ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse431032021.pdf
https://doi.org/10.30534/ijatcse/2021/431032021

A Review on the Security of the Internet of Things (IoT)

Hafiz MusabIqbal[1], Hashim Ali Khokhar[2],Usman Ahmed Raza[3]
[1] Department of Computer Science, Lahore Leads University, Lahore, Pakistan, musabiqbal301@gmail.com
[2] Department of Computer Science, Lahore Leads University, Lahore, Pakistan,hashim.khokhar1227@gmail.com
[3] Department of Computer Science, Lahore Leads University, Lahore, Pakistan, usmanahmedraza@gmail.com

ABSTRACT

Internet of things (IoT) is a wireless medium that facilitate to human for the communication over the internet via sensors to control their home appliance with their mobile phones, smart watches. It makes to easy human life. IoT used in human's daily life like homes, offices and hospitals etc. But the most important thing is data (in which include user's personal information like passwords or location etc.) security while data transmitted from one end to another end over the internet. The main focus of this paper is IoT related security and vulnerabilities that are caused the security and existing solutions and compare the existing study results to measure the issues.

Key words: Internet of Things, security, Review

1. INTRODUCTION

"Things" in the Internet of Things (IoT) comprises devices, apps, sensors, actuators and interfaces that capture and share data through the Internet. IoT devices have sensors and device capacities that can be used in many environments. The devices are fitted. Figure 1 provides several popular IoT implementations like smart homes, smart cities, health care, wearable, etc. The exponential increase in the amount of IoT devices used would hit 41 billion in 2020 with a demand of $8,9 trillion[40], as illustrated in the International Data Company survey of 2013. (IDC). It is the human position that distinguishes between IoT and the conventional network. The IoT devices will develop, evaluate and take action details on person behaviours [41]. IoT-based apps provide services that provide tremendous benefits to human lives, but they cost a great deal because of the privacy and protection of the user. It is an increasingly growing network that is going to transform people's lives and the next big advancement in internet technology. The simple idea of IoT is to connect embedded sensors or images every day to objects to make them intelligent objects. IoT's main elements include mobility, wireless networking, embedded sensors, a wide range of technical applications and support for various devices [42]. IoT represents the world's parent class on virtual and tangible objects and promotes knowledgeable network communication. The key features of IoT are sensing, access to information, diverse access to services, applications and protection and confidence [43].

Creating IoT in the previous century is one of the most important and striking activities. Technologies like WSN and RFID tags are evolving in the area of Internet technologies [44]. Both technologies create direct connectivity to the Internet. As a consequence, a dramatic amount of possible threats and hazards were rendered to the defence of an intelligent thing. These conditions of safety are not widely known and, without adequate protection, IoT devices can be utilized and attacked for malicious purposes with greater over the internet is more challenging nowadays that depends on a different cause. In this review paper, we will discuss the security in IoT, security threats and proposed different solutions. Figure 1 shows the applications internet of things.

risk [19]. There is therefore an important understanding of security threats and security solutions.

In simple words, we can say that the security of the exchanged data is most important in IoT. Secure transmission

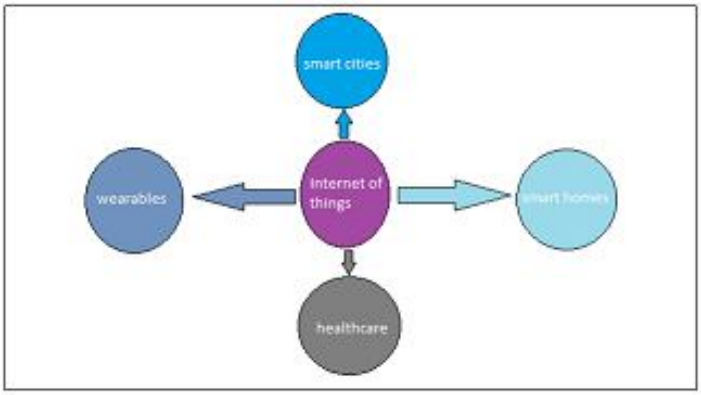

Figure 1: applications of internet of things

2. DISCUSSION

2.1 Security in the IoT

Increasing IoT defences have been built into a set of concerns that must be easily addressed as a consequence of vulnerabilities. Researchers also found core weak points in a broad variety of IoT-baby displays that hackers may use for various malicious activities, such as tracking live data, adjusting camera settings and enabling other users to access and exploiting the monitor on the remote[1]. Another example is a gang of hackers who have built an energy system in part of Ukraine for cyber attacks. Further avenues to target critical infrastructure, such as power grids, hydropower projects, chemical factories, and more frequently, are being pursued at the outset [2].

With a poor login, there is always a huge problem. You have to take note of your password. After a fixed period a security check and password reset are really important, otherwise, the login credentials and access to user accounts will be invented easily. Fixed firmware is the next vulnerability. Call to reprogram or update applications or boost protection vulnerabilities. However, firmware acknowledges no interactive upgrades. An unsecured malicious device is indeed a disaster possibility. The attackers are intentionally taking advantage of this flaw. Routers and consoles are highly prone to attacks. The blame is the Wi-Fi network not insured. A home network is also not secure as a person does not take care to protect his or her wireless network. If the authorization mechanism is not grasped the network will be exposed to everyone in the Wi-Fi area and data transfer snoops [3], [4], [5] will be hit.

It is essential to consider the attributes that determine protection when determining what a stable IoT is. In the standard IoT program, the securities specifications to be considered are grouped into four main categories: (i) confidentiality, (ii) integrity, (iii) authentication, and (iv) availability. Table 1 compares these four categories.

2.1.1 **Confidentiality**: The privacy and independence of user identity and international intervention is connected to the new realm of anonymity. Unauthorized access to confidential data across various mechanisms[7] is usually impacted by privacy deficiency. In comparison, the unauthorized disclosure of the information is always a secrecy denial[7]. Protection threats The risk of privacy for IoT-oriented computers includes the transfer of classified information to adjacent users or the transmitting of details to unlicensed users[8]. Each device and sensor in the IoT network may entail a potential secrecy danger. Because of any unreliable security or backdoor entry schemes, many network users are potentially susceptible to their protection [9].

2.1.2 **Integrity**: To preserve data credibility and validity, Data Honesty refers to the protection of sensitive information and errors by transmission or receipt (by cybercriminals). Malignant customers can change this when content is in the newspapers[9]. Serious errors caused by canal imperfection, electromagnetic interference and instrumental constraints will also alter the information passed. Only if the approved consumer has access to the data utilizing the secure interface[11] will data protection be retained on IoT devices.

2.1.3 **Availability**: Data access means all authorized customers have immediate access to computer resources. One of the key priorities of IoT resources is to include data whenever possible in the routine as well as in crises [10]. Since IoT services are often used by large businesses, the immediate availability of data is one of IoT service providers' main priorities. The biggest obstacle for IoT networking is the denial of service assault and the probability of bottlenecks that can hinder information delivery and deprive end-users of data [12].

2.1.4 **Authenticity**: Authenticity stands for the availability of network access to only legitimate customers. Authentication threats apply to improvements in tracking and sensing data used for improper storage of confidential data. It cannot just be viewed by the non-authenticated person, it may change or erase data and thus impact data integrity [6]. IoT presents authentication dangers, mostly due to the ineffectiveness of the authentication, tag duplication, spoofing and RFID operation. A denial of user access and the leakage of sensitive info, flooding of the networks and more would undermine the whole network in addition to this technical breach of authentication [9].

2.2 IoT Security Threats

Recently, some academics have proposed classifying risks to the edge of computation [13], and some academics have grouped them into a few facets of the IoT. In keeping with the diversity of IoT[14], for example, IoT defence risks are broken into two groups. Classification of heterogeneity and interoperability[15],[16]. These scientists have extensively classified certain basic IoT problems, but certain attributes or technological classifications are unique and not universal. The main aim is to identify IoT protection threats more effectively and clearly so that IoT protection models and strategies are aware.

2.2.1 **Node Replication**: A node sensor identification is copied to the same network as a new sensor, which misdirects the packets, receives the wrong sensor readings, or disconnects the network, disturbing the performance of a sensor network [18].

2.2.2 **Tag Cloning**: The latest one removes the initial tag and copies the new tag ID. In the absence of physical security for the RFID tags (Radio Frequency Identification), the attacker will overwrite the initial one quickly [18].

2.2.3 **Tag Spoofing**: The tags of two distinct products would be replaced by a similar attack. The high price tag in grocery stores is supplemented by a low price tag, to buy the products for a reduced price. [18] [19].

2.2.4 **Eavesdropping**: Refer to the on-going communication process, which represents an initial step in starting the other attacks. These assaults on unsecured wireless networks are simpler to conduct as contact is carried out in a secure accessible wireless channel [20].

2.2.5 **Jumping**: The interaction with wireless equipment is a weakening of the IoT network, which results in the breakdown or impredecible enforcement of the system by transmitting radio frequency signals without implementing a certain protocol [21].

2.2.6 **Insecure Software**: Different flaws in IoT involve vulnerable software/firmware [21]. This will contribute to other concerns such as the injection of Malicious Code, in which a malicious code is inserted into the system to rob some type of user data.

2.2.7 **Sinkhole Attack**: This attack renders the compromised node appealing to the neighbouring nodes when the adversary transforms all data flow from every other node to the impacted node that contributes to packets falling, i.e. all communication silences, whilst the machine is foiled to assume that the data is obtained on the other hand. This attack makes the compromised node enticing. This assault also contributes to the further use of resources that may contribute to a DoS attack [22].

2.2.8 **Daniel of Services Attack**: DoS seeks inaccessible IoT devices [19] by disruption of operation to its planned customers. This assault is close to one in the middleware layer where the availability of the program may be destroyed by attackers [23].

2.2.9 **Keystroke Timing Attack**: The keystrokes are a hardware time-related assault. If a keystroke occurs, an interrupt handler is performed. An aggressor's program will detect keystrokes through computing timings by never reading keyboard buffers or any tale. And this attack has been mounted in languages including Javascript.

Click fake button interrupts are used to remedy this problem.[27] A fake keyboard press cannot be differentiated by a fake push interrupt. The solution will however not protect those accidents (e.g., key handlers).

2.3 IoT Security Solutions

2.3.1 **Protected Grouping**: WSN consists of a vast number of compact automated lightweight nodes. Sensor nodes are needed to bind the nodes together. It is vital that considering the possibility of using general defence, participants will communicate with each other securely when conducting a particular task. Solutions, where members in static communities are guarded by stronger nodes, are exempted [24].

2.3.2 **Secure Data Aggregation**: A variety of threats from denial of service attacks appear to vulnerably result in sensor networks and data aggregation techniques. Data flow is the most critical issue in the networks since data flows are growing. To minimize operating costs and network load, the sensor nodes incorporate measurements before they are submitted to the base station. This kind of knowledge appeals to an assailant [25]. If a competitor owns an aggregating node and decides to disregard the report or create a fake report, the creditability of produced results would be compromised. This needs an understanding of the network as a whole. The key objective in this sector is to use resilient functions to uncover and disclose forged reports by demonstrating the genuineness of data. However, improvement in this field, such as the amount of data provided by interactive algorithms, may still be needed [26], [24].

2.3.3 **Encryption**: Encryption can be used to authenticate digital signature terminals via encrypted hash algorithms. [19] Furthermore, symmetrical and asymmetry-encoded algorithms such as RSA, DSA, BLOWFISH, and DES are used to prevent unwanted access to terminal information. Common knowledge with the encryption algorithm protects information from being split, dropped or replayed.[23]

2.3.4 **Authentication**: The method of authentication restricts entry through integrated identification to unauthorized users. Certain cooperating resources authenticate and consumers may pick the corresponding details to be exchanged. The biggest obstacle in these two levels for securities nevertheless is the implementation of modern methods in mass usage (e.g. cloud and virtualization) [23]. The cloud infrastructure will potentially be influenced and the insider's threat is one of the worse challenges. Similarly, DOS and data theft, etc. was exposed to virtualization. Much study is important for a stable atmosphere in both fields.

2.3.5 **Google Native Client**: As much of the functionality has now been published in binary format, JavaScript does not always support rewriting and running in the browser sandbox. Google's Native Client [28] is a curious way to treat binary code without trust. It means the CPU is operating a binary code, but the code will be checked and modified until it is executed. Various directives are not allowed and are considered dangerous. Furthermore, jumps are limited to specified addresses and such jumps are modified to ensure that they do not leap. Without these constraints, binary programming cannot be achieved at all. This technique lets the sandbox disable the most unpredictable controls. A thorough study has not yet been carried out of the meltdown and continuum attacks.

2.3.6 **Physical Security**: Physical security from plugging in contaminated USB sticks for IoT users, e.g. those with USB [29]. To enhance physical stability, monitoring and debugging methods should be removed and hardware-dependent frameworks such as Trustworthy Platform Modules (TPMs) should be included [30].

2.3.7 **Data Security**: Several encryption technologies guarantee electronic protection to avoid risks of computer theft. Besides, firewalls to deter more harmful activity by wrongful users [31] are added to avoid such malicious activities. Table 1 shows the comparison of the security tiers.

Table 1, Compare the security solutions in IOT (C = Confidentiality, I = Integrity, AV = Availability, A = Authenticity)

Reference	Methods for achieving security	Security Requirements			
		C	I	AV	A
[42]	ICMetric (cryptographic keys) coupled with SRRP	✓	✓	✓	✓
[43]	ICMetric (cryptographic keys)	✓	✓	✓	✓
[44]	ICMetric (cryptographic keys)	✓	✓	✓	✓
[30]	Dynamic IoT security based on the principles of the immune system	×	×	×	×
[31]	Key management, watermarking	×	×	×	✓
[32]	Nano-electronic security primitives	✓	×	✓	✓
[33]	ECC cryptography	✓	✓	✓	✓
[34]	DTLS handshake and RSA keys	✓	✓	✓	✓
[35]	AES and ECC hybrid encryption algorithm	✓	✓	×	✓

3. CONCLUSION

In this review, we presented the security issues of IoT and their appropriate solutions. And compared the security tier of the IoT by different reference and find the results. We analyse in this review that are the different types of security in IoT and the security is the main concern for everybody while transmitted data. In order to secure such classified material, the latest wave of intelligent devices could be incorporated into constructive approaches. The Artificial Intelligence-built devices would surely improve intelligence to help manage with security issues.

ACKNOWLEDGMENT

We warmly thank full to our faculty member M. Usman Ahmed Raza who had motivated us and helped us withthis work.

REFERENCES

[1] "Why IoT Security Is So Critical?," [Online]. Available: https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical.

[2] "How the Internet of Things will affect security & privacy." [Online]. Available: http://www.businessinsider.com/internet-of-things-securityprivacy-2016-8.

[3] E. Zeng, S. Mare, and F. Roesner, "End User Security & Privacy Concerns with Smart Homes," in *Symposium on Usable Privacy and Security (SOUPS*, 2017, pp. 1–16.

[4] J. Bugeja, A. Jacobsson, and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," *IEEE DOI*, vol. 10, no. 1109, pp. 172–174, 2016.

[5] H. Lin and I. NeilW. Bergmann, "Privacy and Security Challenges for Smart Home Environments, Information (2016)," *p*, pp. 1–15, doi: 10.3390/info7030044.

[6] R. H. Weber, *Internet of Things---New Security and Privacy Challenges*. Amsterdam, The Netherlands: Elsevier, 2010.

[7] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[8] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of things(IoT)," *Int.J.Comput.Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[9] D. Kozlov, J. Veijalainen, and Y. Ali, """Security and privacy threats in IoT architectures,"' inProc.7th," *Int.Conf.BodyAreaNetw pp*, vol. 7, pp. 256–262, 2012.

[10] H. Suoa, J. Wana, C. Zoua, and J. Liua, """Security in the Internet of Things: A review,""" 2012, pp. 648–651.

[11] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, *'"Proposed security model and threat taxonomy for the Internet of Things (IoT),"' in Recent Trends in Network Security and Applications*. Berlin, Germany: Springer-Verlag, 2010.

[12] M. Alrowaily and Z. Lu, ""Secure edge computing in iot systems: Review and case studies," in *" in 2018 IEEE/ACM Symposium on Edge Computing (SEC)*, 2018, pp. 440–444.

[13] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "'Network intrusion detection for iot security based on learning techniques,'" *IEEE Commun. Surv. Tutorials*, 2019.

[14] J. Granjal, E. Monteiro, and J. S. Silva, "'Security for the internet of things: a survey of existing protocols and open research issues,' IEEE Communications Surveys & Tutorials, vol. 17, no. 3," *p*, vol. 17, no. 3, pp. 1294–1312, 2015.

[15] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "'Internet of things: A survey on enabling technologies, protocols, and applications,'" *IEEE Commun. Surv. tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[16] Jihad Dazine and A. Maizate*, "'Internet of Things Security,'" *IEEE*, 2018.

[17] K. Raju and V. Bapauji, "'Internet of Things (IoT): Security and privacy threats.,'" *IEEE Int. Conf. Robot Autom, 2016*, vol. 26, p. 2018, 2018, [Online]. Available: https://www.researchgate.net/publication/305302451.

[18] M. Husamuddin and M. Qayyu, "'Internet of Things: A study on Security and Privacy Threats.,'" *Second Int. Conf. Anti-Cyber Crimes (ICACC), 2017*, 2018, [Online]. Available: https://ieeexplore.ieee.org/document/7905270.

[19] E. A. I. Yaqoob, A. I. A. A. M. H. Rehman, and M. A. A.-garadi, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Networks 129*, pp. 444–458, 2017.

[20] K. S. M. A. Khan, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, pp. 395–411, 2017.

[21] M. U. Farooq, A. K. M. Waseem, and A. S. Mazhar, "Critical Analysis on the Security Concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, pp. 1–6, 2015.

[22] W. Zhang, *Security Architecture of the Internet of Things Oriented to Perceptual Layer*. IEEE, 2013.

[23] W. Al Shehri, "'A survey on Security in Wireless Sensor Networks.,'" *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 1, pp. 25–32, Mar. 2017, [Online]. Available: http://aircconline.com/ijnsa/V9N1/9117ijnsa03.pdf.

[24] M. Saraogi, "Security In Wireless Sensor Networks," *p*, vol. 26, no. 2018, pp. 1–12, Mar. 2018, doi: 10.1.1.105.5923.

[25] K. Sharma, M. K. Ghose, D. Kumar, R. P. K. Singh, and V. K. Pandey, "'A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks,'" *Int. J. Adv. Sci. Technol.*, vol. 26, no. 2018, pp. 31–44, Mar. 2010, [Online]. Available:

http://modul.repo.mercubuanayogya.ac.id/modul/files/openjournal/JournalOfDesign/4_263.pdf.

[26] M. Schwarz *et al.*, *KeyDrown: Eliminating Keystroke Timing SideChannel Attacks*. San Diego, CA, USA: Network and Distributed System Security Symposium, 2018.

[27] B. Yee *et al.*, "Native Client: A Sandbox for Portable Untrusted x86 Native Code," 2009.

[28] A. F. Mohammed, "Security Issues in IoT , IJSRSET," *IJSRSET*, pp. 933–940, 2017.

[29] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2017.

[30] C. Liu, Y. Zhang, and "a H. Zhang, "Novel Approach to IoT Security Based on Immunology"," Dec. 2013.

[31] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, 2011.

[32] G. S. Rose, "Security meets nanoelectronics for Internet of things applications," 2016, pp. 181–183.

[33] G. L. dos Santos, V. T. Guimarães, G. da Cunha Rodrigues, L. Z. Granville, and L. M. R. Tarouco, "A DTLS-based security architecture for the Internet of Things," 2015, pp. 809–815.

[34] T. Kothmayr, C. Schmitt, W. Hu, M. Br¨unig, and " G. Carle, "DLTS based security and two-way authentication for the Internet of Things,"," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[35] M. Xin, "A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System," 2015, pp. 62–65.

[36] I. Analytics, "*Why the internet of things is called internet of things: Definition*. disambiguation,": history, 2014.

[37] I. Saif, S. Peasley, and A. Perinkolam, "*Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age,.*" 2015.

[38] A. V Dastjerdi and R. Buyya, "'"Fog computing: Helping the Internet of Things realize its potential,"'" *Computer (Long. Beach. Calif).*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[39] ''IoT privacy H. LinandN. W. Bergmann, "'"IoT privacy and security challenges forsmart home environments,"'" *Information*, vol. 7, no. 3, p. 44, 2016.

[40] A. Mosenia and N. K. Jha, "'A comprehensive study of Internet of Things.,'" *Emerg. Top. Comput.*, vol. 26, no. 2018, pp. 586–602, Mar. , [Online]. Available: https://ieeexplore.ieee.org/document/7562568.

[41] M. Husamuddin and M. Qayyu, "'Internet of Things: A study on Security and Privacy Threats.,'" *Second Int. Conf. Anti-Cyber Crimes (ICACC), 2017*, vol. 26, Mar. 2018, [Online]. Available: https://ieeexplore.ieee.org/document/7905270.

[42] R. Tahir, H. Tahir, K. McDonald-Maier, and A. Fernando, "A novel ICMetric based framework for securing the Internet of Things," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 2016, pp. 469–470.

[43] A. B. T. Hopkins, K. D. McDonald-Maier, E. Papoutsis, and W. G. J. Howells, "'Ensuring data integrity via ICmetrics based security infrastructure,'" in *Conference on Adaptive Hardware and Systems*, 2007, pp. 75–81.

[44] Y. Kovalchuk and G. Howells, "'Overview of ICmetrics Technology – Security Infrastructure for Autonomous and Intelligent Healthcare System,'" *Int. J. u- e-Service Sci. Technol.*, vol. 4, no. 3, pp. 49–60, 2011.

[45] AzlizaYacob ,ZirawaniBaharum , NurSukinah Aziz, Noor SuhanaSulaiman and Wan Mohd Amir Fazamin Wan Hamzah, "A Review of Internet of Things (IoT): Implementations and Challenges", International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3), 2020, 373 - 376