ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

SECURITY REQUIREMENTS AND CHALLENGES IN INTERNET OF THINGS (IOT)

Amanpreet Kaur

Assistant Professor, Amritsar Law College, Amritsar, aman_batala15@yahoo.in

ABSTRACT

Industry 4.0, smart cities, and smart homes are just a few examples of how the Internet has expanded beyond the virtual realm in the previous twenty years. Increased energy efficiency, streamlined and automated procedures, and improved comfort are just a few of the numerous advantages brought to consumers by the Internet of Things (IoT), but it also raises new privacy and security issues. The proliferation of Internet-enabled gadgets opens up interesting possibilities for technological progress. The manufacturing and widespread integration of Internet of Things (IoT) items into daily life raises new security concerns. In order to facilitate data analytics on other devices, sensors will gather private and public information in unprecedented quantities and communicate it across a wireless channel that can be readily monitored(1). More and more gadgets are being made, but many of them skimp on security to be "first to market." In addition, the protocols upon which modern security methods rely were developed with higher-powered, more feature-rich devices in mind, such as desktop computers and cellular phones. Many of the security issues plaguing the Internet of Things currently have no good answers due to the relative youth of the underlying technologies. Security measures tailored to the evolving Internet of Things (IoT) are essential for ensuring that users' information remains private and safe(2). This article describes some of the most pressing issues with the Internet of Things and ranks their relative importance to assist pinpoint areas of weakness that need to be addressed. Solutions that are specific to the limitations of the IoT are provided with a focus on these critical issues. To better manage the disparate nature of IoT infrastructure, a framework based on security features is designed to categorize devices into distinct groups. To demonstrate the viability of IoT devices and networks, a unique physical device authentication approach is given. As outlined in the aforementioned framework, further low-power approaches are developed and assessed to determine the many security options accessible to IoT devices.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

Keywords: Security, IoT, Industry4.0, Smart Cities, Network, Sensor

INTRODUCTION

The prevalence of Internet of Things (IoT) devices is increasing, and analysts predict that by 2020, there will be more than 50 billion of them. As technology in electronics and communications improves, more and more little devices may be placed in inaccessible areas to gather data in real time for an expanding range of uses. The proliferation of these IoT devices will make it possible to gather and analyse vast quantities of data, which can then be used to improve efficiency and cut down on waste across a variety of sectors, including the consumer, industrial, personal, health, transportation, and environmental sectors(3). As a result of the Internet's potential, industries that did not previously depend on it are rushing to be early adopters of new technology, and security may be an afterthought.

Concerns have been raised in several of these industries about the competency of the developers building and producing gadgets that might leave them vulnerable to a wide variety of assaults that have never been seen before. Unfortunately, until adequate solutions are developed, many of these gadgets will be vulnerable to assaults since they lack the necessary hardware to implement existing security measures. There is a persistent and growing danger that assaults on Internet of Things devices and networks may occur. Because even a single hacked node may wreak havoc on a network, current Internet security solutions on computers and mobile devices are still unable to keep up with the volume of threats they face every day. As the Internet of Things (IoT) expands, the number of connected devices and, by extension, the number of potential security holes, will increase substantially(4). Devices of this kind will have access to and disclose sensitive information on individuals, cars, and vital infrastructure at ever-increasing rates, posing a greater danger to the security of our nation's industrial infrastructure. Overall, security design advancements have lagged behind IoT's technology breakthroughs; this dissertation aims to assist bridge that gap by offering IoT security solutions for low-powered gadgets.

DEFINITION OF SECURITY

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved,** UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

When it comes to consumer development and implementation, security by its own definition is a strategy that guarantees safety. This raises the question of how security considerations always apply in the development and debugging process in the case of many contemporary hardware applications and IoT designs. Learning to access product and other development needs can introduce security standards. Wireless sensor networks (WSN) have evolved in recent decades as a technology applicable to a variety of disciplines from interesting research fields (e.g., industrial monitoring in complex infrastructure)(5). Progress in cyber security for wireless communications has also resulted in notable enhancements, Such as improved iterations of public key authentication technology and rigorous self-healing procedures. However, the interaction between security standards, application functionality and scope and network security is often overlooked or overlooked in sensor network protection. However, the protective mechanisms employed to safeguard the network are heavily influenced by the unique application's interpretation and requirements. In addition, new WSN standards are being developed, but some security challenges are being ignored, as these guidelines focus primarily on maintaining connectivity between networks. There are two objectives of this component. Our first goal is to provide an overview of the interaction between conditions, frameworks, and validation methods(6).Then, we'll go into detail on how different hardware, software, and network designs affect the detection and incorporation of security features. In the end, we will present a summary of the current status of sensor cybersecurity approaches, including an analysis of the security models in use and the primary obstacles that must be overcome. For our own final ease of use, we plan to specify the existing network system requirements, including the data encryption protocols in place. In addition, we will provide a summary of these diverse needs, with an emphasis on their security features.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

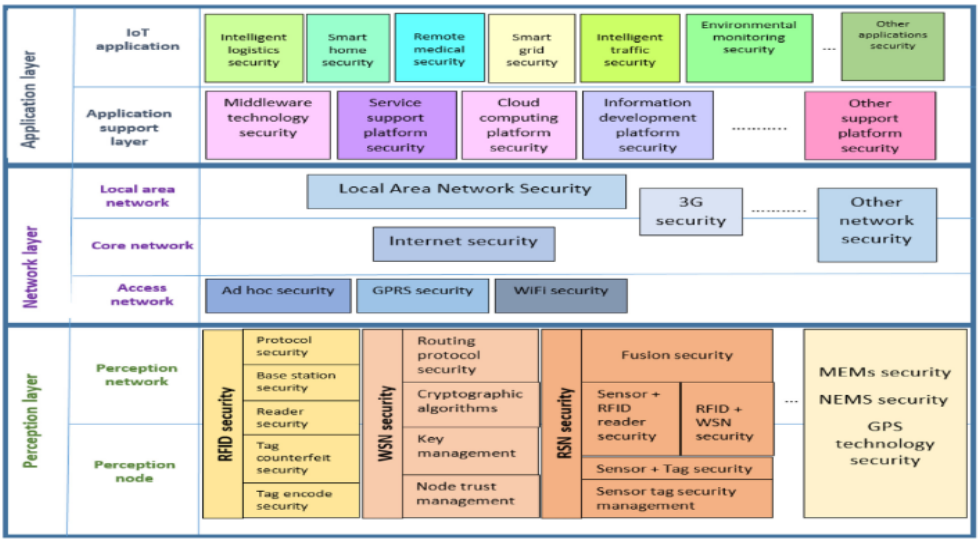

Fig. 1. Typical IoT security architecture.

Security Issues, challenges and considerations

Because of the ever-increasing prevalence of computing devices, IoT has gained tremendous momentum in recent times. Still, security is a major concern for the Internet of Things, the top topic asked by many potential investors, and a major roadblock to widespread adoption. Some of the most pressing problems that must be solved before widespread adoption of IoT may occur are then identified(7). When it comes to the Internet of Things (IoT), trust and security aspects are vital, and they in turn depend on the presence of certain safeguards. Security in the Internet of Things (IoT) refers primarily to protecting sensitive data and digitally-enabled devices, such as smartphones. Software and sensor network technologies used in device communications, smart device solutions and mobile technologyare the primary determinants of the Internet of Things. Inadequate security measures and poor encryption practises must now be considered once again from the outset of the design phase in order to ensure the complete and total safety of all components, including individual computers and whole networks. The proliferation of sophisticated new systems across a wide range of locations and technologies is a result of the IoT ecosystem.(8) As the number of interconnected smart devices continues to expand, so too does the scope of the system-wide security issues that must be addressed. In addition, application architecture (for example, limited power or widespread adoption of smart devices) can cause

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

unpredictability and scalability issues, meaning that IoT advances will never be used explicitly if they rely on traditional protective frameworks. The survival and security of these devices may be jeopardised by a wide range of challenges, both anticipated and unexpected; as a result, device adaptability will be of paramount importance.

Fig 2. Some of the security challenges in IoT devices.

The risk of being "recognised" is equivalent to the risk of associating a specific individual with specific information about that person, such as an email address and a username or a nick name. The risk arises when an individual's identity is tied to a level of anonymity, which compromises their privacy and exposes them to further threats(9). Analyzing and keeping tabs on individuals, for instance, or gathering data from a variety of sources. There is a recent emphasis on the risk of categorization in the pattern recognition stage of downstream facilities, where massive amounts of data are collected in one place regardless of their location or relevance to the issue.`

SOLUTIONS TO SECURITY OF IOT

DEVELOP A SECURITY MINDSET

To construct secure Internet of Things applications inside the framework, developers must adopt practises similar to those already in place. Companies nowadays are turning to the sensor network industry because of the risks associated with adopting security capabilities. They are now an additional outlay of money. However, the subsequent worries after a data breach are even more harmful(10). To succeed as a commercial-level technical executive, you need to make cultivating

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

a positive attitude and a sense of belonging in the workplace a priority from the very beginning. A return to normalcy in certain metrics is facilitated by the possession of a healthy mental attitude. It is essential to put in the time and effort required to find and hire competent IT professionals and provide them with the necessary tools.

ENCYPTION TECHNOLOGY

Sensor networks' potential value stems on the context in which information may actually be usefully relayed. Many new bugs appear at once. There has to be a smooth transfer of data from the authorising computer to the web, the database, and the computers and equipment that will be using the data. This paper shows how a resort's fish tank thermometer was used to get access to the personal information of resort guests, illustrating the misuse of IoT apps and connected channels(11). Using password authentication to secure servers and databases is a good first line of defence against attacks like this. Despite the fact that there are already a plethora of businesses creating accessible authentication software. You may use freely available encryption software without first verifying its functionality, which is convenient. Information security professionals from across the world work together to create and test this software, making it a powerful resource for keeping sensitive data safe.

BUILDING SECURITY IN IOT DEVELOPMENT

Since 21.4 million smart speakers are expected to be in use by 2020, this is a major issue. At least 20% of US internet users have conducted a search with google assistant, and 22% of US users have completed a purchase with the associated Digital app, thus this trend is only expected to grow(13). Since then, many creators of IoT systems have forgone providing any kind of security in favour of getting their products to market as quickly as possible. However, security is becoming becoming more of a concern as customers become more wary of how businesses will treat their personal information. The implementation of the General Data Protection Regulation (GDPR) is one of the most important events affecting businesses and still affecting people today. Companies who fail to add security to their IoT applications might expect a backlash from their customers in the near future(14). While many are unaddressed, fortunately, a wide range of potential answers exists. It is preferable to avoid the risk of technical liability and instead see protection as an inherent

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

part of the manufacturing process that makes implementing any future upgrades very challenging. Because of the IoT's physical components, real-world damage might theoretically be done. Threats to public infrastructure exist alongside those to individual privacy.

HARDWARE IS KEY

Although some of the required tools may be in place now, the previous safety practises can't be maintained indefinitely. In fact, IoT systems aren't even managed by individual users. All government infrastructure and large pieces of machinery are funded by the public via companies. Currently, businesses and individuals may protect their digital information by using VPN technology, but the complexity and varied nature of IoT objects provide challenges that VPN cannot solve on its own(15). This is because regular technological updates aren't feasible, unlike with electronic equipment, and the design was made with future generations in mind for the realm of the general public and major market items. Each fix will be traceable thanks to the embedded processors used to bolster the applications' security. However, processors will give even more security than bespoke software programmes would, as programmers will create applications that are impossible to crack using publicly available versions. In addition to improving the level of encryption the processors would provide, providing a unique identification to each processor that is placed in a given system makes the latter more secure and transparent(16). By working together via the authentication framework, your IoT computer will be protected from its CPU all the way to its server.

ORGANIZING IOT DEVICES' PROTECTION DEVELOPMENT CYCLE

Perform the process of developing security devices across the computer and the connected network, while also reducing the danger layer that has been commonly disregarded, necessitates a comprehensive but deep cyber security strategy. Security is an integral part of the Internet of Things (IoT) ecosystem that will speed up the iteration cycle of IoT applications:

- Repurposing existing appliances and purchasing new ones
- Implementing cutting-edge items in the infrastructure,
- Making steady enhancements to apps,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

- Passing controlled main authorizations,
- Data-intensive system foundations.

CONCLUSION

The IoT is a cutting-edge technology that has advanced significantly in terms of software efficiency. The Internet of Things provides several benefits for everyone involved, including businesses, experts, and consumers. How security for IoT systems will be enforced has been a major topic of discussion, with viable approaches to the problem receiving a lot of attention. Companies must now strike a balance between increasing the reliability of the Internet of Things and speeding up the distribution of goods that use the IoT throughout the market. Increased contextual use of Sensor networks makes it impossible to ignore security concerns. Although access control implementation adds time and money to the time it takes to bring a product to market, the value of the information it protects is well worth the effort. Tech firms need to adopt a new way of thinking and finding motivation to create additional security measures to seal the gap between their own company's data and the government's. The ability to combine digital and analogue operations has been made possible by several recent frameworks and methods. Share electronic sensors to work together for secure data. However, the procedure may be made faster, more effective, and less risky in the face of security threats if the client just offers a required material at the necessary time and rejects the remainder of the data.

REFERENCES

[1] L. Columbus, “Roundup of internet of things forecasts and market estimates, 2016”, Forbes, 2016, https : / / www . forbes . com / sites / louiscolumbus / 2016 / 11 / 27 / roundup - of - internet - of - things - forecasts - and - market - estimates-2016/#2b7dc31292d5.

[2] L. Dignan, “Iot devices to generate 79.4zb of data in 2025, says idc”, ZDnet, 2019,

https://www.zdnet.com/article/iot- devices- to- generate- 79- 4zb-of-data-in-2025-says-idc.

[3] J. R. Anna Gerber, Connecting all the things in the internet of things, https : / /developer.ibm.com/technologies/iot/articles/iot-lp101-connectivity-network-protocols/, 2020.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved,** UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

[4] Internet of things world forum (iotwf) leaders announce new iot reference model and iotwf talent consortium, https://telecomreseller.com/2014/10/14/internet-of-things-world- forum-iotwf-leaders-announce-new-iot-reference-model-and-iotwf-talent-consortium/.

[5] S. Farahani, "Chapter 3 - zigbee and ieee 802.15.4 protocol layers", in ZigBee Wireless Networks and Transceivers, S. Farahani, Ed., Burlington: Newnes, 2008, pp. 33 –135, ISBN: 978-0-7506-8393-7. DOI: https://doi.org/10.1016/B978- 0- 7506- 8393- 7.00003- 0. [Online]. Available:http://www.sciencedirect.com/science/article/pii/B9780750683937000030.

[6] C.Xie, and S.T. Deng, Research and Application of Security and Privacy in Industrial Internet of Things Based on Fingerprint Encryption, ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 102-110, 2017.

[7] M.Suresh, M. Neema, Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Procedia Technology, Vol. 25, pp. 248-255, 2016.

[8] T.Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, DTLS based security and two-way authentication for the Internet of Things, Ad Hoc Networks, Vol. 11, Issue 8, pp. 2710-2723, 2013.

[9] A.Darwish, M.M. El-Gendy and A.E. Hassanien, A New Hybrid Cryptosystem for Internet of Things Applications, Multimedia Forensics and Security, pp. 365-380, 2017.

[10] Ritambhara, A. Gupta, M. Jaiswal, An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT), International Conference on Computing, Communication and Automation (ICCCA), pp. 422 - 427, 2017.

[11] G.S.Arias, C.G. Garcia, and B.C. Pelayo G-Bustelo, Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things, Future Generation Computer Systems, Vol. 74, pp. 444-466, 2017.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

[12] I.Hussain, M.C. Negi; N. Pandey, A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer, International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 464-470, 2017.

[13] X.Jia, D. He, Q. Liu, K.K.R. Choo, An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment, Ad Hoc Networks, Vol. 71, pp. 78-87, 2018.

[14] M.L.Das, Strong Security and Privacy of RFID System for Internet of Things Infrastructure, International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2013: Security, Privacy, and Applied Cryptography Engineering, pp. 56-69, 2013.

[15] S.Sasirekha, S. Swamynathan, S. Suganya, An ECC-Based Algorithm to Handle Secure Communication Between Heterogeneous IoT Devices, Advances in Electronics, Communication and Computing, pp. 351-362, 2017.

[16] S.Perez, D. Rotondi, D. Pedone, L. Straniero, M.J. Nunez, F. Gigante, Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts, International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2017: Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 917-926, 2017.

[17] M.Beltran, Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things, Computers & Security, Vol. 77, pp. 595-611, 2018

[18] K.H. Wang, C.M. Chen, W. Fang, T.Y. Wu, A secure authentication scheme for Internet of Things, Pervasive and Mobile Computing, Vol. 42, pp. 15-26, 2017.

[19] M.S. Farash, M. Turkanovic, S. Kumari, M. Holbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks, Vol. 36, Part 1, pp. 152-176, 2016.

[20] Z. Mahmood, A. Ullah, H. Ning, Distributed Multiparty Key Management for Efficient

Authentication in the Internet of Things, IEEE, Vol. 6, pp. 29460-29473, 2018.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Oct 2022

[21] R.H. Weber, Internet of things: Privacy issues revisited, Computer Law & Security Review, Vol. 31, Issue 5, pp. 618-627, 2015.