

REFERENCES

- Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). "A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective". *Symmetry*, 11(6), 774. doi:10.3390/sym11060774
- Afrianto, I., Heryandi, A., Finandhita, A., & Atin, S. (2020, July). "Prototype of e-document application based on digital signatures to support digital document authentication". In *IOP Conference Series: Materials Science and Engineering* (Vol. 879, No. 1, p. 012042). IOP Publishing.
- Ahanger, T. A., & Aljumah, A. (2019). "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms". *IEEE Access*, 7, 11020-11028. doi:10.1109/access.2018.2876939
- Ahmed, A. A. (2021). "Lightweight Digital Certificate Management And Efficacious Symmetric Cryptographic Mechanism Over Industrial Internet of Things". *Sensors*, 21(8), 2810.
- Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). "Malicious Insiders Attack In Iot Based Multi-Cloud E-Healthcare Environment: A Systematic Literature Review". *Multimedia Tools and Applications*, 77(17), 21947-21965. doi:10.1007/s11042-017-5540-x
- Alam M. A. (2016). "Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems". 2016;3(03):86–93.
- Alam, S., Siddiqui, S.T., Ahmad, A., Ahmad, R., & Shuaib, M. (2020). "Internet of Things (IoT) Enabling Technologies, Requirements, and Security Challenges: In Advances in Data and Information Sciences". *Springer*: Berlin/Heidelberg, Germany, pp. 119–126.
- Aleisa, N., & Renaud, K. (2017). "Privacy of the Internet of Things: A Systematic Literature Review". *Proceedings of the 50th Hawaii International Conference on System Sciences* (2017). doi:10.24251/hicss.2017.717
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications". *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376. doi:10.1109/comst.2015.2444095
- Ali, A., Rahim, H., Ali, J., Pasha, M., Masud, M., Rehman, A., Chen, C., & Baz, M. (2021). "A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority". *Applied Sciences*. <https://doi.org/10.3390/app11219999>.
- Ali, G., Dida, M. A., & Elikana Sam, A. (2021). "A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications". *Future Internet*, 13(12), 299.
- Almajali, S., Salameh, H. B., Ayyash, M., & Elgala, H. (2018, April). A Framework for Efficient and Secured Mobility Of IoT Devices In Mobile Edge Computing". In 2018

- Third International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 58-62). *IEEE*.
- Anusas-Amornkul, T. (2019, August). "Strengthening Password Authentication Using Keystroke Dynamics and Smartphone Sensors". In *Proceedings of the 9th International Conference on Information Communication and Management* (pp. 70-74).
- Assiri, S., Cambou, B., Booher, D., Miandoab, D., & Mohammadinodoushan, M. (2019). "Key Exchange using Ternary system to Enhance Security". 2019 *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0488-0492. <https://doi.org/10.1109/CCWC.2019.8666511>.
- Aswale, P., Shukla, A., Bharati, P., Bharambe, S., & Palve, S. (2019). "An Overview of Internet of Things: Architecture, Protocols and Challenges". In *Information and Communication Technology for Intelligent Systems*. Springer: Berlin/Heidelberg, Germany, pp. 299–308.
- Babaer, H., & Al-Ahmadi, S. (2020). "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking". *IEEE Access*, 8, 92098-92109. <https://doi.org/10.1109/ACCESS.2020.2994587>.
- Bafandehkar M, Yasin S, Mahmud R, Hanapi ZM. "Comparison of ECC and RSA Algorithm in Resource Constrained Devices". 2013;0–2.
- Bahaddad, A. A., Almarhabi, K. A., & Alghamdi, A. M. (2022). "Factors Affecting Information Security and the Implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA)". *Applied Sciences*, 12(24), 12707.
- Bai, L., Zhu, L., Liu, J., Choi, J., & Zhang, W. (2020). "Physical Layer Authentication in Wireless Communication Networks: A Survey". *Journal of Communications and Information Networks*, 5(3), 237-264.
- Bansal, S., & Kumar, D. (2020). "IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication". *Int. J. Wireless. Information. Network*. 2020, 27, 1–25
- Baqeel, H., & Saeed, S. (2019, April). "Face Detection Authentication on Smartphones: End Users Usability Assessment Experiences". In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). *IEEE*.
- Baxter, P., & Jack, S. (2008). "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers". *The Qualitative Report*, 13(4), 544-559. <https://doi.org/10.46743/2160-3715/2008.1573>
- Bränström, R., Kristjánsson, S., Ullén, H., & Brandberg, Y. (2002). "Stability Of Questionnaire Items Measuring Behaviours, Attitudes and Stages Of Change Related To Sun Exposure". *Melanoma Research*, 12, 513-519.
- Buja, A. G. (2018). "Security Analysis Techniques Using Differential Relationships For Block Ciphers". *Ph.D Thesis*. Universiti Teknikal Malaysia Melaka.

- Cai, H., Xu, B., Jiang, L., & Vasilakos, A.V. (2016). "IoT-based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges". *IEEE Internet Things Journal*. 4, 75–87.
- Chatzigiannakis I, Vitaletti A, Pyrgelis A. "A Privacy-Preserving Smart Parking System Using An Iot Elliptic Curve Based Security Platform". *Comput Commun* [Internet]. 2016;89–90:165–77. Available from: <http://dx.doi.org/10.1016/j.comcom.2016.03.014>
- Cherdantseva, Y., & Hilton, J. (2013). "A Reference Model of Information Assurance and Security". *2013 International Conference on Availability, Reliability and Security*. doi:10.1109/ares.2013.72
- Chifor, B. C., Bica, I., Patriciu, V. V., & Pop, F. (2018). "A Security Authorization Scheme For Smart Home Internet Of Things Devices". *Future Generation Computer Systems*, 86, 740-749.
- Chu, H., & Ke, Q. (2017). "Research methods: What's in the name?." *Library & Information Science Research*, 39, 284-294. <https://doi.org/10.1016/j.lisr.2017.11.001>.
- Claycomb, W. R., & Nicoll, A. (2012). "Insider Threats to Cloud Computing: Directions for New Research Challenges". *2012 IEEE 36th Annual Computer Software and Applications Conference*. doi:10.1109/compsac.2012.113
- Cordova, R. S., Maata, R. L. R., & Halibas, A. S. (2019, November). "Blowfish Algorithm Implementation on Electronic Data in A Communication Network". In 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA) (pp. 1-4). *IEEE*.
- Daniel, R. M., Rajsingh, E. B., & Silas, S. (2020). "An Efficient ECK Secure Identity Based Two Party Authenticated Key Agreement Scheme with Security Against Active Adversaries". *Information and Computation*, 275, 104630.
- Das, A. K., Zeadally, S., & He, D. (2018). "Taxonomy and Analysis of Security Protocols for Internet of Things". *Future Generation Computer System* 2018. 89, 110 – 125.
- Dastres, R., & Soori, M. (2020). "Secure Socket Layer (SSL) In the Network And Web Security". *International Journal of Computer and Information Engineering*, 14(10), 330-333.
- Davoli, L., Veltri, L., Ferrari, G., & Amadei, U. (2019). "Internet of Things on Power Line Communications: An Experimental Performance Analysis". In Smart Grids and Their Communication Systems; Kabalci, E., Kabalci, Y., Eds. *Springer*: Singapore, 2019; pp. 465–498.
- Deep, S., Zheng, X., & Hamey, L. (2019). "A survey of Security and Privacy Issues in the Internet of Things from The Layered Context". *arXiv* 2019. arXiv:1903.00846
- Dharminder, D., Mishra, D., & Li, X. (2019). "Construction of RSA-Based Authentication Scheme in Authorized Access to Healthcare Services". *Journal of Medical Systems*, 44. <https://doi.org/10.1007/s10916-019-1471-6>.
- Dhillon & Kalra PDK. "Elliptic Curve Cryptography for Real Time". *IEEE*. 2016;1–6

- Dhumane, A., Prasad, R., & Prasad, J. (2016). "Routing Issues in Internet of Things: A Survey". In *Proceedings of the International Multiconference of Engineers and Computer Scientists*, Hong Kong. Volume 1, pp. 13-20
- Diemert, D., & Jager, T. (2021). "On the Tight Security of TLS 1.3: Theoretically Sound Cryptographic Parameters for Real-World Deployments". *Journal of Cryptology*, 34, 1-57. <https://doi.org/10.1007/s00145-021-09388-x>.
- Easttom, C. (2022). "Asymmetric Algorithms". In *Modern Cryptography: Applied Mathematics for Encryption and Information Security* (pp. 233-252). Cham: Springer International Publishing.
- Gallegos, J., Kar, D., Ray, I., Ray, I., & Peccoud, J. (2020). "Securing The Exchange of Synthetic Genetic Constructs Using Digital Signatures". *ACS synthetic biology*. <https://doi.org/10.1021/acssynbio.0c00401>.
- GaneshKumar, K., & Arivazhagan, D. (2014). "Generating a Digital Signature Based on New Cryptographic Scheme for User Authentication and Security". *Indian Journal of Science and Technology*, 7, 1-5. <https://doi.org/10.17485/IJST/2014/V7IS6/59844>.
- Gopal, N. (2019). "Smart Contract for Digital Certificate using Blockchain Technology". *International Journal for Research in Applied Science and Engineering Technology*. <https://doi.org/10.22214/ijraset.2019.5488>.
- Grobauer, B., Walloschek, T., & Stöcker, E. (2011). "Understanding Cloud Computing Vulnerabilities". *IEEE Security and Privacy*. 9, 50–57. doi:10.1109/MSP.2010.115.
- Gu, P., & Chen, L. (2020, December). "An Efficient Blockchain-Based Cross-Domain Authentication and Secure Certificate Revocation Scheme". In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)* (pp. 1776-1782). IEEE.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions". *Future Generation Computer System*. 29, 1645–1660
- Hameed, S., Khan, F.I., & Hameed, B. (2019). "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review". *Journal Computer Network Communication*. 2019, 9629381.
- Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). "A Lightweight Mutual Authentication Protocol for the IoT". In *International Conference on Mobile and Wireless Technology* (pp. 3-12). Springer, Singapore.
- Hammood, W., Ruzaini, A., Hammood, O., Salwana, M., Al-Sharafi, M., & Hasan, A. (2020). "A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number". *IOP Conference Series: Materials Science and Engineering*, 769. <https://doi.org/10.1088/1757-899X/769/1/012061>.
- Hannan, M. A., Faisal, M., Ker, P. J., Begum, R. A., Dong, Z. Y., & Zhang, C. (2020). "Review Of Optimal Methods And Algorithms For Sizing Energy Storage Systems To

- Achieve Decarbonization In Microgrid Applications”. *Renewable and Sustainable Energy Reviews*, 131, 110022.
- Harnik, D., Pinkas, B., & Shulman-Peleg, A., (2017). “Side Channels in Cloud Services: Deduplication in Cloud Storage”. *IEEE Security and Privacy*. 8, 40–47. doi:10.1109/MSP.2010.187
- Harsha. A & Patil. B. (2017). “A Review: Security of Data in Cloud Storage using ECC Algorithm”. *Bonfring Int J Softw Eng Soft Comput*. 2017;6(Special Issue):143–6
- Hasan, M., & Mohan, S. (2019). “Protecting Actuators in Safety-Critical IoT Systems from Control Spoofing Attacks”. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things* (pp. 8-14).
- Hatamian, M. (2020). “Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers”. *IEEE Access*, 8, 35429-35445.
- Hedberg Jr, T. D., Krifa, S., & Camelio, J. A. (2019). “Method For Enabling a Root of Trust In Support Of Product Data Certification And Traceability”. *Journal Of Computing and Information Science in Engineering*, 19(4), 041003.
- Henricks, A., & Kettani, H. (2019, October). “On Data Protection Using Multi-Factor Authentication”. In *Proceedings of the 2019 International Conference on Information System and System Management* (pp. 1-4).
- Huang, X., & Wang, W. (2015). “A Novel and Efficient Design for an RSA Cryptosystem with a Very Large Key Size”. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 62, 972-976.
- Hussain, M., & Jain, U. (2020). “Simple And Secure Device Authentication Mechanism For Smart Environments Using Internet Of Things Devices”. *International Journal of Communication Systems*, 33.
- Im, J. H., Jeon, S. Y., & Lee, M. K. (2020). “Practical Privacy-Preserving Face Authentication For Smartphones Secure Against Malicious Clients”. *IEEE Transactions on Information Forensics and Security*, 15, 2386-2401.
- Iyanda, A. R., & Fasasi, M. E. (2022). “Development of Two-factor Authentication Login System Using Dynamic Password with SMS Verification”. *International Journal of Education and Management Engineering*, 12(3), 13.
- Jameel, F., Chang, Z., Huang, J., & Ristaniemi, T. (2019). “Internet Of Autonomous Vehicles: Architecture, Features, And Socio-Technological Challenges”. *IEEE Wireless Communications*, 26(4), 21-29.
- Jeyakumar, I. H. J., Wagner, S., & Roßnagel, H. (2019). “Implementation of Distributed Light Weight Trust Infrastructure For Automatic Validation Of Faults In An IoT Sensor Network”. *Open Identity Summit*. 2019.
- Kaaniche, N., & Laurent, M. (2017). “Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms”. *Computer Communications*. 111, 120–141. doi:10.1016/j.comcom.2017.07.006.

- Karimi, K., & Krit, S. (2019, July). "Smart Home-Smartphone Systems: Threats, Security Requirements and Open Research Challenges". In 2019 International Conference of Computer Science and Renewable Energies (ICCSRE) (pp. 1-5). *IEEE*.
- Karthikeyan, S., Patan, R., & Balamurugan, B. (2018). "Enhancement of Security in the Internet of Things (IoT) by Using X.509 Authentication Mechanism". *Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-13-2685-1_22.
- Kashif, M., Mehfuz, S., Shkeel, I., & Ahmad, S. (2023, May). "Employing an ECC-Based Hybrid Data Encryption Method to Improve Multitenancy Security in Cloud Computing". In 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON) (pp. 79-83). *IEEE*.
- Kavin, B. P., & Ganapathy, S. (2021). "A New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud Using Elliptic Curves". *Int. Arab J. Inf. Technol.*, 18(2), 180-190.
- Kim, J., & Bahn, H. (2019). "Analysis of Smartphone I/O Characteristics — Toward Efficient Swap in a Smartphone". *IEEE Access*, 7, 129930-129941. <https://doi.org/10.1109/ACCESS.2019.2937852>.
- Kothmayr, Thomas. (2013). "DTLS Based Security and Two-Way Authentication for The Internet Of Things". *Ad Hoc Network*. vol. 11, no. 8, pp. 2710-2723.
- Krawczyk, P. (2014). "When The EU Qualified Electronic Signature Becomes An Information Services Preventer". *Digital Evidence and Electronic Signature Law Review*, 7. <https://doi.org/10.14296/DEESLR.V7I0.1920>.
- Kulah, Y., Dincer, B., Yilmaz, C., & Savas, E. (2019). "SpyDetector: An Approach for Detecting Side-Channel Attacks At Runtime". *International Journal of Information Security*, 18(4), 393–422. <https://doi.org/10.1007/s10207-018-0411-7>
- Kumar, P., & Sharma, S. K. (2022). "An Empirical Evaluation of Various Digital Signature Scheme In Wireless Sensor Network". *IETE Technical Review*, 39(4), 974-984.
- Kumar, P.R., Raj, P.H., & Jelciana, P. (2018). "Exploring Data Security Issues and Solutions in Cloud Computing". *Procedia Computer Science*. 125, 691–697. doi:10.1016/j.procs.2017.12.089
- Lara-Nino, C., Díaz-Pérez, A., & Morales-Sandoval, M. (2018). "Elliptic Curve Lightweight Cryptography: A Survey". *IEEE Access*, 6, 72514-72550. <https://doi.org/10.1109/ACCESS.2018.2881444>.
- Li, L., Liu, B., Zhou, Y., & Zou, Y. (2018). SFN: "A New Lightweight Block Cipher". *Microprocessors and Microsystems*, 60, 138–150. <https://doi.org/10.1016/j.micpro.2018.04.009>
- Li, Y., Gao, M., Yang, L., Zhang, C., Zhang, B., & Zhao, X. (2020). "Design of and Research on Industrial Measuring Devices Based on Internet of Things Technology". *Ad. Hoc. Network*. 2020, 102, 102072

- Li, Z., Qouneh, A., Joshi, M., Zhang, W., Fu, X., & Li, T. (2015). "Aurora: A Cross-Layer Solution for Thermally Resilient Photonic Network-on-Chip". *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 23, 170-183. <https://doi.org/10.1109/TVLSI.2014.2300477>.
- Linden, J., Marquis, R., & Mazzella, W. (2017). "Forensic Analysis of Digital Dynamic Signatures: New Methods for Data Treatment and Feature Evaluation". *Journal of Forensic Sciences*, 62. <https://doi.org/10.1111/1556-4029.13288>.
- Liu, B., Xiao, L., Long, J., Tang, M., & Hosam, O. (2020). "Secure Digital Certificate-Based Data Access Control Scheme in Blockchain". *IEEE Access*, 8, 91751-91760. <https://doi.org/10.1109/ACCESS.2020.2993921>.
- Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., & Chen, J. (2015). "Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud". *IEEE Trans. Comput.* 64, 2609–2622. doi:10.1109/TC.2014.2375190
- Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe. (2017). "A Security Framework for the Internet of Things in the Future Internet Architecture". *Future Internet* 2017, 9, 1–27
- Mellenbergh, G., Adèr, H., Baird, D., Berger, M., Cornell, J., Hagenaars, J., & Molenaar, P. (2003). "Conceptual Issues of Research Methodology For The Behavioral, Life And Social Sciences". *The Statistician*, 52, 211-218. <https://doi.org/10.1111/1467-9884.00352>.
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2016) "Internet of Things: Vision, Applications and Research Challenges". *Ad Hoc Networks*. vol. 10, no. 7, pp. 1497–1516
- Mohsen, N. A., & Jha, N. K. (2016). "A Comprehensive Study of Security of Internet-of-Things". *IEEE Trans. Emerg. Top. Comput.* 2016, 5, 586–602.
- Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). "A Survey of IoT Security Based on A Layered Architecture Of Sensing And Data Analysis". *Sensors*, 20(13), 3625.
- Nia, M., Sajedi, A., & Jamshidpey, A. (2014). "An Introduction to Digital Signature Schemes". *ArXiv*, abs/1404.2820.
- Nimmy, K., Sankaran, S., Achuthan, K., & Calyam, P. (2021). "Lightweight And Privacy-Preserving Remote User Authentication for Smart Homes". *IEEE Access*, 10, 176-190.
- Nwabuwe, A., Sanghera, B., Alade, T., & Olajide, F. (2023). "Fraud Mitigation in Attendance Monitoring Systems using Dynamic QR Code, Geofencing and IMEI Technologies". *International Journal of Advanced Computer Science and Applications*, 14(4).
- O'Dea, S. (2021). "Forecast number of mobile users worldwide 2020-2025". Retrieved March 15, 2022, from <https://www.statista.com/statistics/218984/number-of-globalmobile-users-since-2010/>
- Oh, B., Ahn, J., Bae, S., Son, M., Lee, Y., Kang, M., & Kim, Y. (2023). "Preventing SIM Box Fraud Using Device Model Fingerprinting". *In NDSS Symposium*.

- Oudah, M. S., & Maolood, A. T. (2022). "Lightweight Authentication Model for IoT Environments Based on Enhanced Elliptic Curve Digital Signature and Shamir Secret Share". *International Journal of Intelligent Engineering & Systems*, 15(5).
- Paar, C., & Pelzi, J. (2010). "Understanding Cryptography". *Springer*.
- Pangan, A. M. S., Lacuesta, I. L., Maborang, R. C., & Ferrer, F. P. (2022). "Authenticating Data Transfer Using RSA-Generated QR Codes". *European Journal of Information Technologies and Computer Science*, 2(4), 18-30.
- Phun, J. A. P. Y., & Safitri, C. (2021, November). "Smartphone Authentication with Hand Gesture Recognition (HGR) Using LiDAR". In 2021 5th International Conference on Informatics and Computational Sciences (ICICoS) (pp. 93-98). *IEEE*.
- Poorni, R., Lakshmanan, M., & Bhuvaneshwari, S. (2019, July). "DIGICERT: A Secured Digital Certificate Application Using Blockchain Through Smart Contracts". In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 215-219). *IEEE*.
- Ramesh, K., Ganeshkumar, P., Gokul, B., & Sharma, K. Y. (2022, February). "Digital Certificate-Based User Authentication to Access Networks and Hosts". In International Conference on Computing, Communication, Electrical and Biomedical Systems (pp. 437-445). Cham: *Springer International Publishing*.
- Rashid, F., Miri, A., & Woungang, I. (2012). "A Secure Data Deduplication Framework for Cloud Environments". In *Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, Paris, France*. pp. 81–87. doi:10.1109/PST.2012.6297923
- Razi, F., Suandi, I., & Fahmi, F. (2019). "Energy Consumption Optimization by Increasing the Processor Speed of Moving Communication Devices in Transport Layer Protocol". *Jurnal Litek: Jurnal Listrik Telekomunikasi Elektronika*, 16(2), 30-35.
- Rishu, V. K., & Sinha, S. A. (2021). "Advancements in Encryption Techniques for Enhanced Data Security Over Cloud". *Journal of Cybersecurity and Information Management*, 8(2), 51-59.
- Roman, R., Zhou, J., & Lopez, J. (2013). "On the Features and Challenges of Security and Privacy in Distributed Internet of Things". *Computer Networks*, vol. 57, no. 10, pp. 2266 – 2279.
- Roy, A., & Karforma, S. (2014). "Authentication of user in E-Governance: A Digital Certificate based approach". *International Journal of scientific research and management (IJSRM)*, 2(8), 1212-1221.
- Saho, N. J. G., & Ezin, E. C. (2020, October). "Comparative Study on The Performance Of Elliptic Curve Cryptography Algorithms With Cryptography Through RSA Algorithm". In *CARI 2020-Colloque Africain sur la Recherche en Informatique et en Mathématiques Appliquées*.

- Salunke, R., Bansod, G., & Naidu, P. (2019). "Design and Implementation of a Lightweight Encryption Scheme for Wireless Sensor Nodes". In *Advances in Intelligent Systems and Computing* (pp. 566–581). Springer, Cham. https://doi.org/10.1007/978-3-030-22868-2_41
- Sann, Z., Soe, T., Knin, K., & Win, Z. (2019). "Performance Comparison of Asymmetric Cryptography (Case Study-Mail Message)". *APTIKOM Journal on Computer Science and Information Technologies*, 4(3), 105-111.
- Sharma, V., Kim, J., Kwon, S., You, I., Lee, K., & Yim, K. (2018). "A Framework for Mitigating Zero-Day Attacks in IoT". *arXiv* 2018. arXiv:1804.05549
- Sicari, S., Rizzardi, A., & Grieco, L.A. (2015). "A Security, Privacy and Trust in Internet of Things: The Road Ahead". *Computer Network*. 2015, 76, 146–164
- Siddiqui, Z., Gao, J., & Khan, M. K. (2022). "An Improved Lightweight PUF-PKI Digital Certificate Authentication Scheme for The Internet of Things". *IEEE Internet of Things Journal*, 9(20), 19744-19756.
- Silva, R., Ferreira, J., Rivera, J., Souza, S., & Nascimento-e-Silva, D. (2020). "Definition, Elements And Stages Of Elaboration Of Research Protocols". *Research, Society and Development*. <https://doi.org/10.33448/RSD-V9I10.8721>.
- Sinha R, Srivastava HK, & Gupta S. (2013). "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography". *Int J Sci Eng*. 2013;4(5):720–5
- Suárez-Albela M, Fraga-Lamas P, Castedo L, Fernández-Caramés T. "Clock Frequency Impact on the Performance of High-Security Cryptographic Cipher Suites for Energy-Efficient Resource-Constrained IoT Devices". *Sensors* [Internet] 2018;19(1):15. Available from: <http://www.mdpi.com/1424-8220/19/1/15>
- Sudha, K. S., & Jeyanthi, N. (2021). "A Review on Privacy Requirements and Application Layer Security In Internet Of Things (IoT)". *Cybernetics and Information Technologies*, 21(3), 50-72.
- Thronicke, W. (2013). "Scalable Monitoring System for Clouds". In *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, Dresden, Germany. 9–12
- Tirfe, D., & Anand, V. K. (2022). "A Survey on Trends of Two-Factor Authentication. In Contemporary Issues in Communication, Cloud and Big Data Analytics". *Proceedings of CCB 2020* (pp. 285-296). Springer Singapore.
- Uahhabi, Z., & Bakkali, H. (2016). "An Approach for Evaluating Trust in X.509 Certificates". 2016 11th *International Conference for Internet Technology and Secured Transactions (ICITST)*, 196-203. <https://doi.org/10.1109/ICITST.2016.7856696>.
- Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). "Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, And Future Trends: A Comprehensive Survey". *Computer Science Review*, 47, 100530.

- Wahlström, J., Skog, I., Händel, P., & Nehorai, A. (2016). "IMU-Based Smartphone-to-Vehicle Positioning". *IEEE Transactions on Intelligent Vehicles*, 1, 139-147. <https://doi.org/10.1109/TIV.2016.2588978>.
- Williams, Patricia, A. H., & Vincent. M. (2016). "Always Connected: The Security Challenges of The Healthcare IoT". *IEEE 3rd World Forum on IoT (WF-IoT)*. 2016, doi:10.1109/wf-iot.2016.7845455 2
- Xie, N., Li, Z., & Tan, H. (2020). "A Survey of Physical-Layer Authentication in Wireless Communications". *IEEE Communications Surveys & Tutorials*, 23(1), 282-310.
- Xu, L., Shao, G., Cao, Y., Yang, H., Sun, C., Zhang, T. & He, X. (2019, October). "Research on Telecom Big Data Platform of LTE/5G Mobile Networks". In 2019 *IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)* (pp. 756-761). IEEE.
- Yaqoob, I., Hashem, I.A.T., Ahmed, A., & Kazmi, S.A. (2019). "Internet of Things Forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges". *Future Generations Computer System*. 2019, 92, 265–275
- Yaswanth, A., & Reddy, K. T. (2023). "A Novel Dynamic Randomized Secret Key Model Based on One-Time Password Authentication". *International Journal of Intelligent Systems and Applications in Engineering*, 11(3), 850-858.
- Yin, R.K., (1984). "Case Study Research: Design and Methods". Beverly Hills, Calif: *Sage Publications*.
- Yu, S., & Guo, S. (2016). "Big Data Concepts, Theories, and Applications". *Springer International Publishing: Cham, Switzerland*. (pp. 1–437). doi:10.1007/978-3-319-27763-9
- Yu, Y., He, J., Zhu, N., Cai, F., & Pathan, M. (2018). "A New Method for Identity Authentication Using Mobile Terminals". *Procedia Computer Science*, 131, 771-778.
- Yuvaraj, N., Raja, R. A., Karthikeyan, T., & Pragmahash, K. (2022). "Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) Using Opposition Frog Leaping Algorithm to Resist Man-In-Middle Attack". *Wireless Personal Communications*, 123(2), 1715-1731.
- Zhang, Q. (2021, January). "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption". In 2021 2nd International Conference on Computing and Data Science (CDS) (pp. 616-622). *IEEE*.
- Zhu, T., Qu, Z., Xu, H., Zhang, J., Shao, Z., Chen, Y., Prabhakar, S., & Yang, J. (2020). "RiskCog: Unobtrusive Real-Time User Authentication on Mobile Devices in the Wild". *IEEE Transactions on Mobile Computing*, 19, 466-483. <https://doi.org/10.1109/TMC.2019.2892440>.

Zhu, W., & Lin, J. (2016). "Generating Correlated Digital Certificates: Framework and Applications". *IEEE Transactions on Information Forensics and Security*, 11, 1117-1127. <https://doi.org/10.1109/TIFS.2016.2516818>.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA