AI SECURITY CHALLENGES IN IOT ENVIRONMENT

Priya L, Sathya A
Department of Information Technology
Rajalakshmi Engineering College
Chennai, India

Abstract: *In recent times, IOT has started playing a major role in the industry and also convergence of other technologies like artificial intelligence and other automation is given importance. When it comes to automation Artificial Intelligence plays a great role in terms of ease of use and also it's feasibility in long term is efficient in terms of economic growth and robustness. IOT can be the best way to collect data to serve AI which performs better with more and more data, they can be built better together. The aim of building an intelligent virtual environment with the technologies may bring in harm in terms of security and one's privacy. As the usage has increased the effects of the same are also in large scale. The purpose of the study assess different security concerns and their effects on an individual and the society. Though it is efficient in terms of industry it is important to satisfy the users' expectations beyond the actual job. This study analyzed different threats on could face via the AI in IOT. The major concerns was data which according to the Indian constitution is a fundamental right to have privacy and is applicable to every individual in the world.*

Keywords: **Internet of Things, artificial Intelligence, Data, Challenges, Security, Bandwidth, Cloud**

1. INTRODUCTION

Internet plays a vital role in our day to day life. It extends its scope to interconnect the devices across the world using a set of communication protocols. In the beginning, the Internet was limited to surfing fixed websites and enabling users to communicate with each other by e-mail service. At present, new and multiple Internet technologies have emerged. The number of connected smart devices is increasing exponentially day by day, so the Internet of Things (IoT) is the ideal solution for managing and monitoring these smart devices. An IOT can enable physical components to communicate with each other without the need for human interaction. When these data is going to play an important role in development, it has to be accurate and usable. For this it should be integrated. The data obtained shouldn't be tampered easily by any third party. It has to be properly integrated and authorized. Before that the data must be used abiding to the owner' wish. It must be confidential and privacy should be maintained. The purpose of this study is to provide a global conceptual overview of the AI security challenges in IOT environment especially on areas such as data integrity, data authentication and authorization, data confidentiality, data availability, bandwidth and cloud storage and how they affect the IoT environment.

2. INTERNET OF THINGS

The Internet of Things (IoT) is the fast growing Paradigm in the world of wireless Network Telecommunication. The main objective of this technology is to provide connectivity between heterogeneous network devices. IoT permits people and things to be connected anytime, anyplace, with anything and anyone, using any network and any service. IoT can be defined as a technology that allows "things" to be automated where tasks are repetitive or based on decision making. This helps enabling machine to machine communication and also enables the systems to work independently.

Kevin Ashton mentioned this idea in 1999 during a presentation at Proctor & Gamble. He said that the usage of IoT technology is equivalent to the use of radio frequency identification (RFID) technology and connecting it to the Internet. According to Gartner, 20 billion IoT devices are expected to be connected to the Internet by 2020.

When usage increases, the risks and loopholes in the technology might be used in a way that could have deleterious effects on the users.

IoT helps connect things to a common medium, the Internet and access it. IoT can be implemented in areas where monitoring, detection, tracking are the major jobs. This increases connectivity between the objects and also help make communication between different objects easier. As connectivity increases, it becomes more centralized and hence reduces the need for force to manage the tasks and maintain devises.

A. Applications of IoT

There are numerous application of IoT till date. This includes Smart homes, Health monitoring devices, smart wearable devices etc. There are researches happening to bring in smart manufacturing and smart factories. One of the most potential products of IoT is smart wearable devices, IoT in health care, energy management and IoT for agriculture.

3. ARTIFICIAL INTELLEGENCE

Artificial Intelligence (AI) means training the system in such a way that it can operate on its own without any human intervention. The devices learn by taking actions and classifying them to right or wrong if wrong correcting them i.e. by experience. AI can be performed by Machine Learning (ML) techniques which include computer algorithms and Natural Language Processing, Robotics. AI is classified into 3 main categories: (1) Analytics (2) Decision making (3) Self-awareness. AI is dependent on the computer reasoning the happening based on data it holds. Most of the AI systems are data driven. AI can be applied to places where jobs are monotonous or decisions are stereotyped. The efficiency of these models depends on how much data is available that are true and can be added as en experience, Larger the data higher is its efficiency. The systems can now be automated and centralized through AI and ML algorithms which are classified into two categories: (1) Supervised (2) Unsupervised. The algorithms are chosen based on its purpose it has to elucidate.

4. AI IN IOT

IoT in general needs instructions from the user or inputs from sensor. If AI is coalesced with IoT, it might not be necessary to depend on external inputs to perform actions. IoT has the capability to collect data and process it as instructed. The data is used dynamically for performing required action. If we use these data to train a model, at a point of time, the device can work correctly without depending on external components. This could reduce cost and also as the epoch results might be centralized and hence there won't be need of inputs (or sensors). This could also save time that would be taken to process the input but also provide a better user experience as it will be customized accordingly. The cumulative data can help to predict the correlation between different events in the environment. This could help analyze the patterns. The other advantage of convergence of AI and IoT is through the patterns the system can prescribe the next event that could possibly take place and hence ensure safety. AI can help IoT devices to be fully independent and hence become smarter.

A. How AI and IoT can be integrated?

One possible method is using cloud to store the data obtained through IoT devices. This cloud acts as a data warehouse which in return can be used as the inputs for the ML models. This technology has been in use by various industries in the market. The big Data based ML models are increasingly used in search engines and social networks. But instead of user data, it can be replaced with the inputs from the IoT devices.

5. AI SECURITY ISSUES IN IOT

Though it is easy to obtain data from IoT devices, it has substantial security concerns that must be addressed. The following are some issues that arise:

A. Data Integrity

Data integrity is maintaining and assuring the accuracy and consistency of data over its entire lifetime. It is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

Data integrity has to be standardized in order to achieve better processes and higher quality products by following some principles. According to the ALCOA principle, the data should have the following five qualities to maintain data integrity such as attributable, legible, contemporaneous, original and accurate.

Attributable: Each and every bit of data should be attributed to the generated person. This consists of details such as who has performed the action and timestamp. This helps to determine easily who has changed the data.

Legible: All recorded data should be permanently readable that is the data cannot be changed unwillingly. The data will be used multiple times by different people. If only one person can read the actual records, then the data is more or less unusable.

Contemporaneous: Data is always recorded at the time the action was performed. That is the time for data collection is accurate with the recording time of a data.

Original: The original record should be preserved in order to maintain the data integrity. If there is any duplicates, the developer of the original record must authenticate the copies.

Accurate: The document must be error free. The alternatives must be kept ready if there is any issue in the original process. Data quality must be maintained.

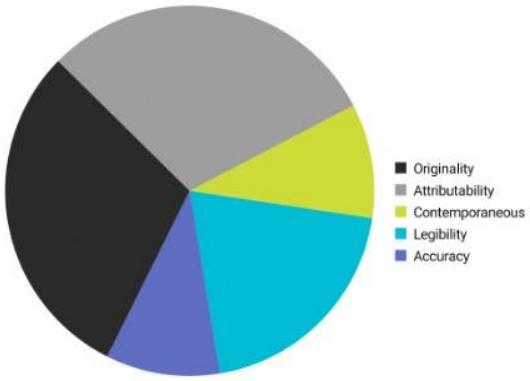

Figure 1 Security issues in IoT

There are some factors that affect the integrity of the data stored in a database such as human error, transfer errors, bugs & viruses, compromised hardware. Risks to data integrity can easily be minimized by:

1. Limiting access to data and changing permissions to restrict changes to information by unauthorized parties.
2. Backing up data.
3. Using logs to keep track of when data is added, modified, or deleted.
4. Conducting regular internal audits using error detecting software.

The cyclic redundancy checks (CRC) is a way to ensure data integrity and detect message encryption errors by adding a fixed-length value to detect network errors in IoT.

B. Data Authentication and Authorization

The major problems that large ecosystem face is authenticating and protecting the identities of all connected devices. IOT devices usually have lower memory. To implement security protection, we need large amount of memory. Increase in memory size increases the cost of the product. Due to increase in cost, several developers are developing the product without security protection and prevention. Unavailability of security can cause many attacks by the hackers who can modify the data or hack the data for money. Authentication and authorization issues play an essential role in IoT security. They verify the identity of users or devices and then grant access to non-suspicious IoT objects or services. The developer of the product must provide access to those people who are in a higher position. He only has the rights to authenticate the users with the unique identifier.

C. Confidentiality and Privacy

IoT devices might be used for different purposes may it be for medical purposes, the users might want to keep the details confidential as it might be altered or misused. This applies to home safety devices. This information can be misused and permanently altered which leads to catastrophe.

According the constitution, every individual has the right to decide whether their information can be shared or not. Most of the times the information are taken without any

actual permission requested to the user. The privacy is not restricted to data but it also includes vulnerability for using Wi-Fi. There are no proper privacy standard both in AI and IoT.

D. Availability

Though large amount of data is generated from IoT, they all might not be true, and the cost for storing large data is pretty high even in terms of cloud. The cloud too has its security issues which isn't addressed yet. There might be latency in fetching the information too if it is to be accessed by the device. On the other hand there is a possibility that data can be in unusable state. This can be due to corrupted ones or the data might go missing due to many reasons like transmission loss or faulty system. These issues might bother the data availability. These issues lead to the need for redundant data which is again a costlier process.

E. Bandwidth

As per 2018, 1% of the internet is used by IoT and others work on 3G and 4G network wiFi which is not efficient in long run and not secured. If all the devices are connected to the internet, then the traffic in the network will increase as it is predicted that at least 20 billion devices will be connected. It will become harder to accommodate all the devices in the range of safe bandwidth and to achieve faster network speed at the same time. In case of AI network usage would increase rapidly to transfer data and process the same.

F. Virtual Private network

IOT devices can join and leave the network at anytime and anywhere. This cause the network topology to be dynamic. A major vulnerability is openness to networked systems. As the devices are connected to the internet, attackers can easily access network and upload malware to devices. The network should be secure for using an automated application. It is preferred to use a secure virtual private network (VPN).

The security of a virtual network space solely depends on controlling and securing all assets that connect into it, which obviously includes physical access security. According to a 2018 Symantec study, there was a 600% increase in the number of IoT attacks between 2016 and 2017. The standard application of VPNs across IoT networks could make those networks significantly more robust than they currently are. When a device is connected to a VPN, all of the traffic running to and from it is encrypted. Even if someone were to intercept network traffic they would be virtually unable to interpret it. A VPN can help protect against DDoS attacks by shielding the user IP address, making it difficult for hackers to launch a targeted attack.

6. SECURITY FRAMEWORK FOR IOT INDUSTRY 4.0

The main aim of industry 4.0 is to automate and exchange data to manufacture cyber physical systems that helps bring up smart manufacturing and more IoT to the environment.

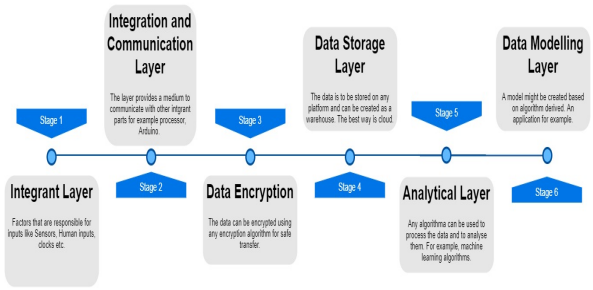

Figure 2 Security Framework

The above figure describes about the architecture of IoT in industry 4.0 which invloves secured transfer and processing of data obtained. The following are the different layers of the IOT architecture:

A. Integrant Layer

In this layer different input devices like sensors, user inputs, gestures etc. are collected through various devices accordingly. This layer is the most important layer for the collection of data and hence accuracy and originality is very important.

B. Integration and Communication Layer

This layer helps interface different integrant and provide a medium to communicate with each other. The best example is a processor to which all the components are connected.

C. Data Encryption

The data to be stored on cloud or an any centralized warehouse id to be encrypted so that it couldn't be tampered. This helps secured transfer and storage of data. Also, Check-bits can be added so as to reduce data loss.

D. Data Storage Layer

Once all the data are gathered from different sources they need to be stored in an efficient manner. The data can be stored in many ways which should be easier to retrieve and scalable.

E. Analytical Layer

To make best use of the data it needs to be processed and analyzed. There are many tools available and algorithms that bring in the best correlation and insights that can be implemented in various field. One best possibility is AI to bring in some patterns and make automation possible in a cheaper method.

F. Data Modelling Layer

After going through analysis, the best method can be chosen and hence a model can be created and can be benefited. These models would help increase the usability of the product and also develop business based on the needs of the society.

7. CONCLUSION

From the study, it has been concluded that security in IoT must be improved by concentrating on the data integrity, authentication and confidentiality and privacy should be maintained in order to avoid any breach of privacy of individual. Hence, there exist a research challenges in the area of IoT security. The IoT architecture must include secured transfer and storage of data for future use of the same.

REFERENCES

[1] Security Challenges and Limitations in IoT Environment, Suha Ibrahim Al-Sharekh, Khalil H.A.Al-Shqeerat, Qassim University, Computer Science Department, Saudhi Arabia.

[2] Evaluatin Privacy and Security Threats in IoT-based Smart Home Environment, SupriyaNagarkarmReseachScholo, Department of Computer Science, Dr.Vikas Prasad, Associate Professor, School of General Managemant, National Institute for Construction Management and Research, Pune, India.

[3] IoT-aided robotics applications: Technological implications, target domains and open issues, L.A. Grieco , A. Rizzo , S. Colucci , S. Sicari , G. Piro , D. Di Paola , G. Boggia, Computer Communication Department.

[4] Early filtering of ephemeral malicious accounts on Twitter , Sangho Lee , Jong Kim, Computer Communication Department.

[5] In-Situ AI: Towards Autonomous and Incremental Deep Learning for IoT Systems, Mingcong Song ; Kan Zhong ; Jiaqi Zhang ; Yang Hu ; Duo Liu. Published by IEEE.

[6] Security threats and issues in automation IoT, Pal Varga ; Sandor Plosz ; Gabor Soos ; Csaba Hegedus. Published by IEEE.

[7] A Survey on Security and Privacy Issues in Internet-of-Things, Yuchen Yang ; Longfei Wu ; Guisheng Yin ; Lijie Li ; Hongbin Zhao. Publisher by IEEE.

[8] Synergy of IoT and AI in Modern Society: The Robotics and Automation Case, National Technical University of Athens, Greece Submitted on August 15, 2018. Published on September 12, 2018, Spyros G Tzafestas, National Technical University of Athens, Greece.

[9] Analyzing the Major Issues of the 4th Industrial Revolution1, Jeonghwan Jeon, Yongyoon Suh.

[10] Innovation Potentials and Pathways Merging AI, CPS, and IoT, Matthias Klumpp ID, University of Twente, Department of Industrial Engineering and Business Information Systems (IEBIS), Drienerlolaan 5, 7522 NB Enschede, The Netherlands, FOM University of Applied Sciences, Institute for Logistics and Service Management, Leimkugelstr. Published on 24 January 2018.

[11]Building Ethically Bounded AI, FrancescaRossi, NicholasMattei, USA.

[12] IoT-Enhanced Human Experience Amit P. Sheth Wright, Biplav Srivastava, Florian Michahelles, State University - Main Campus