IoT Smart Healthcare Security Challenges and Solutions

Imdad Ali Shah, N. Z. Jhanjhi, Sarfraz Nawaz Brohi (/affiliate/sarfraz-nawaz-brohi/463061/)

Source Title: Advances in Computational Intelligence for the Healthcare Industry 4.0 (/gateway/book/332779)
Copyright: © 2024
Pages: 14
ISBN13: 9798369323335ISBN13 Softcover: 9798369345481EISBN13: 9798369323342
DOI: 10.4018/979-8-3693-2333-5.ch012

Cite Chapter Favorite ★

View Full Text HTML > (/gateway/chapter/full-text-html/345574)

View Full Text PDF > (/gateway/chapter/full-text-pdf/345574)

Abstract

The primary objective of this chapter is to examine the security concerns of people in their smart homes and focus on the healthcare equipment that comes packaged with future homes that are vulnerable to cyber-attacks, resulting in data breaches. Patients not physically present in a healthcare institution can have their health metrics, such as heart rate, blood pressure, temperature, and more, automatically collected by IoT devices. This eliminates the need for patients to travel to the doctor or gather the data themselves. A crucial component of healthcare procedures is patient care, healthcare IoT applications can potentially improve patient outcomes and the calibre of care given by physicians, nurses, clinicians, pharmaceutical companies, and the government. Wireless healthcare monitoring devices are regarded as a medical revolution widely utilized in hospitals and other healthcare settings. However, on the internet of items paradigm, security and privacy for interconnected items should be considered. A systematic approach to security and privacy safeguards must be employed in creating devices, connecting objects, communicating, handling, and storing data, and destroying such devices and data in the context of healthcare and remote health monitoring. In recent years, smart homes and healthcare have become increasingly popular. It is required to use a more secure method to assure security and privacy. As a result, these techniques can provide security and privacy in Smart health regarding remote patient monitoring and healthcare, communications, data handling, and device failure due to data loss. The smart house and its services, as we currently understand them, create a highly heterogeneous context, posing a substantial problem for future consumers and producers. Healthcare services expose vulnerabilities in interconnected medical devices and pose an unknown threat to human life. This study helps new researchers and related healthcare institutions.

Request access from your librarian to read this chapter's full text.

Introduction

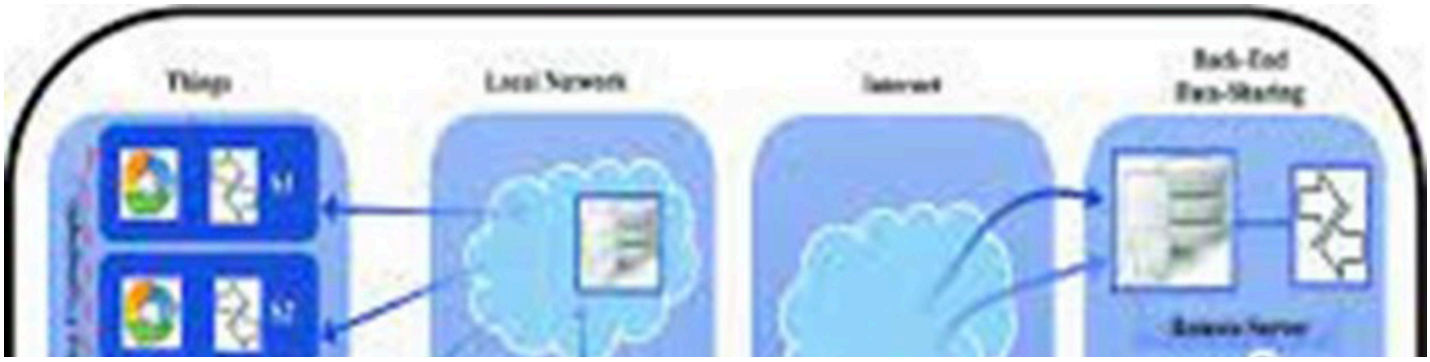
The healthcare industry uses the IoT to enhance patient monitoring, lower costs, and promote innovation in patient care. Healthcare has seen a rise in both medical 4.0 and health 2.0, while industry 4.0 refers to the integration of IoT in the production and consumer sectors. It has made it possible to develop cutting-edge approaches to asset management, medical equipment maintenance, drug administration, autonomous assistive solutions, early warning system development, and treatment plan maintenance. While other functions are still crucial for healthcare, remote patient monitoring is one of the main healthcare IoT (HIoT) areas that saves millions of lives and money(Dimitrov, 2016; Qadri et al., 2020). Wireless Body Sensor Networks (WBSN) are widely accepted as the fundamental Internet of Things technology incorporated into the healthcare industry. As previously mentioned, wearables for fitness tracking are a typical application of the IoT. Nonetheless, IoT has enormous potential for usage in healthcare and could be helpful for early detection, accurate diagnosis, and efficient treatment(Burhan et al., 2018; Food & Administration, 2018). Consumer devices such as continuous glucose monitoring (SGM), blood pressure cuffs, ingestible sensors, linked inhalers, and other devices intended to capture data on patients' vital signs are now the focus of IoT for medical device integration. Another example of this kind of device is the new Apple Watch, which is equipped with detectors for symptoms of Parkinson's illness. Depending on the nature of the disease and the data needs of the caregivers, WBAN connects sensors and actuators to the patient's body. It allows medical professionals to gather data automatically and use decision-support guidelines to enable early therapeutic intervention. For HIoT systems to be secure, to treat patients effectively, and to protect their privacy, security, and privacy protocols are essential. On the other hand, the medical industry is where security lapses and privacy concerns are most documented. Figure 1 Overview of the chapter’s study plan.

Figure 1. Overview of the chapter’s study plan

(https://igiprodst.blob.core.windows.net:443/source-content/9798369323335_332779/979-8-3693-2333-5.ch012.f01.png?sv=2015-12-11&sr=c&sig=M5qmfqraPe7hMkIltDj2u0WijlYjNTc3ZcPCH361LBY%3D&se=2024-10-28T12%3A59%3A31Z&sp=r)

Smart healthcare is receiving a lot of attention from academia, government, industry, and the healthcare community due to the development of intelligent sensory media, objects, and cloud technologies. With a tremendous amount of data and countless services, the Internet of Things (IoT) has recently made the goal of a more innovative world a reality. In this case, cloud computing works well as an enabler because it provides a customizable stack of processing, storage, and software resources at a low-cost S(Rahmani et al., 2018; Wazid et al., 2017). Chronic diseases are a significant problem in the global healthcare industry. According to medical statements, human mortality is increasing due to chronic diseases. Treatment of this disease accounts for more than 70% of a patient's income. Therefore, reducing the risk of death for patients is crucial. Advances in medical research have made it easier to collect health-related data. Patient demographics, medical analysis results, and disease history are all included in healthcare data. Induced disease may vary depending on a particular place's geography and living habitat. Therefore, in addition to disease data, the patient's environmental conditions and living environment should also be recorded in the dataset. Although the healthcare business is not alone in confronting major cybersecurity threats, the repercussions of a failure to prevent digitally illegal attacks are separate failures. Figure 2 Overview IoT in Healthcare System Architecture.

Figure 2. Overview IoT in Healthcare system architecture



References

Follow Reference Abbas N. Asim M. Tariq N. Baker T. Abbas S. (2019). A mechanism for securing IoT-enabled applications at the fog layer.Journal of Sensor and Actuator Networks, 8(1), 16. 10.3390/jsan8010016

Follow Reference Aghili S. F. Mala H. Shojafar M. Peris-Lopez P. (2019). LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT.Future Generation Computer Systems, 96, 410–424. 10.1016/j.future.2019.02.020

Follow Reference Al-Issa Y. Ottom M. A. Tamrawi A. (2019). eHealth cloud security challenges: A survey.Journal of Healthcare Engineering, 2019.31565209

Follow Reference Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). *Medibchain: A blockchain based privacy preserving platform for healthcare data.* Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China. 10.1007/978-3-319-72395-2_49

Alamri, A. (2019). Big data with integrated cloud computing for prediction of health conditions. *2019 International conference on platform technology and service (PlatCon)*.Research Gate.

Follow Reference Ali, M. S., Vecchio, M., Putrus, G. D., Kanhere, S. S., & Antonelli, F. (2020). A decentralized peer-to-peer remote health monitoring system. *sensors, 20*(6), 1656. 10.1007/978-3-319-72395-2_49

(https://igiprodst.blob.core.windows.net:443/source-content/9798369823335_332779/979-8-3693-2333-5.ch012.f02.png?sv=2015-12-11&sr=c&sig=M5qmfqraPe7bMkIltDj2u0WiiIYiNTc3ZcPCH361LBY%3D&se=2024-10-28T12%3A59%3A31Z&sp=r)

adopted from Vithya Vijayalakshmi

Continue Reading (/gateway/chapter/full-text-html/345574)

Alkinani, M. H., Almazroi, A. A., Jhanjhi, N. Z., & Khan, N. A. (2021). 5G and IoT based reporting and accident detection (RAD) system to deliver first aid box using unmanned aerial vehicle. *sensors, 21*(20), 6905.

Awad Abdellatif, A., Al-Marridi, A. Z., Mohamed, A., Erbad, A., Fabiana Chiasserini, C., & Refaey, A. (2020). SSHealth: Toward Secure, Blockchain-Enabled Healthcare Systems. *arXiv e-prints*, arXiv: 2006.10843.

Balakrishnan, S., Ruskhan, B., Zhen, L. W., Huang, T. S., Soong, W. T. Y., & Shah, I. A. (2023). Down2Park: Finding New Ways to Park. *Journal of Survey in Fisheries Sciences*, 322-338.

Burhan, M., Rehman, R. A., Khan, B., & Kim, B.-S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *sensors, 18*(9), 2796.

Follow Reference Challa S. Das A. K. Gope P. Kumar N. Wu F. Vasilakos A. V. (2020). Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems.Future Generation Computer Systems, 108, 1267–1286. 10.1016/j.future.2018.04.019

Follow Reference Challa S. Das A. K. Odelu V. Kumar N. Kumari S. Khan M. K. Vasilakos A. V. (2018). An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks.Computers & Electrical Engineering, 69, 534–554. 10.1016/j.compeleceng.2017.08.003

Follow Reference Chen L. Lee W.-K. Chang C.-C. Choo K.-K. R. Zhang N. (2019). Blockchain based searchable encryption for electronic health record sharing.Future Generation Computer Systems, 95, 420–429. 10.1016/j.future.2019.01.018

Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M. A., Mukherjee, M., & Khan, F. A. (2019). Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *sensors, 19*(14), 3119.

Follow Reference Dimitrov D. V. (2016). Medical internet of things and big data in healthcare.Healthcare Informatics Research, 22(3), 156. 10.4258/hir.2016.22.3.15627525156

Follow Reference Du M. Chen Q. Chen J. Ma X. (2020). An optimized consortium blockchain for medical information sharing.IEEE Transactions on Engineering Management, 68(6), 1677–1689. 10.1109/TEM.2020.2966832

Food and Drug Administration. (2018). *Content of premarket submissions for management of cybersecurity in medical devices.* Food and Drug Administration (FDA).

Follow Reference Hardin T. Kotz D. (2019). Blockchain in health data systems: A survey. 2019 sixth international conference on internet of things: Systems, management and security (IOTSMS), Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges.IEEE Communications Surveys and Tutorials, 22(3), 1686–1721.

Follow Reference Khalid U. Asim M. Baker T. Hung P. C. Tariq M. A. Rafferty L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems.Cluster Computing, 23(3), 2067–2087. 10.1007/s10586-020-03058-6

Follow Reference Khan A. Jhanjhi N. Z. Omar H. A. H. B. H. Haji D. H. T. B. A. (2024). Risk Management and Cybersecurity in Transportation and Warehousing. In Cybersecurity Measures for Logistics Industry Framework (pp. 1–35). IGI Global.

Follow Reference Khan F. A. Haldar N. A. H. Ali A. Iftikhar M. Zia T. A. Zomaya A. Y. (2017). A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments.IEEE Access : Practical Innovations, Open Solutions, 5, 13531–13544. 10.1109/ACCESS.2017.2714258

Follow Reference Kleinaki A.-S. Mytis-Gkometh P. Drosatos G. Efraimidis P. S. Kaldoudi E. (2018). A blockchain-based notarization service for biomedical knowledge retrieval.Computational and Structural Biotechnology Journal, 16, 288–297. 10.1016/j.csbj.2018.08.00230181840

Follow Reference Kotz D. Gunter C. A. Kumar S. Weiner J. P. (2016). Privacy and security in mobile health: A research agenda.Computer, 49(6), 22–30. 10.1109/MC.2016.18528344359

Follow Reference Kumar M. Kumar A. Verma S. Bhattacharya P. Ghimire D. Kim S. Hosen A. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues.Electronics (Basel), 12(9), 2050. 10.3390/electronics12092050

Follow Reference Laraib, A., Sial, A., & Ujjan, R. M. A. (2024). Addresses the Security Issues and Safety in Cyber-Physical Systems of Drones. In *Cybersecurity Issues and Challenges in the Drone Industry* (pp. 381-404). IGI Global. 10.4018/979-8-3693-0774-8.ch016

Follow Reference Maamar, Z., Kajan, E., Asim, M., & Baker Shamsa, T. (2019). Open challenges in vetting the internet-of-things.Internet Technology Letters, 2(5), e129.

Follow Reference Maria A. Nazurl I. Nz J. (2019). A lightweight and secure authentication scheme for IoT based E-health application.IJCSNS Int. J. Comput. Sci. Netw. Secur, 19(1), 107–120.

Follow Reference Moosavi S. R. Nigussie E. Levorato M. Virtanen S. Isoaho J. (2018). Performance analysis of end-to-end security schemes in healthcare IoT.Procedia Computer Science, 130, 432–439. 10.1016/j.procs.2018.04.064

Follow Reference Najmi, K. Y., AlZain, M. A., Masud, M., Jhanjhi, N., Al-Amri, J., & Baz, M. (2023). A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability.Materials Today: Proceedings, 81, 377–382.

Follow Reference Porambage P. Ylianttila M. Schmitt C. Kumar P. Gurtov A. Vasilakos A. V. (2016). The quest for privacy in the internet of things.IEEE Cloud Computing, 3(2), 36–45. 10.1109/MCC.2016.28

Follow Reference Qadri Y. A. Nauman A. Zikria Y. B. Vasilakos A. V. Kim S. W. (2020). The future of healthcare internet of things: A survey of emerging technologies.IEEE Communications Surveys and Tutorials, 22(2), 1121–1167. 10.1109/COMST.2020.2973314

Follow Reference Rahmani A. M. Gia T. N. Negash B. Anzanpour A. Azimi I. Jiang M. Liljeberg P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach.Future Generation Computer Systems, 78, 641–658. 10.1016/j.future.2017.02.014

Shah, I. A. (2024). Drone Industry Security Issues and Challenges in the Context of IoD. *Cybersecurity Issues and Challenges in the Drone Industry*, 310-323.

Follow Reference Shah I. A. Jhanjhi N. Z. Brohi S. N. (2024). Use of AI-Based Drones in Smart Cities. In Cybersecurity Issues and Challenges in the Drone Industry (pp. 362–380). IGI Global. 10.4018/979-8-3693-0774-8.ch015

Follow Reference Shah I. A. Jhanjhi N. Z. Ujjan R. M. A. (2024a). Drone Technology in the Context of the Internet of Things. In Cybersecurity Issues and Challenges in the Drone Industry (pp. 88–107). IGI Global. 10.4018/979-8-3693-0774-8.ch004

Follow Reference Shah I. A. Jhanjhi N. Z. Ujjan R. M. A. (2024b). Use of AI Applications for the Drone Industry. In Cybersecurity Issues and Challenges in the Drone Industry (pp. 27–41). IGI Global. 10.4018/979-8-3693-0774-8.ch002

Follow Reference Talal, M., Zaidan, A., Zaidan, B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S., Alsalem, M., Lim, C. K., Tan, K. L., & Shir, W. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review.Journal of Medical Systems, 43, 1–34.

Tariq, N., Asim, M., Al-Obeidat, F., Zubair Farooqi, M., Baker, T., Hammoudeh, M., & Ghafir, I. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *sensors, 19*(8), 1788.

Follow Reference Wang, H., Li, K., Ota, K., & Shen, J. (2016). Remote data integrity checking and sharing in cloud-based health internet of things.IEICE Transactions on Information and Systems, 99(8), 1966–1973.

Follow Reference Wazid M. Das A. K. Kumar N. Conti M. Vasilakos A. V. (2017). A novel authentication and key agreement scheme for implantable medical devices deployment.IEEE Journal of Biomedical and Health Informatics, 22(4), 1299–1309. 10.1109/JBHI.2017.272154528682267

Follow Reference Xu J. Xue K. Li S. Tian H. Hong J. Hong P. Yu N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data.IEEE Internet of Things Journal, 6(5), 8770–8781. 10.1109/JIOT.2019.2923525

Follow Reference Yang Y. Liu X. Deng R. H. Li Y. (2017). Lightweight sharable and traceable secure mobile health system.IEEE Transactions on Dependable and Secure Computing, 17(1), 78–91. 10.1109/TDSC.2017.2729556

Follow Reference Yang Y. Zheng X. Guo W. Liu X. Chang V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system.Information Sciences, 479, 567–592. 10.1016/j.ins.2018.02.005

Follow Reference Zhang A. Lin X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain.Journal of Medical Systems, 42(8), 140. 10.1007/s10916-018-0995-529956061

Request Access

You do not own this content. Please login to recommend this title to your institution's librarian or purchase it from the IGI Global bookstore (/chapter/iot-smart-healthcare-security-challenges-and-solutions/345574).

Username or email:
Soobiasaeed1@gmail.com

Password:
••••••••

Log In >

Forgot individual login password? (/gateway/login/reset-password/)

Create individual account (/gateway/login/create-account/)

Research Tools
Database Search (/gateway/) | Help (/gateway/help/) | User Guide (/gateway/user-guide/) | Advisory Board (/gateway/advisory-board/)

User Resources
Librarians (/gateway/librarians/) | Researchers (/gateway/researchers/) | Authors (/gateway/authors/)

Librarian Tools
COUNTER Reports (/gateway/librarian-tools/counter-reports/) | Persistent URLs (/gateway/librarian-tools/persistent-urls/) | MARC Records (/gateway/librarian-tools/marc-records/) | Institution Holdings (/gateway/librarian-tools/institution-holdings/) | Institution Settings (/gateway/librarian-tools/institution-settings/)

Librarian Resources
Training (/gateway/librarian-corner/training/) | Title Lists (/gateway/librarian-corner/title-lists/) | Licensing and Consortium Information (/gateway/librarian-corner/licensing-and-consortium-information/) | Promotions (/gateway/librarian-corner/promotions/)

Policies
Terms and Conditions (/gateway/terms-and-conditions/)

(http://www.facebook.com/pages/IGI-Global/138206739534176?ref=sgm)

(http://twitter.com/igiglobal)
(https://www.linkedin.com/company/igiglobal)

(http://www.world-forgotten-children.org)

(https://publicationethics.org/category/publisher/igi-global)

Copyright © 1988-2024, IGI Global - All Rights Reserved