IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Optimization Functions Apply to IoT Security

Surendra Kumar Patel*
Assistant Professor
Dept. of Information Technology
Govt.Nagarjuna P.G. College of Science,
Raipur, Chhattisgarh, India

Abstract—The Internet of Things is actually a current technology which is used to various fields; it means taking all the things in the world and connecting them to the Internet. There is a significant risk of exposure to billions of connected devices, identity theft and data theft, device manipulation, data tampering, server / network manipulation and later application platforms. Security is the main concern in the adoption of the Internet of Things technology, with the concern that rapid growth may be necessary without taking into accounts the profound security challenges and regulatory changes. Therefore, this document addresses several security objectives, their challenges, and optimization of existing security functions. Therefore, this research addresses several security objectives, their challenges, and optimization of existing security functions. This paper also delineates security challenges at different architectural levels, attacks and trust elements and optimization of basic security functions in terms of data storage, energy efficiency, flexibility, computation time, and associated costs.

Keywords—IoT Security, Security Attack, Security threat, Security Function.

I. INTRODUCTION

IoT means Internet of Things. The Internet of Things is a web of objects that contains IP addresses connected to the Internet and the communication between these objects and other Internet-enabled devices and systems. In other words, anything that has connected devices and can send data from one place to another or to people on the Internet is called Internet of Things (IoT). In addition to traditional devices such as computers and laptops, smart phones and tablets, a variety of devices and objects that use built-in technology to communicate and interact with the external environment [1-4] the display of objects can be used over the Internet. Security of things including networks, thermostats, cars, electricity. Home and business lighting equipment, alarm clocks, speakers, lighting equipment and more [2].

The current technologies for IoT security primarily come from the concepts of tradition network security. Most of them focus on identity authentication, access control, privacy protection, encryption, security protocol, and etc [5-9]. The security ways are in the stage of passive defence. To construct effective defence measures for IoT security, researchers proposed some methods and models of active defence. Murkowski et al [10] developed a system of intrusion detection according to the past access frequency of thing labels. Yang et al [11] presented a distributed intrusion detection method for nodes of wireless sense networks. Wu et al [12] proposed a security transport model for IoT confidentiality. The on top of illustrated system, method and reproduction provide solution and aspect of the IoT security problems. However, they don't form an effective IoT security architecture and cannot provide an appropriate approach to resolve problems of IoT security.

Internet of Things (IoT) devices connects the world from 2015 to 2025 (in billions).

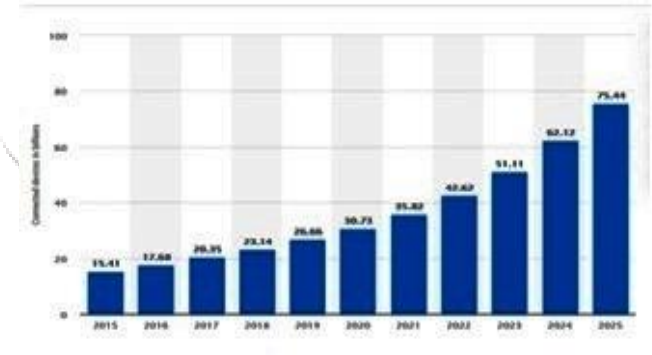

Figure-1: Published by Statista Research Department, Nov 14, 2019[31].

Looking at Figure-1, the amount of mechanical iodine increases every year. We need to consider the security of open behaviour. Internet firewalls are designed to prevent Internet devices from communicating with each other over a wireless network [3]. IoT security is a security component associated with the Internet of Things that aims to protect IoT devices and websites from cybercrime. While IoT devices provide better connectivity between devices, they use up resources and save time and money. And the many benefits of IoT security for consumers are just one. There are a number of hard cases that make IoT devices difficult to read.

II. IoT Challenges

Security vulnerabilities are the biggest challenge in IoT. IoT database can be your company, organization, customer or yours. This document must be protected and kept confidential against theft and vandalism. For example, an IoT application may store IoT health or retail solutions and improve device connectivity. But there is a problem with the ability to scale. Availability and response time Security is an issue when information is delivered securely online. Security procedures can be enforced through legal requirements such as the Health Insurance Mobility and Liability Procedure (HIPA) when transporting data across borders. In addition to various security challenges, major IoT challenges are also being addressed [12].

1) **Confidential Information:** Some TV manufacturers collect information about their customers to analyze their viewing habits. Thus, the information collected by smart TVs becomes a challenge for confidential information during transmission [13].

2) Data Security: Data security is also a big challenge. Although the information is well put together, it is important to hide information from surveillance devices on the Internet.

3) Concern: Insurance companies are installing IoT devices on their vehicles to collect information about health and condition of drivers for making insurance decisions.

4) Lack of standards: Because there are so many standards for IoT devices and IoT manufacturers, it can be extremely difficult to differentiate between devices that allow and enable Internet connections [13].

5) Technology Concerns: The increasing use of IoT devices has also increased the human traffic for these devices. In the case of the need to increase network capacity, it is difficult to store large amounts of data for analysis and other final data [19].

6) Security and Security Concerns: There are many operations in the field of IoT security. Active networks can be divided into software protection. Software Security and Network Security [13]

a) System Security: System security is usually focused on all IoT systems to solve various challenges. Create separate security and sufficient security to meet website security.

b) Security applications: Security applications work with IoT applications to address security vulnerabilities as needed.

i) Network Security: Network security and security of IoT network infrastructure for a network of various IoT devices.

III. Security in the Internet of Things

Common security solutions such as firewalls, IDS, antivirus and software are not optimized for IoT devices. There are three main reasons for this [14] (1) Infrastructure type: An application can use multiple IoT devices. Wireless communication (such as via Wi-Fi or Bluetooth) or (such as IoT lamps can be controlled via IoT light sensors) can result in a complex and robust network that can be difficult to guarantee the implementation of security policies. (such as firewalls) (2) Signature and behavioral anomalies: Some security methods store device anomalies and signatures to detect and detect threats. Due to the differences between IoT devices and manufacturers, these methods are insufficient because the devices must be constantly updated and maintained to support them (3) Better Methods: IoT devices are powerful. Low power consumption and does not make optimum use of software. A common security method requires all of the above to be activated. This way, no IoT device is required. (and use of password or delivery errors) may occur in the organization.

Technology used for security purpose in IoT

A. Database: IoT network layer and application layer are closely related. Therefore, we have to choose between hop-to-end and end-to-end encryption. If we use hop encryption, we can specify the connection to be developed. Want in the communication industry; we can make good use of all the companies using different applications. In this way road safety is clearly visible in business enterprises. This results in a normal user experience. Now, this full-hop gaming functions have features like low latency, high performance, low cost, etc. Due to standard analysis in the delivery node using e-hop encryption, each node can receive clear messages. Hence there is a need for high reliability of transmission nodes [15].

B. Secure Communication: Incorporate the communication model with the solution. These solutions can provide reliability, authenticity and LSness for communications such as IPSec to T/SSL. TLS/SSL is designed to connect to form the transport layer and IPSec is designed to secure it. Security at one level Authenticity, authenticity and networkability can be guaranteed at each level. There are also complication obligations that are unfortunately not widespread. And road safety nets are still heavily used these days. Since small devices do not have enough power in IoT, network security is not vulnerable. Today, the topic of communication in IoT is often the current topic of the next generation. Most of the information is transmitted via the Internet [15].

C. Data Security: The integrity and integrity of the data is monitored. And the certainty of sensor data is a lesser requirement. Because when an attacker can put the sensor on the side of the body. He considers himself equally important. And the relatively low privacy requirements with the sensors themselves another important topic for sensor research is privacy. And privacy is also one of the big issues. We must take steps to protect the privacy of people and things in the world. Often people are not aware of censorship in their lives. We need to set rules to protect people's privacy. There are several suggestions in the text to solve this problem in the image section: Ten First of all, the user should know how he feels. Second, the user has to decide whether he feels like it or not. And third, remain anonymous. If consumers are not aware of these guidelines, there should be rules.

IV. Security Challenges in IoT

Security is the most important factor that IoT development can handle. Providing security for IoT technologies is a real challenge. Because IoT technology is very broad and the

areas of research are many. That's why we focus on security challenges related to performance, efficiency, cost, data, and wireless sensor networks among other areas. And other security challenges [10]

Inadequate Capabilities: Technical skills and capabilities are essential factors required for prevention of planning, implementation, development and management of defence. Violation of these factors can lead to system failure in IoT. Furthermore, lack of skills and capabilities can slow the adoption of IoT technologies [4, 5]. The number of professionals who properly implement IoT technologies is limited. Using IoT technology and meeting its challenges requires a lot of personal skills.

2. Integration vs Safe Balance: Pricing plays an important role in any IoT project. On the one hand, tools and equipment play an important role in improving security. And reduce the chances of this happening in any other way. The need for high quality materials necessitates high financial costs [12, 13].

3. Privacy: With IoT, everyone can access users' devices from anywhere. This affects the confidentiality of sensitive information. Therefore, certain rules or regulations must be established to prevent privacy breaches – for example, some IoT devices share data with other devices. In this case, the data will be compromised. This allows attackers and hackers to access IoT systems and then install malware and break confidential and confidential information [8, 9].

4. Weak security models and innovations: More than 24 billion IoT devices are connected around the world. It is difficult to identify all relevant security vulnerabilities. The demand for IoT tools is forcing IoT developers to produce them faster. This challenge leaves IoT users vulnerable to threats and attacks, no matter how secure they are. a quantity of strategy or deployed devices may not receive the required security updates. Implementing updates to IoT devices can be challenging. Why some devices don't support updates. And some older devices may not support the new update. When devices are vulnerable, they are vulnerable to attacks and other security vulnerabilities [10].

5. Resource capacity and low capacity: The power supply of IoT devices is so high that the battery cannot be easily charged. That is, it is limited. Therefore, the performance of the network is due to insufficient battery capacity of the machine. In addition, the workforce is also a major challenge in developing compatible IoT devices and networks, so the power source is very important. especially on battery powered devices [10].

Difficulties in ensuring IoT security, such as differences in ownership of physical communications, key requirements, security, size, onboard reliability. And the security features make it difficult to access various inspection documents. Assess potential risks to identified IoT infrastructure by collecting and responding. A lot of research has been done on things like core management, classification, configuration, security, and permissions for IoT architectures. These studies build on new exchanges of cryptographic protocols and systems such as software defined networks (SDNs) and block selection, which are being used to improve existing IoT security vulnerabilities so that the design of these devices does not take security into account. Because the device operating system is still relatively simple these days. Many times there are IoT drones along with smart city drones for virtual reality vehicles. Self-propelled drones (SDVs) for robotic drones and the grid (DER) for small windows to transport energy items [17].

V. IoT Vulnerability Projects

The table below shows the IoT vulnerabilities defined by the OWASP [32].

Vulnerability	**Attack Surface**
Enumeration of Username	-Administrative Interface -Device Web Interface -Cloud Interface -Mobile Application
feeble Passwords	-Administrative Interface -Device Web Interface -Cloud Interface -Mobile Application
Account stop somebody from getting in	-Administrative Interface -Device Web Interface -Cloud Interface -Mobile Application
Unencrypted Services	-Device Network Services
Two-Factor substantiation	-Administrative Interface -Cloud Web Interface -Mobile Application
Poorly Implemented Encryption	-Device Network Services
Update Sent Without Encryption	-Update Mechanism
Update Location Writable	-Update Mechanism
Denial of Service	-Device Network Services
Removal of Storage Media	-Device Physical Interfaces
No Manual Update Mechanism	-Update Mechanism
Missing Update Mechanism	-Update Mechanism
Firmware and Storage Extraction	-JTAG/SWD interface -In-Situ dumping -Intercepting a OTA update -Downloading from the manufacturer's webpage -eMMC tapping
Manipulating the Code Execution Flow of the Device	-JTAG/SWD interface -Side channel attacks such as glitching
Obtaining Console Access	-Serial interfaces (SPI/UART)
Insecure 3rd-Party Components	-Software

VI. Basic Security Optimization Function

Table-1 [22] compares several existing solutions and their impact on improving the security of the infrastructure used. They are protected by all applicable security themes. It is a standalone, data-driven security approach except for the last set. It can be concluded from this table that there is a need for IoT security solutions.

Generally, network optimization is defined as the technology used to improve the performance of the network for any environment.

Table-1: Comparison between existing solutions in IoT security and its effects.

Existing Solution/Comparison parameters	Optimization of basic security functions			
	Efficiency Energy	Flexible	Computational Time	Cost
An FPGA Implementation of a Flexible Secure ECC Processor		√	√	
H/W-S/W Implementation of Public –Key Cryptography for Wireless Sensor Network		√		√
A safety measures come within reach of for off-chip memory in surrounded microprocessor system				√
The compiler-hardware based come within reach of to software protection for embedded systems		√		√
A data-driven approach for embedded security				

Optimization Problems

Security risks can be mitigated by replacing vulnerabilities. However, due to operating costs, it is not always possible to replicate all vulnerabilities at the same time. This vulnerability may use a variety of methods to complicate the application of the prioritization method [22, 23, 24, 25] and claims that many of these methods are ineffective. They developed a heuristic algorithm to accelerate patch optimization [26] using an ant optimization algorithm to detect a small number of key features [27] to better address these vulnerabilities. Use graphical software attack lines to find the best way to set this up. Product protection has been added to the site (for example, a hosted firewall). The author uses a probabilistic Bernoulli model and replaces the graphic simulation with a parallel graphic system. In this article, we present another problem to ensure that IoT Toolkit on-premises have the least impact on network security [30].

CONCLUSION

Security is an important topic in IoT, as we have seen. And why IoT is used in sectors and services such as business and healthcare. Protecting sensitive and sensitive data from fraud is even more important now. This article discusses the challenges of IoT and security in IoT tools with a focus on safety in applied technologies such as road safety. Communications Security Data Security Action in these road defense wars is also somewhat inadequate. Since IoT devices have no security path, many IoT devices have limited restrictions. It doesn't already have access to the well-known education it's interested in. In this way the IoT security challenge becomes the biggest risk for IoT device makers. However, having these IoT tools is the biggest problem.

In this research, we focus on creating data in IoT technologies, such as the reality of distributed storage. Its primary purpose is to protect and manage information over which the record owner has no control. The only requirement for obtaining confidential information in a previous study is the use of asymmetric encryption methods. In a large IoT environment, content is shared by a large number of users across websites and services. And lead to a wider audience. That's why software exists to protect sensitive information. Payments from unauthorized persons include fraud prevention, service and stock changes. The use of encryption is associated with integrating backup storage and encrypted security in an IoT environment using symmetric encryption techniques for real-time data encryption and encryption. During the stay for the safety of the people

REFERENCES

[1] https://www.webopedia.com/TERM/I/internet_of_things.html .

[2] https://www.hcltech.com/technology-qa/what-is-an-iot-device.

[3] https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html.

[4] Mainetti, L., Manco, L., Patrono, L., Sergi, I. and Vergallo, R., 2015, December. Web of topics: An iot-aware modeldriven designing approach. In IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 46-51K. Elissa, “Title of paper if known,” unpublished.

[5] T. Kavitha, D. Sridharan. Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security, 2010, (5): 31-44.

[6] Y. Zhou, Y. G. Fang, Y. C. Zhang. Securing wireless sensor networks: a survey. IEEE Communications Surveys and Tutorials, 2008, 10: 6-28.

[7] V. Oleshchuk. Internet of things and privacy preserving technologies. Proc. of 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology(Wireless VITAE), Aalborg, Denmark, May, 2009,

[8] A. Juels. RFID security and privacy: a research survey. IEEE Journal onSelected Areas in Communications, 2006, 24(2): 381–394.

[9] Y. B. Zhou, D. G. Feng. Design and Analysis of Cryptographic

[10] Protocols for RFID. Chinese Journal of Computers, 2006, 29 (4) : 581-589.

[11] Lee, I. and Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), pp.431-440.

[12] 20] Kumara, N.M. and Mallickb, P.K., 2018. Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, pp.1815-1823.

[13] Alharby, S., Harris, N., Weddell, A. and Reeve, J., 2018. The security trade-offs in resource constrained nodes for iot application. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 12(1), pp.52-59.

[14] Middha, K. and Verma, A., 2018. Internet of Things (Iot) Architecture, Challenges, Applications: A Review. International Journal of Advanced Research in Computer Science, 9(1).

[15] Haroon, A., Shah, M.A., Asim, Y., Naeem, W., Kamran, M. and Javaid, Q., 2016. Constraints in the IoT: the world in 2020 and beyond. Constraints, 7(11).

[16] Suha Ibrahim Al-Sharekh1, Khalil H. A. Al-Shqeerat2 (IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.2, February 2019).

[17] Navneet Verma, Suman Sangwan, Sukhdeep Sangwan, Devender Parsad (International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019).

[18] (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.

[19] 17. H. Ning, H. Liu, and L. T. Yang, “Cyber entity security in the internet of things,” Computer, vol. 46, no. 4, pp. 46–53, 2013.

[20] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV. https: //doi.org/10.1145/2834050.2834095.

[21] Sunilkumar Malge, Pallavi SinghInternational Journal of Trend in Scientific Research and Development (IJTSRD) @ www.ijtsrd.com eISSN: 2456-6470.

[22] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R., "Proposed embedded security framework for internet of things (iot)", In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1-5, 2011.

[23] MAJun-chun,WANGYong-jun,SUNJi-yin,andCHENShan.2011.A minimum cost of network hardening model based on attack graphs. Procedia Engineering 15 (2011), 3227–3233.

[24] Steven Noel, Sushil Jajodia, Brian O'Berry, and Michael Jacobs. 2003. Efficient minimum-cost network hardening via exploit dependency graphs. In 19th Annual Computer Security Applications Conference, 2003. Proceedings. IEEE, 86–95.

[25] Tania Islam and Lingyu Wang. 2008. A heuristic approach to minimum-cost network hardening using attack graph. In 2008 New Technologies, Mobility and Security. IEEE, 1–5.

[26] M Abadi and S Jalili. 2006. An ant colony optimization algorithm for network vulnerability analysis. Iranian Journal of Electrical and Electronic Engineering 2, 3 (2006), 106–120.

[27] Polad et al. HadarPolad,RamiPuzis,andBrachaShapira.2017. Attack graph obfuscation. In International Conference on Cyber Security Cryptography and Machine Learning. Springer, 269–287.

[28] Almohri et al. [3[[3] Hussain MJ Almohri, Layne T Watson, Danfeng Yao, and Xinming Ou. 2016. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. IEEE Transactions on Dependable and Secure Computing 13, 4 (2016), 474–487.

[29] Noel et al. [25[[25] Steven Noel and Sushil Jajodia. 2008. Optimal ids sensor placement and alert prioritization using attack graphs. Journal of Network and Systems Management 16, 3 (2008), 259–275.

[30] Deployment Optimization of IoT Devices through Attack Graph Analysis WiSec '19, May 15–17, 2019, Miami, FL, USA.

[31] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[32] OWASP, "IoT Vulnerabilities Project," Article