REFERENCES

1. Aakash, D., & Shanthi, P. (2016). Lightweight security algorithm for wireless node connected with IoT. Indian J. Sci. Technol, 9, 1-8.

2. Abie, H., & Balasingham, I. (2012, February). Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks (pp. 269-275).

3. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. International Journal of Scientific and Research Publications, 8(7), 495-516.

4. Ahemd, M. M., Shah, M. A., & Wahid, A. (2017, April). IoT security: A layered approach for attacks & defenses. In 2017 International conference on Communication Technologies (ComTech) (pp. 104-110). IEEE.

5. Ahmed, S., & Ahmed, T. (2022). Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review. International Journal of Scientific and Research Publications (IJSRP),12(7).

6. Albrecht, M. R., Driessen, B., Kavun, E. B., Leander, G., Paar, C., & Yalçın, T. (2014). Block ciphers–focus on the linear layer (feat. PRIDE). In Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I 34 (pp. 57-76). Springer Berlin Heidelberg.

7. Al Shuhaimi, F., Jose, M., & Singh, A. V. (2016, September). Software defined network as solution to overcome security challenges in IoT. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) (pp. 491-496). IEEE.

8. Althoubi, A., Alshahrani, R., & Peyravi, H. (2021). Delay analysis in iot sensor networks. Sensors, 21(11), 3876.

9. Al-Qaseemi, S. A., Almulhim, H. A., Almulhim, M. F., & Chaudhry, S. R. (2016, December). IoT architecture challenges and issues: Lack of standardization. In 2016 Future technologies conference (FTC) (pp. 731-738). IEEE.

10. Ashok, A., Brison, M., & LeTallec, Y. (2017). Improving cold chain systems: Challenges and solutions. Vaccine, 35(17), 2217-2223.

11. Aziz, M. A., Ragheb, M. A., Ragab, A. A., & El Mokadem, M. (2018). The impact of enterprise resource planning on supply chain management practices. The Business & Management Review, 9(4), 56-69.

12. Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE) (pp. 1-5). IEEE.

13. Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2017). GIFT: A small present: Towards reaching the limit of lightweight encryption. In Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings (pp. 321-345). Springer International Publishing.

14. Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: a literature review. International journal of production research, 57(15-16), 4719-4742.

15. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-6). IEEE.

16. Birkel, H., & Müller, J. M. (2021). Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability–A systematic literature review. Journal of Cleaner Production, 289, 125612.

17. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J.., & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9 (pp. 450-466). Springer Berlin Heidelberg.

18. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R.,& Yalçın, T. (2012). PRINCE–a low-latency block cipher for pervasive computing applications. In Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18 (pp. 208-225). Springer Berlin Heidelberg.

19. Bormann, C.; Castellani, A.P.; Shelby, Z.(2012).Coap: An application protocol for billions of tiny Internet nodes. IEEE Internet Comput.,16, 62–67.

20. Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236).

21. 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.

22. Chatterjee, K., Chaudhary, R. R. K., & Singh, A. (2022). A lightweight block cipher technique for IoT based E-healthcare system security. Multimedia Tools and Applications, 81(30), 43551-43580.

23. Chander, S. (2022). Lightweight Cryptography Algorithms for Security of IoT Devices: A Survey. IRJET, 842-850.

24. Chaurasia, N., & Kumar, P. (2023). A Comprehensive Study on Issues and Challenges Related to Privacy and Security in IoT. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 100158.

25. Chen, J., Gong, Z., Tang, Y., & Dong, X. (2022). A comprehensive analysis of lightweight 8-bit sboxes from iterative structures. Journal of Information Security and Applications, 70, 103302.

26. Chen, L., Thombre, S., Järvinen, K., Lohan, E. S., Alén-Savikko, A., Leppäkoski, H., ... & Kuusniemi, H. (2017). Robustness, security and privacy in location-based services for future IoT: A survey. Ieee Access, 5, 8956-8977.

27. Chom Thungon, L., Ahmed, N., & Hussain, M. I. (2018). Comparison of aes and present block cipher for 6LoWPAN based internet-of-things. International Journal of Computational Intelligence & IoT, 1(2).

28. Cirani, S., Ferrari, G., & Veltri, L. (2013). Enforcing security mechanisms in the IP-based internet of things: An algorithmic overview. Algorithms, 6(2), 197-226.

29. Dadhaneeya, H., Nema, P. K., & Arora, V. K. (2023). Internet of things in food processing and its potential in industry 4.0 era: A review. Trends in Food Science & Technology.

30. Dai, H. N., Wang, H., Xiao, H., Li, X., & Wang, Q. (2016, August). On eavesdropping attacks in wireless networks. In 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES) (pp. 138-141). IEEE.

31. De Vass, T., Shee, H., & Miah, S. J. (2018). The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. Australasian Journal of Information Systems, 22.

32. Dulababu, T., Lakshmi, R. B., & Girish, B. (2018). Supply Chain Management: Opportunities and Challenges. Advances in Management, 11(4), 9-12.

33. Đurđević, N., Labus, A., Bogdanović, Z., & Despotović-Zrakić, M. (2017). Internet of things in marketing and retail. Int. J. Adv. Comput. Sci. Appl, 6(3).

34. Dwivedi, A. D., & Srivastava, G. (2023). Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. Internet of Things, 21, 100677.

35. El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet, 15(2), 54.

36. Elleithy, K. M., Blagovic, D., Cheng, W. K., & Sideleau, P. (2005). Denial of service attack techniques: Analysis, Implementation and Comparison. Journal of Systemics, Cybernetics, and Informatics 3.1, 66-71.

37. Fan, T., Tao, F., Deng, S., & Li, S. (2015). Impact of RFID technology on supply chain decisions with inventory inaccuracies. International Journal of Production Economics, 159, 117-125.

38. Farwa, S., Shah, T., & Idrees, L. (2016). A highly nonlinear S-box based on a fractional linear transformation. SpringerPlus, 5(1), 1-12.

39. Ferdush, J., Begum, M., & Uddin, M. S. (2021). Chaotic lightweight cryptosystem for image encryption. Advances in Multimedia, 2021, 1-16.

40. Gan, A. (2021). Review on Cryptography Techniques in Network Security. Journal of ICT in Education, 8(1), 125-135.

41. Grønbæk, I. (2008, August). Architecture for the Internet of Things (IoT): API and interconnect. In 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008) (pp. 802-807). IEEE.

42. Gupta, K., & Shukla, S. (2016, February). Internet of Things: Security challenges for next generation networks. In 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH) (pp. 315-318). IEEE.

43. Gurtu, A., & Johny, J. (2021). Supply chain risk management: Literature review. Risks, 9(1), 16.

44. Gyory, N., & Chuah, M. (2017, January). IoTOne: Integrated platform for heterogeneous IoT devices. In 2017 International Conference on Computing, Networking and Communications (ICNC) (pp. 783-787). IEEE.

45. Haddara, M., Gøthesen, S., & Langseth, M. (2022). Challenges of cloud-ERP adoptions in SMEs. Procedia computer science, 196, 973-981.

46. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017, October). A lightweight IoT security protocol. In 2017 1st cyber security in networking conference (CSNet) (pp. 1-8). IEEE.

47. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.

48. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.

49. Haulder, N., Kumar, A., & Shiwakoti, N. (2019). An analysis of core functions offered by software packages aimed at the supply chain management software market. Computers & Industrial Engineering, 138, 106116.

50. Horrow, S., & Sardana, A. (2012, August). Identity management framework for cloud based internet of things. In Proceedings of the First International Conference on Security of Internet of Things (pp. 200-203).

51. Hu, C., Zhang, J., & Wen, Q. (2011). An identity-based personal location system with protected privacy in IoT. In 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology (pp. 192-195). IEEE.

52. Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. Procedia computer science, 132, 109-117.

53. Li, F., & Xiong, P. (2013). Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal, 13(10), 3677-3684.

54. Li, Z., Yin, X., Geng, Z., Zhang, H., Li, P., Sun, Y., ... & Li, L. (2013, January). Research on PKI-like Protocol for the Internet of Things. In 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation (pp. 915-918). IEEE.

55. Mani, Z., & Chouk, I. (2017). Drivers of consumers' resistance to smart products. Journal of Marketing Management, 33(1-2), 76-97.

56. Marimuthu, L., & Valliammai, A. (2016). Problem And Prospects Of Fisherman In India With Special Reference To Nagapattinam. Asia Pacific Journal of Research Vol: I. Issue XXXVI.

57. Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., ... & Buchanan, W. J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Personal Communications, 127(2), 1405-1432.

58. Mercier, S., Villeneuve, S., Mondor, M., & Uysal, I. (2017). Time–temperature management along the food cold chain: A review of recent developments. Comprehensive reviews in food science and food safety, 16(4), 647-667.

59. Mewada, S., Sharma, P., & Gautam, S. S. (2016). Classification of efficient symmetric key cryptography algorithms. International Journal of Computer Science and Information Security, 14(2), 105.

60. Michiardi, P., & Molva, R. (2002, September). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security September 26–27, 2002, Portorož, Slovenia (pp. 107-121). Boston, MA: Springer US.

61. Mishra, R., Okade, M., & Mahapatra, K. (2023). Novel substitution box architectural synthesis for lightweight block ciphers. IEEE Embedded Systems Letters.

62. Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(4), 307-312.

63. Mohan, A., Krishnan, R., Arshinder, K., Vandore, J., & Ramanathan, U. (2023). Management of postharvest losses and wastages in the Indian tomato supply chain- a temperature-controlled storage perspective. Sustainability, 15(2), 1331.

64. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing, 5(4), 586-602.

65. Nayancy, Dutta, S., & Chakraborty, S. (2022). A survey on implementation of lightweight block ciphers for resource constraints devices. Journal of Discrete Mathematical Sciences and Cryptography, 25(5), 1377-1398.

66. Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, Q. Z. (2016). IoT middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal, 4(1), 1-20.

67. Novais, L., Maqueira, J. M., & Ortiz-Bas, Á. (2019). A systematic literature review of cloud computing use in supply chain integration. Computers & Industrial Engineering, 129, 296-314.

68. O'caoimh, R., Sweeney, C., Hynes, H., McGlade, C., Cornally, N., Daly, E.,& Molloy, W. (2015). COLLaboration on AGEing-COLLAGE: Ireland's three-star reference site for the European Innovation Partnership on Active and Healthy Ageing (EIP on AHA). European Geriatric Medicine, 6(5), 505-511.

69. Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., & Ajao, L. A. (2018). Two layers trust-based intrusion prevention system for wireless sensor networks. Adv. Electr. Telecommun. Eng, 1, 23-29.

70. Pahlevanzadeh, B., Koleini, S., & Fadilah, S. I. (2020, December). Security in IOT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. In International Conference on Advances in Cyber Security (pp. 267-283). Singapore: Springer Singapore

71. Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. Arabian Journal for Science and Engineering, 46, 4015-4037.

72. Panchami, V., & Mathews, M. M. (2023). A substitution box for lightweight ciphers to secure internet of things. Journal of King Saud University-Computer and Information Sciences, 35(4), 75-89.

73. Pathan, A., Kokate, R., Mutha, A., Pingale, P., & Gadakh, P. (2016). Digital India: IoT based intelligent interactive super market framework for shopping mall. Eng. Sci, 1, 1-5.

74. Patidar, V., Sud, K. K., & Pareek, N. K. (2009). A pseudo random bit generator based on chaotic logistic map and its statistical testing. Informatica, 33(4).

75. Patil, M. (2015). Challenges for supply chain management in today's global competitive environment. European Journal of Business Management, 4.

76. Paudel, N., & Neupane, R. C. (2019, September). A general architecture for a real-time monitoring system based on the internet of things. In Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control (pp. 1-12).

77. Ponnusamy, K., & Rajagopalan, N. (2018). Internet of things: A survey on IoT protocol standards. Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2016, Volume 2, 651-663.

78. Prathiba, A., & Bhaaskaran, V. K. (2018). Lightweight S-box architecture for secure internet of things. Information, 9(1), 13.

79. Rahman, Z., Yi, X., Billah, M., Sumi, M., & Anwar, A. (2022). Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home. Electronics, 11(7), 1083.

80. Ravi, S., Raghunathan, A., Kocher, P., & Hattangady, S. (2004). Security in embedded systems: Design challenges. ACM Transactions on Embedded Computing Systems (TECS), 3(3), 461-491.

81. Razaq, A., Alolaiyan, H., Ahmad, M., Yousaf, M. A., Shuaib, U., Aslam, W., & Alawida, M. (2020). A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups. Ieee Access, 8, 75473-75490.

82. Richey, R. G., Roath, A. S., Adams, F. G., & Wieland, A. (2022). A responsiveness view of logistics and supply chain management. Journal of Business Logistics, 43(1), 62-91.

83. Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018, August). Securing the internet of things (IoT): A security taxonomy for IoT. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 163-168). IEEE.

84. Robertazzi, T. G., & Robertazzi, T. G. (2017). Software-defined networking. Introduction to Computer Networking, 81-87.

85. Saba, S. J., Al-Nuaimi, B. T., & Suhail, R. A. (2023, March). A review of traditional, lightweight and ultra-lightweight cryptography techniques for IoT security environment. In AIP Conference Proceedings (Vol. 2475, No. 1). AIP Publishing.

86. Sarma, A., Matos, A., Girao, J., & Aguiar, R. L. (2008). Virtual identity framework for telecom infrastructures. Wireless Personal Communications, 45, 521-543.

87. Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of electrical and computer engineering, 2017.

88. Shah, T., & Qureshi, A. (2019). S-box on subgroup of Galois field. Cryptography, 3(2), 13.

89. Sha, K., Wei, W., Yang, T. A., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future generation computer systems, 83, 326-337.

90. Sharma,S.,& Gupta, Y. (2017). Study on cryptography and techniques. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(1), 249-252.

91. Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A privacy preserving communication protocol for IoT applications in smart homes. IEEE Internet of Things Journal, 4(6), 1844-1852.

92. Soursos,S., Žarko, I. P., Zwickl, P., Gojmerac, I., Bianchi, G., & Carrozzo, G. (2016, June). Towards the cross-domain interoperability of IoT platforms. In 2016 European conference on networks and communications (EuCNC) (pp. 398-402). IEEE.

93. Sundaram, B. V., Ramnath, M., Prasanth, M., & Sundaram, V. (2015, March). Encryption and hash based security in Internet of Things. In 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-6). IEEE.

94. Suryadevara, S., & Ali, S. (2020, June). Preperformance Testing of A Website. In CS & IT Conference Proceedings (Vol. 10, No. 7). CS & IT Conference Proceedings.

95. Tadejko, P. (2015). Application of Internet of Things in logistics–current challenges. Ekonomia i Zarządzanie, 7(4), 54-64.

96. Tao, H., & Peiran, W. (2010, December). Preference-based privacy protection mechanism for the internet of things. In 2010 Third International Symposium on Information Science and Engineering (pp. 531-534). IEEE.

97. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177-28193.

98. Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future generation computer systems, 108, 909-920.

99. To'xtajon,Q.(2023).Lightweight Cryptography In IoT Networks. Innovations in Technology and Science Education, 2(10), 999-1007.

100. V rat, P., Gupta, R., Bhatnagar, A., Pathak, D. K., & Fulzele, V. (2018). Literature review analytics (LRA) on sustainable cold-chain for perishable food products: research trends and future directions. Opsearch, 55, 601-627.

101. Wang, Y., Lei, P., & Wong, K. W. (2015). A method for constructing bijective S-box with high nonlinearity based on chaos and optimization. International Journal of Bifurcation and Chaos, 25(10), 1550127.

102. Weber,R.H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30.

103. Wenjun, L. (2010). IoT makes the City Smarter. Sci. Cult, 10, 12-13.

104. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of Things. In 2010 3rd international conference on advanced computer theory and engineering (ICACTE) (Vol. 5, pp. V5-484). IEEE.

105. Wu, Y., Noonan, J. P., & Agaian, S. (2011, October). Dynamic and implicit latin square doubly stochastic s-boxes with reversibility. In 2011 IEEE International Conference on Systems, Man, and Cybernetics (pp. 3358-3364). IEEE.

106. Xiao, H., Wang, L., & Chang, J. (2022). The differential fault analysis on block cipher FeW. Cybersecurity, 5(1), 28.

107. Xiao, L., Xu, H., Zhu, F., Wang, R., & Li, P. (2020). SKINNY-based RFID lightweight authentication protocol. Sensors, 20(5), 1366.

108. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of things Journal, 4(5), 1250-1258.

109. Yang, Z. (2010). The development of the Internet of Things. J. Nanjing Univ. Posts Telecommun. Soc. Sci, 12, 8-9.

110. Yao, J. (2017). Optimisation of one-stop delivery scheduling in online shopping based on the physical Internet. International Journal of Production Research, 55(2), 358-376.

111. Zeinab, K. A. M., & Elmustafa, S. A. A. (2017). Internet of things applications, challenges and related future technologies. World Scientific News, 67(2), 126-148.

112. Zhang, W., & Qu, B. (2013). Security architecture of the Internet of Things oriented to perceptual layer. International Journal on Computer, Consumer and Control (IJ3C), 2(2), 37-45.

113. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2014). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive.

114. Zhang, Y., Zhao, L., & Qian, C. (2017). Modeling of an IoT-enabled supply chain for perishable food with two-echelon supply hubs. Industrial Management & Data Systems, 117(9), 1890-1905.

115. Zhou, W., & Piramuthu, S. (2015). IoT and supply chain traceability. In Future Network Systems and Security: First International Conference, Paris, France, June 11-13, 2015, Proceedings 1 (pp. 156-165). Springer International Publishing.

LIST OF PUBLICATIONS

1. Divya James & TKS Lakshmi Priya (2023). "An innovative approach for Dynamic Key Dependent S-Box to enhance security of IoT systems*". Measurement: Sensors*, 30, 100923, ISSN 2665-9174.

2. Divya James & TKS Lakshmi Priya. (2023). "An integrated IoT architecture to monitor nutrient level along the food supply chain." *Indian Journal of Nutrition and Dietetics*, Online ISSN: 2348-621X, Vol.60, No.1.

3. Divya James & TKS Lakshmi Priya (2023). "Security enabled IoT architecture for cold chain packaging applications." in *Proceedings of the International Conference on Emerging Trends in Industry 4.0 and Sustainable Concepts*, ISBN: 978-93-5782-946-5, pp.730-733.

4. Divya James & TKS Lakshmi Priya. (2021). An IoT-Based Traceability Framework for Small-Scale Farms. *In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020*, Volume 1 (pp. 841-851). Springer Singapore.

5. Divya James & TKS Lakshmi Priya. (2020). Improving the product services using IoT for controlling in-transit parameters. *Our Heritage*, ISSN 0474-9030, Vol-68, Issue-44.

6. Divya James, Alagusundari.N & TKS Lakshmi Priya (2019). "A top-down Survey on Security Aspects of the IoT." *International Journal of Innovative Research in Management, Engineering and Technology*, ISSN 2456-0448, Volume-4, Issue-6.

Avinashilingam Institute for HomeScience and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category 'A' by MHRD
Re-accredited with A++ Grade by NAAC, CGPA 3.65/4, Category I by UGC
Coimbatore - 641 043, Tamil Nadu, India

Appendix L2

(Item No 5 of Check List) Details of Research Publications

S.No	Article	Journal	Other Details Vol/No/Page No/ Year	Published in UGC-CARE / Scopus Indexed/ Web of Science
1	IMPROVING THE PRODUCT SERVICES USING IoT FOR CONTROLLING IN-TRANSIT PARAMETERS	OUR HERITAGE	VOL-68 ISSUE-44 FEBRUARY 2020	UGC-CARE
2	AN INTEGRATED IoT ARCHITECTURE TO MONITOR NUTRIENT LEVEL ALONG THE FOOD SUPPLY CHAIN	INDIAN JOURNAL OF NUTRITION AND DIETETICS	VOL-60 NO-1 JANUARY-MARCH 2023	UGC-CARE

*Proof of list of Journals from Internet to be attached along with copies of papers.

Scholar : MS. DIVYA JAMES Divyajames

Supervisor : Dr. TKS LAKSHMIPRIYA

Checked By:

HoD/ Dean of Respective School

24/7/2023

The scholar Miss. Divya James published her article in the following journals:

1. Our Heritage - indexed in UGC Care Group I from June 2019 to February 2020. The scholar published her article in February 2020 issue. This journal is multidisciplinary.
2. She published her article in "The Indian Journal of Nutrition and Dietetics" January - march 2023 issue. This journal title is indexed & active in UGC care Group I from January 2021 to present.

J. Jul

24.07.23.

Measurement: Sensors 30 (2023) 100923

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

An innovative approach for dynamic key dependent S-Box to enhance security of IoT systems

Divya James [a,*], TKS Lakshmi Priya [b]

[a] Dept.of CSE, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, 641 043, India
[b] Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, 641 043, India

ARTICLE INFO

Keywords:
Internet of things
Dynamic S-Box
Logistic map
Security
Cold chain

ABSTRACT

The Internet of Things (IoT) foresees pervasive and connected smart nodes that interact independently while offering varied services. Today, IoT nodes are a treasure house of data and hence security has become a major concern in IoT networks. Conventional cryptography faces many challenges during implementation in IoT devices. These challenges can be tackled by lightweight cryptography which is highly secure with less resource requirements. The vital characteristic of security is fulfilled by one out of 6 inner structures such as Substitution-Permutation Network, Feistel Network, General Feistel Network, Add-Rotate-XOR, Non Linear-Feedback Shift Register and Hybrid. PRESENT, which is a NIST approved lightweight cryptographic algorithm with SPN structure uses fixed or static S-Box. This permits attackers to explore S-Box and identify weaknesses of the algorithm. Key dependent approaches are better because it impedes an attacker from any offline analyses of attacks on the S-Box. Additionally, this is susceptible to linear and differential attacks. The static S Box does not possess superior diffusion and does not have a good rate of avalanche effect. So, the solution is to create a robust dynamic key dependent algorithm with nonlinear S-Boxes to secure the communication between IoT devices and platform. Security analysis is done on Non-linearity, Differential and Linear Cryptanalysis and Avalanche characteristics, besides, encryption of IoT data to demonstrate its aptness for cold chain security applications.

1. Introduction

Privacy and Information security is a rampant problem nowadays. Internet of Things consists of devices connected over a network in order to exchange data. As the number of connected devices increases, issues like confidentiality, integrity and data authenticity become major challenges. Hence, network security and data encryption have assumed great relevance today.

Cryptography is the process of data encryption-decryption that removes major challenges in Internet of Things network. Majority of the traditional cryptographic algorithms like Data Encryption Standard, Advanced Encryption Standard used today are developed for desktop and server contexts, making these unsuitable for small devices. The primary challenges in implementing conventional cryptography are: Low battery power (or no battery), fragile computational power, little physical space, limited memory (registers, RAM, ROM), and real-time reaction. Lightweight cryptography emphasizes on aspects like limited memory, low processing power, less power consumption, and real-time response while considering devices with limited resources. Therefore, lightweight encryption algorithms that provide fast and reliable encryption systems for resource constrained devices are considered [1]. Algorithms, designed and implemented according to memory footprint, execution time, security level and resource utilization form a particular set of algorithms called lightweight cryptography algorithms [2]. Furthermore, lightweight cryptography is applicable both to resource-constrained devices and resource-rich devices that it interacts with, like servers and smartphones. The physical cost and performance traits are met by the lightweight encryption algorithms through simplistic round functions on $\leq$ 64 bit using $\leq$80 bit key with easy scheduling.

The final characteristic of security is satisfied by utilizing any of 6 internal structures like Substitution-Permutation, Feistel or General Feistel Network, Add-Rotate-XOR, Non Linear-Feedback Shift Register or Hybrid for immunity against any security attack. Block ciphers and stream ciphers are 2 types of ciphers in plain text format wherein the former is encrypted into a block of bits and the latter is encrypted into

* Corresponding author.
E-mail addresses: 18pheop003@avinuty.ac.in (D. James), tkslp.csr@gmail.com (T.L. Priya).

https://doi.org/10.1016/j.measen.2023.100923
Received 8 June 2023; Received in revised form 13 September 2023; Accepted 7 October 2023
Available online 10 October 2023

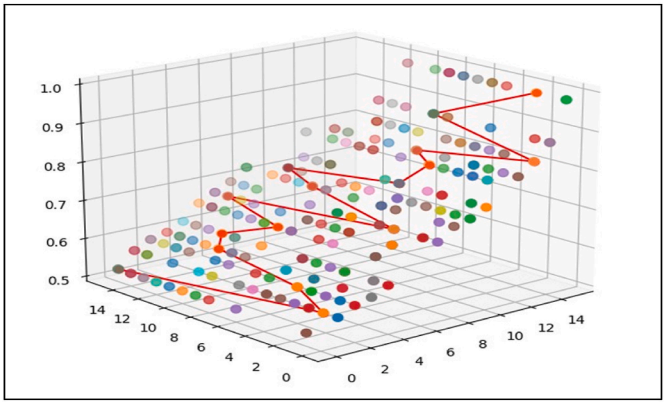


Fig. 1. 3D Non-Linear Representation of 16 × 16 SBox Generated with Chaotic Logistic map.

cipher symbol values. Data confidentially relates to encryption of digital data [3]. Modern block ciphers, like Advanced Encryption Standard and PRESENT are grounded on the Shannon principle of confusion and diffusion. The non-linear auxiliary table S-Box serves as the confusion component. The fixed or static S-Box enables the attacker to explore S-Box and identify its weaknesses. In this paper, an algorithm for the generation of robust S-Box is proposed that utilises another confusion technique while maintaining acceptable security with less overheads of memory and processing cost. Further, this can help develop a novel lightweight dynamic key dependent algorithm to secure the communication between IoT devices and platform for cold chain applications.

Logistic constraints, inaccessible warehouses, and closed consumer outlets, during COVID-19 pandemic, have badly affected supply chains especially in small scale cold chain sectors. This renders the need for simple and small-scale technological solutions that could monitor, manage, secure, and facilitate decision-making for reducing losses. The solution must be capable of utilizing IoTs in the pervasive smart phones that most small businesses in the unorganized sector possess. It must be able to integrate the power of cloud storage with the data handling capacity of hand-held devices via the Internet as the backbone, in a feasible manner. Thus, securing data becomes an essential requirement in such situations, and so simple security algorithms must be a part of the solution to be provided. Further, for data collection during transit, smart containers with sensors must be made an integral part of the system. Small business firms could then monitor, track, and receive notifications about their goods as they move along the cold chain.

The primary contribution of this research paper is:

1. Proposing algorithm for the generation of a robust 16 × 16 S-Boxes using Chaotic Logistic Map.
2. Developing a newly defined technique for generating Dynamic key dependent S-Box.
3. Analysing S-Boxes through performance parameters like Non-linearity, Differential & linear approximation probability and avalanche characteristics.

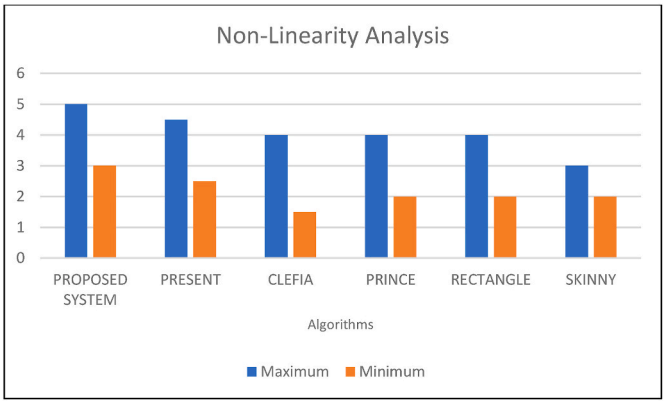


Fig. 2. Non-linearity analysis of SPN structure lightweight algorithms.

Section 2 deals with the relevant work regarding cryptographic algorithms and its limitations. Section 3 explains the recommended S-Box design for security enhancement of IoT system. Section 4 elucidates about performance analyses of recommended S-Box and Section 5, concludes with its future aspects.

2. Related work

A network of physically connected objects, appliances, and gadgets that have sensors, software, and connectivity is known as the "Internet of Things.". These gather and exchange internet data, enabling interaction with their environment and with each other. IoT works on four different components like devices, gateways, cloud service and applications [4]. These work together for enabling collection, communication, processing, and analysis of data in IoT systems. The basic components, architecture and enabling technologies of IoT are discussed herewith.

Three-layer architecture is the basic layered architecture for IoT, comprising [5] of Perception layer, Network layer and Application layer. This helps in modularizing and organizing the IoT system, by making it more manageable, scalable, and flexible. It also facilitates the development of interoperable and reusable components, to enable faster deployment of IoT solutions and promote ecosystem growth. IoT has varied applications across several industries. The essential features of Internet of Things (IoT) [6] in varied applications across several industries has been discussed. IoT's Technological components, can enhance the small-scale cold chain's efficiency, reduce risks, and ensure product quality throughout the supply chain.

Cryptography is a fundamental component of securing data and communications. This entails the conversion of plaintext (original data) into ciphertext (encrypted data) and vice versa using mathematical algorithms and methods. Several types of cryptography [7], serve different purposes and offering varying levels of security. Though the benefits are many when it comes to securing data and communications, this also brings with it certain limitations [8]. A lightweight scheme based on the Addition substitution and XOR is proposed for e-healthcare system security [9]. Many block cipher and stream cipher related lightweight algorithms are hereby proposed and evaluated [10].

Symmetric and asymmetric cryptosystems are two different categories of cryptosystems. Symmetric cryptosystem is further classified into 2 types - Block cipher and Stream cipher. Symmetric block ciphers are prevalent and easy to implement due to their operations like substitution, permutation, key addition and mixing which provide cryptographic strength [11]. Block ciphers are further divided into six internal structures, of which substitution permutation network can tweak data through substitution box and permutation table. AES is [12] a widely accepted symmetric encryption algorithm. However, it is not desirable for resource constrained devices as it requires large memory space and high power for computation.

There are many lightweight algorithms based on substitution and permutation network. Based on SPN structure, the present [13] employs a 64-bit block with 80-bit and 128-bit key versions. PRESENT has round key generation layer, substitution layer and permutation layer. It has a 4-bit fixed or static S-Box which enables attack on a single set of S-Box. RECTANGLE [14] is a lightweight block cipher with the operations like AddRoundKey, Substitution Column and Shift row. The total number of rounds are reduced to 25. GIFT [15] is simple with faster key scheduling algorithms. Two versions of GIFT are: 28 rounds of GIFT-64 using 64-bit blocks, and 40 rounds of GIFT-128 with 128-bit blocks. A SPN NETWORK called PRINCE [16] performs 64-bit input while using

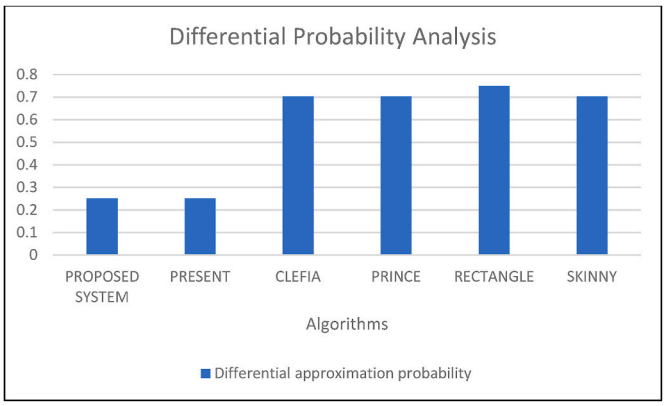


Fig. 3. Differential approximation probability analysis.

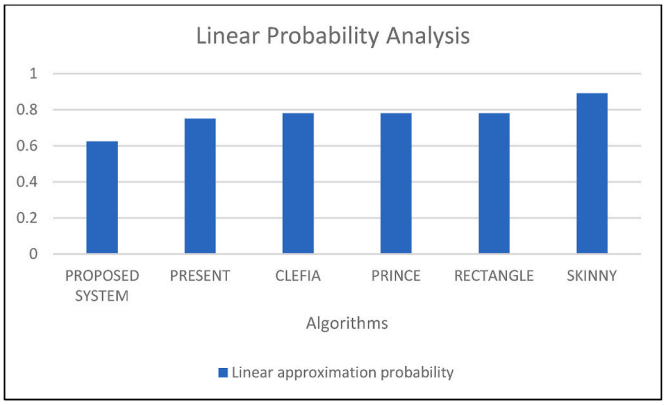


Fig. 4. Linear approximation probability analysis.

128-bit key. PRIDE [17] has 20 rounds with the introduction of linear layer which makes PRIDE more efficient. The inherent limitations of static S-Box used in Lightweight cryptography algorithms are elucidated [18]. Hence, most lightweight cryptographic algorithms use fixed or static S-Box which permit attackers to find the weak points within the algorithm.

There are many mathematical methodologies for the generation and creation of S-Box. Pratibha, A. [19], emphasized the importance of lightweight secure S- Box architectures for the IoT devices. Wu.et al. [20] uses the methodology of Latin square to generate S-Box. Farwa S recommended S-Box based on a fractional linear transformation for image encryption [21]. But many of these lack perfect cryptographic properties. Patidar, V. et al. [22] used chaotic logistic map to generate pseudorandom numbers. For image encryption, J. Ferdush et al. [23] suggested a standard architecture and technique based on Arnold and logistic chaotic maps. For Advanced Encryption Standards, Rahman, Z. et al. [24] used the chaotic and logistic Map-Based Key Generation Technique. Masood, F. et al. [25] suggested using Chen's chaotic system, Brownian motion, and the Henon chaotic map for encrypting medical images. So, chaotic logistic map has perfect cryptographic properties to generate a non-linear pseudorandom number. Shah T. et al. [26] analysed the power of S-Box through the manipulation of balance property, nonlinearity, both differential & linear approximation probability, and stringent avalanche criterion. Panchami, V. et al. [27] analysed parameters of S-Box of various Lightweight cryptographic algorithms. Jinhai Chen [28] has done an analysis of software and hardware performances of lightweight 8-bit S-Boxes. Panahi, P. et al. [29] discussed the specific encryption performance parameters of lightweight cryptographic algorithms. M. Matsui [30], Wang, Y. [31], used the parameters like non-linearity, linear cryptanalysis for measuring the performance of S-Boxes.

From the literature review, we could conclude that key dependent approaches are better because these impede an attacker from any offline analyses of an attack on a set of S-Box. Hence, we hereby propose a newly defined technique to generate dynamic key dependent S-Boxes.

3. Proposed system

This section details the method to generate a 16 × 16 proposed S-Box by utilizing chaotic logistic map. The main algorithm is elucidated in Section.3.1. The mode of selecting the Dynamic S-Boxes is described in Section. 3.2.

3.1. S-BOX generation

Logistic map a famous one-dimensional chaotic map, is iterated under specified conditions for generating this S-Box. The algorithm for generating S-Box is shown below. In mathematics, the definition is:

$$x_{n+1} = rx_n(1 - x_n)$$

where $0 < r \leq 4$ $x_n \in (0, 1]$. No matter what the value of x_0 is, x_n will decrease when r is given values between (0,1). Choose the initial values, $0 < r \leq 4$ ($r = 3.99$), $x_0 \in (0, 1)$. A combined chaotic map is iterated to produce chaotic sequences. The data range of chaotic sequences might increase their randomness and diversity due to the uniform distribution in the [0,1] interval. Chaotic Logistic map helps to generate a non-linear S-Box.

Algorithm. for 16 × 16 S-Box Generation

Algorithm for 16 * 16 S-Box Generation

Start

1. Let x=0
2. Let u = 3.99, d = a random number between [0,1]
3. Let ray [] = []
4. While x<16
    a. d = u*d*(1-d)
    b. r = rounded value of (d*16) %16
    c. If r is not in ary
        i. Append r to ary
    d. X = x+1
5. End Loop

Stop

3.2. Dynamic S-Box Selection

The selection of an SBox for each round of algorithm is based on a dynamic basis. This is performed in PRESENT algorithm, where round key generation is the same, though the S-Box for each round is different. The algorithm is described below:

Algorithm. for Dynamic S-Box Selection

Start

1. Master Key, K =K_{79}, K_{78} ....K_0
2. Import key, rounds, Sbox_temp, Sbox_n, Sbox from main function
3. i = 1
4. While i<rounds+1
   a. Right shift key by 16 and append it to round keys
      [Round keys are $K_{i=}K_{63}$, K_{62},..$K_{0=}K_{79}$,K_{78}....K_{16}]
   b. Let k be the last round key
   c. Let x=0, i=0
   d. Extract 8,16, 24, 32, 40, 48, 56, 64 bits and store it in x as a 4-bit number that has bit 0 = (8th XOR 16th), bit 1 = (24th XOR 32nd), bit 2 = (40th XOR 48th), bit 3 = (56th XOR 64th)
   e. Store Sbox[x] in Sbox_temp
   f. Append Sbox_temp to Sbox_n
   g. For each round the key register is updated thus:
      i. $[K_{79}K_{78}\ldots\ldots K_1K_0] = [K_{18}K_{17}\ldots\ldots\ldots K_{20}K_{19}]$
      ii. $[K_{79}K_{78}K_{77}K_{76}] = S[K_{79}K_{78}K_{77}K_{76}]$
      iii. $[K_{19}K_{18}K_{17}K_{16}K_{15}] = [K_{19}K_{18}K_{17}K_{16}K_{15}] \oplus round\_counter$
5. End Loop
6. Output round keys to main function

Stop

This shows that maximum non linearity achieved by these S-Boxes in GF (2^4) is 6. Maximum non linearity of Dynamic S-Box obtained is 5. The 3D representation of 16 × 16 S-Box generated using Chaotic Logistic Map is in Fig. 1. Each S-Box contains 16 integer values where a line is plotted for a single S-Box value. Since it is perfectly non-linear, points are not giving a straight line wherein relationship between the points is non-linear.

Fig. 2 shows the non-linearity analysis of SPN structure lightweight algorithms. It is evident from Fig. 2 that our suggested S-Box has a maximum Nonlinearity of 5. To withstand linear cryptanalysis, its nonlinearity must be sufficiently high. The investigation reveals that our suggested S-Box offers a maximum nonlinearity of 5, which is higher than that of any other lightweight S-Box. The recommended S-Box has a minimum nonlinearity of 3, which is lesser for all other lightweight S-Boxes.

4. Performance analysis

Since fixed or static S-Box of PRESENT algorithm permits attackers to investigate S-Box and identify weaknesses of the algorithm, a non-linear S-Box is generated using Logistic Chaotic Map. Nonlinearity, Strict Avalanche Effect, Differential and Linear Approximation Probability are all taken into consideration during the analysis.

4.1. Non-linearity

Let Boolean function f be a bent function on F_2^4 then function f has maximum Nonlinearity [26] achieved when n is even:

$N_f\ (max) = 2^{n-1} - 2^{n/2-1}$

4.2. Differential approximation probability

Differential approximation probability of an S-Box [26,27] is measure for Differential Uniformity:

$$DP(\Delta x \rightarrow \Delta y) = \frac{\#\left\{x \epsilon \frac{X}{S(x)} \bigoplus S(x \bigoplus \Delta x) = \Delta y\right\}}{2^n}$$

Where Δx and Δy are input and output differentials for all the possible

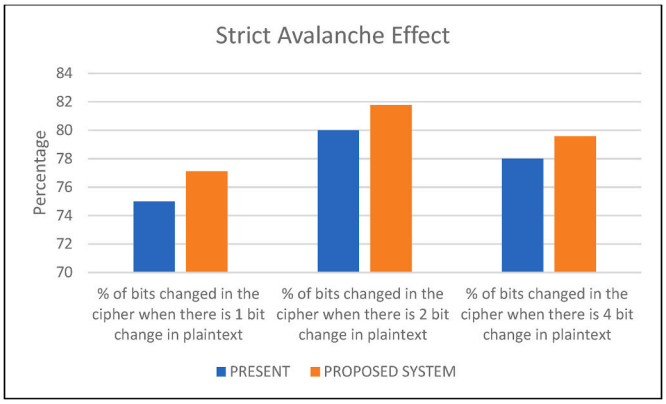


Fig. 5. Strict Avalanche Effect w. r.t Plain text to Cipher Text.

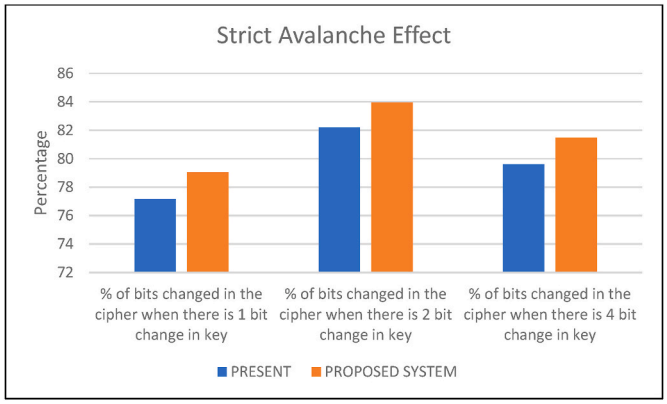


Fig. 6. Strict Avalanche Effect w. r.t Key to Cipher Text.

inputs 2^n

Differential uniformity, also known as differential delta uniformity, is the greatest value in the Differential distribution table. The ideal differential bound (highest differential in each S-Box) is differential probability = 0.25 for 4 × 4 S-Boxes. In Fig. 3, the results of the application of input and output differentials to the most likely output XOR of the suggested S-Box are shown. Matrix maximum is 4/16 = 0.25, demonstrating the great resilience of the suggested S-Box to support this differential technique.

4.3. Linear approximation probability

The highest degree of an event's dissimilarity is represented by this Linear Approximation Probability (LP) [27]:

$$\mathrm{LP} = \max \left| \frac{\#\{x/x.\Gamma x = S(x).\Gamma y\}}{2^n} - \frac{1}{2} \right|$$

Where Γ_x is input mask; Γ_y output mask and x input vector of all possible inputs 2^n

The S-Box's nonlinear property will be stronger the less the chance of linear approximation. Fig. 4 Demonstrates that this S-Box's LP value is lower than values for other S-Boxes, allowing for stronger resistance to linear cryptanalysis.

4.4. Strict avalanche effect

Strict avalanche criterion (SAC) was first advocated in 1986 by Webster and Tavares [26]. Fig. 5 shows the Strict Avalanche Effect w. r.t Plain text to Cipher Text. More than 77 % output probability bit changes, when there is a one bit, two bit and four-bit change in plaintext.

Fig. 6 shows the Strict Avalanche Effect w. r.t Key to Cipher Text. More than 78 % output probability bit changes, when there is a one bit, two bit and four-bit change in key.

5. Conclusion

This paper hereby proposes the dynamic S-Box generation mode based on chaotic maps. Then we introduce selection of S-Box for each round using the round key, which evolves S-Box towards optimal direction. Through experimentation and comparison, with earlier works, the conclusion is that this S-Box has strong nonlinearity, both differential & linear approximation probability, and strict avalanche effect. Hence this can resist any linear or differential attack. Besides, S-Box can be applied on IoT data for cold chain packaging and other fields. The proposed system can help in encryption and decryption of IoT Data for cold chain applications.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Vishal A. Thakor, Mohammad Abdur Razzaque, Muhammad RA. Khandaker, Lightweight cryptography algorithms for resource-constrained IoT devices: a review, comparison and research opportunities, IEEE Access 9 (2021) 28177–28193.

[2] D. Aakash, P. Shanthi, Lightweight security algorithm for wireless node connected with IoT, Indian J. Sci. Technol. 9 (2016) 1–8, https://doi.org/10.17485/ijst/2016/v9i30/99035.

[3] Asim Ali, et al., A novel systematic byte substitution method to design strong bijective substitution box (S-box) using piece-wise-linear chaotic map, Peer J. Comput. Sci. 8 (2022), e940.

[4] V. Choudhary, S. Tanwar, A concise review on internet of things: architecture and its enabling technologies, Comput. Int. Eng. Manag. Appl.: Select Proc. CIEMA 2022 (2023) 443–456.

[5] Vandana Choudhary, Sarvesh Tanwar, A concise review on internet of things: architecture and its enabling technologies, Comput. Int. Eng. Manag. Appl.: Select Proc. CIEMA 2022 (2023) 443–456.

[6] Harsh Dadhaneeya, K. Prabhat, Nema, and Vinkel Kumar Arora. "Internet of Things in Food Processing and its Potential in Industry 4.0 Era: A Review, Trends in Food Science & Technology, 2023.

[7] Shahzad Ahmed, Tauseef Ahmed, Comparative Analysis of Cryptographic Algorithms in Context of Communication: A Systematic Review, 2022.

[8] Subhash Chander, Lightweight cryptography algorithms for security of IoT devices: a survey, IRJET (2022) 842–850.

[9] Kakali Chatterjee, Ravi Raushan Kumar Chaudhary, Ashish Singh, A lightweight block cipher technique for IoT based E-healthcare system security, Multimed. Tool. Appl. 81 (30) (2022) 43551–43580.

[10] Muhammad Rana, Quazi Mamun, Rafiqul Islam, Lightweight cryptography in IoT networks: a survey, Future Generat. Comput. Syst. 129 (2022) 77–89.

[11] Abdul Razaq, et al., A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups, IEEE Access 8 (2020) 75473–75490, https://doi.org/10.1109/ACCESS.2020.2989676.

[12] Chom Thungon, Leki, Nurzaman Ahmed, Md Iftekhar Hussain, Comparison of aes and present block cipher for 6LoWPAN based internet-of-things, Int. J. Comput. Int. IoT 1 (2018) 2.

[13] Andrey Bogdanov, et al., PRESENT: an ultra-lightweight block cipher, in: Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9, Springer Berlin Heidelberg, 2007.

[14] Wentao Zhang, et al., RECTANGLE: a Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms, Cryptology ePrint Archive, 2014.

[15] Subhadeep Banik, et al., GIFT: a small present: towards reaching the limit of lightweight encryption, in: Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, Springer International Publishing, 2017.

[16] J. Borgho, et al., Prince-a Low-Latency Block Cipher for Pervasive Computing Applications-Proc. of Advances in Cryptology, 2012, pp. 208–225.

[17] Martin R. Albrecht, et al., Block ciphers–focus on the linear layer (feat. PRIDE), in: Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I 34, Springer Berlin Heidelberg, 2014.

[18] Samih M. Mostafa, Ibrahim M. Darwish, Mohamed R. Saadi, Improved lightweight security approach routing protocol in internet of things, Internet of Things 11 (2020), 100208.

[19] A. Prathiba, V.S. Kanchana Bhaaskaran, Lightweight S-box architecture for secure internet of things, Information 9 (1) (2018) 13.

[20] Yue Wu, P. Joseph, Noonan, Sos Agaian, Dynamic and implicit Latin square doubly stochastic s-boxes with reversibility, in: 2011 IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 2011, https://doi.org/10.1109/ICSMC.2011.6084188.

[21] Shabieh Farwa, Tariq Shah, Lubna Idrees, A highly nonlinear S-box based on a fractional linear transformation, SpringerPlus 5 (1) (2016) 1–12, https://doi.org/10.1186/s40064-016-3298-7. PMID: 27730020; PMCID: PMC5037109.

[22] Vinod Patidar, Krishan K. Sud, Narendra K. Pareek, A pseudo random bit generator based on chaotic logistic map and its statistical testing, Informatica 33 (2009) 4.

[23] Jannatul Ferdush, Mahbuba Begum, Mohammad Shorif Uddin, Chaotic lightweight cryptosystem for image encryption, Adv. Multimed. 2021 (2021) 1–16.

[24] Ziaur Rahman, et al., Enhancing AES using chaos and logistic map-based key generation technique for securing IoT-based smart home, Electronics 11 (7) (2022) 1083.

[25] Fawad Masood, et al., A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations, Wireless Pers. Commun. 127 (2) (2022) 1405–1432.

[26] Tariq Shah, Ayesha Qureshi, S-box on subgroup of Galois field, Cryptography 3 (2) (2019) 13, https://doi.org/10.3390/cryptography3020013.

[27] V. Panchami, Mahima Mary Mathews, A substitution box for lightweight ciphers to secure internet of things, J. King Saud Univ.- Comput. Inf. Sci. 35 (4) (2023) 75–89.

[28] Jinhai Chen, et al., A comprehensive analysis of lightweight 8-bits boxes from iterative structures, J. Inf. Secur. Appl. 70 (2022), 103302.

[29] Pejman Panahi, et al., Performance evaluation of lightweight encryption algorithms for IoT-based applications, Arabian J. Sci. Eng. 46 (2021) 4015–4037, https://doi.org/10.1007/s13369-021-05358-4.

[30] Mitsuru Matsui, Linear cryptanalysis method for DES cipher, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer Berlin Heidelberg, Berlin, Heidelberg, 1993.

[31] Yong Wang, Peng Lei, Kwok-Wo Wong, A method for constructing bijective S-box with high nonlinearity based on chaos and optimization, Int. J. Bifurcat. Chaos 25 (10) (2015), 1550127.

The Indian Journal of Nutrition and Dietetics
ISSN: 0022-3174; eISSN: 2348-621X
www.ijndonline.org

DOI:10.21048/IJND.2023.60.1.29955

An integrated IoT Architecture to Monitor Food Quality along the Supply Chain

Divya James[1] and Lakshmi Priya, T.K.S.[2]

(1. Department of CSE, 2. Professor, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore - 641 043, India)

E-mail: 18pheop003@avinuty.ac.in

(Received 12th April, 2022)

Abstract

Drop in nutrition value during food logistics impacts the health of consumers. Vegetables, fruits, fish, milk lose nutrients during logistics if it is not properly monitored. Real-time tracking and monitoring, large data handling and secure business transactions are key to the effective operation of supply chains. The COVID-19 pandemic has taught us the need for handling unforeseen situations in various sectors. Limitations to logistic operations, inaccessible warehouses, shutdown of consumer outlets for an unexpected duration, have affected the supply chain drastically. This has laid emphasis on the need for technology-based solutions that can monitor, control and make quick decisions, that can reduce losses. With this scenario as a background, a system architecture has been proposed to detect the nutrient value of food by periodically monitoring temperature and humidity in real-time and alerting the cold chain entities in cold chain environments. This architecture is proposed as an integration of Internet of Things (IoT) with cloud-based storage, to provide real-time data collection at the end-user, seamless storage and computation in the cloud and secure transactions at the business layer. An experimental setup of the system architecture has been configured and the implementation has been tested at a preliminary level. The performance of the application is analyzed and the proposed web application is efficient for large scale supply chain applications, provided scaling of hardware resources.

Keywords: *Supply chain management, nutrients, cold chain, internet of things, cloud, security*

Introduction

Nutrients help to make energy, growth of all organisms, growth of brain and body parts. The food we eat is a major source of nutrients. Rapid spreading of COVID-19 and the post health issues shows the importance of eating food having high nutrition. Balanced diet includes vitamins, proteins, minerals, fats etc. and physical activity which is very essential to keep body healthy. Balanced diet is one which

includes all nutrients required for the body in right quantity on regular intervals. Nutrient content of the food is at most important to keep us healthy and protect from diseases. Eating more food than required for the body creates more calories that eventually convert into fat and weight gain. Also eating too less creates weight loss. Vegetables, fish, meat, milk, egg, fruits give nutrients required for the body. Nutrient content in food can be preserved by freezing, dehydration and pasteurization. Cooking methods like microwave, steaming is nutrient friendly. It is important to monitor the nutrient contents of food items in farming, transportation, distribution units. Supply Chain Management plays a key role to detect the nutrient contents starting from farm units to end user. The temperature controlled supply chain system, referred to as the *Cold Chain*, is the current trend and its application areas include frozen products like ice-creams, seafood, poultry, chilled products like vegetables, fruits and pharmaceuticals products like vaccines. Cold chain industry still lacks end-to-end visibility and cross-functional collaboration.

In this paper, an architecture for the cold chain that will periodically monitor temperature and humidity in real-time is proposed and notify the cold chain entities to changes in the food's nutritional value. A prototype of the system has been developed to demonstrate the architecture.

The paper is structured as follows: Section II briefs the importance of nutrient contents in food, survey of Supply Chain Management literature and the technology gaps in Supply Chain Management which open up the scope for research and development. The proposed integrated system architecture for cold chain is introduced in Section III followed by the prototype implementation in Section IV. Section V describes the performance analysis and the paper concludes with pointers to future prospects.

Proposed integrated system architecture for Cold Chain - SiC-chain

In this section, an integrated system architecture to solve the challenges in monitoring the nutrients and alarming the cold chain entities is proposed with its key features. The proposed architecture harnesses the power of the existing matured technologies (namely Internet of Things and Cloud) and security features in order to monitor the cold chain eco-system, a state-of-the-art system, which can overcome the challenges in monitoring the nutrient parameters in cold chain systems.

Key features of the proposed architecture

Preservation of nutrients using Internet of Things

This feature enables to monitor the nutrient parameters in real time and alarm the cold chain entities. With real-time tracking, Internet of Things devices can automatically flag shipments, alert Supply Chain Management entities and help to maintain the nutrient content of the food.

Securing the nutrient values

Nutrient parameters collected using Internet of Things devices are important to be secured in transit. Food nutrient is most critical for humans, so security of nutrient values in transit is important. To secure the nutrient parameters and communication, certificate and token-based authentication along with Transport Layer Security for Internet of Things devices is enabled within supply chain entities.

Storage of nutrient parameters

In a cloud environment, storage and computing are no more a burden to the supply chain nodes. Using cloud services nutrient parameters are always accessible for Supply Chain Management entities which is important for Supply Chain Management entities to take decision.

This architecture is proposed as an integration of Secure - Internet of Things and Cloud for the cold chain environment and therefore named as *SiC-chain.*

A. Architecture

The SiC-chain architecture consists of four layers: (i) SiC-chain Sensing layer (ii) SiC-chain Networking Layer (iii) SiC-chain Data Processing Layer (iv) SiC-chain Application Layer as described in Figure 1.

(i) *SiC-chain Sensing layer*

This layer uses sensors for monitoring the parameters of food. In cold chain entities, data sensing and collection tasks in real-time are carried out by the devices in sensing layer. The Internet of Things devices are trusted as each device in Supply Chain Management is authorized by the Device Type and unique Device ID.

(ii) SiC-chain Networking layer

This layer transmits the nutrient parameters collected in real time from the *SiC-chain* sensing layer to next higher layer – the *SiC-chain* data processing layer. The Internet of Things devices are authenticated by auto-generated authentication token.

SiC-chain data processing layer

This layer constitutes the cloud-based web services for cold chain environment. It is responsible for storage of parameters so that cold chain entities can see the nutritent values and it is accessible anytime.

SiC-chain application layer

In our architecture, this layer shares necessary interfaces like a smart real-

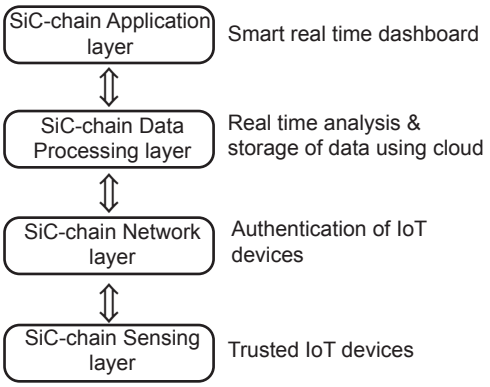


Figure 1
Proposed *SiC-chain* layered architecture

time dashboard. This layer includes an intelligent platform or dashboard for real-time monitoring of nutrient parameters.

B. Layers and technological elements of SiC-chain

Supply chain activities can be automated using the integrated architecture, *SiC-chain.* The mapping of layers and technological elements in the proposed architecture at the entities of the cold chain, is described below:

Mapping of SiC-chain sensing layer into Supply Chain Management

The real-time data from Internet of Things devices like temperature, humidity, moisture and bacteria sensors can be used to monitor the environmental factors and thereby maintaining the quality of the food materials. These sensors in conjunction with the Global Positioning System module track the location, and protect Supply Chain Management system from external intervention. Table I lists sample Internet of Things devices that can deploy to detect the parameters in the supply chain.

Mapping of SiC-chain Networking layer into Supply Chain Management

The *SiC-chain* networking layer consists of hardware, software and messaging protocols. The real-time payload from the Internet of Things devices say, nutrient parameters is passed to the *SiC-chain* data processing layer through the messaging protocol Message Queuing Telemetry Transport over WiFi *via* the Network layer. Here in Supply Chain Management, each device has a unique device ID and once the device is authenticated, the real-time data is passed to the cloud-based web services. The message flow of Message Queuing Telemetry Transport protocol is shown in the Figure 2.

TABLE I

Sample Sensors for Preserving the Nutrients on *SiC-chain*

Supplier	Manufacturer	Wholesaler	Retailer	Consumer
● Temperature sensor ● Humidity sensor ● Moisture sensor ● Bacteria sensor ● RFID tags ● GPS module	● Temperature sensor ● Humidity sensor ● Light intensiry sensor ● Proximity sensor ● pH sensor ● Load sensor ● Bacteria sensor ● RFID tags ● GPS module	● Gas sensor ● Smoke sensor ● Electrochemical sensor ● Colorimetric freshness sensor ● Embedded machine sensors ● Vibration sensor ● Chemical sensor ● Shock sensor ● Pressure sensor ● IoT enabled camera	● Gas sensor ● Flame detector ● Ultrasonic sensor ● Tilt sensor ● IR sensors ● RFID tags ● Smoke sensor ● Vibration sensor ● Acelerometer ● Temperature sensor ● GPS module ● IoT enabled cameras	● RFID tags ● GPS module ● Camera

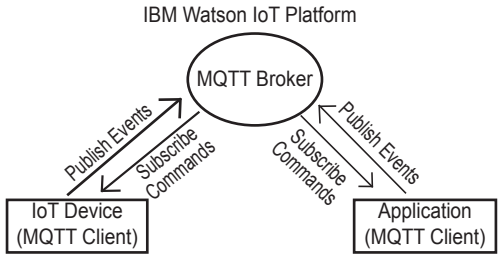


Figure 2

Message flow of MQTT protocol in *SiC-chain*

Mapping of SiC-chain Data Processing layer into Supply Chain Management

The real-time information like the nutrient parameters received in the *SiC-chain* data processing layer is stored in persistent Cloudant database. Figure 3 shows interaction for seamless storage of *SiC-chain* between supplier and manufacturer.

Mapping of SiC-chain Application layer into Supply Chain Management

The *SiC-chain* application layer is the user-oriented layer. All the supply chain entities require a dashboard to interact within *SiC-chain* architecture, application layer provides a smart real time dashboard. All the Supply Chain Management entities can access the application through their smart phones, Personal Digital Assistant and laptops. Figure 4 shows the smart real-time dashboard for Supply Chain Management entities.

C. Operations of SiC-chain

For effective and smooth working of the *SiC-chain* environment, the following operations have been identified and formalized for the *SiC-chain* environment: (i) Enrollment and (ii) Secure communication of data between the Internet of Things devices and platform.

Enrollment: In the proposed architecture, suppliers, manufactures, wholesalers, retailers and consumers can enroll in the application. There are four entities: client application, authentication service, server and cloudant database. Supplier registers with the authentication service by providing email and password. The authentication service sends a token back to the supplier. This token along with

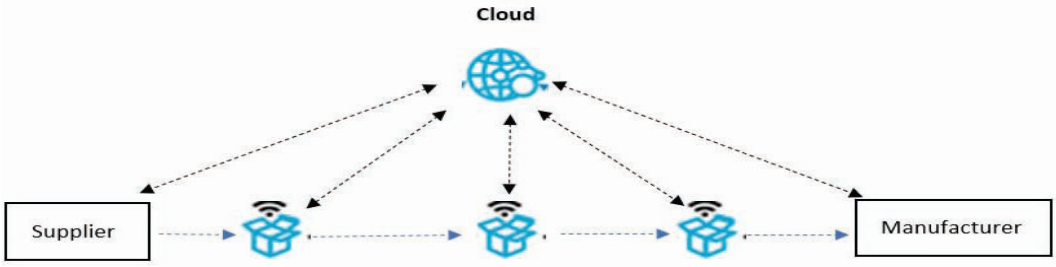


Figure 3

Interaction for seamless storage of data in *SiC-chain*

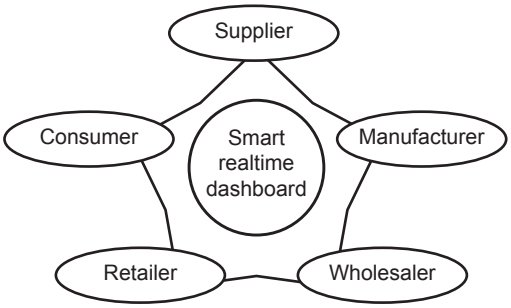


Figure 4
Smart real time dashboard in *SiC-chain*

user data is sent to the server using an Application Programming Interface Call. The node.js server extracts and validates the token with the authentication service. Once the token is validated, the user data is stored in the database.

Figure 5 shows the timing diagram for enrollment of supply chain entities. All the enrolled supply chain entities can view the dashboard.

Secure communication: Internet of Things devices initially registers with the Watson Internet of Things platform which serves as the Message Queuing Telemetry Transport broker. Once the Wi-Fi connection is established, a self-signed certificate is generated by openSecure Sockets Layer. This certificate is stored on the device and the Internet of Things platform, which is verified when connection is established. Devices are connected to Watson Internet of Things platform using device ID and token-based authentication mechanism. IBM cloud platform subscribe to a topic *via* Message Queuing Telemetry Transport broker which is published by

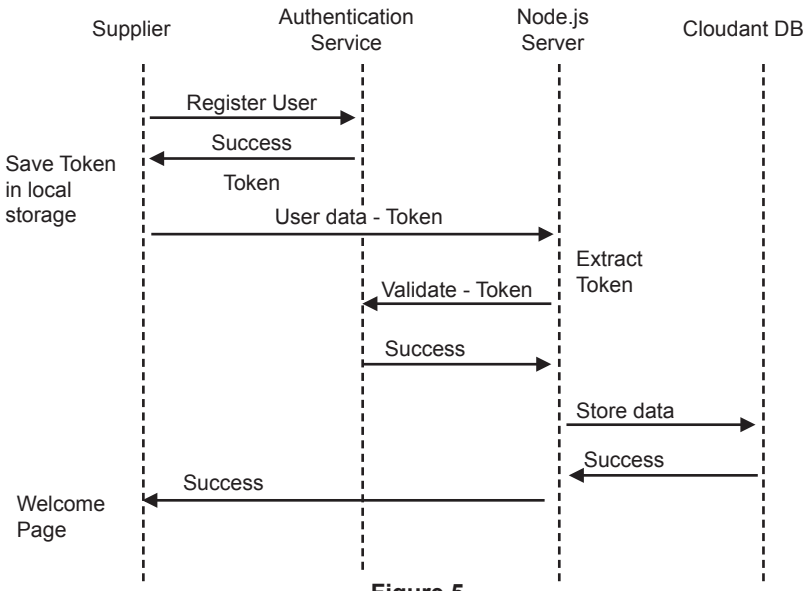


Figure 5
Timing diagram for enrollment of supply chain entities

the Internet of Things device. The nutrient parameters are stored in cloudant database and can be seen in smart dashboard.

Implementation

Implementation environment of SiC-chain

At the implementation side we have Supply Chain Management entities, cloud and Internet of Things network. Supply Chain Management entities include suppliers, manufacturers, wholesalers, retailers and consumers. Internet of Things sensors are used to collect environmental conditions in real time. The temperature and humidity values are pushed to cloud through Message Queuing Telemetry Transport over HTTP protocol. These values are sent to the persistent *Cloudant NoSQL* Database. The data is fetched to real time dashboard along with other parameters where the entities of supply chain can achieve transaction level trust and data transparency. The implementation environment of *SiC-chain* is depicted in Figure 6.

TABLE II

Development Technologies for the *SiC-chain* Architecture

Component	Description
Hardware	ESP8266 (NodeMCU board)
Memory	12GB
Operating System	Windows
Library and Framework	WIFI Client, PubSubClient, IBM Watson IoT Platform, NodeRed
Sensors	Temperature and Humidity sensors
IDE	Arduino 1.8.19
DBMS	IBM NoSQL Cloudant
Programming language	Node.js, React

Development technologies

Table II describes the development technologies for implementing *SiC-chain* architecture.

Results and Discussion

This section explains the results obtained in the prototype.

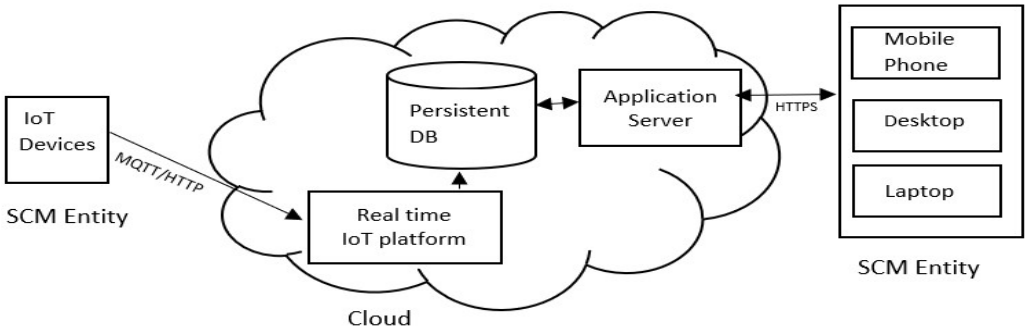


Figure 6
Implementation environment of *SiC-chain*

Real Time Data Collection

The hardware implementation set up is depicted in Figure 7.

As shown in Figure 7, temperature and humidity sensors are connected to ESP8266 module. The ESP8266 is connected to PC *via* USB cable. The integrated development environment used is Arduino Integrated development environment where the program is executed and temperature and humidity payload is displayed. It is published in IBM Watson Internet of Things platform through Message Queuing Telemetry Transport protocol via WIFI Client library.

Secure communication between the device and Internet of Things platform using Secure Sockets Layer / Transport Layer Security

In order to secure communication between the devices and Internet of Things platform, a self-signed certificate is generated for Message Queuing Telemetry Transport traffic, added them to the Internet of Things Watson platform and the ESP8266 code, for enabling an Secure Sockets Layer/Transport Layer Security connection, server certificate is verified against the root CA certificate installed on the ESP8266. The ESP8266 code verifies the certificate details, establishes the connection and displays the real time temperature and humidity value in Arduino Integrated development environment.

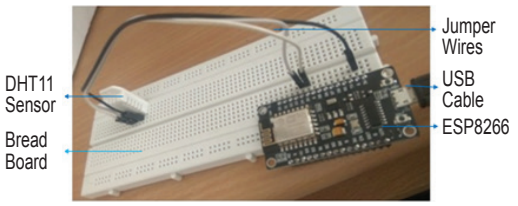


Figure 7
Hardware implementation setup

Data Processing and Storage

The Internet of Things platform uses open-source Message Queuing Telemetry Transport protocol to allow devices and applications to connect to the Internet of Things platform. Node-RED can receive the data that was transmitted from the device over Message Queuing Telemetry Transport to Watson Internet of Things Platform. It helps to store the data in Cloud Storage.

Time

Throughput is the number of packets that successfully reach at their destinations[27]. Table III describes the throughput for valid read/write operations.

Storage Space

Documents stored in cloud includes JSON documents and indexes. In order to store 10 JSON documents, it requires around 36KB of storage space. Considering the above, the total space required for the

TABLE III
Throughput for Read / Write Operations

Operations	Requests	Throughput
Reads	20	11 ops/sec
Writes	10	10 ops/sec

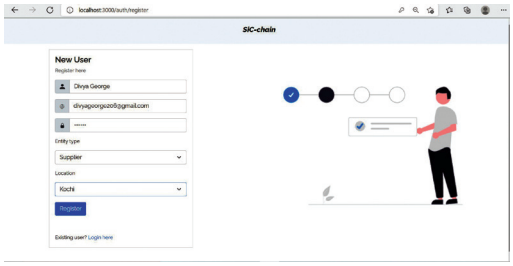


Figure 8
New User Registration

application is less than 1GB of cloud data storage. This storage space can increase depending on the increase of suppliers and manufacturers.

Smart Dashboard

Figure 8 illustrates sample screenshot of the dashboard.

TABLE IV
Performance Test Cases

Test Case ID	Transaction Name	Step Description	Expected Output
TC_001	Supplier_login	1. Open brower 2. Enter URL 3. Enter valid E-mail & Password 4. Click Login button	Supplier should be landed on *SiC-chain* login page and should be logged in successfully
TC_002	Supplier_List_fish	Supplier click on List Fish menu	All Fishes are listed
TC_003	Supplier_Add fish	Suppler clicks Add Fish menu, enter fish details, click Add button	Add fish page is displayed and fishes added to supplier database
TC_004	Supplier_LogOut	Supplier clicks the logout menu	Supplier should be logged out successfully
TC_005	Manufact_Login	1. Open browser 2. Enter URL 3. Enter valid E-mail & Password. 4. Click Login button	Manufacturer should be landed on *SiC-chain* login page and should be logged in successfully
TC_006	Manufact_List_Fish	Manufacturer click List Fish	All Fish details are listed
TC_007	Manufact_All Supplier	Manufacturer click All Suppliers	Manufacturer click All Suppliers link to view all suppliers
TC_008	Manufact_Add_to_ favourite	Manufacturer select favorite suppliers and add to favorites	Manufacturer can add favourite suppliers to list
TC_009	Manufact_Buy_Fish	Manufacturer click Buy	Manufacturer can add favourite supplies to list
TC_010	Manufact-My Inventory	Manufacturer click List Fish menu	All Fishes bought by manufacturer are seen in inventory
TC_011	Manufac_LogOut	Manufacturer clicks Logout menu	Manufacter should be logged out successfully

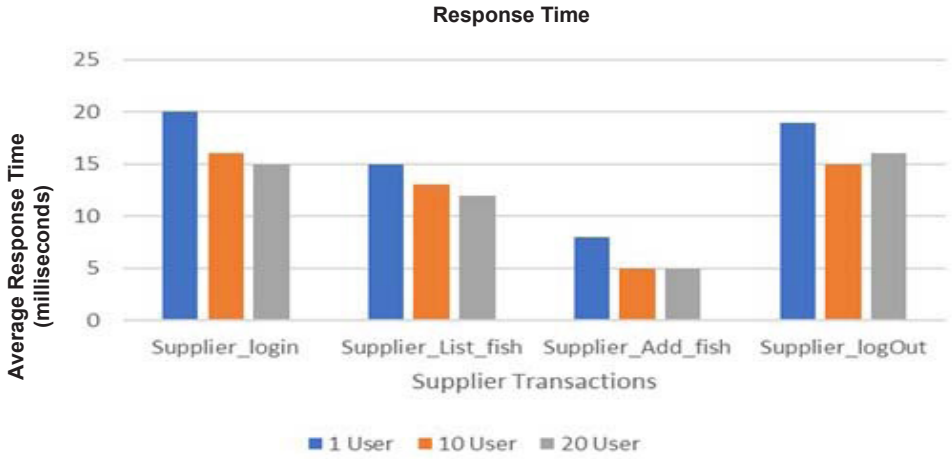


Figure 9

Response time of the supplier transactions

Performance analysis

This section presents performance analysis of proposed *SiC-chain* architecture. Here performance testing is run using Apache JMeter. Apache JMeter[28] is a testing tool used to analyze and measure the performance of applications.

To calculate response time, every request and response generated by the HTTP protocol are recorded using Apache JMeter. JMeter generates requests to target servers and simulate the number of users. The overall running time of test is set as 60 minutes.

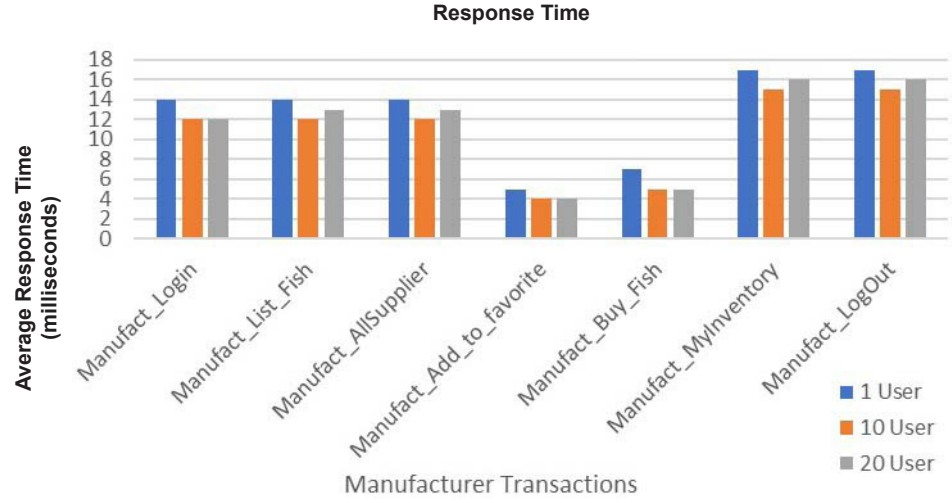


Figure 10

Response time of the manufacturer transactions

TABLE V

Throughput for Supplier and Manufacturer Transactions

Transactions	No. of users	Throughput (per second)
Supplier	1	0.38782
	10	3.68286
	20	7.27128
Manufacturer	1	0.57184
	10	5.30609
	20	10.34536

(i) Response Time

The response over time is calculated by using the request-responses collected from JMeter. Factors affecting response time are network bandwidth, user count, queries submitted. Elapsed Time is the time elapsed from the start of the test, which is displayed in hours, minutes and seconds.

The performance test cases for *SiC-chain* website are shown in Table IV.

Apache JMeter measures the elapsed time from the start of the test, which is displayed in hours, minutes, and seconds. Performance test is executed for a period of 60 minutes and infinite iterations are considered. It means elapsed time of the test is 60 minutes. Response Time is recorded against elapsed time. From Figure 9, even though we have increased the users from 1 to 10 to 20, after performing the load test, web application is giving a consistent response time for supplier transactions.

The test cases for manufacturer transactions are depicted in Table IV. The test is executed for a period of 60 minutes.

From the Figure 10, even though we have increased the users from 1 to 10 to 20, after performing the load test, web application is giving a consistent response time for manufacturer transactions.

Throughput

Table V shows throughput for supplier and manufacturer transactions for 1 user, 10 users and 20 users.

The response time and throughput remain almost same when performance test is run for 1 user, 10 users and 20 users. The proposed web application is efficient for large scale supply chain applications, with scaling of hardware resources.

Conclusion and Future Prospects

An architecture for the cold chain has been proposed to detect nutrient value of food by periodically monitoring certain parameters in real-time and alerting the cold chain entities. The Internet of Things allows real-time traceability and sharing of product movement throughout the Supply Chain Management. The Message Queuing Telemetry Transport protocol used in conjunction with Transport Layer Security helps to secure the communication between devices and Internet of Things platform. Cloud technology enhances

the overall performance through efficient resource usage, flexibility and system scalability. In future we will be focusing to secure the messages while transferring the data thereby maintaining confidentiality in a supply chain channel.

REFERENCES

1. Richey, R.G., Roath, A.S., Adams, F.G. and Wieland, A. A responsiveness view of logistics and supply chain management. *J. Business Logistics*, 2022, **43**, 62-91.
2. Birkel, H. and Müller, J.M. Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability–A systematic literature review. *J. Cleaner Produc.*, 2021, **289**, 125612.
3. Amiri, S., Moghanjougi, Z.M., Bari, M.R. and Khaneghah, A.M. Natural protective agents and their applications as bio-preservatives in the food industry: An overview of current and future applications. *Italian J. Fd. Sci.*, 2021, **33**, 55-68.
4. Bibi, F., Guillaume, C., Gontard, N. and Sorli, B. A review: RFID technology having sensing aptitudes for food industry and their contribution to tracking and monitoring of food products. *Trends in Food Science and Technology*, 2017, **62,** 91-103.
5. Ahmed, M., Rahaman, M.O., Rahman, M. and Kashem, M.A. (2019, December). Analyzing the Quality of Water and Predicting the Suitability for Fish Farming based on IoT in the Context of Bangladesh. In *2019 International Conference on Sustainable Technologies for Industry 4.0* 2019, 1-5, IEEE.
6. Mercier, S., Villeneuve, S., Mondor, M. and Uysal, I. Time-temperature management along the food cold chain: A review of recent developments. *Comprehensive Reviews in Food Science and Food Safety*, 2017, **16**, 647-667.
7. Pebdeni, A.B., Roshani, A., Mirsadoughi, E., Behzadifar, S. and Hosseini, M. Recent advances in optical biosensors for specific detection of E. coli bacteria in food and water. *Fd. Control*, 2022, 108822.
8. Singh, J. and Singh, S.P. Damage reduction to food products during transportation and handling. In *Handbook of Farm, Dairy and Food Machinery Engineering* Academic Press. 2019, 741-770.
9. Li, L., Pegg, R.B., Eitenmiller, R.R., Chun, J.Y. and Kerrihard, A.L. Selected nutrient analyses of fresh, fresh-stored, and frozen fruits and vegetables. *J. Fd. Compos. Analy.*, 2017, **59**, 8-17.
10. Rahman, L.F., Alam, L., Marufuzzaman, M. and Sumaila, U.R. Traceability of sustainability and safety in fishery supply chain management systems using radio frequency identification technology. *Fds*, 2021, **10**, 2265.
11. Priyaa, P. K., Sathyapriya, S. and Arockiam, L. Nutrition monitoring and calorie estimation using internet of things (IoT). *Int. J. Innov. Technol. Explor. Eng.*, 2019, **8**, 2669-2672.
12. Gurtu, A. and Johny, J. Supply chain risk management: Literature review. *Risks*, 2021, **9**, 16.
13. Zhang, Y., Zhao, L. and Qian, C. Modeling of an IoT-enabled supply chain for perishable food with two-echelon supply hubs. *Industrial Management and Data Systems*, 2017.
14. Ashok, A., Brison, M. and LeTallec, Y. Improving cold chain systems: Challenges and solutions. *Vaccine*, 2017, **35**, 2217-2223.

15. Vrat, P., Gupta, R., Bhatnagar, A., Pathak, D.K. and Fulzele, V. Literature review analytics (LRA) on sustainable cold-chain for perishable food products: research trends and future directions. *Opsearch*, 2018, **55**, 601-627.

16. Aziz, M.A., Ragheb, M.A., Ragab, A.A. and El Mokadem, M. The impact of enterprise resource planning on supply chain management practices. *The Business and Management Review*, 2018, **9**, 56-69.

17. Haulder, N., Kumar, A., and Shiwakoti, N. An analysis of core functions offered by software packages aimed at the supply chain management software market. *Computers and Industrial Engineering*, 2019, **138**, 106116.

18. LakshmiPriya, T.K.S. and Alagusundari, N. Smart Printed Paperboard for Green Infrastructure. In *Emerging Technologies for Agriculture and Environment*. Springer, Singapore. 2020, 2020.

19. James, D. and Lakshmi Priya, T.K.S. Improving the product services using IoT for controlling in-transit parameters. *Our Heritage,* 2020, **68**, 376-382.

20. James, D. and Lakshmi Priya, T.K.S. An IoT-Based Traceability Framework for Small-Scale Farms. In *Emerging Technologies in Data Mining and Information Security* (pp. 841-851). Springer, Singapore. 2021.

21, Rejeb, A., Keogh, J.G. and Treiblmaier, H. Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet*, 2019, **11**, 161.

22. Litke, A., Anagnostopoulos, D. and Varvarigou, T. Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment. *Logistics*, 2019, **3**, 5.

23. James, D. and Lakshmi Priya, T.K.S. A Top-Down Survey on Security Aspects of the Internet of Things (IoT). International Journal of Innovative Research in Management, Engineering and Technology*,* 2019, **4***,*150-156.

24. Emira, H.H.A. Authenticating IoT devices issues based on blockchain. *Journal of Cybersecurity and Information Management*, 2020, **1**, 35.

25. Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, 2018, **88**, 173-190.

26. Novais, L., Maqueira, J.M. and Ortiz-Bas, Á. A systematic literature review of cloud computing use in supply chain integration. Computers and Industrial Engineering, 2019, **129,** 296-314.

27. Althoubi, A., Alshahrani, R. and Peyravi, H. Delay analysis in IoT sensor networks. *Sensors*, 2021, **21**, 3876.

28. Suryadevara, S. and Ali, S. Preperformance Testing of a Website. In *CS and IT Conference Proceedings*, CS and IT Conference Proceedings, 2020, **10**, 7.

Security Enabled IoT Architecture for Cold Chain Packaging Applications

[1]Mrs.Divya James, [2]Dr.T.K.S.Lakshmi Priya
Department of CSE, School of Engineering
Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
[1]18pheop003@avinuty.ac.in, [2]tkslp_pt@avinuty.ac.in

Abstract – *Rapid spreading of COVID - 19 and the post health issues shows the importance of eating food having high nutrition. Different temperatures, humidity, vibrations in storage, transportation and packaging can affect the deterioration of food quality. This can affect the attributes such as color, texture, odor, taste and parameters such as vitamin and bacterial content or chemical changes. So, quality and certainty of food origin are expected to be known by the supply chain entities. In current supply chain management especially in the cold chain industry, availability of real time data of environmental factors like temperature and humidity and secure transactions within supply chain management entities is a major concern. In order to ensure the safety and security of food especially during packaging and transportation, an architecture is developed that combines IoT sensors with cloud technologies and a lightweight cryptographic method. The architecture monitors temperature and humidity in real time and ensures the security of sensor data through the lightweight cryptographic algorithm-PRESENT. The architecture can include IoT devices fixed on primary, secondary and tertiary packages and allows the products to be monitored in real time and increases the efficiency of operations of packaging companies. An implementation of the proposed architecture has been demonstrated and analyzed.*

Keywords – *Lightweight cryptography, Cloud, Security, Internet of Things, Coldchain*

I. Introduction

Supply Chain Management (SCM) [1][2] may be defined as the process by which how a product from one end reaches the other end.ie: from suppliers to consumers. Reduced costs, increased efficiency and increased transparency are some of the benefits of supply chain management[3][4].The temperature-controlled supply chain system, referred to as the Cold Chain[5].Cold chain industry still lacks end-to-end visibility, security and cross-functional collaboration[6].

IoT consists of devices connected over a network to exchange data. Packages can be classified into primary, secondary and tertiary packages. In the primary package, each can or bottles can be connected to IoT devices. Secondary packages consist of multiple cans which can be put inside the cardboard boxes. Each carboard boxes can be connected to IoT devices to monitor the spoilage of food. For logistics purpose, multiple cardboard boxes can be embedded into containers where the GPS module and IoT devices can be integrated for tracking and monitoring the products.

Security is one of the major concern in IoT. Since the number of connected devices increases, confidentiality, integrity and authenticity of data are major challenges in IoT network. Cryptography is the process of encryption and decryption of data thereby removes the major challenges in IoT network. Majority of the traditional cryptographic algorithms like DES,AES used today are developed for desktop and server contexts, as a result they are not suitable for small devices. Therefore, lightweight encryption algorithms (LWC) are considered which provides fast and reliable encryption systems for resource constrained devices. [7].

Here we have suggested a security enabled IoT architecture incorporating IoT sensors through lightweight cryptographic algorithm and cloud to ensure the safety and security of food. The architecture monitors temperature and humidity in real time and ensures the security of sensor data through the lightweight cryptographic algorithm-PRESENT. The following sections describes the literature survey, proposed architecture, results and performance analysis.

II. Literature Survey

Short Food Supply Chains (SFSCs)[8] are attracting interest for their potential to bring about social, and economic benefits in comparison to more conventional practices. Shortening food supply [9] chains may not always reduce the environmental hazards. Transportation of food, storage of food are some of the major components that can affect the quality of food.

Food can be classified into perishable and non-perishable. Perishable food [10] include meat and dairy products. Non-perishable[11]food include canned goods, cereals, pulses, starchy roots, and dried fruits. Temperature control of products is essential for maintaining the product quality. A K-means clustering method[12] can be used for the classification of temperature and humidity values related to cold chain logistics. Still, it won't solve the issues to monitor the environmental conditions .There are promising sensors[13][14] like and indicators which can indicate the quality of food. Release of gases like carbon dioxide, oxygen, volatile organic compounds and biogenic amines (BAs) are detected using gas sensors.[15][16]

ISBN : 978-93-5782-946-5

Because of the compatibility and availability of tools, zigbee technology is a better option for supply chain management. In the paper [17] , the strength of MQTT and HTTP protocols based on Cloud and Fog data is analysed through performance parameters for real time sensor data. It was proved that MQTT protocol is better than HTTP protocol for sensor traffic. A complete packaging, intelligent quality evaluation and monitoring are significant factors in the transition of conventional Cold Chain Logistics [18] to smart, green, and efficient cold chain logistics. Another sector of cold chain includes the administration of vaccines[19] to all categories of people in a timely manner. In this industry, better packaging designs are necessary for maintaining real-time information, tracking deliveries, and coordinating platforms.

The creation of new cryptographic algorithms that are optimized for a limited few devices has been the subject of extensive research over the past decade. These cryptographic methods are frequently referred to as "lightweight" algorithms.Majority of the cryptographic algorithms used today were developed for desktop and server contexts, as a result they are not suitable for small devices[20]. Therefore, lightweight cryptographic approach is proposed that solves many of the problems of traditional cryptography when used on devices with constrained physical size, computational requirements, limited memory, and power consumption.

Lightweight cryptography helps to secure networks of smart things due to its efficiency and footprint reduction[21].The PRESENT block cipher[22], is an SPN network recognized by NIST with 31 rounds. The length of the plain text is 64 bits and the algorithm can have 80 and 128-bit secret keys.Key addition, a layer of nonlinear substitution, and a layer of bit-wise permutation comprise each iteration of PRESENT.

In food supply chain, especially in cold chain industry, quality, security and certainty of food origin are expected to be known by the entities of supply chain. But the challenge to preserve the quality and security still remains. In this paper, a security enabled IoT architecture is proposed that monitors temperature and humidity in real time and ensures the security of sensor data through the lightweight cryptographic algorithm-PRESENT. The industrial/ digital revolution -IoT & Cloud can bring a solution to this problem.

III. Proposed Architecture

In this section, an integrated system architecture for cold chain industry is proposed. The proposed architecture named as SiCchain - Secure - IoT and Cloud for cold chain applications. As we can say that cold chain products can be physically tagged by IoT enabled sensors. During transit, spoilage of food occurs due to food pathogens, pH changes, toxins and ammino acids. To detect spoilage of food and emission of gases, sensors can continuously transmit and monitor, and the parameters can be stored along with time and location using IoT and cloud technology. The sensor values have been made secure using lightweight cryptographic algorithm-PRESENT. The proposed architecture facilitates and tracks the possession changes through the entities in the distribution channel.

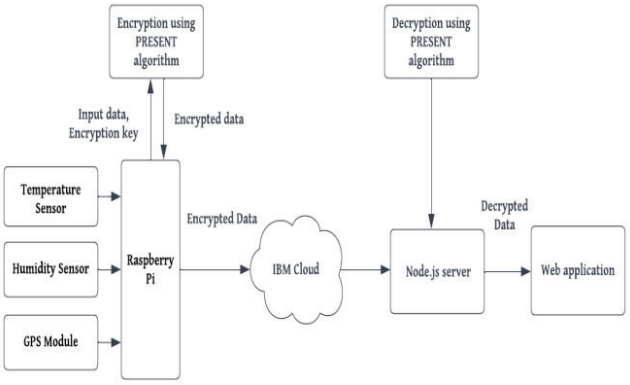


Figure 1. Proposed architecture of SiC-chain

Figure 1, shows the proposed architecture of SiC-chain. In SiC-chain, we have trusted IoT devices to monitor environmental factors that are connected to the Raspberry Pi. The sensors that are used are the temperature sensor which measures the temperature values, the humidity sensors that reads the humidity value. The GPS module is used to find the location. The readings from the IoT traffic are taken using sensors and are sent to the Raspberry Pi. The values are then encrypted using lightweight cryptographic algorithm-PRESENT. The encrypted values are then stored in IBM Cloud and are decrypted in Node.js server using PRESENT, a lightweight cryptographic algorithm. The decrypted values are then published to the web application.

IV. Experimental Results & Performance Analysis

Figure 2 and Figure 3 shows the encryption and decryption at raspberry pi and node.js server.

The temperature and humidity values along with the device ID is fetched .The values are encrypted and uploaded to cloud via MQTT broker. These values are decrypted in Node.js server . Once decrypted ,the values are shown in the dashboard of the web application. The temperature, humidity values along with the current location using GPS module helps to track and monitor the spoilage of food kept in primary, secondary and tertiary packages.

ISBN : 978-93-5782-946-5

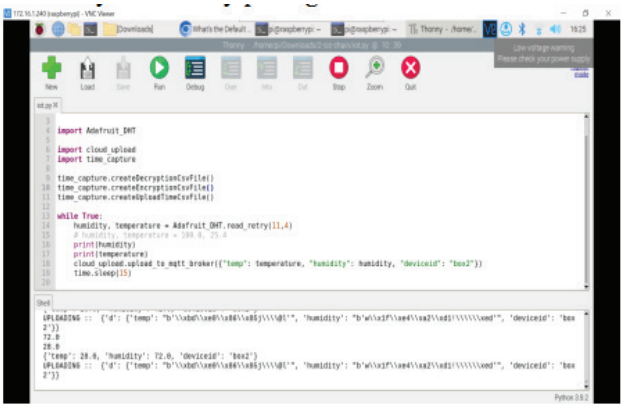


Figure 2.Encryption @ Raspberry PI

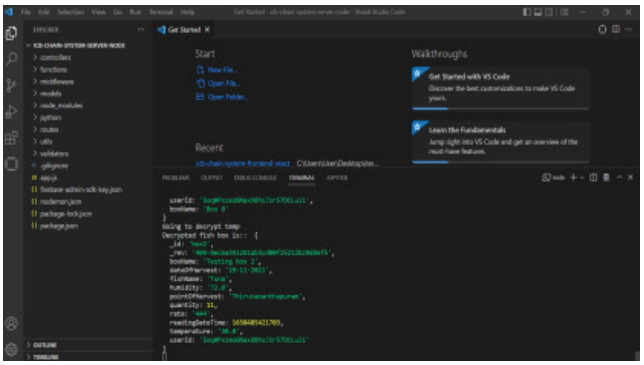


Figure 3.Decryption @ Node.js Server

The parameters selected for the performance evaluation of lightweight cryptographic algorithm are encryption time, throughput of encryption, cloud upload time. The encryption time is the total time taken to produce a cipher-text from plain-text. The input data is of 64 bits. Encryption time as shown in Figure 4 is difference between the start time and end time. It is measured in CPU clocks cycles/sec.

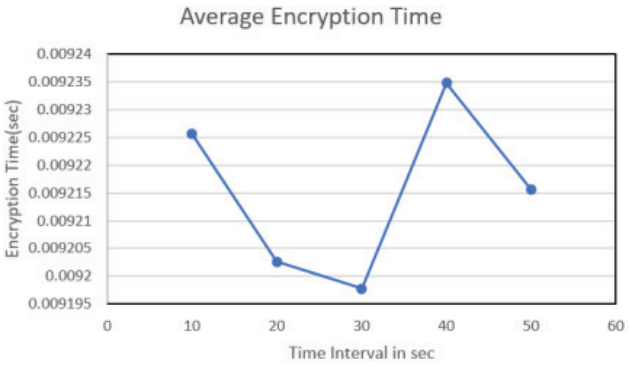


Figure 4. Average Encryption time

The throughput computed as shown in Figure 5 defines the speed of encryption. Throughput is measured in bytes/sec.

$$\text{Throughput} = \frac{\text{No: of bytes}}{\text{Encryption Time}}$$

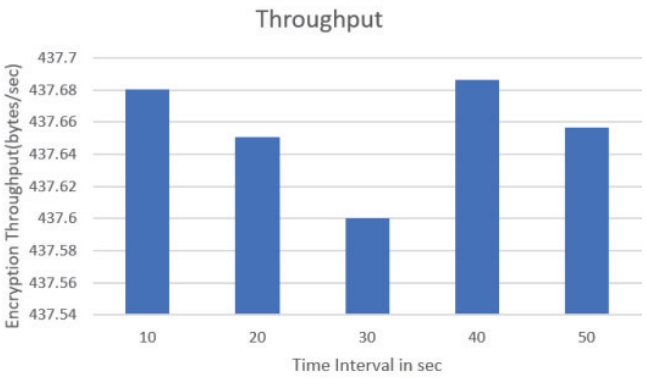


Figure 5. Throughput

Cloud upload time is the time taken to upload the encrypted values to cloud. The average cloud upload time is computed as 0.003798s.

Thus, the proposed architecture is tested and evaluated. The average encryption time and throughput remain almost same and low for 64-bit input is taken at an interval of 10, 20, 30, 40 and 50 sec. The proposed web application is efficient for large scale supply chain applications.

CONCLUSION

In the paper we have proposed an IoT architecture with security features that integrates IoT sensors with the cloud and a lightweight cryptographic method to guarantee the security and safety of food. The Internet of Things (IoT) allows real-time tracking, ensuring the food safety and cloud technology enhances the overall performance through efficient resource usage and system scalability. An implementation of the proposed architecture has been demonstrated. A secure real-time data transfer between sensors and application is incorporated using lightweight cryptographic algorithm – PRESENT, in order to avoid the eavesdropping and manipulation of temperature and humidity values within the cold chain industry. The performance analysis of ultra-lightweight block cipher-PRESENT were carried out and it can be concluded that the PRESENT consumes less memory and computation time. The throughput of real time data remains same for a time interval of 10-50sec. Most of the security credentials required for IoT authentication can be solved using such solutions. Further, it may be used for resource constrained IoT devices.

REFERENCES

[1] R. G. Richey, A. S. Roath, F. G. Adams, and A. Wieland, "A Responsiveness View of logistics and supply chain management," *J. Bus. Logist.*, 2021.

[2] H. Birkel and J. M. Müller, "Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability – A systematic literature review," *J. Clean. Prod.*, vol. 289, no. 125612, p. 125612, 2021.

[3] R. Dubey and S. S. Ali, "An exploratory study on logistics competency and firm performance," *Int. J. Logist. Syst. Manag.*, vol. 14, no. 2, p. 179, 2013.

ISBN : 978-93-5782-946-5

[4] T. Dulababu, R. B. Lakshmi, and B. Girish, "Supply Chain Management: Opportunities and Challenges," *Advances in Management*, vol. 11, no. 4, pp. 9–12, 2018.

[5] S. Mercier, M. Mondor, U. McCarthy, S. Villeneuve, G. Alvarez, and I. Uysal, "Optimized cold chain to save food," in *Saving Food,* Elsevier, 2019, pp. 203–226.

[6] Deloitte Global supply Chain Risk survey - blockchain-internet-things- supply-chain-traceability. 2013.

[7] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access,* vol. 9, pp. 28177-28193, 2021.

[8] L. Tanasă, "Benefits of short food supply chains for the development of rural tourism in Romania as emergent country during crisis," *Agricultural Economics and Rural Development,* vol. 11, no. 2, pp. 181–193, 2014.

[9] E. Majewski et al., "Are Short Food Supply Chains More Environmentally Sustainable than Long Chains? A Life Cycle Assessment (LCA) of the Eco-Efficiency of Food Chains in Selected EU Countries," *Energies,* vol. 13, no. 18, p. 4853, Sep. 2020.

[10] H.-K. Chen, C.-F. Hsueh, and M.-S. Chang, "Production scheduling and vehicle routing with time windows for perishable food products," *Comput. Oper. Res.,* vol. 36, no. 7, pp. 2311–2319, 2009.

[11] S. Kumar and A. Nigmatullin, "A system dynamics analysis of food supply chains – Case study with non-perishable products," *Simul. Model. Pract. Theory,* vol. 19, no. 10, pp. 2151–2168, 2011.

[12] M. M. Aung and Y. S. Chang, "Temperature management for the quality assurance of a perishable food supply chain," *Food Control,* vol. 40, pp. 198–207, 2014.

[13] B. Kuswandi, M. Moradi, and P. Ezati, "Food sensors: Off-package and on-package approaches," *Packag. Technol. Sci.,* vol. 35, no. 12, pp. 847–862, 2022.

[14] M. Weston, S. Geng, and R. Chandrawati, "Food sensors: Challenges and opportunities," *Adv. Mater. Technol.,* p. 2001242, 2021.

[15] A. T. Abduho and G. G. Madjos, "Abundance, supply chain analysis and marketing of crustacean fishery products of Tinusa Island, Sumisip, Basilan Province, Philippines," *Philippines. Aquaculture, Aquarium, Conservation & Legislation,* vol. 11, no. 6, pp. 1844–1858, 2018.

[16] A. Bhardwaj, N. Sharma, V. Sharma, T. Alam, and S. Shafia, "Smart Food Packaging Systems," in *Smart and Sustainable Food Technologies,* Singapore: Springer Nature Singapore, 2022, pp. 235–260.

[17] I. M. Hemiary, "Performance analysis of internet of things protocols based fog/cloud over high traffic," *Journal of Fundamental and Applied Sciences,* vol. 10, no. 6S, pp. 176–181, 2018.

[18] Q.-S. Ren, K. Fang, X.-T. Yang, and J.-W. Han, "Ensuring the quality of meat in cold chain logistics: A comprehensive review," *Trends Food Sci. Technol.,* vol. 119, pp. 133–151, 2022.

[19] M. L. Fahrni et al., "Management of COVID-19 vaccines cold chain logistics: a scoping review," *J. Pharm. Policy Pract.,* vol. 15, no. 1, p. 16, 2022.

[20] R.O'Caoimh et al., "COLLaboration on AGEing-COLLAGE: Ireland's three star reference site for the European Innovation Partnership on Active and Healthy Ageing (EIP on AHA)," *Eur. Geriatr. Med.,* vol. 6, no. 5, pp. 505–511, 2015.

[21] G. Bansod, N. Raval, and N. Pisharoty, "Implementation of a new lightweight encryption design for embedded security," *IEEE Trans. Inf. Forensics Secur.,* vol. 10, no. 1, pp. 142–151, 2015.

[22] C. G. Thorat and V. S. Inamdar, Implementation of new hybrid lightweight cryptosystem. *Applied computing and Informatics.* 2018.

ISBN : 978-93-5782-946-5

An IoT-Based Traceability Framework for Small-Scale Farms

Divya James and T. K. S. Lakshmi Priya

Abstract In many sectors such as supply chain, manufacturing, regular farms, health care, and pharmaceutical industries, traceability at real time and item level is important. This paper inquires the challenges of supply chain holders in the farming sector and proposes solutions using IoT (Internet of Things) for automatic tracking particularly for supporting functions like demand planning, inventory management, transportation in supply chain management. We introduce a framework of centralized traceability system based on IoT connecting all the elements providing end-to-end solutions thereby minimizing the overall loss. IoT security is of urgent concern because of the growing number of IoT products, the complexity of protocols used in IoT, and the manufacturers' limited safety measures embedded in the devices. New vulnerabilities such as man-in-the-middle attacks, denial of service attacks occur due to unsecured channels of communication. We extend the proposed framework by adopting a security model to prevent man-in-the-middle attacks in an IoT environment. Furthermore, temperature and humidity values are tracked and analyzed using sensors at different timestamps.

Keywords Internet of things (IoT) · Traceability · Security · Farms

1 Introduction

Supply chain deals with the transfer of goods and data between input suppliers, processors, wholesalers, retailers, and consumers. Current supply chains allow business to be integrated thereby minimize loss, increase resources, improve market

D. James (✉)
Department of Computer Science and Engineering, School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
e-mail: divyajames@gmail.com

T. K. S. Lakshmi Priya
School of Engineering, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
e-mail: tkslp.dr@gmail.com

A. E. Hassanien et al. (eds.), *Emerging Technologies in Data Mining and Information Security*, Advances in Intelligent Systems and Computing 1286,
https://doi.org/10.1007/978-981-15-9927-9_81

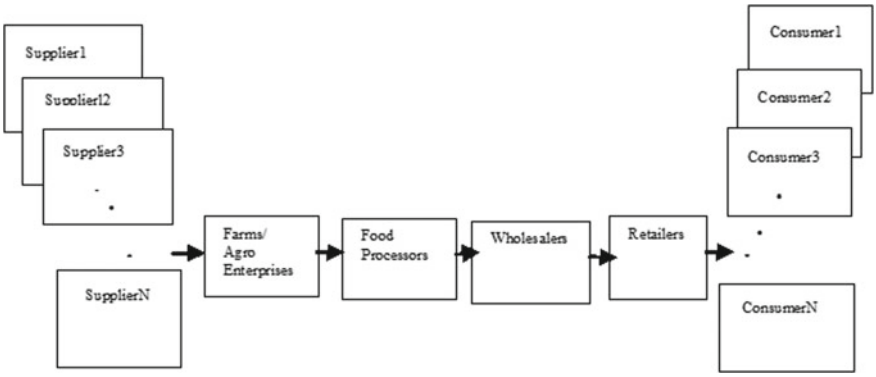


Fig. 1 Supply chain management in Farms

time, and maintain consumers. The success behind supply chain lies in how well the activities co-ordinate among the holders and thereby increasing the efficiency of the system. Figure 1 shows the major holders of supply chain in the farming sector.

The different holders in the supply chain operation comprise of Input Supliers, Farms, Food Processors, Wholesalers, Retailers, and Consumers. Nevertheless, the supply chains of various farms or agro-enterprises are riddled with difficulties resulting from the agricultural sector's inherent problems. The agri-supply chain network is determined by various challenges such as lack of market requirement data, demand for small quantity, lack of transparency, inadequate storage capacity, and poor transportation. Latest technologies like RFID tag, wireless sensors for tracking, and tracing of raw materials has been recognized and tested in the food industry [1]. In order to achieve privacy and end-end security, symmetric and asymmetric algorithms are designed to meet possible attacks like denial of service attack [2], man-in-the-middle attack [3], and eavesdropping attack [4].

The supply chain management network needs to refurnish so as to maximize profits and offer delivery mechanisms that aim to counter perishable products to stretch the marketable time. This paper proposes a low-cost and secure traceability framework based on IoT connecting all the elements in supply chain thereby minimizing the overall loss.

The organization of the paper is as follows: Sect. 2 describes the background study. In Sects. 3, 4, and 5, we present the proposed framework, methodology, experiments, and results of traceability system. Sections 6 describes the conclusion and future scope.

2 Theoretical Background

This segment reviews related topics which are classified into Internet of Things (IoT) in the supply chain, Traceability in IoT, and Security issues in IoT. Gaps in the study are found after literature review.

2.1 IoT in Supply Chain

The IoT, through network of computers, helps in overcoming the shortcomings of supply chain by providing a solution in the form of real time location which helps in finding the exact location of a consignment at any instance of time.

IoT has emerged as a ground-breaking network with knowledge sharing capabilities in the supply chain. The influence and performance of IoT on supply chain integration especially in the farming sector is yet to be explored. The cross-sectional survey [5] indicates a strong and significant relationship between IoT adoption and its effect on retail producers, consumers, and intermediaries. The functions of IoT in supply chain include demand planning, manufacturing, inventory management, transportation, and customer service. Demand planning is the collection of data by sensors, then analyze it using forecasting or prediction models in order to make accurate forecasts. Manufacturing is used to increase visibility, efficiency, and scalability at each step of the production process. It also increases efficiency and diminishes waste from ingredients. Inventory management improves demand visibility and prevents shrinking of stockouts and inventory. It helps to keep track of inventory information in real time. It helps to make the service more efficient and eliminates risks and accidents. Transportation helps to improve cooperation among carriers, shippers, and consumers. Customer Service helps to strengthen the customer relationship through real-time communication.

2.2 Traceability in IoT

Technological implications [6] in the identification of commodity, process, and characterization of environment, the collection, analysis, storage and transmission of information, and the overall integration of systems are needed to implement traceable agricultural supply chain system. Laboratory, online instruments, and non-destructive tests are used to measure firmness and to maintain internal quality assurance. Smart sensor techniques have attained considerable popularity in agriculture in the recent years. Regattieri.et al. [7] described a traceability system for the identification and routing of products for food supply chain. Promising technologies like alphanumeric codes, bar codes, and RFID systems are used. The cost of the TAG and the need of standardization are the two lines of development needed in the framework. Huang

and Liu [8] introduce the concepts of RFID technology and database integration technology in supply chain tracking system. Here also monitoring of product information is integrated and stored in the database. The use of RFID and NFC along with GPS technology [9, 10] in the entire logistics system of agricultural products would help to foster the development of trade, of agro-enterprises. An aeroponic system [11] is built to track key parameters using a wireless sensor network. The network provides other benefits, including quicker response to climatic conditions and better monitoring of crop quality, resulting in lower labor costs. However, the monitoring system does not provide a tracking system that plant scientists or growers may need to know about how the environmental parameters relate to plant growth.

2.3 Security Issues in IoT

Selective forwarding, Synchroniztion attacks, Replay attack, Denial of Service, Man-in-the-middle attacks, SQL injection are possible in IoT environments. Hassija et al. [12] suggested the security risks, enhancements, and solution architectures that IoT applications need. The work outlines the protection and privacy problems concerning various IoT applications. Blockchain, Fog computing, Machine learning, and edge computing-based solutions are proposed for securing IoT environments and applications. Burhan et al. [13] suggested a modern and standardized six-layer protected architecture for IoT. The paper addressed the communications technologies that IoT applications use. Hammi M et al. [14] created a robust, fast, and lightweight symmetric encryption algorithm for IoT devices. Arsalan Mosenia et al. [15] outlined weaknesses that IoT's edge side layer faces. Yang et al. [16] addressed the drawbacks of IoT devices that are most important. Chen et al. [17] focuses on location-specific security issues in IoT. Metsis et al. [18] addressed IoT middleware-related security problems.

The objective of this work is to secure, track, and trace the holders of supply chain in farms by using a centralized system to store transaction records giving priority to security, quality assurance (QA), and real-time data availability. The proposed framework makes supply chain management more efficient by using reliable technology like IoT. The web app interface allows the input suppliers, processors, and consumers as well as middlemen in the supply chain to view updates in real time and make decisions.

3 Proposed Framework

The abstract representation of the proposed framework consists of three layers. Considering a diary farm scenario, the upper layer consists of supply chain elements with input suppliers, farms or agro-enterprises, processors, wholesalers, retailers, and consumers. The middle layer describes the challenges associated with supply

chain elements and the lower layer consists of a centralized traceability system using IoT as shown in Fig. 2a.

The detailed representation of the challenges and proposed IoT-based solutions is depicted in the following Fig. 2b.

The role of input suppliers is to obtain material from producers in small quantity, pack them into containers for each manufacturer in large quantity and send to manufacturers. Farms in turn do the milking of cattle, supply food and water to cattle, pack

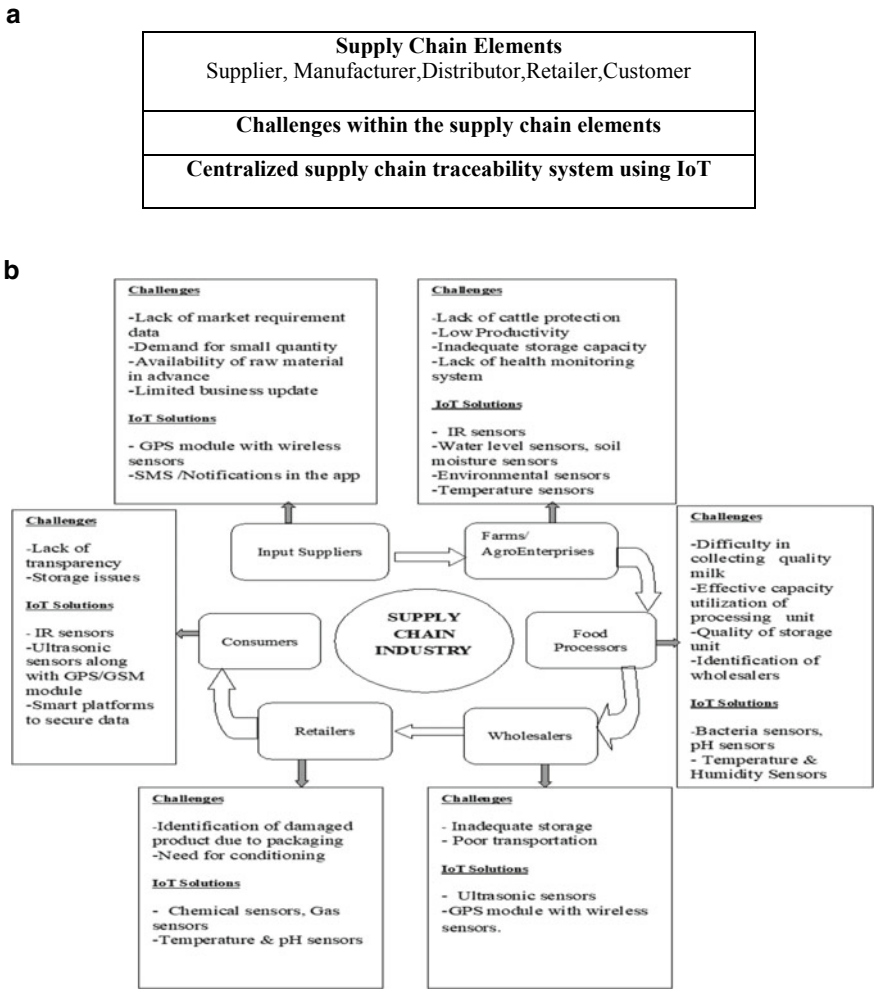


Fig. 2 **a** Abstract representation of the proposed framework **b** Challenges and IoT-based solutions with supply chain elements **c** Workflow of the proposed framework for small scale farms

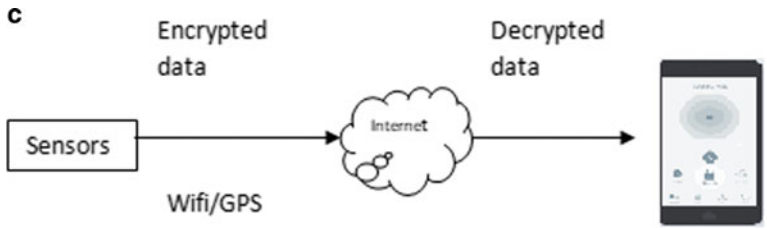


Fig. 2 (continued)

milk in containers, maintain and ensure working conditions of equipments. Processors collect milk from farms, process, and arrange for the wholesalers. The wholesaler's role is to collect milk from processors and deliver it to the retailer. The retailer collects milk from wholesaler and store, delivers to consumers as required. The consumers get milk from retailer. Based on business perspective, types of suppliers can be organized and unorganized sectors. Farms or Agro-Enterprises can be individual or society-based, small-scale, or large-scale industry. Merchant wholesalers, Logistics wholesalers, Specialized wholesalers are the different categories of wholesalers. Retailing can be done in-store-based and non-store-based. Consumers are the final endusers. So there are a lot of challenges connected with each entity in the supply chain. Our methodology proposes solutions based on IoT for automatic tracking of items through a centralized tracebility system and thereby creating logs to trace back the activities. Since there is a security breach in the system, data in transit is protected and made available only to the holders in the chain.

The system described above is applicable to large-scale farms. For small-scale farms, a strong and cost-effective system is required. To accomplish this goal, we use low-cost sensors like temperature, humidity, ultrasonic, and IR sensors along with GPS module and Wi-Fi connectivity. These sensors along with GPS module tracks the item, storage unit utilization, and even resists external human intervention. In order to protect data in transit strong encryption is done using AES algorithm. All the holders in the supply chain are able to track the system. The simplified version of the system is much like in Fig. 2c.

4 Methodology

The methodology provides a common portal connecting all the elements and providing an end-to-end solution. The operational diagram of the traceability framework with the sensors set for tracing parameters such as temperature, humidity at input suppliers, farms, processors, wholesalers, and retailers are shown in Fig. 3.

The data from various sensors are collected via Raspberry Pi. This data together with the GPS coordinates is sent to the remote server with the help of Wi-Fi connectivity which is achieved using Wi-Fi module. The data sent to the remote server is

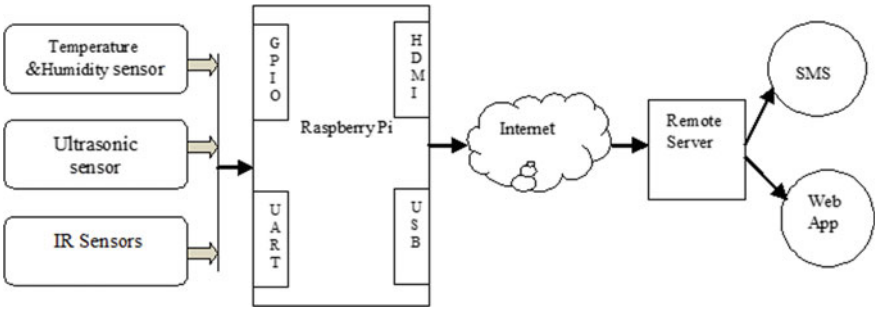


Fig. 3 Operational diagram of the traceability framework

Table 1 Sensors used and their Functionality

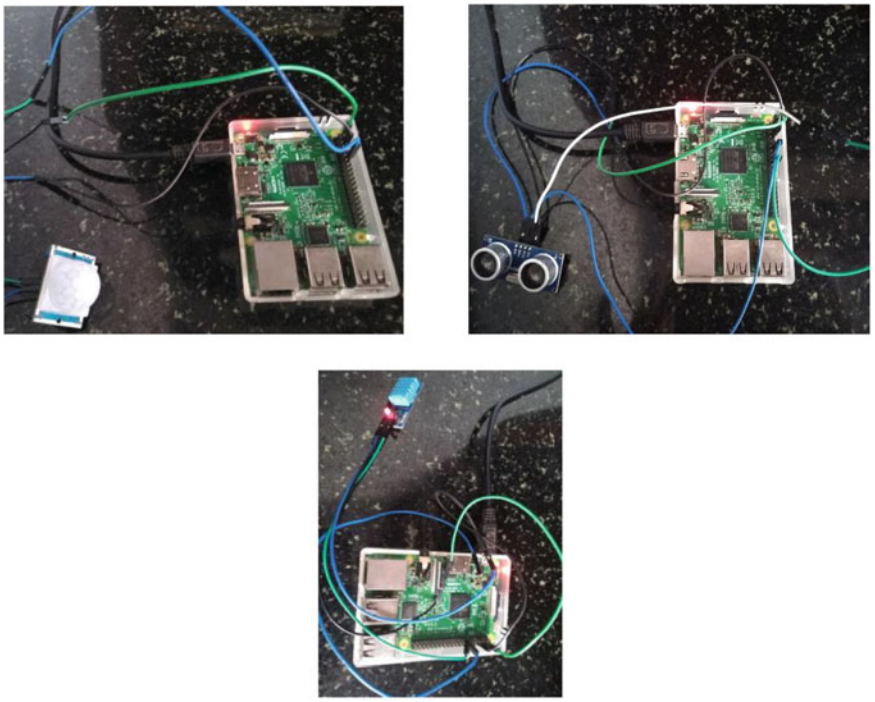
Sensors	Sensor location	Sensor Functionality
Temperature and Humidity	Food Processors, Wholesalers, Retailers	To track the damaged item
Ultrasonic	Input Suppliers	Effective capacity utilization of storage units
IR	Farms	Cattle Protection

encrypted with AES-256 to prevent man-in-the-middle attacks on the messages sent between the hardware device and server. The data is then analyzed and the server sent the decrypted data as SMS or notifications in the web application to the holders in the supply chain. Table 1 shows the sensor details and its functionality and location fixed.

5 Experiments and Results

The implemented design is shown in Fig. 4a which shows the integration of all hardware components. IR, Ultrasonic, and Temperature and Humidity sensors are interfaced using the Raspberry Pi. The web application connects with the server and displays the tracked data. Figure 4b displays the temperature and humidity of a package at different timestamp and Fig. 4c and d show the analysis of temperature and humidity values, respectively.

a



b

Tracking Log

Log of all temperature and humidity data with timestamp and packageID

ASSET	TEMPERATURE	HUMIDITY	TIMESTAMP
#A103	35.7*C	36	12:00
#A103	33.8*C	35	14:00
#A103	33.4*C	35	15:49
#A103	32*C	33	16:00
#A103	32*C	32.72	16:00
#A103	33*C	33.4	17:00
#A103	33*C	33.1	18:00
#A103	33*C	33.87	19:00
#A103	32.7*C	35.2	20:00

Fig. 4 **a** Integration of IR, ultrasonic and DHT sensors with Raspberry Pi. **b** Screenshot of tracking log, **c** temperature analysis, **d** humidity analysis

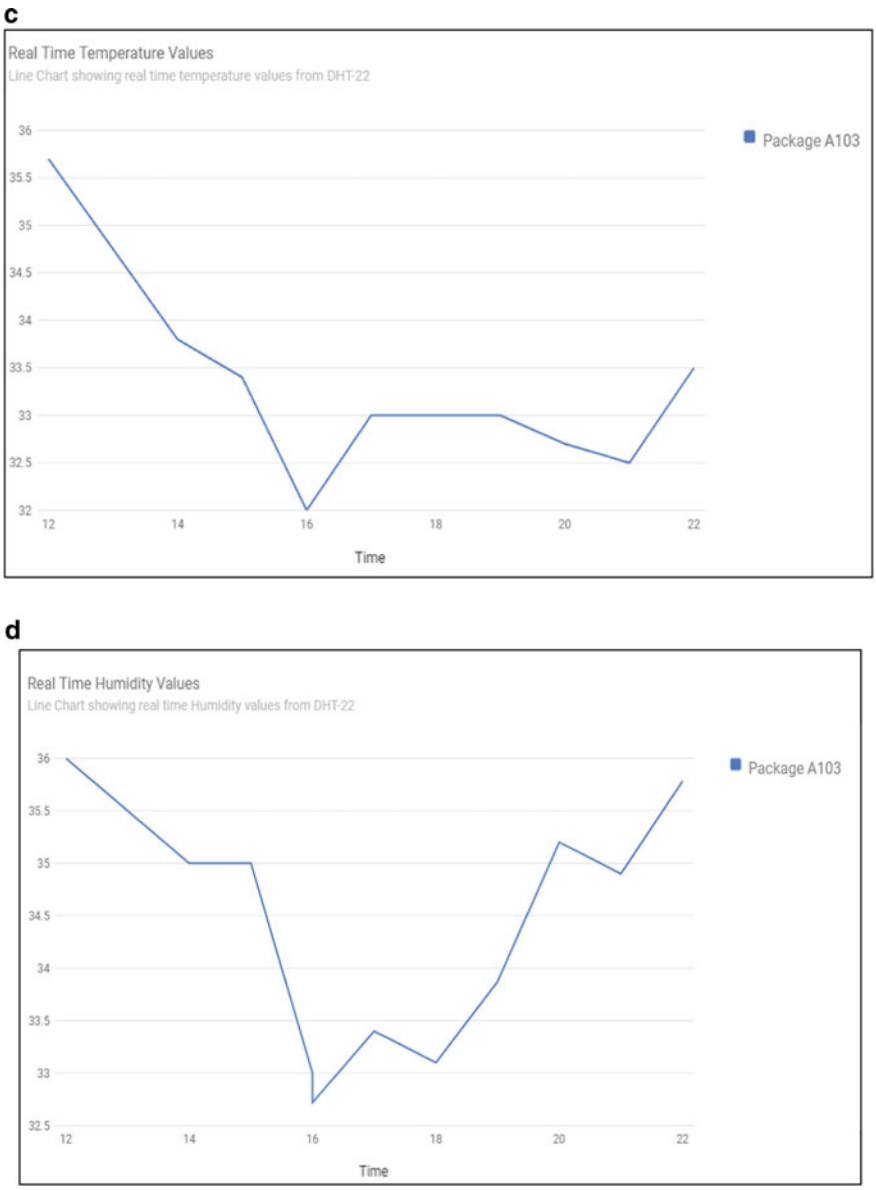


Fig. 4 (continued)

6 Conclusion and Future Scope

Traceability framework is essential in small-scale farms for tracking the conditions of shipments and storage units starting from input suppliers to consumers. Our proposed approach introduced a low-cost framework for centralized traceability based on IoT connecting all the elements, providing end-to-end solutions thereby minimizing the overall loss. The framework is protected by adopting a security model to protect from man-in-the-middle attacks within an IoT environment. Our future scope lies in developing a novel security model thereby making a secure environment within the IoT framework.

References

1. Zhou, W., Piramuthu, S.: IoT and supply chain traceability. In: Future Network Systems and Security, pp. 156–165 (2015)
2. Elleithy, K.M., Blagovic, D.: Denial of service attack techniques: analysis, implementation and comparison. Syst. Cybern. Inform. **3**, 66–71 (2006)
3. Bhushan, B., Sahoo, G., Rai, A.K.: Man-in–the-middle attack in wireless and computer networking-A review. In: 3rd International Conference on Advances in Computing, Communication & Automation(ICACCA) (Fall) (2017)
4. Dai, H.N., Wang, H., Xiao, H., Li, X., Wang, Q.: On eavesdropping attacks in wireless networks. In: IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) and 15th International Symposium on Distributed Computing and Applications for Business Engineering (DCABES), pp. 138–141 (2016)
5. De Vass, T., Shee, H., Miah, S.J.: The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. Australas. J. Inform. Syst. **22**, 1–29 (2018)
6. Opara, L.U.: Traceability in agriculture and food supply chain: a review of basic concepts, technological implications, and future prospects. J. Food Agric. Environ. **1**(1), 101–106 (2003)
7. Regattieri, A., Gamberi, M., Manzini, R.: Traceability of food products: general framework and experimental evidence. J. Food Eng. **81**(2), 347–356 (2007)
8. Huang, L., Liu, P.: Key technologies and alogrithms' application in agricultural food supply chain tracking system in E-Commerce. In: International Conference on Computer and Computing Technologies in Agriculture, Beijing, China, pp. 269–281(2014)
9. Mainetti, L., Mele, F., Patrono, L., Simone, F., Stefanizzi, M.L.,Vergallo, R.: An RFID-based tracing and tracking system for the fresh vegetables supply chain. Int. J. Antennas Propag. 1–15 (2013)
10. Gan, W., Zhu, Y., Zhang, T.: On RFID application in the tracking and tracing system of agricultural product logistics. In: International Conference on Computer and Computing Technologies in Agriculture, Nanchang, China, pp. 400–407 (2010)
11. Lakhiar, I.A., Jianmin, G., Syed, T.N., Chandio, F.A., Buttar, N.A., Qureshi, W.A.: Monitoring and control systems in agriculture using intelligent sensor techniques: a review of the aeroponic system. J. Sensors 1–18 (2018)
12. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743(2019)
13. Burhan, M., Rehman, R., Khan, B., Kim, B.S.: IoT Elements, layered architectures and security issues: a comprehensive survey. Sensors, **18**(9), 2796, 1–37 (2018)

14. Hammi, M.T., Livolant, E., Bellot, P., Serhrouchni, A., Minet, P.: A lightweight IoT security protocol. In: 1st Cyber Security in Networking Conference (CSNet), pp. 1–8 (2017)
15. Mosenia, A., Jha, N.K.: A comprehensive study of security of Internet-of-Things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2017)
16. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security andprivacy issues in Internet-of-Things. IEEE Internet Things J. **4**(5), 1250–1258 (2017)
17. Chen, L., Thombre, S., Järvinen, K., Lohan, E.S., Alén-Savikko, A., Leppäkoski, H., Bhuiyan, M.Z.H., Bu-Pasha, S., Ferrara, G.N., Honkala, S., Lindqvist, J., Ruotsalainen, L., Korpisaari, P., Kuusniemi, H.: Robust-ness, security and privacy in location-based services for future IoT: a survey. IEEE Access **5**, 8956–8977(2017)
18. Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: IoT middleware: a survey on issues and enabling technologies. IEEE Internet Things J. **4**(1), 1–20 (2017)

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

Improving the product services using IoT for controlling in-transit parameters

Divya James, Research Scholar, Department of Computer Science & Engineering, School of Engineering, Avinashilingam Institute of Home Science and Higher Education

divyajames@gmail.com

Dr.TKS. Lakshmi Priya, Professor, School of Engineering, Avinashilingam Institute of Home Science and Higher Education

tkslp.dr@gmail.com

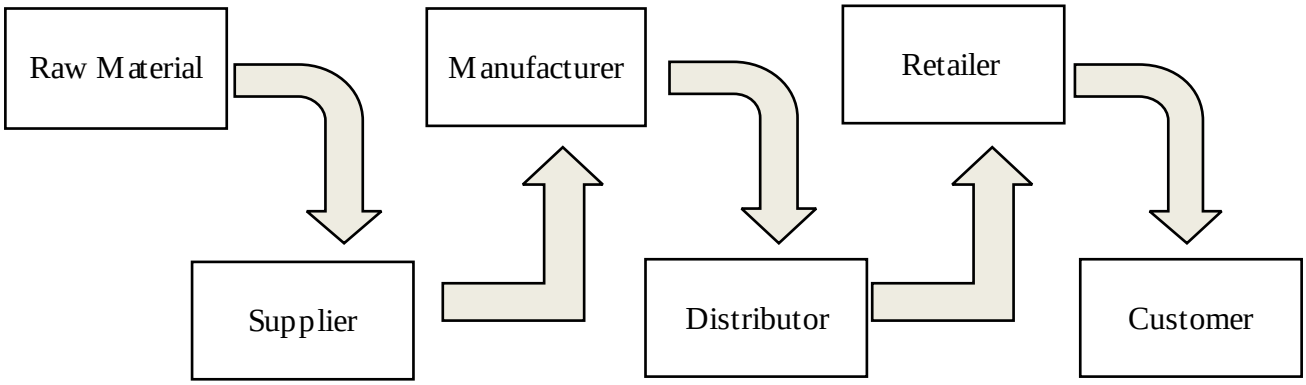
***Abstract*-Supply Chain Networks faces a critical need to monitor and maintain in-transit parameters like temperature route. time sensitivity for live monitoring of products. Different Supply Chain technologies used does not solve many of the existing problems. Elements currently leave their data scattered across various supply chain databases and eventually end up losing access to old data. Elements interact with transactional records in a broken manner and it often takes time to retrieve old transaction records.**

Supply chain in today's world faces a lot of challenges of which the major risk is the lack of end-to-end visibility. Owing to the high complexity of the supply chain, there is no data transparency and less secure transactions throughout the chain. To provide a secure mechanism, we use an integrated approach with IoT. The proposed architecture is a centralized electronic record management system, which securely streamlines the transaction and enables data economics, leveraging the properties of the IoT. The modular design of the approach makes it easy to integrate with the Supply Chain providers' existing database. Using IoT to provide data transparency and by using a temperature guided route optimization algorithm, this methodology provides a secure way of transporting goods that have temperature constraints. Additionally, we discuss the implementation details which provides an ultimate solution to the approach.

Keywords-IoT, Supply chain, Logistics, In-transit Parameters

I. INTRODUCTION

Supply chain management means and refers to the flow of goods from supplier at one end to customer at other end in a cost effective manner. The block diagram of supply chain management is depicted as follows:



ISSN: 0474-9030
Vol-68-Issue-44-February-2020

Fig 1:Supply Chain Management

The four users are Suppliers, Manufacturers, Distributors and Consumers. The Suppliers collects theraw materials and passes it on to the manufacturers who use them to produce finished products. Once these products are ready, they are sent to the primary warehouses where they can be dispatched directly or otherwise sent to local warehouses for local dispatch. Finally, once the product reaches the customers, he/she updates feedback regarding the quality of the product received through the system.In addition, the supply chain management and logistics also have a distribution channel.

Channels for distribution include wholesalers, retailers, distributors and the Internet. The producer sells direct to the customer in a direct distribution channel. Indirect channels require many intermediaries before the product ends up in consumer's pockets. The difference in rates extends to both wholesale and retail sales.

Some of the problems encountered by supply chain management includecareful stock handling, mismanagement of data andlive monitoring of products throughout the logistics chain. There are many problems with current systems used in the Supply Chain field.Elements currently leave their data scattered across various supply chain databases and eventually end up losing access to old data. Live monitoring of perishable products like frozen food, meat in supply chain & logistics are undetected. In the healthcare sector, there is an urgent need to monitor and maintain optimum in-transit parameters like temperature, route and time sensitivity. Internet of Things is one of the emerging optimal solutions to overcome these challenges. IoT can allow real-time visibility of Supply Chain Management where the people in the chain can track the inventory at any given time point using a web/mobile application.

In this paper, we first present the current scenario of supply chain management and logistics and its challenges. In the next section a literature review/background study of IoT in marketing sectors and supply chain management are discussed. Then we propose a methodology for monitoring in-transit parameters using IoT in supply chain networks. Additionally, we discuss the implementation details and techniques which provides an ultimate solution to the approach.

II.**BACKGROUND STUDY**

Currently IoT systems are used in logistics sector where the application has been used to track the items placed in racks in the supermarket. Also in the shopping mall people are connected through IoT to know about the new offers of a product in different shops [1]. Applications such as customer tracking and analysis, dynamic pricing has been identified by incorporating IoT with data mining techniques [2]. A mathematical model [3] has been proposed in conjunction with IoT to find out the best pattern from

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

several categories for e-commerce applications. Here Internet of things has been used an instrument for marketing in the digital marketing sector. IoT has created an impact on warehouse and yard management[4],shrinkage and misplacement of inventory[5] and accurate and timely delivery of products using sensor enabled RFID networks [6].By taking autonomous decisions using sensor networks[7]positive benefits has been received by the manufacturer, distributor and customer.

From the background study we can conclude that live monitoring of product for controlling the in-transit parameters like temperature, route and time are not widely available using IoT. IoT technology can be integrated into existing supply chain marketing and logistics sector thereby improving the services of products. So our proposed methodology would contribute India's trade goal among SAARC Countries [8,9] for the development and stability in the neighbourhood. It will also enable to expand and deeper the engagement with SAARC Countries.

III. PROPOSED METHODOLOGY

The abstract representation of proposed methodology consists of two layers. The upper layer consists of supply chain elements with suppliers, manufacturers, distributors, retailers and customers and lower layer consist of a centralized record management system using IoT as shown in Fig 2.

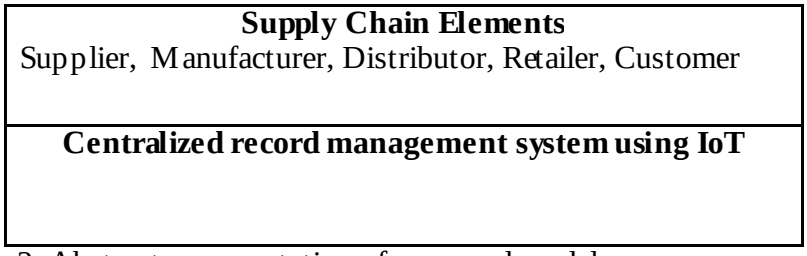


Fig 2: Abstract representation of proposed model

The detailed representation of the proposed methodology is depicted in the following diagram:

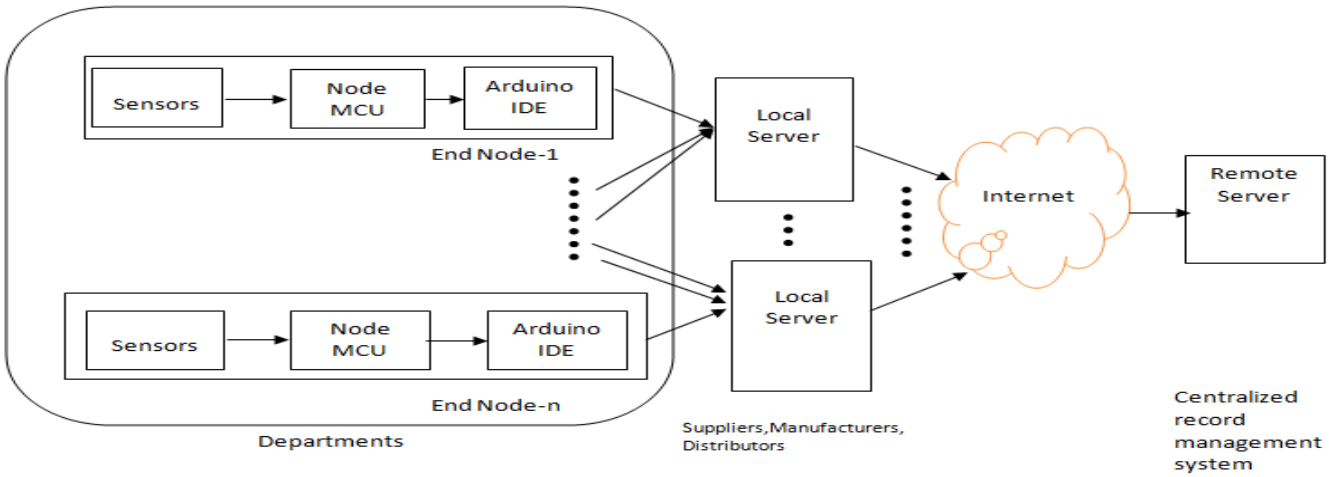


Fig. 3Operational diagram of Proposed Methodology

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

Each of the elements in the supply chain management has an end node installed in them. The role of the end node is to acquire data using sensors and send the data to the local server. The local server acquires the data analyses, processes and make predictions on the data. From the local server the data is transferred to the centralized record management system which is the remote server. All end nodes are connected to local servers and all local servers are connected to remote servers.

Sensors used in the methodology are DHT 22 sensors, which is used to measure the temperature and humidity. Node MCU is a prototyping board which in turn has a microcontroller module board mounted on it and Arduino IDE is the programming environment .

The procedure of the proposed methodology is as follows:

Step 1:Node MCU acquires temperature and humidity from DHT22 sensors.

Step 2:The temperature and humidity data is fed into the Arduino IDE module which is visible in a local terminal.

Step 3:Arduino IDE Module sends the data to the local servers.

Step 4:Through internet connectivity the data is sent to the web/mobile application through remote servers.

The methodology could be applied to supply chain management and logistics sectors while transporting vaccines and frozen foods. In case of frozen foods, the suppliers collect these resources and are passed on to the manufacturers .The manufactured products reach the distributors. From the distributors it is delivered to the customers via retailers. Proposed methodology provides a single app interface connecting all the users involved in the cold chain management. Temperature sensors along with GPS module periodically monitors the in-transit parameters like temperature and route. If any abnormality is found it is alarmed by sending notifications to all actors along the supply chain .The customers can also provide feedback about how the product was delivered and about its quality.

A portion of the layer -2 of abstract architecture has been implemented and tested.The advantages of the current methodology are all the elements in the current system have an interface like web/mobile application to access the real-time data and details about shipment. They can monitor optimum in-transit parameters like temperature, route and time sensitivity. They can keep track of the consignment in real-time. Security and data transparency in supply chain layers are enforced through IoT.

IV. **WORK IN PROGRESS**

The implemented design is shown in Fig4 which shows the integration of all hardware components. DHT22 and Node MCU module are interfaced using the Arduino IDE. The web application connects with

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

the server and displays the sensed data. Fig5 and Fig6 displays the temperature and humidity data in the local terminal and server. Table 1 shows the details of system components.

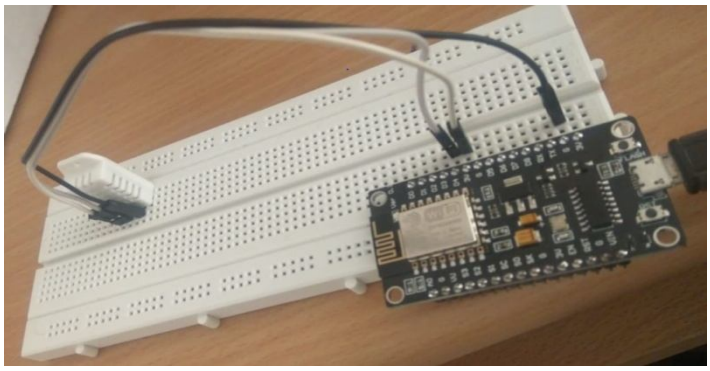


Fig 4: Hardware Implementation set up

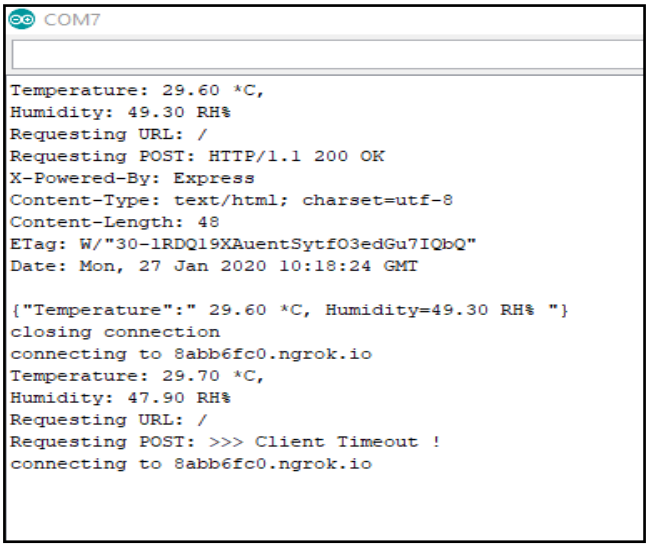


Fig 5:Temperature and Humidity values displayed in the Arduino IDE

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

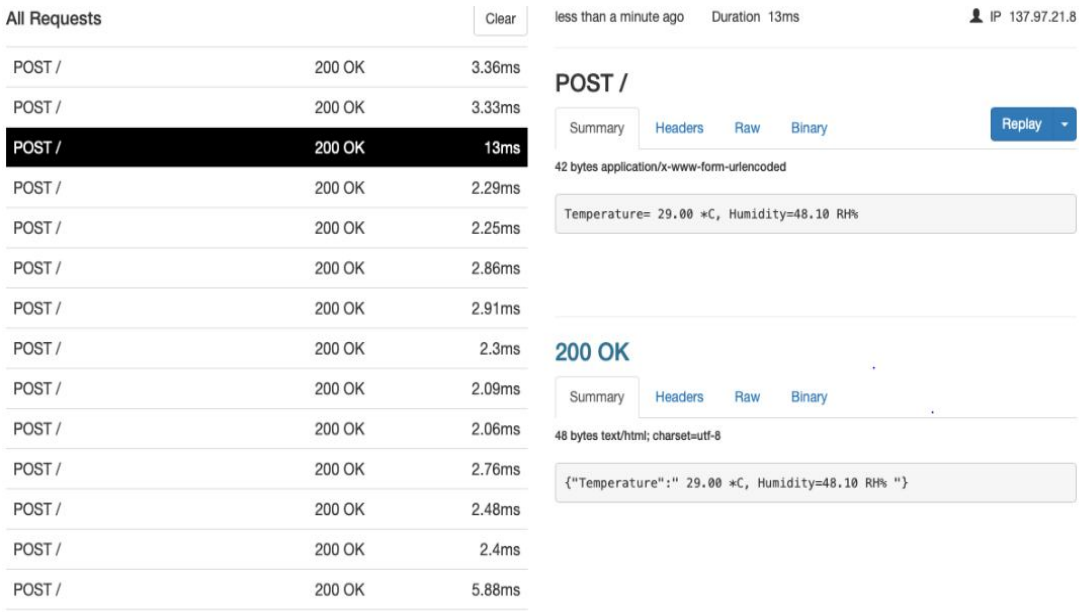


Fig 6:Temperature and Humidity data displayed in the server

TABLE 1: SYSTEM COMPONENT DETAILS

System Component	Details
Sensor	DHT22
Connectivity	Wi-Fi ESP8266
Microcontroller	NodeMCU
Remote Server	NodeJS

V. CONCLUSION AND FUTURE WORK

The proposed approach changes the way how elements of supply chain and logistics providers interact with each other. Proposed Methodology also integrates IoT to increase data transparency and availability throughout the supply chain and logistics which can be implemented across the borders of SAARC Countries. Since the approach uses a temperature guided route optimization algorithm, optimization is done to benefit the supply chain industries so that such industries can route their consignments which have complex temperature constraints optimally to both temperature and distance. In future, we would like to complete the work and test the record management system in real time giving priority to security and real-time data availability.

ISSN: 0474-9030
Vol-68-Issue-44-February-2020

REFERENCES

[1] Arjoo Pathan, Rujuta Kokate, Abhijeet Mutha, Priyanka Pingale, Prashant Gadakh. Digital India: " IoT Based Intelligent Interactive Super Market Framework for Shopping Mall". Engineering Science. Vol. 1, No. 1, 2016, pp. 1-5.

[2] Nataša Đurđević, Aleksandra Labus, Zorica Bogdanović, Marijana Despotović-Zrakić : "Internet of things in marketing and retail",International Journal of Advances in Computer Science and its Applications,Volume 6,Issue 3,2016,pp.7-11.

[3]Mani, Z., & Chouk, I.,"Drivers of consumers' resistance to smart products". Journal of Marketing Management, 33,2016,pp.76–97.

[4] Tadejko, P. "Application of Internet of Things in Logistics–Current Challenges." Economics and Management 7 (4): 54–64,2015

[5] Fan, T., F. Tao, S. Deng, and S. Li.. "Impact of RFID Technology on Supply Chain Decisions with Inventory Inaccuracies." International Journal of Production Economics 159: 117–125,2015.

[6]Yao, J. "Optimisation of One-Stop Delivery Scheduling in Online Shopping Based on the Physical Internet." International Journal of Production Research 55 (2): 358–376, 2017.

[7] Ben-Daya*et al*.,"Internet of things and supply chain management: a literature review". International Journal of Production Research,2017, 1–24.

[8] Vilas B. Khandare & Someshwar N. Babar,"Trade among SAARC Countries",IJIBF,Volume 2, Number 1 , January-June, 2012 , pp. 127-137

[9] Abdel-Basset, M., Mohamed, M., Chang, V., & Smarandache, F. ",IoT and Its Impact on the Electronics Market: A Powerful Decision Support System for Helping Customers in Choosing the Best Product". Symmetry, 11(5), 2019,611.

IJIRMET
ISSN (Online): 2456-0448
International Journal Of Innovative Research
In Management, Engineering And Technology
Available online

A TOP-DOWN SURVEY ON SECURITY ASPECTS OF THE INTERNET OF THINGS(IOT)

Divya James
Research Scholar, School of Engineering,Avinashilingam Institute of Home Science and Higher Education.
divyajames@gmail.com

Alagusundari.N
Research Scholar, School of Engineering, Avinashilingam Institute of Home Science and Higher Education
alagusundari124@gmail.com

Dr.TKS Lakshmipriya
Professor, School of Engineering, Avinashilingam Institute of Home Science and Higher Education
tkslp.dr@gmail.com

To access & cite this article
Website: www.ijirmet.com

ABSTRACT

Internet of Things (IoT) is becoming the most significant computing platform. With recently developed applications such as Smart Transportation, Smart City, Smart Home, IoT technologies are significantly changing our lifestyle. Novel Solutions are essential to protect the IoT systems from the attacks. The objective of the Internet of Things is to provide security and privacy to the users. This paper aims to analyses security challenges resulted from the characteristics of IoT systems. It also discusses the attacks and open problems in different layers. Finally, it analyses the impact of IoT security in smart home appliances.

KEYWORDS : IoT, Security, Attacks, Smart Homes

I. INTRODUCTION :

IoT (Internet of Things) comprises of a network of physical devices,vehicles,home appliances and other items embedded with electronics,software,sensors,actuators and network connectivity which enables these objects to get connected and exchange data.

IoT is also an Internet Technology connecting devices, machines and tools to the Internet using wireless technologies like Bluetooth, WiFi, Zigbee.

IoT[1] results in the unification of technologies such as low power embedded systems, cloud computing, big data, machine learning and networking.The two solutions for the networking technologies are either to expand the existing network or to build a separate system from scratch. IoT works on four differentcomponents, and it is depicted visually in Fig1.

SENSORS

Sensors are devices used to collect data from the environment.

IOT GATEWAYS

IoT Gateways acts as an intermediate node to collect data from the end devices and transmit it to the internet.

CLOUD/SERVER INFRASTRUCTURE

The data collected by the sensors have to be stored and processed intelligently within the cloud infrastructure.

APPLICATIONS

Applications will support the end users to control and monitor the smart devices from remote locations.

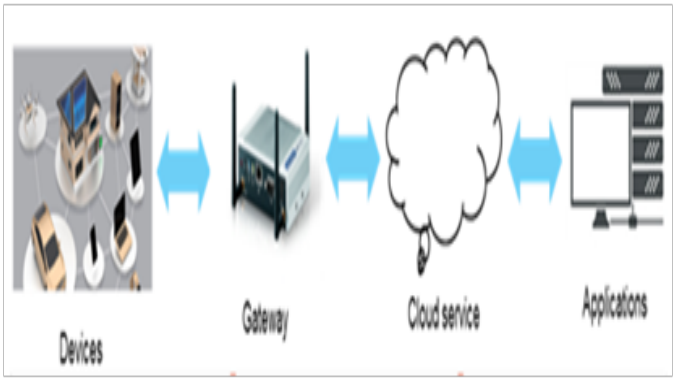


Fig1: Environment Diagram

Applying security mechanisms in an IoT system is more challenging than with a traditional network, due to the heterogeneity of the devices and protocols as well as the scale or the number of nodes in the system. The challenges in applying IoT security mitigation which is due to physical coupling, heterogeneity, resource constraints, privacy, scalability, trust management and unpreparedness for security.

II. THE NEED FOR SECURITY IN IOT :

THE DIFFERENT LAYERS[2] OF IOT CONSIST OF:

Perception layer

Aforementioned is the physical layer for sensing and collecting information from the environment.

Network layer

This layer transfers the sensor data from the perception layer to the next layer and vice versa through the networks.

Application layer

This layer is responsible for delivering application-specific services to the user. It defines various applications that can be deployed using IoT. Each layer has its's security[3] concerns:

PERCEPTION LAYER SECURITY PROBLEMS:

The primary technologies used in the perception layers are WSN, RFID and other types of sensing and identification techniques. Frequent attacks of the perception layer are:

Node Capture

The nodes which present at the network gateway are more likely to be compromised which might result in the leakage of relevant information which endangers the security of the entire network.

Fake Node and Malicious Data

The adversary adds a malicious node to the existing system through which they can circulate malicious codes and information over the network, thus infecting the whole system.

Denial of Service Attack

DoS and DDoS attacks are the most common and vicious attacks over a network. These attacks lead to depletion of network resources and unavailability of service.

Replay Attack

The adversary replays a previous message to the destination node to compromise the network trust and authentication schemes

.

Network layer security problems: Threats to most common security services like confidentiality, integrity and availability may happen at the network layer. Attacks like eavesdropping, Man in - the middle, DoS/DDoS, Network Intrusion are common threats at this layer.

Heterogeneity:

Due to the use of different technologies and protocols security and network coordination is hard to maintain. Thus, making the system vulnerable.

Scalability Issues

IoT comprises of a large number of devices, and more devices may enter or leave the network at different times which raises issues like lack of authentication, network congestion etc. It also depletes a lot of resources.

Data Disclosure

By using social engineering techniques the adversary might be able to obtain sensitive information from the network. As these devices collectively have vast amounts of data, using specific data retrieval techniques, it is easy to extract information from the nodes.

Application layer security problems This layer needs different security standards as per the application requirements, which makes the task of securing the application hard and complicated. Some of the security and privacy issues at this layer are :

Mutual authentication and node identification

Each application has a different set of users which require various degrees of access privileges. Thus, to prevent any illegal access effective authentication schemes should be applied.

Information Privacy

User privacy[4] plays a significant role in each communication. Sometimes the techniques which are being used to process data might be vulnerable which leads to data loss and over a long term can do considerable damages to the system.

Data Management

Due to substantial data collections, the system complexity increases which require a lot of resources and sophisticated algorithms to manage data and may also result in data loss.

Application Specific Vulnerabilities

While developing modules for an application some vulnerabilities might be left behind which are unknown to the user. These can be exploited by the adversary later on.

III. CASE STUDY :

SMART HOME TECHNOLOGY

Smart Home is becoming increasingly popular recently [5]. Gartner's IT Hype Cycle 2016 Report identifies that smart connected home is an emerging technology. By 2022 a typical house could contain 500 or more intelligent devices. Smart Home has the vision of adding intelligence to everyday home objects, such as appliances, door locks, surveillance cameras, furniture, garage doors, and so on and making them communicate with existing cyber-infrastructure. The addition of intelligence to physical objects offers many benefits to better human lives, including increased convenience, safety, security, and efficient usage of natural resources. For example, the Smart Home can adjust the blinds to save energy based on the environmental changes, automatically open the garage door when it senses an authorised vehicle approaching, or automatically order medical service when an emergency is detected. In Smart Home, traditional physical home devices become a part of the extension of the existing Internet. The consequence can be severe if the machines compromise. For example, successfully hacking smart lock will enable strangers to enter the house; compromising of baby monitors can scare babies remotely by strangers; hacking microwave can cause a fire at home. Owners of Smart Home may not want to live in Smart Home if security is a concern. Instead, they may expect to improve the safety of the house by using smart surveillance services. However, continuously collecting data from Smart Home devices can reveal private activities of homeowners as indicated in [6,7]. It poses severe threats to the homeowner's privacy.

Fig 2: Smart Home Devices

Smart home controller like cell phones are used to control and manage the devices[8] using IoT. Most the appliance in the kitchen are smart, example like refrigerator, microwaves, dishwasher etc. In the living room starting from the smart TV, it goes on with a smart lighting system. IoT plays a major role in connecting all the smart systems with a controller. Then the ways and the services provided are discussed.

ALGORITHMS AND METHODS

The interactive home environment is being created by different algorithms and methods. Artificial Neural Networks are used to detect and recognise the resident's pattern. Another model of the neural network is human behaviour modelling. Neural networks are popular because they don't require prior knowledge about the systems.

Distributed intelligent systems are multi-agent systems, which cooperate by sharing knowledge. Each agent is responsible for its domain area. Hence health monitoring from remote is made possible.

Bayesian statistics also helps in developing remote access of the inhabitant's locations and their conditions. These methods use the last known sensor state to improve the accuracy of the location prediction. They also use the immediate state to predict the future.

Case Base Reasoning and prediction algorithms make decisions. Context awareness can be achieved by these algorithms. Active Lezi and other predictive algorithms work the previous history for predicting the next activities. Recent changes in the user's behavior are also considered by the systems. Fuzzy logic is far better than the binary logic in controlling the home appliance. Fuzzy logic uses multi-valued logic for reasoning. Recent changes in user behavior will also reflect in the system.

Finally, image processing methods also help in human activity recognition. The skin colour of the face and hand tracing helps to do the process of image processing. The future smart home is likely to adopted image processing. Intelligent homes are devoted to provide safety and comfort for older adults.

The above discussed algorithms and methods used in smart home applications is given in the table below.

Table 1: Algorithms and Methods used in smart homes

Algorithms and Methods	Purposes
Artificial Neural Networks	Predicts the future states of home
Detects the daily activities	
Distributed intelligent systems	Health monitoring
Hidden Markov model	Behavioural model created
Bayesian Statistics	To determine the location
Summarization algorithm	Changes in the system are tracked
Statistical Predictive algorithm	Predict the daily life activities
Active LeZi Data compression	Predicting the next activities
Case Base Reasoning	Makes decisions based on the previous state
Fuzzy logic	Home appliance control

SMART HOME UTILITIES AND SERVICES

Smart home technology has significant improvement in health care like patient monitoring[9,10], telemedicine, and wellness monitoring. Smart home keeps on tracking the user's state and generate an alarm when an abnormal vital sign is detected.

Table 2 represents the summary of smart home utilities and services. The smart home is providing a wide range of services which provides satisfaction for the consumers. Additional research has been required for service to be cost-effective, efficient and acceptable.

Table 2: Smart home utilities and Services

Services	Functions
To provide comfort	Lighting, temperature
According to the resident's desire	
Remote access monitoring	Appliance monitoring and controlling via mobile phone and computers from distance location
Automate the home appliance	Voice operated home appliance
Wellness monitoring	Support elderly and disabled persons from remote locations

One of the main aims of the smart home is to reduce the interaction between the user and the devices. As discussed smart homes can control parameters like light, temperature, according to the user's choice.IoT helps develop a smart home with intelligence of what next to be done.

IV. CONCLUSION :

Smart home technology is increasing because of industrial demand. The work explains the attacks and challenges in different layers of IoT.Also it gives a general view on the algorithms and methods used for the smart home and its utilities. In the future smart home and the IoT are becoming the centre of intelligent services.

V. REFERENCES :

1. Mardianabinti Mohamad Noor, Wan Haslina Hassan, Current research on Internet of Things (IoT) security: A survey,Computer Networks 148 (2019) 283–294
2. K.Sha,W.Wei,T.Andrew,Yang,Z.Wang,W. Shei,On security challenges and open issues in Internet of Things, Futur. Gener. Computer. Syst. 83 (2018) , 326-337
3. A.Tewari,B.B.Gupta,Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Futur. Gener. Computer. Syst. 83 (2018) , 1-13
4. Tianyi Song, Ruinian Li, Bo Mei, Jiguo Yu, Xiaoshuang Xing, and Xiuzhen Cheng, A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes, IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 6, DECEMBER 2017.
5. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, 2019. "The Influence of 'Adventure Tourism Activities' in promoting tourism business in mountain stations", African Journal of Hospitality, Tourism and Leisure, Volume 8 (2).
6. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, Nov 2018. "A Study On consumer satisfaction and preference of colour TV brands in Chennai city", International Research Journal of Management and Commerce, Volume4, Issue 10.
7. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, "A Study on Attrition: Turnover intentions of employees", Jan 2019. International Journal of Civil Engineering and Technology (IJCIET), Volume 10, Issue 9.
8. Dr. S. Rabiyathul Basariya, and Dr. Nabaz Nawzad Abdullah, Dec 2018. "A STUDY ON CUSTOMER'S SATISFACTION TOWARDS E-BANKING", International Research Journal of Management and Commerce, Volume 5, Issue 12,
9. Dr. S. Rabiyathul Basariya, "A study On Customer Satisfaction towards Shopping Malls", International Journal of Business Intelligence and Innovations, Volume 1, Issue 2, special edition Oct-2015.F
10. A.Jacobsson, P. Davidsson, Towards a model of privacy and security for smart homes, in Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT2015),2015.
11. I.Rouf, et al., Neighborhood watch:Security and privacy analysis of automatic meter reading systems, in Proceedings of 2012 ACM Conference on Computer and Communications Security, 2012.
12. NicoSurantha,WingkyR.Wicaksono,Design of Smart Home Security System using object recognition and PIR Sensor, Procedia Computer Science 135 (2018) 465–472
13. Seungyong Yoon and Jeongnyeo Kim.

Remote security management server for IoTdevices,International Conference on Information and Communication Technology Convergence (ICTC),IEEE Conference Publications,2017

14. Shih-Hao Chang, Rui-Dong Chiang, Shih-Jung Wu, and Wei-Ting Chang,:A Context-Aware, Interactive M-Health System for Diabetics, IEEE Computer Society, (pp. 14-22), May-June 2016
15. Hammi M, Livolant E, Bellot P, Serhrouchni A, Minet P. A Lightweight IoT Security Protocol. In1st Cyber Security in Networking Conference (CSNet2017) 2017 Oct.

Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category A by MHRD)
Re-accredited with 'A++' Grade by NAAC.CGPA 3.65/4, Category I by UGC
Coimbatore – 641 043, Tamil Nadu, India

PLAGIARISM CHECK REPORT (THESES)

1.	Name of the Research Scholar	Divya James
2.	Roll No. and Year of Registration	18PHEOP003, 2019
3.	Department	Computer Science and Engineering
4.	Name of the Research Guide	Dr. T.K.S. Lakshmi Priya
5.	Title of the Thesis / Dissertation	SiC-Chain : A simple, secure IoT System Architecture for small scale Cold Chain Applications
6.	Similarity Content (%) Identified	**7%**
7.	Software Used	Turnitin
8.	Date of Verification	25-10-2023

Note : The report is excluding 14 Consecutive words, Review of Literature and Quoted Materials.

Checked by :

25/10/23
Information Scientist

Divya James
Research Scholar

25.10.2023
Assistant Librarian

Research Guide

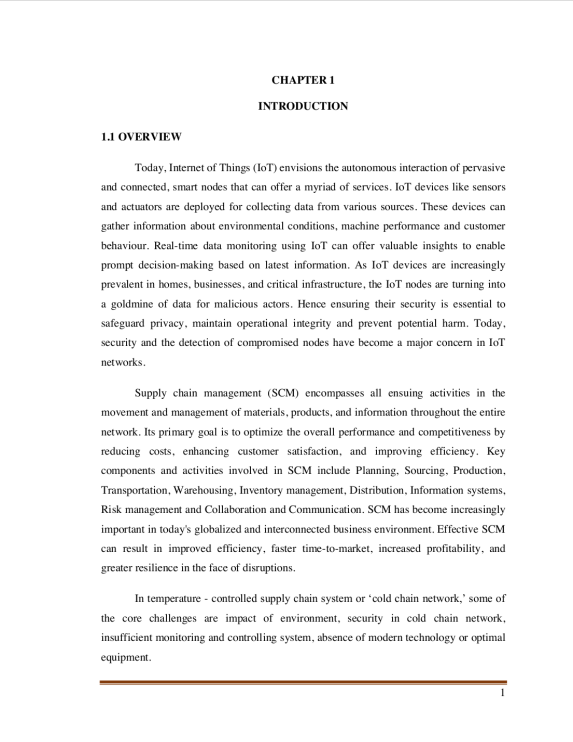
Date: 25-10-2023

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Library Adu
Assignment title:	New 2022
Submission title:	SiC-Chain : A simple, secure IoT System Architecture for sma...
File name:	Divya_James_Plagiarism_To_Check.docx
File size:	4.27M
Page count:	77
Word count:	13,864
Character count:	80,098
Submission date:	25-Oct-2023 03:35PM (UTC+0530)
Submission ID:	2178355119



CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Today, Internet of Things (IoT) envisions the autonomous interaction of pervasive and connected, smart nodes that can offer a myriad of services. IoT devices like sensors and actuators are deployed for collecting data from various sources. These devices can gather information about environmental conditions, machine performance and customer behaviour. Real-time data monitoring using IoT can offer valuable insights to enable prompt decision-making based on latest information. As IoT devices are increasingly prevalent in homes, businesses, and critical infrastructure, the IoT nodes are turning into a goldmine of data for malicious actors. Hence ensuring their security is essential to safeguard privacy, maintain operational integrity and prevent potential harm. Today, security and the detection of compromised nodes have become a major concern in IoT networks.

Supply chain management (SCM) encompasses all ensuing activities in the movement and management of materials, products, and information throughout the entire network. Its primary goal is to optimize the overall performance and competitiveness by reducing costs, enhancing customer satisfaction, and improving efficiency. Key components and activities involved in SCM include Planning, Sourcing, Production, Transportation, Warehousing, Inventory management, Distribution, Information systems, Risk management and Collaboration and Communication. SCM has become increasingly important in today's globalized and interconnected business environment. Effective SCM can result in improved efficiency, faster time-to-market, increased profitability, and greater resilience in the face of disruptions.

In temperature - controlled supply chain system or 'cold chain network,' some of the core challenges are impact of environment, security in cold chain network, insufficient monitoring and controlling system, absence of modern technology or optimal equipment.

1

SiC-Chain : A simple, secure IoT System Architecture for small scale Cold Chain Applications

by Library Adu

Submission date: 25-Oct-2023 03:35PM (UTC+0530)
Submission ID: 2178355119
File name: Divya_James_Plagiarism_To_Check.docx (4.27M)
Word count: 13864
Character count: 80098

SiC-Chain : A simple, secure IoT System Architecture for small scale Cold Chain Applications

ORIGINALITY REPORT

7%	2%	6%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Divya James, TKS Lakshmi Priya. "An innovative approach for dynamic key dependent S-Box to enhance security of IoT systems", Measurement: Sensors, 2023 Publication	5%
2	Submitted to Cranfield University Student Paper	1%
3	idr.mnit.ac.in Internet Source	<1%
4	Esau Taiwo Oladipupo, Oluwakemi Christiana Abikoye. "Improved authenticated elliptic curve cryptography scheme for resource starve applications", Computer Science and Information Technologies, 2022 Publication	<1%
5	ijtre.com Internet Source	<1%
6	Submitted to Universiti Tenaga Nasional Student Paper	<1%