A systematic review on Internet of Things

John A, Assistant Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

In the IOT, ordinary items may have identifying capabilities and can communicate with one another over the internet. IoT application domains extend all the way from smart homes, smart cities, wearables, and e-health to many more use cases. As a result, the trillions of devices that will be linked will be tens and possibly hundreds of billions. In the future, there will be smart gadgets that will gather data, process it, and make choices on their own. Security is essential under these situations, and particularly with regard to authentication, since there is a danger that a rogue device may do harm in an IoT system if it is not properly authorised. This article presents a thorough treatment of the IoT security topic, including present and recently developed technology. This device is able to review a number of authentication procedures presented in the literature, which gives you a sense of the size of that research topic. This is an excellent opportunity for academics and developers to tackle the realm of authentication methods by using a multi-criteria categorization we had previously developed.

KEYWORDS: IOT, Security, IT.

Introduction

Increasingly, devices such as sensors and actuators are being linked to the Internet of Things (IoT), which results in a huge network of networks linking all of these types of devices. This kind of technological innovation is often used in many diverse sectors, including public health, smart grids, smart transportation, waste management, smart homes, cities, agriculture, and energy management.

At the same time, there are security challenges connected to ensuring IoT networks cannot be compromised while not permitting their use as an attack vector (e.g., Mirai botnet [5,6]). The issues that exist due to resource constraints and IoT devices are “heightened” due to IoT's communication and security protocols being inefficient and practically infeasible with IoT. The Internet of Things-related security problems are becoming increasingly concerning due to the increasing ubiquity of IoT devices, as well as their usage in important applications, which make security breaches potentially lethal. A risk may be estimated by analysing a flaw revealed in 2017 FDA recall of 500,000 pacemakers due to concerns that a hacker may leverage security flaws to take control of the heart-beat controlling gadget.

There are several different security standards which IoT networks will have to comply with, and it depends on the specific applications to which the network will be put. In order to have a secure IoT network, applications must adhere to certain confidentiality, integrity, and/or authentication standards. Moreover, authentication is critical for IoT, because of the importance of trusting the devices that are connected to the network. A single hacked node may create calamities [1].

One of the main problems with IoT devices is that they are unique, making existing authentication approaches completely infeasible. Cryptographic algorithms built for resource-limited IoT nodes are not appropriate for main-powered, high processor, and/or big memory devices. With the introduction of these methods, the lightweight authentication systems started to surface. Several of them are ideal for different contexts, such as the Internet of Things (IoT) or the Wireless Sensor Network (WSN) (which can be considered suitable for IoT).

This article provides a unified approach to the security issues and functional needs found in the IoT context. It summarises a number of various IoT authentication systems in an up-to-date survey. This study extends prior research by presenting and analysing the authentication techniques based on several factors, including benefits and drawbacks.

IoT

The IoT model seeks to link a range of diverse machine types in order to serve a wide number of applications (for example, identifying, locating, tracking, monitoring, and controlling). Applying a large number of heterogeneous computers leads to traffic which then requires that you deal with the issues associated with storing large amounts of data. This is why the TCP/IP architecture, which has been utilised for network connectivity for a long time, does not work for IoT applications because it lacks the requisite capabilities like security and privacy (such as information privacy, machine safety, data confidentiality, data encryption, and network security) [12].

Even if there are several IoT designs, it's still crucial that a reference architecture be built [14,15]. While the literature often uses a three-layer design as an example, Figure 1a illustrates an alternative implementation that follows the fundamental architectural model presented in the literature [13,16–18]. This comprises of: perceptual processing, network infrastructure, and app functionality

Security

When we said that using connected things in daily life is potentially life-threatening, we were speaking about security risks. Hackers may use smartness that's built into houses, automobiles, and power grids to launch damaging incidents. As the years have gone by, there have been a multitude of hacking scenarios and attacks offered to demonstrate the impact of a security breach, particularly with regard to the increased use of Internet of Things (IoT) applications containing private information (personal, industrial, governmental, etc.). There are three IoT security problems. They include authentication, authorisation, and integrity [19-21].

Conclusion

Several studies in the field investigated the possibilities for IoT authentication. In the current work, the authors have classified IoT authentication methods according to their respective use cases and based on four categories: IoS devices, IoE devices, M2M communication, and IoV vehicles (IoV). Information on authentication methods is presented in terms of the model, objectives, key processes, complexity of computing, and communication overhead. In , the authors discussed IoT authentication systems and their capabilities. In order to organise the information in two distinct ways, the authors came up with two classifications: one based on the distribution or centralization of authentication techniques, and the other based on the features of the authentication process. The authors in conducted an analytical assessment of the material that already existed. they discussed the concerns and difficulties of authentication in IoT and laid up a researchable way to study the current authentication schemes According to the authors of , there are many authentication techniques utilised in the IoT environment, including lightweight and mutual authentication techniques, with a focus on cross-platform authentication techniques that may be done without discrimination or comparison contains a comprehensive assessment of major and “recent” IoT authentication approaches, but without making any attempt to classify them. [22-25] was able to identify research papers focused on security and authentication approaches as well as develop a categorization system for them. The paper in documented the present state of the art of authentication in the IoT space, including the many obstacles and preferred authentication solutions while avoiding any direct comparisons. The authors of offered a summary of authentication techniques, and presented the results of comparing different authentication strategies in a literature review. Additionally, each technique was scrutinised according to the amount of resources it used (e.g., energy, memory, computation and communication).

References

1. Ahmad, M., Amin, M. B., Hussain, S., Kang, B. H., Cheong, T., & Lee, S. (2016). Health Fog: a novel framework for health and wellness applications. *Journal of Supercomputing*, *72*(10), 3677–3695. https://doi.org/10.1007/s11227-016-1634-x
2. Alam, F., Mehmood, R., Katib, I., & Albeshri, A. (2016). Analysis of Eight Data Mining Algorithms for Smarter Internet of Things (IoT). In S. E. (Ed.), *Procedia Computer Science* (Vol. 58, pp. 437–442). Elsevier B.V. https://doi.org/10.1016/j.procs.2016.09.068
3. Chiuchisan, I., Costin, H.-N., & Geman, O. (2014). Adopting the internet of things technologies in health care systems. In H. C.-G. Gavrilas M. Ivanov O. (Ed.), *EPE 2014 - Proceedings of the 2014 International Conference and Exposition on Electrical and Power Engineering* (pp. 532–535). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICEPE.2014.6969965
4. Dlodlo, N., & Kalezhi, J. (2015). The internet of things in agriculture for sustainable rural development. In N. S. Jat D.S. Muyingi H. (Ed.), *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015* (pp. 13–18). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ETNCC.2015.7184801
5. Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2016). Internet of Things: A Definition and Taxonomy. In A.-B. K. AlBeiruti N. Al-Begain K. (Ed.), *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 72–77). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/NGMAST.2015.71
6. Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. *Journal of*

Network and Computer Applications, *81*, 111–124. https://doi.org/10.1016/j.jnca.2016.08.007

7. Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., & Wehrle, K. (2013). Towards viable certificate-based authentication for the Internet of Things. *HotWiSec 2013 - Proceedings of the 2013 ACM Workshop on Hot Topics on Wireless Network Security and Privacy*, 37–41. https://doi.org/10.1145/2463183.2463193
8. Kamel Boulos, M. N., & Al-Shorbaji, N. M. (2014). On the Internet of Things, smart cities and the WHO Healthy Cities. *International Journal of Health Geographics*, *13*. https://doi.org/10.1186/1476-072X-13-10
9. Kamilaris, A., & Pitsillides, A. (2016). Mobile Phone Computing and the Internet of Things: A Survey. *IEEE Internet of Things Journal*, *3*(6), 885–898. https://doi.org/10.1109/JIOT.2016.2600569
10. Kumar, P. M., & Devi Gandhi, U. (2018). A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers and Electrical Engineering*, *65*, 222–235. https://doi.org/10.1016/j.compeleceng.2017.09.001
11. Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). IoT-Based Prognostics and Systems Health Management for Industrial Applications. *IEEE Access*, *4*, 3659–3670. https://doi.org/10.1109/ACCESS.2016.2587754
12. Laplante, P. A., & Laplante, N. (2016). The Internet of Things in Healthcare: Potential Applications and Challenges. *IT Professional*, *18*(3), 2–4. https://doi.org/10.1109/MITP.2016.42
13. Lee, Y. H., Jang, M., Lee, M. Y., Kweon, O. Y., & Oh, J. H. (2017). Flexible Field-Effect Transistor-Type Sensors Based on Conjugated Molecules. *Chem*, *3*(5), 724–763. https://doi.org/10.1016/j.chempr.2017.10.005
14. Machado, K., Rosário, D., Cerqueira, E., Loureiro, A. A. F., Neto, A., & de Souza, J. N. (2013). A routing protocol based on energy and link quality for internet of things applications. *Sensors (Switzerland)*, *13*(2), 1942–1964. https://doi.org/10.3390/s130201942
15. Mandula, K., Parupalli, R., Murty, C. H. A. S., Magesh, E., & Lunagariya, R. (2016). Mobile based home automation using Internet of Things(IoT). *2015 International Conference on Control Instrumentation Communication and Computational Technologies, ICCICCT 2015*, 340–343. https://doi.org/10.1109/ICCICCT.2015.7475301
16. Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V, Gomes, P. H., Libralon, G. L., Meneguete, R. I., Filho, G. P. R., Giancristofaro, G. T., Pessin, G., Krishnamachari, B., & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010
17. Mohammed, J., Lung, C.-H., Ocneanu, A., Thakral, A., Jones, C., & Adler, A. (2014). Internet of things: Remote patient monitoring using web services and cloud computing. *Proceedings - 2014 IEEE International Conference on Internet of Things, IThings 2014, 2014 IEEE International Conference on Green Computing and Communications, GreenCom 2014 and 2014 IEEE*

International Conference on Cyber-Physical-Social Computing, CPS 2014, 256–263. https://doi.org/10.1109/iThings.2014.45

18. Muhammad, G., Rahman, S. M. M., Alelaiwi, A., & Alamri, A. (2017). Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. *IEEE Communications Magazine*, *55*(1), 69–73. https://doi.org/10.1109/MCOM.2017.1600425CM
19. Ndiaye, M., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). Software defined networking for improved wireless sensor network management: A survey. *Sensors (Switzerland)*, *17*(5). https://doi.org/10.3390/s17051031
20. Santos, J., Rodrigues, J. J. P. C., Silva, B. M. C., Casal, J., Saleem, K., & Denisov, V. (2016). An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. *Journal of Network and Computer Applications*, *71*, 194–204. https://doi.org/10.1016/j.jnca.2016.03.014
21. Singh, R., Singh, E., & Nalwa, H. S. (2017). Inkjet printed nanomaterial based flexible radio frequency identification (RFID) tag sensors for the internet of nano things. *RSC Advances*, *7*(77), 48597–48630. https://doi.org/10.1039/c7ra07191d
22. Spanò, E., Di Pascoli, S., & Iannaccone, G. (2016). Low-Power Wearable ECG Monitoring System for Multiple-Patient Remote Monitoring. *IEEE Sensors Journal*, *16*(13), 5452–5462. https://doi.org/10.1109/JSEN.2016.2564995
23. Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., Halunga, S., & Fratu, O. (2015). Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications. *Journal of Medical Systems*, *39*(11). https://doi.org/10.1007/s10916-015-0327-y
24. Tarouco, L. M. R., Bertholdo, L. M., Granville, L. Z., Arbiza, L. M. R., Carbone, F., Marotta, M., & De Santanna, J. J. C. (2012). Internet of Things in healthcare: Interoperatibility and security issues. *IEEE International Conference on Communications*, 6121–6125. https://doi.org/10.1109/ICC.2012.6364830
25. Yeh, K.-H. (2016). A Secure IoT-Based Healthcare System with Body Sensor Networks. *IEEE Access*, *4*, 10288–10299. https://doi.org/10.1109/ACCESS.2016.2638038