A Symmetric Scheme for Securing Data in Cyber-Physical Systems / IoT Sensor-Based Systems based on AES and SHA256

Rajan CHATTAMVELLI
Vellore Institute of Technology, Vellore, India
rajan.chattamvelli@vit.ac.in

Abstract

Cyber-Physical technologies and Internet have modernized and enhanced the lifestyle of people in this present era. Internet of Things (IoT) is also being seen as the new technology that is changing human discernment about daily life. Many cyber-physical devices generate a lot of sensitive data, which needs to be secured. All the applications of CPS / IoT fundamentally, need symmetric keys for the encryption / decryption of the sensitive data generated. This paper seeks to propose a symmetric scheme for securing data in a Cyber-Physical system using IoT sensor-based technology, which will be based on AES and SHA256 encryption / decryption method.

Index terms: elliptic curve cryptography, encryption algorithm, hash function, hybrid cryptosystems, modified AES algorithm, symmetric cryptography

References

[1]. J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocess. Microsyst., vol. 77, 2020, doi: 10.1016/j.micpro.2020.103201.

[2]. U. Farooq, N. Ul Hasan, and I. Baig, "Securing Internet of Things (IoT) through an Adaptive Framework," 16th Int. Multi-Conference Syst. Signals Devices, SSD 2019, pp. 387–392, 2019, doi: 10.1109/SSD.2019.8893153.

[3]. K. Parasuraman and A. Anbarasa Kumar, "Cyber Security: A New Approach of Secure Data Through Attentiveness in Cyber Space," in Lecture Notes on Data Engineering and Communications Technologies, 2020.

[4]. I. Fatima, A. Anjum, S. U. R. Malik, and N. Ahmad, "Cyber Physical Systems and IoT: Architectural Practices, Interoperability, and Transformation," IT Prof., vol. 22, no. 3, pp. 46–54, 2020, doi: 10.1109/MITP.2019.2912604.

[5]. P. Gauravaram, "Cryptographic Hash Functions: Cryptanalysis, Design and Applications," Inf. Secur., 2007.

[6]. D. Rachmawati, J. T. Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," J. Phys. Conf. Ser., vol. 978, no. 1, 2018, doi: 10.1088/1742-6596/978/1/012116.

[7]. H. Krawczyk, "New hash functions for message authentication," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 921, pp. 301–310, 1995, doi: 10.1007/3-540-49264-X_24.

[8]. W. J. Buchanan, Cryptography. 2017.

[9]. M. Bellare, K. G. Paterson, and P. Rogaway, "Security of symmetric encryption against mass surveillance," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8616 LNCS, no. PART 1, pp. 1–19, 2014, doi: 10.1007/978-3-662-44371-2_1.

[10]. Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on Cyber-physical Systems," vol. 4, no. 1, pp. 27–40, 2017.

[11]. J. Shi, J. Wan, and Hehua Y. Hui Suo, "A Survey of Cyber-Physical Systems," 2011.

[12]. A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security - A Survey," IEEE Internet Things J., vol. 4, no. 6, pp. 1802–1831, 2017, doi: 10.1109/JIOT.2017.2703172.

[13]. A. A. Letichevsky, O. O. Letychevskyi, V. G. Skobelev, and V. A. Volkov, "Cyber-Physical Systems," Cybern. Syst. Anal., vol. 53, no. 6, pp. 821–834, 2017, doi: 10.1007/s10559-017-9984-9.

[14]. H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," Sensors (Switzerland), vol. 20, no. 13, pp. 1–20, 2020, doi: 10.3390/s20133625.

[15]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[16]. C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-Physical Systems and Internet of Things NIST Special Publication 1900-202 Cyber-Physical Systems and Internet of Things," NIST Spec. Publ. 1900-202, 2019.

[17]. H. Isakovic, E. A. Crespo, and R. Grosu, "An energy sustainable cps/iot ecosystem," vol. 10, pp. 2–3, 2021.

[18]. N. Aleisa, "A comparison of the 3DES and AES encryption standards," Int. J. Secur. its Appl., vol. 9, no. 7, pp. 241–246, 2015, doi: 10.14257/ijsia.2015.9.7.21.

[19]. H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," J. King Saud Univ. - Eng. Sci., vol. 32, no. 2, 2020, doi: 10.1016/j.jksues.2018.07.002.

[20]. A. U. Rahman, S. U. Miah, and S. Azad, "Advanced encryption standard," Pract. Cryptogr. Algorithms Implementations Using C++, no. December, pp. 91–126, 2014, doi: 10.1201/b17707.

[21]. M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," BCC 2018 - Proc. 2nd ACM Work. Blockchains, Cryptocurrencies, Contract. Co-located with ASIA CCS 2018, pp. 47–55, 2018, doi: 10.1145/3205230.3205238.

[22]. D. Ravilla and C. S. R. Putta, "Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs," 2015 Int. Conf. Electron. Des. Comput. Networks Autom. Verif. EDCAV 2015, pp. 154–159, 2015, doi: 10.1109/EDCAV.2015.7060558.

[23]. M. R. L. Perez, B. Gerardo, and R. Medina, "Modified SHA256 for securing online transactions based on blockchain mechanism," 2018 IEEE 10th Int. Conf. Humanoid, Nanotechnology, Inf. Technol. Commun. Control. Environ. Manag. HNICEM 2018, pp. 0–4, 2019, doi: 10.1109/HNICEM.2018.8666341.

[24]. I. H. Latif and E. Erçelebi, "Implementation of Hybrid Cryptosystem using AES-256 and SHA-2 256 by LabVIEW," Ijarcce, vol. 6, no. 1, pp. 351–357, 2017, doi: 10.17148/ijarcce.2017.6169.

[25]. N. A. Fauziah, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "Design and implementation of AES and SHA256 cryptography for securing multimedia file over android chat application," 2018 Int. Semin. Res. Inf. Technol. Intell. Syst. ISRITI 2018, no. October 2019, pp. 146–151, 2018, doi: 10.1109/ISRITI.2018.8864485.

[26]. H. Zodpe and A. Sapkal, "Journal of King Saud University – Engineering Sciences An efficient AES implementation using FPGA with enhanced security features," J. King Saud Univ. - Eng. Sci., 2018, [Online]. Available: https://doi.org/10.1016/j.jksues.2018.07.002.

[27]. Rolf Oppliger, Contemporary Cryptography, vol. 110, no. 9, 2017.