Internet of Things (IoT) Security: Issues, Challenges and Solutions.

*Saira Afzal[1], Abdullah Faisal[1,2], Imran Siddique[2] ,Mariam Afzal[3]

[1] Department of Information Technology, Lahore Leads University, Lahore (Pakistan).

[2] Department of Computer Science, Afro Asian Institute, Lahore (Pakistan).

[3] University of Narowal, Punjab, (Pakistan).

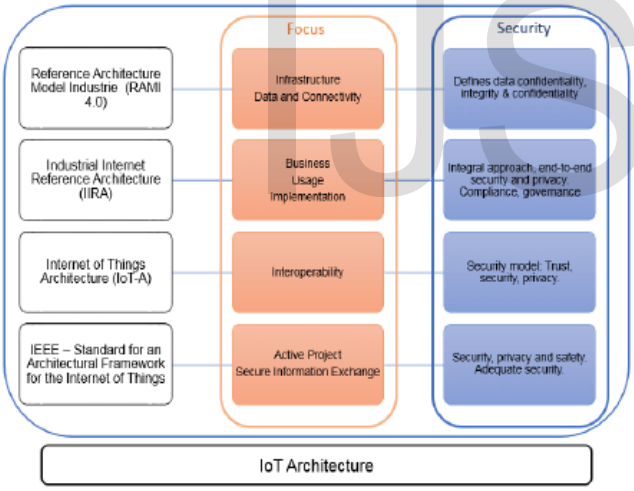
*Corresponding Author: sairaafzal322@gmail.com

***Abstract*--**The Internet of Things (IoT) paradigm envisions a world in which billions of interconnected objects are equipped with artificial intelligence, internet access, and sensing and actuation capabilities. Instead of a small number of powerful computing devices in our lives, the theory assumes that we should have a large number of devices that are comparatively less powerful. In other words, providing computational and internet capability in just about every mundane entity we have. An earlier buzzword for roughly the same definition was "ubiquitous computing". The Internet of Things has just improved the idea of internet convergence. The problem of IoT protection is extremely complicated. Integrity violations may come from a variety of outlets, none of which are mutually exclusive. Since this technology is only in its early stages, both consumers and suppliers are looking for the best options. Malware threats and system hijacking, poor consumer knowledge due to a lack of understanding, a lack of official patches, and rogue IoT applications are all examples of Internet of Things security issues. Keeping the IoT network apart from the others, for example, is one step users should take to mitigate the effects of poor protection. By avoiding plug-and play functionality, you can save time and money. Not using cloud computing Passwords for IoT devices should be special and complicated.

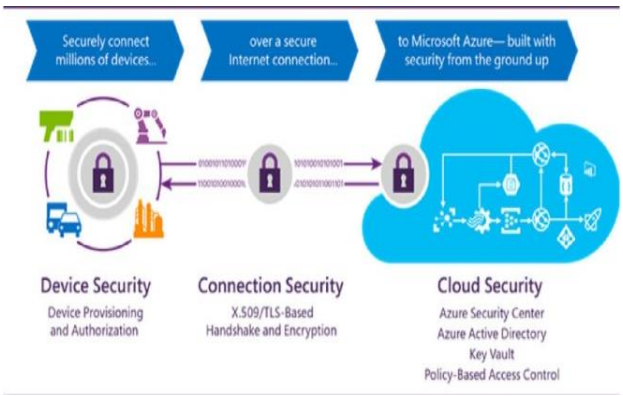
***Index Term*—**Internet of Things, Security, Issues, Encryption, Cloud Computing.

I. INTRODUCTION

Rather than relying on a technology's ostensibly beneficial advantages, I have always made it a point to go through the shortcomings first. There are now "things" that communicate with the Internet without our involvement, in addition to humans and our machines. These "Things" are constantly interacting with the Internet, whether it's a refrigerator sending an alert on the food inside or our car sending messages to the mechanic on its oil levels. In many ways, the Internet of Things is fantastic. However, technology has not yet evolved, and it is not completely secure. The Internet of Things (IoT) has gotten a lot of press because of its wide use potential. Many observers predicted that 2015 will be an existential year for IoT at the start of the year. We have



stated that this year would be the year of the IoT Enterprise segment. Sluggish growth and progress as a result of IoT protection also raised concerns. The media was relentless in demonstrating the shortcomings and loopholes in linking anything with the internet. The security problems posed by the Internet of Things are true, and they must be tackled first. However, it has been proved time and time again that any new technology faces its fair share of obstacles and criticism.



IoT security concerns are unavoidable, but they do not deter you from designing IoT apps.

Fig.1: IoT Architecture

II. IOT SECURITY ISSUES

Protection and testing mechanisms are critical in the implementation of any IoT program. We've highlighted the top security issues you can consider to help you build more stable and attack-proof internet of things connected devices and applications.

Fig. 2: Azure IoT Security Architecture

A. IoT Security-Data encryption

The Internet of Things (IoT) apps accumulate a large amount of data. Data storage and processing are essential components of the IoT ecosystem. The most of this information is personal and must be encrypted. Wherever the data is present online, one can use Secure Sockets Layer protocol, or SSL, to fix this IoT security problem. SSL certification is now used for websites to encrypt and secure consumer data on the internet. This is just half of the equation; the other half involves safeguarding the wireless protocol. Encryption is often needed when data is transmitted wirelessly. Sensitive

information, such as locations, can only be accessible to the person in question. As a result, be sure to use a wireless protocol that includes encryption.

B. IoT Security Data Authentication

Also after good data encryption, there is always a risk that the system will be compromised. Protection is jeopardized if there is no way to verify the accuracy of data sent to and from an IoT computer. Assume one built a temperature sensor for smart homes. Even if the data is encrypted, if there is no way to verify the source of the data, someone can make up false data and send it to the sensor, telling it to cool the room even though it is cold, or vice versa. Authentication problems may not be obvious at first, but they do pose a security risk.

C. IoT Security Side Channel Attack

Even with encryption and authentication in place, side channel attacks are still possible. Such attacks are more concerned about how it is delivered than with the information itself. For example, if anyone has access to data such as timing, power consumption, or electromagnetic leak, any of this data will be used in side channel attacks.

D. Hijacking of IoT Devices and Ransom-ware

Ransom-ware, a virus that encrypts and prevents access to users' confidential data, can attack IoT devices with poor measures of security. The real trouble starts when a hacker who compromised the computer with ransom-ware requests ransom money in order for the victim's files to be opened. It might sound dystopian, but it is a fact - although an uncommon one at the moment. However, in the underground hacker world, this is becoming more common. It's a frightening idea to see a house that's been locked up or a smart car that won't operate until the ransom is paid. Attacks like Ransom-ware have the potential to lock users out of IoT computers and associated platforms, as well as uninstall devices and steal data. Because of the rapid growth in the number of IoT devices around the world, this particular IoT protection problem would be volatile in terms of potential permutations. However, since most IoT data is saved in the cloud, this ransom-ware does not have any sensitive data to lock.

E. Lack of updates and insufficient testing

One of the reliability problems with IoT systems is that manufacturers are often too sloppy when it comes to rigorous monitoring and timely app upgrades.

Resultantly, the Internet of Things computer running obsolete applications may be vulnerable to a variety of ransom-ware and hacker attacks, as well as other security flaws. Another frightening probability is that when a computer transfers its data to the cloud after an upgrade, there can be downtime. If the link is not encrypted at this time, the upgrade files can be left vulnerable, allowing hacker’s access.

For preventing IoT security problems, regular automatic updates are important. It is the responsibility of the vendor to their software that will help to discover the bugs and some ransom-ware type common attacks.

F. Home Intrusion

Home intrusions or home invasions IoT security problem. The idea of "smart houses" was born as Internet of Things technologies became a feature of
an increasing number of homes. This home automation poses a significant risk because rogue devices with weak protection mechanisms can broadcast IP addresses. Hackers could be able to find the address of the computer owner using so-called Shodan searches. The potential for misuse is obvious, and it may also lead to the user's address hitting criminal circles.
Connecting with VPNs and protecting login credentials are two ways to avoid this IoT security violation, which we'll go through later in the post.

G. IoT driven Financial Crime

Financial crime and synthetic identity theft may increase for e-payment organizations that use the IoT. Several of these businesses are experimenting with IA and deep learning, but others quickly realize the value of combining data across many business layers. This is to ensure that deep learning is used to identify fraud patterns and complicated signals in a timely manner. Because of regulatory and technical challenges, all financial firms will face difficulties in launching these new versions. If they develop their model lifecycle and risk management plans to account for the growing danger of IoT security breaches.

H. Remotely access of smart vehicle

The hijacking of smart vehicles is an IoT security problem that is similar to home invasion. Vulnerable IoT devices will open the door to serious dangers, such as remote access to the smart car. This deliberate intrusion poses a significant risk to public safety because they can result in injuries. This vehicle control may also be vulnerable to attack, because an attacker can demand payment in exchange for accessing the vehicle or for engine activation. Fortunately, since these attacks often occurred before the mainstream use of wireless networks, the developers had plenty of time to react accordingly.

I. Counterfeit and rogue IoT Devices

Perimeter closing and controlling all single the gadgets of user's even single user is a major IoT security problem. The rapid growth in popularity and manufacturing volume of Internet of Things products has created a problem with home networks.

J. Lack of Knowledge in IoT area Users are also getting used to the Internet of Things' quirks and characteristics because it is such a modern application. Malwares, viruses and attacks are all areas where people have effectively perfected their own security.

The consumer illiteracy, perhaps the most serious IoT issue as puts anyone at risk, even consumers and others who are attached to their own IoT devices in any way. Through attacking people with the Internet of Things, social engineering attacks take advantage of easiest to avoid by human aspects.

The disastrous 2010 attack on an Iranian nuclear facility was an especially serious case of such misuse of the unprepared human element. IoT Security Hardware Issue.

The hardware for the internet of things has been a challenge from the beginning. For all

of the excitement and unexpected interest in IoT applications, chipmakers such as ARM and Intel are strengthening their processors for increased security with each new generation, but the practical scenario does not seem to ever close the security gap.

The issue is that, due to new architecture of chips designed especially for IoT applications, their costs will rise, making them costlier. Furthermore, the complicated architecture would necessitate more battery capacity, which would be a difficulty for IoT applications. Such chips cannot be used in low-cost portable IoT systems, necessitating a new strategy.

III. IOT SECURITY SOLUTIONS

Having a rigorous research process in place is the only way to mitigate the hardware security risks of the internet of things.
Some of security solution as

A. Device Range

The IoT device's range coverage network is critical. one must be very precise when it comes to the range metrics for the app or tablet. For example, if you're using Zigbee technology to control the device's network, one will need to figure out how many repeaters one 'll need inside a building to give the computer enough connectivity range. However, one cannot simply add any number of repeaters because the power of the machine reduces as the number of repeaters increases. As a result, system range testing would allow one to discover the sweet spot where one can optimize range without exceeding the limit.

B. Capacity and Latency

Capacity refers to the network's bps (bits per second) handling speed, while latency refers to the total time it takes for data to migrate between application endpoints. To boost performance, developers are still looking for ways to increase ability and latency in their IoT applications. The problem is that these two variables are inversely proportional, which means that improving one degrades the other. Latency and power balancing should be carefully checked in data-intensive systems and applications.

C. Test for Manufacturability

It's rare that one'll build the own IoT system from the ground up. In most cases, one'll be using third-party components and modules in program. It's important to test these modules for proper operation. Manufacturers do assembly line checking on their own, so one can double-check. Additionally, after all of the components are assembled on a board, checking is necessary to ensure that no defects have been introduced due to soldering and wiring. Manufacturability testing is needed to ensure that the application functions as expected.

D. Make Strong Passwords and Change Them Often

Changing passwords on internet accounts, laptops, and handheld devices on a daily basis has become the standard in recent years. It should be standard for Internet of Things devices by now. For security reasons, each IoT system has its own password, which one can update at least once a year, stop using standard or generic passwords, and make very complicated and difficult to crack. Password managers can

help one recall them all, because they can be cracked as well.

E. Do not Count the Cloud Computing

Cloud technology is certainly easy, but it is still a highly insecure and attack-prone new technology. Per product one purchase from an IoT manufacturer typically comes with cloud storage space. Although it may be tempting to choose something that is free, keep in mind that access the saved data in cloud requires an active link, which can be hacked while one accessing the cloud accounts. Often, ensure that the data is encrypted or, better still, that you store the files and data locally, away from the grasp of fraudsters.

Stay away from universal plug-and-play features.

1) A majority of IoT units have a Universal Plug & Play feature that allows several devices to link to each other. This ensures one won't have to customize each computer separately.
2) While this gives a clear benefit to the Internet of Things environment in the home or office, be cautious.
3) Local networks are used to link Universal Plug & Play protocols.
4) As we've learned, these networks are vulnerable to outside threats and can be readily hacked.
5) If the attack were effective, it may effect a large number of IoT devices by allowing attackers to control from remote location.

F. Make use of a backup network

Wi Fi users also build several networks, and define their access as limited for them or their friends.

This method of creating a second network can be used for IoT devices because it aids in data collection.

1) Protect the confidential files from unauthorized entry.

2) Put an end to all efforts to take control of IoT devices and install malware.

3) Fully isolate the IoT system from the outside world, protecting protected info.

4) Make sure the IoT device is up to date on a regular basis.

Automatic upgrades must be in order to search for official updates from the system vendor, as mentioned regarding the lack in updates as one of the IoT protection concerns. This applies security patches to the computing or digital devices which will prevents attackers from infiltrating them.

Daily IoT product updates have the following benefits:

1) Peace of mind in ensuring that the devices are up to date with the most up-to-date security protocols, allowing one to avoid the most recent types of threats.

2) It provides high level of protection to our offices, home and areas in which we need high level of security like banks etc.

IV. CONCLUSION

Adopting a multi-layer security-by-design approach to IoT development is critical for handling computers, files, web and cloud-based IoT applications and services, as well as coping with threats and issues as they occur. Neglecting protection in IoT systems can result in device errors, capital losses, and even destruction.

Integrating protection by default – ensuring that security features are calibrated to their most protected configurations at all levels, including before, after, and after production – allows one to protect data privacy and integrity when providing highly accessible IoT data, content, and services.

V. FUTURE DIRECTION

Safety questions about the Internet of Things are being researched by the industry as well as a division of academics that understands and examines the promise of these technologies. By 2020, more and more businesses will recognize the promise of IoT, with corporate funding accounting for more than half of all IoT spending. This means that, in order to satisfy corporate demands, vendors would need to double down on their cyber security activities. Ordinary users would have to play a role as well, by training themselves and staying current on IoT security technologies and their significance. This, like other advancements, starts with concerted attempts at a higher level. The US Congress passed a cyber-security bill in March 2019 with the aim of ensuring all IoT devices purchased by the government have at least basic security features. Embedded encryption is now available in some IoT devices from some manufacturers. We can also anticipate the emergence of technologies of IoT security and its development role in industry that surely will focus on and advance development in areas. Machine learning-based attack prediction and intrusion detection on IoT systems, Secure IoT systems architecture Data privacy and IoT interface management strategies.

To ensure proper operation and protection, the security solutions mentioned above should be strictly enforced. Since IoT devices are still in their infancy, being cautious about their protection is beneficial. Before one begin developing any IoT program, one must do extensive research to gain as much knowledge as possible. There will still be trade-offs, such as more protection with a bad user interface, but as previously said, one must find the sweet spot. Often, don't try to get the goods on the market without sufficient long-term help preparation. Since IoT computers are so inexpensive, there's a good risk that vendors will neglect to include security upgrades and patches. This is not a long-term growth strategy for the internet of things. Always be on the lookout for risks as an IoT device creator. Security breaches are almost certain to occur, and one should be prepared. In the event of an attack, one can already have an escape strategy in place to protect as much data as possible. Finally, still take the opportunity to educate clients and staff on the most recent IoT security risks and solutions.

REFERENCES

[1] Gilchrist, Alasdair. IoT security issues. Walter de Gruyter GmbH & Co KG, 2017.

[2] Zhang, Zhi-Kai, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In 2014 IEEE 7th international conference on service-oriented

computing and applications, pp. 230-234. IEEE, 2014.

[3] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.

[4] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." In 2015 ieee world congress on services, pp. 21-28. IEEE, 2015.

[5] Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures." In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336-341. IEEE, 2015.

[6] Riahi, Arbia, Yacine Challal, Enrico Natalizio, Zied Chtourou, and Abdelmadjid Bouabdallah. "A systemic approach for IoT security." In 2013 IEEE international conference on distributed computing in sensor systems, pp. 351-355. IEEE, 2013.

[7] Gou, Quandeng, Lianshan Yan, Yihe Liu, and Yao Li. "Construction and strategies in IoT security system." In 2013 IEEE international conference on green computing and communications and IEEE internet of things and IEEE cyber, physical and social computing, pp. 1129-1132. IEEE, 2013.

[8] Frustaci, Mario, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino. "Evaluating critical security issues of the IoT world: Present and future challenges." IEEE Internet of things journal 5, no. 4 (2017): 2483-2495.

[9] Kamble, Ashvini, and Sonali Bhutad. "Survey on Internet of Things (IoT) security issues & solutions." In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 307-312. IEEE, 2018.

[10] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future Generation Computer Systems 82 (2018): 395-411.

[11] Karthika, P., R. Ganesh Babu, and P. A. Karthik. "Fog computing using interoperability and IoT security issues in health care." In Micro-Electronics and Telecommunication Engineering, pp. 97-105. Springer, Singapore, 2020.

[12] Mohanta, Bhabendu Kumar, Debasish Jena, Utkalika Satapathy, and Srikanta Patnaik. "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology." Internet of Things (2020): 100227.

[13] Kumar, Vinod, Rakesh Kumar Jha, and Sanjeev Jain. "NB-IoT security: A survey." Wireless Personal Communications 113, no. 4 (2020): 2661-2708.

[14] Borovska, Plamenka, and Desislava Ivanova. "In silico knowledge data discovery in the context of IoT ecosystem security issues." In AIP Conference Proceedings, vol. 2333, no. 1, p. 030004. AIP Publishing LLC, 2021.

[15] Da Xu, Li, Yang Lu, and Ling Li. "Embedding Blockchain Technology into IoT for Security: A Survey." IEEE Internet of Things Journal (2021).

[16] Patnaik, Ranjit, Neelamadhab Padhy, and K. Srujan Raju. "A Systematic Survey on IoT Security Issues, Vulnerability and Open Challenges." In Intelligent System Design, pp. 723-730. Springer, Singapore, 2021.

[17] Bhargava, Akansha, Gauri Salunkhe, Sushant Bhargava, and Prerna Goswami. "A Comprehensive Study of IoT Security Risks in Building a Secure Smart City." Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings (2021): 401.

[18] Mohanty, Jayashree, Sushree Mishra, Sibani Patra, Bibudhendu Pati, and Chhabi Rani Panigrahi. "IoT Security, Challenges, and Solutions: A Review." Progress in Advanced Computing and Intelligent Engineering (2021): 493-504.

[19] Saha, Himadri Nath, Reek Roy, Monojit Chakraborty, and Chiranmay Sarkar. "IoT-Enabled Agricultural System Application, Challenges and Security Issues." Agricultural Informatics: Automation Using the IoT and Machine Learning (2021): 223-247.

[20] Parmar, Monika, Neeraj Kumar, Harsimran Jit Kaur, Abha Sharma, Sandhya Sharma, and Mamatha Sandhu. "Analysis and Comparison of Different Blockchain Algorithms in IoT Security." In IOP Conference Series: Materials Science and Engineering, vol. 1022, no. 1, p. 012059. IOP Publishing.

Authors Profile:

Saira Afzal

M.Phil Information Technology, Lahore Leads University, Lahore (Pakistan).

Abdullah Faisal

Currently working as a Lecturer in Department of Computer Science, Afro Asian Institute, Lahore (Pakistan).

Imran Siddique

Currently working as a Lecturer in Department of Computer Science, Afro Asian Institute, Lahore (Pakistan).

Mariam Afzal

Bachelor of Science in Physics BS (Phy)
University of Narowal Punjab, (Pakistan).