocols are the preferred option. Also need to consider energy efficient adaptation in developments of application.

References

[1] Article, "IoT 301: Mastering IoT development"
[2] IoT Analytics "Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers"
[3] Tarun Kumar Goyal & Vineet Sahula "Lightweight Security Algorithm for Low Power IoT Devices"
[4] Muhammad Usman SITS "A Lightweight Encryption Algorithm for Secure Internet of Things"
[5] Masanobu Katagi and Shiho Moriai "Lightweight Cryptography for the Internet of Things"
[6] https://www.futurelearn.com/courses/general-data-protection-regulation.

doi: 10.32622/ijrat.76S201928