IOT-CHALLENDES AND OPPORTUNITIES

Pallavi Murghai Goel, Associate Professor, Department of Computer Applications,
Galgotias University

ABSTRACT

The internet of things (IoT) is made up of the notion of the free flow of information between different low-power embedded devices which utilise the Internet to connect. The IoT is projected to be extensively used and to be applicable in several fields of life. IoT requests have recently received enormous attention and enterprises are thrilled about the financial value of the data created by the deployment of these networks. In contrast, IoT has different security and privacy considerations that restrict the proliferation of end-users. In this work, we have identified, classified and addressed numerous threats to security and state-of-the-art efforts to address these difficulties.

KEYWORDS: IOT, Challenges, Opportunities

INTRODUCTION

Emerging advancements in embedded technology and the Internet have allowed items around us to be interconnected. We are looking for a future in which IoT devices are invisibly integrated into the world around us and generate a huge quantity of data. These data should be preserved and processed in order to make them intelligible and valuable.

An IoT model includes a number of players, including mobile carriers, software developers, pro-viders access technologies, etc. IoT applications are also quite wide-ranging and may be used in production, utility administration, agriculture and healthcare. IoT may be considered as a next generation paradigm for connection between devices and machines that allows action to occur without human interference. A combination of another communication infrastructure is necessary for the development of the IoT world. This has resulted in the invention of intelligent gateways for IoT devices connected to the conventional Internet. The latest efforts are aimed at integrating IoT infrastructure with cloud computing, which enhances IoT's potential.

More and more complicated IoT networks also add to the security issues of these networks. The complexity of the IoT networks is due to the massive number of internet-connected devices and the enormous data created by these devices. IoT attacks are conceivable because infiltration devices inside the IoT network are

an accessible target. Hackers may take control and do harmful operations when hacked and target additional devices near to the compromise node. IoT devices have no malware or virus prevention software. This is a natural result of the minimal memory and low power features of these instruments. The inaccessibility of virus and malware on IoT devices makes them very prone to becoming bots and malicious activities on other network devices. Once an IoT. device is compromised, the attacker may also deter the device's routing and forwarding activities. Besides hacking many other network devices, attackers may also get access to IoT devices' sensitive data. This lack of confidentiality, integrity and data safety in IoT may interfere with the mainstream use of this technology.

CHALLENGES

Each such confidentiality or framework in IoT should handle the following challenges:

Tracking and profiling. Associating an identity with a given person is a danger that may lead to profiling and monitoring. Therefore, one of the main issues is to discontinue IoT activities and to take certain precautionary action.

Tracking and location. Tracking. Localization is another hazard as technologies are attempting to identify and record the whereabouts of each son in time and place. One of the primary problems of IoT security solutions is to develop protocols for IoT interactions which prevent such activities. In e-commerce applications, profiling information about a certain person to infer interests in the correlation between other profiles and data is quite prevalent A major difficulty is to balance company goals with user privacy needs for profiling and data analysis.

Secure transmission of data. Yet another security is that data are delivered securely over the public media without someone being caught and so avoided

OPPRTUNITIES

The latest work addressing the security and privacy problems of cloud-based IoT is available. Cloud-based IoT security and privacy needs as identified by the authors include the privacy of identity, location, node compromise attack, removal/add layer, forward and backward security, and semi constrained and malicious security in the cloud. Another recent endeavour is an effort to examine current data protection technologies. The writers identified the gaps in different plans and suggested that they should be removed. Authors in current IoT apps have been surveyed. In this study, the authors propose to translate their modules into a common system model while simultaneously identifying and studying the behavioural differentiation of the generation of sensor data. The investigation revealed that practically all apps collect information about the location and the time. Any data collected may be of several sorts, including video and audio. The authors examined up-to-date data protection procedures. In addition, possible dangers to user privacy in participatory sensing resulting from uncontrolled personal information disclosure to untrusted persons were highlighted.

The authors also mapped their study to a suggested shared system model for the security analysis of mobile participatory sensing applications ..

A full explanation of security and privacy risks may be found in IoT designs. The talk starts with IoT's detailed architecture. Privacy and security risks are studied in depth at every level of the architecture. State-of-the-art threat scenarios are explored in depth on several levels of ioT architecture. Based on the scenarios outlined, the security challenges at stake include eavesdropping, human assaults and other similar assaults that compromise the confidentiality and integrity of data and the collection of controls over certain components. The authors also investigate the upcoming EU IoT laws. It is necessary to understand the IoT architectural management domains. EU law demands that a person be able to monitor his or her information at all levels of architecture. Further studies need a thorough examination of how this kind of control is technically provided. Energy components of privacy and risks need to be further studied.

CONCLUSION

In this article, we have classified and discussed the cutting edge effort to ensure IoT network security. Data protection efforts, light-weight encryption frameworks, safe transmission and routing, robustness and resistance management, service de- nial and insider threat detection are examined in depth. Data protection is of particular importance in IoT, as the features of such a network differ from the normal Internet network. This paper identifies and discusses such challenges and needs. In addition to privacy, lightweight cryptographic primitives are necessary for the security of the IoT network. All efforts are collated in this regard and future measures are addressed . To safeguard privacy, tech-nics and lightweight context-conscious protocols are developed and virtualization methods are most recently utilised to ensure the integrity of data. Novel methods that employ limited IoT mote resources are needed for lightweight cryptography primitives. In addition, SDN solution offers lightweight cryptographic IoT solutions with the help of centralised SDN controller routing. IoT network encounters problems owing to heterogeneous network assaults on IoT nodes.

REFERENCES

1. Ben-Bassat, A. (2015). Intelligent Automation: The Internet-Of-Things (IoT) with RFID sensors push the envelope of production efficiencies in composites part manufacturing. International SAMPE Technical Conference, 2015-January. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84987662364&partnerID=40&md5=24cf8e1c678936f94e29c891f6647d15

2. DeMartino, C. (2016). Wireless technologies flood the IoT landscape. Microwaves and RF, 55(5), 70–72. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84998775217&partnerID=40&md5=cbe99fac5a3c3105f63b97ca09b4fc2e

3. Ding, W. (2012). The study of IOT based on RFID. Applied Mechanics and Materials, 203, 139–141.

https://doi.org/10.4028/www.scientific.net/AMM.203.139

4. Habib, A., Ansar, S., Akram, A., Azam, M. A., Amin, Y., & Tenhunen, H. (2017). Directly printable organic ASK based chipless RFID tag for IoT applications. Radioengineering, 26(2), 453–460. https://doi.org/10.13164/re.2017.0453
5. Jin, H.-Y., & Tian, M. (2012). Research on security issues of RFID technology in IOT. Proceedings of the 2012 National Conference on Information Technology and Computer Science, CITCS 2012, 52–54. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84878132380&partnerID=40&md5=3e763aa308c47ef2e3b40e94af4fc512
6. Kossonon, B. E., & Ya, W. H. (2018). IOT based smart restaurant system using RFID. 4th International Conference on Smart and Sustainable City, ICSSC 2017, 2018-January. https://doi.org/10.1049/cp.2017.0123
7. Ouyang, H., Guan, J., & Li, K. (2013). An UHF RFID reader in IOT. Proceedings - 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer, MEC 2013, 672–675. https://doi.org/10.1109/MEC.2013.6885148
8. Peng, K., & Xu, Y. (2018). Design of Low-Power Bandgap Voltage Reference for IoT RFID Communication. 2018 IEEE 3rd International Conference on Integrated Circuits and Microsystems, ICICM 2018, 345–348. https://doi.org/10.1109/ICAM.2018.8596364
9. Xiang, S., & Gao, Y. (2011). Discussion on IoT structure and analysis on property of RFID system. 2011 International Conference on Internet Technology and Applications, ITAP 2011 - Proceedings. https://doi.org/10.1109/ITAP.2011.6006377.
10. Bashir, U., Jha, K. R., Mishra, G., Singh, G., & Sharma, S. K. (2017). Octahedron-Shaped Linearly Polarized Antenna for Multistandard Services Including RFID and IoT. IEEE Transactions on Antennas and Propagation, 65(7), 3364–3373. https://doi.org/10.1109/TAP.2017.2705097
11. Charoenpanyasak, S., Sasiwat, Y., Suntiamorntut, W., & Tontisirin, S. (2017). Comparative analysis of RFID anti-collision algorithms in IoT applications. 2016 International Symposium on Intelligent Signal Processing and Communication Systems, ISPACS 2016. https://doi.org/10.1109/ISPACS.2016.7824757
12. DeMartino, C. (2016). Wireless technologies flood the IoT landscape. Microwaves and RF, 55(5), 70–72. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84998775217&partnerID=40&md5=cbe99fac5a3c3105f63b97ca09b4fc2e
13. Fan, K., Liang, C., Li, H., & Yang, Y. (2014). LRMAPC: A lightweight RFID mutual authentication protocol with cache in the reader for IoT. Proceedings - 2014 IEEE International Conference on Computer and Information Technology, CIT 2014, 276–280. https://doi.org/10.1109/CIT.2014.80
14. Hanel, T., Bothe, A., Helmke, R., Gericke, C., & Aschenbruck, N. (2017). Adjustable security for

RFID-equipped IoT devices. 2017 IEEE International Conference on RFID Technology and Application, RFID-TA 2017, 208–213. https://doi.org/10.1109/RFID-TA.2017.8098883

15. Michta, E., Szulim, R., Sojka-Piotrowska, A., & Piotrowski, K. (2017). IoT-based flood embankments monitoring system. In R. R. S. Linczuk M. (Ed.), Proceedings of SPIE - The International Society for Optical Engineering (Vol. 10445). SPIE. https://doi.org/10.1117/12.2280830
16. Petracca, M., Bocchino, S., Azzarà, A., Pelliccia, R., Ghibaudi, M., & Pagano, P. (2013). WSN and RFID integration in the IoT scenario: An advanced safety system for industrial plants. Journal of Communications Software and Systems, 9(1), 104–113. https://doi.org/10.24138/jcomss.v9i1.162
17. Valente, F. J., & Neto, A. C. (2017). Intelligent steel inventory tracking with IoT / RFID. 2017 IEEE International Conference on RFID Technology and Application, RFID-TA 2017, 158–163. https://doi.org/10.1109/RFID-TA.2017.8098639
18. Zeb, S., Satti, J. A., Habib, A., Amin, Y., & Tenhunen, H. (2017). Dual-polarized data dense chipless RFID tag towards IoT applications. 2017 International Symposium on Wireless Systems and Networks, ISWSN 2017, 2018-Janua, 1–5. https://doi.org/10.1109/ISWSN.2017.8250038.
19. Gupta, P., Agrawal, D., Chhabra, J., & Dhir, P. K. (2016). IoT based smart healthcare kit. *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings*, 237–242. https://doi.org/10.1109/ICCTICT.2016.7514585
20. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered IoT users. *Proceedings - 2016 IEEE 1st International Conference on Internet-of-Things Design and Implementation, IoTDI 2016*, 13–24. https://doi.org/10.1109/IoTDI.2015.39
21. Hussein, A. F., Arun Kumar, N., Burbano-Fernandez, M., Ramirez-Gonzalez, G., Abdulhay, E., & De Albuquerque, V. H. C. (2018). An automated remote cloud-based heart rate variability monitoring system. *IEEE Access*, *6*, 77055–77064. https://doi.org/10.1109/ACCESS.2018.2831209
22. Jalali, R., El-Khatib, K., & McGregor, C. (2015). Smart city architecture for community level services through the internet of things. *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, 108–113. https://doi.org/10.1109/ICIN.2015.7073815
23. Li, C., Hu, X., & Zhang, L. (2017). The IoT-based heart disease monitoring system for pervasive healthcare service. In H. R. J. Z.-M. C. T. C. F. C. J. L. C. J. L. C. Toro C. Hicks Y. (Ed.), *Procedia Computer Science* (Vol. 112, pp. 2328–2334). Elsevier B.V. https://doi.org/10.1016/j.procs.2017.08.265
24. Liu, J., Zhang, C., & Fang, Y. (2018). EPIC: A Differential Privacy Framework to Defend Smart Homes Against Internet Traffic Analysis. *IEEE Internet of Things Journal*, *5*(2), 1206–1217. https://doi.org/10.1109/JIOT.2018.2799820

25. Maharjan, P., Toyabur, R. M., & Park, J. Y. (2018). A human locomotion inspired hybrid nanogenerator for wrist-wearable electronic device and sensor applications. *Nano Energy*, *46*, 383–395. https://doi.org/10.1016/j.nanoen.2018.02.033

26. Mauldin, T. R., Canby, M. E., Metsis, V., Ngu, A. H. H., & Rivera, C. C. (2018). Smartfall: A smartwatch-based fall detection system using deep learning. *Sensors (Switzerland)*, *18*(10). https://doi.org/10.3390/s18103363

27. Sathish Kumar, N., Vuayalakshmi, B., Prarthana, R. J., & Shankar, A. (2016). IOT based smart garbage alert system using Arduino UNO. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, *0*, 1028–1034. https://doi.org/10.1109/TENCON.2016.7848162

28. Sodhro, A. H., Pirbhulal, S., & Sangaiah, A. K. (2018). Convergence of IoT and product lifecycle management in medical health care. *Future Generation Computer Systems*, *86*, 380–391. https://doi.org/10.1016/j.future.2018.03.052

29. Sood, S. K., & Mahajan, I. (2017). Wearable IoT sensor based healthcare system for identifying and controlling chikungunya virus. *Computers in Industry*, *91*, 33–44. https://doi.org/10.1016/j.compind.2017.05.006

30. Verma, P., & Sood, S. K. (2018). Cloud-centric IoT based disease diagnosis healthcare framework. *Journal of Parallel and Distributed Computing*, *116*, 27–38. https://doi.org/10.1016/j.jpdc.2017.11.018

31. Xu, T., Zhou, Y., & Zhu, J. (2018). New advances and challenges of fall detection systems: A survey. *Applied Sciences (Switzerland)*, *8*(3). https://doi.org/10.3390/app8030418

32. Dong, L., Shu, W., Han, G., Li, X., & Wang, J. (2017). A Multi-Step Source Localization Method with Narrowing Velocity Interval of Cyber-Physical Systems in Buildings. *IEEE Access*, *5*, 20207–20219. https://doi.org/10.1109/ACCESS.2017.2756855

33. Du, C., Tan, L., & Dong, Y. (2015). Period selection for integrated controller tasks in cyber-physical systems. *Chinese Journal of Aeronautics*, *28*(3), 894–902. https://doi.org/10.1016/j.cja.2015.04.011

34. Ferracuti, F., Freddi, A., Monteriù, A., & Prist, M. (2016). An integrated simulation module for cyber-physical automation systems. *Sensors (Switzerland)*, *16*(5). https://doi.org/10.3390/s16050645

35. Haller, P., & Genge, B. (2017). Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems. *IEEE Access*, *5*, 9336–9347. https://doi.org/10.1109/ACCESS.2017.2703906

36. Han, R., Zhao, X., Yu, Y., Guan, Q., Hu, W., & Li, M. (2016). A cyber-physical system for girder hoisting monitoring based on smartphones. *Sensors (Switzerland)*, *16*(7). https://doi.org/10.3390/s16071048

37. Huang, J., Zhu, Y., Cheng, B., Lin, C., & Chen, J. (2016). A petriNet-based approach for supporting

traceability in cyber-physical manufacturing systems. *Sensors (Switzerland)*, *16*(3). https://doi.org/10.3390/s16030382

38. Jabeur, N., Sahli, N., & Zeadally, S. (2015). Enabling Cyber Physical Systems with Wireless Sensor Networking Technologies, Multiagent System Paradigm, and Natural Ecosystems. *Mobile Information Systems*, *2015*. https://doi.org/10.1155/2015/908315
39. Konstantinov, S., Ahmad, M., Ananthanarayan, K., & Harrison, R. (2017). The Cyber-physical E-machine Manufacturing System: Virtual Engineering for Complete Lifecycle Support. In T. H.-Y. Wang Y. Tseng M.M. (Ed.), *Procedia CIRP* (Vol. 63, pp. 119–124). Elsevier B.V. https://doi.org/10.1016/j.procir.2017.02.035
40. Lei, C.-U., Man, K. L., Liang, H.-N., Lim, E. G., & Wan, K. (2013). Building an intelligent laboratory environment via a cyber-physical system. *International Journal of Distributed Sensor Networks*, *2013*. https://doi.org/10.1155/2013/109014
41. Li, Y., Yang, B., Zheng, T., & Li, Y. (2015). Extended state observer based adaptive back-stepping sliding mode control of electronic throttle in transportation cyber-physical systems. *Mathematical Problems in Engineering*, *2015*. https://doi.org/10.1155/2015/301656
42. Nguyen, V. H., Besanger, Y., Tran, Q. T., & Nguyen, T. L. (2017). On conceptual structuration and coupling methods of co-simulation frameworks in cyber-physical energy system validation. *Energies*, *10*(12). https://doi.org/10.3390/en10121977
43. Wang, Y., Liu, D., & Sun, C. (2017). A cyber physical model based on a hybrid system for flexible load control in an active distribution network. *Energies*, *10*(3). https://doi.org/10.3390/en10030267
44. Yu, Z., Ouyang, J., Li, S., & Peng, X. (2017). Formal modeling and control of cyber-physical manufacturing systems. *Advances in Mechanical Engineering*, *9*(10). https://doi.org/10.1177/1687814017725472
45. Yu, Z., Zhou, L., Ma, Z., & El-Meligy, M. A. (2017). Trustworthiness Modeling and Analysis of Cyber-physical Manufacturing Systems. *IEEE Access*, *5*, 26076–26085. https://doi.org/10.1109/ACCESS.2017.2777438
46. Zheng, M., & Ming, X. (2017). Construction of cyber-physical system–integrated smart manufacturing workshops: A case study in automobile industry. *Advances in Mechanical Engineering*, *9*(10). https://doi.org/10.1177/1687814017733246
47. Geller, J., Grudzinskas Jr., A. J., McDermeit, M., Fisher, W. H., & Lawlor, T. (1998). The efficacy of involuntary outpatient treatment in Massachusetts. *Administration and Policy in Mental Health*, *25*(3), 271–285. https://doi.org/10.1023/A:1022239322212
48. Gia, T. N., Jiang, M., Rahmani, A.-M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015). Fog computing in healthcare Internet of Things: A case study on ECG feature extraction. In J. S. L. L. C. R. A. H. J. M. G. G. N. W. Y. Atzori L. Jin X. (Ed.), *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International*

Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015 (pp. 356–363). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.51

49. He, D., & Zeadally, S. (2015). An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. *IEEE Internet of Things Journal*, *2*(1), 72–83. https://doi.org/10.1109/JIOT.2014.2360121

50. Hiremath, S., Yang, G., & Mankodiya, K. (2015). Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. *Proceedings of the 2014 4th International Conference on Wireless Mobile Communication and Healthcare - "Transforming Healthcare Through Innovations in Mobile and Wireless Technologies", MOBIHEALTH 2014*, 304–307. https://doi.org/10.1109/MOBIHEALTH.2014.7015971

51. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Z. L.-J. Bahsoon R. (Ed.), *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015* (pp. 21–28). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SERVICES.2015.12

52. Hussain, A., Wenbi, R., Da Silva, A. L., Nadher, M., & Mudhish, M. (2015). Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems and Software*, *110*, 253–263. https://doi.org/10.1016/j.jss.2015.08.041

53. Jara, A. J., Alcolea, A. F., Zamora, M. A., Gómez Skarmeta, A. F., & Alsaedy, M. (2010). Drugs interaction checker based on IoT. *2010 Internet of Things, IoT 2010*. https://doi.org/10.1109/IOT.2010.5678458

54. Karafiloski, E., & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In K. L. Latkoski P. Cvetkovski G. (Ed.), *17th IEEE International Conference on Smart Technologies, EUROCON 2017 - Conference Proceedings* (pp. 763–768). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EUROCON.2017.8011213

55. 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

56. 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

57. 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

58. 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

59. Moosavi, S. R., Gia, T. N., Rahmani, A.-M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. In S. E. (Ed.), *Procedia Computer Science* (Vol. 52, Issue 1, pp. 452–459). Elsevier B.V. https://doi.org/10.1016/j.procs.2015.05.013

60. 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