no. 3 (2020).
[21] Juneidi, Salaheddin J. "Covid-19 Tracing Contacts Apps: Technical and Privacy Issues." Int. J. Advance Soft Compu. Appl 12, no. 3 (2020).
[22] Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." In International Workshop on Selected Areas in Cryptography, pp. 1-24. Springer, Berlin, Heidelberg, 2001.
[23] Fluhrer, Scott R., and David A. McGrew. "Statistical analysis of the alleged RC4 keystream generator." In International Workshop on Fast Software Encryption, pp. 19-30. Springer, Berlin, Heidelberg, 2000.
[24] Rezaee, Hamideh, Ah Aghagolzadeh, M. Hadi Seyedarabi, and Snadi Al Zu'bi. "Tracking and occlusion handling in multi-sensor networks by particle filter." In 2011 IEEE GCC Conference and Exhibition (GCC), pp. 397-400. IEEE, 2011.
[25] Jararweh, Yaser, Shadi Alzubi, and Salim Hariri. "An optimal multi-processor allocation algorithm for high performance GPU accelerators." In 2011 IEEE (AEECT), pp. 1-6. IEEE, 2011.
[26] Kanan, Tarek, Raed Kanaan, Omar Al-Dabbas, Ghassan Kanaan, Ali Al-Dahoud, and Edward Fox. "Extracting named entities using named entity recognizer for Arabic news articles." International Journal of Advanced Studies in Computers, Science and Engineering 5, no. 11 (2016): 78-84.
[27] Nandy, Tarak, et al. "Review on security of Internet of Things authentication mechanism." IEEE Access 7 (2019): 151054-151089.
[28] Nawir, Mukrimah, et al. "Internet of Things (IoT): Taxonomy of security attacks." 2016 3rd International Conference on Electronic Design (ICED). IEEE, 2016.
[29] Belapurkar, Abhijit, et al. Distributed systems security: issues, processes and solutions. John Wiley & Sons, 2009.
[30] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer Networks 44.5 (2004): 643-666.
[31] Rajendran, Gowthamaraj, et al. "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures." 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.
[32] Cryptography and Network Security – Principle and Practice – William Stallings – Fifth Edition.
[33] Malki, Z. (2016). Hybrid Cryptography Technique for Information Systems. International Journal of Computer Science and Information Security, 14(3), 234.
[34] Al Mamun, A., Salah, K., Al-Maadeed, S., & Sheltami, T. R. (2017, May). BigCrypt for big data encryption. In 2017 Fourth International Conference on Software Defined Systems (SDS) (pp. 93-99). IEEE.
[35] Seth, S. M., & Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication 1
[36] Kalpana, P., & Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. International Journal of research in computer and communication technology, IJRCCT, ISSN, 2278-5841.
[37] Arora, R., Parashar, A., & Transforming, C. C. I. (2013). Secure user data in cloud computing using encryption algorithms. International journal of engineering research and applications, 3(4), 1922-1926.
[38] Malki, Z. (2016). Hybrid Cryptography Technique for Information Systems. International Journal of Computer Science and Information Security, 14(3), 234.
[39] Sriadhi, S., Rahim, R., & Ahmar, A. S. (2018, June). Rc4 algorithm visualization for cryptography education. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012057). IOP Publishing.
[40] Attack Exploits Weakness in RC4 Cipher to Decrypt User Sessions | Threatpost
[41] Paul, S., & Preneel, B. (2004, February). A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher. In International Workshop on Fast Software Encryption (pp. 245-259). Springer, Berlin, Heidelberg.
[42] Pudovkina, M. (2002). Statistical weaknesses in the alleged RC4 keystream generator. IACR Cryptol. ePrint Arch., 2002, 171.