Name: Dr. Gaurav Pareek

Designation: Assistant Professor

E-mail: gaurav_pareek@diu.iiitvadodara.ac.in

Academic Qualifications:

- Ph. D. in Computer Science and Engineering. Thesis title: “Cryptographic Solutions for Secure Sharing of Outsourced Data”
  Institute: National Institute of Technology (NIT) Goa
  Year: 2020
  Specialization: Cryptography and Information Security
- M. Tech. in Computer Science and Engineering
  Institute: Central University of Rajasthan
  Year: 2013
- B. Tech. in Computer Engineering
  Institute: Government Engineering College Ajmer
  Year: 2011

Research Interests:

- Cryptography, Information Security, Cloud Security, Access Control.

Publications:

Journals:

1. Gaurav Pareek and B R Purushothama. KAPRE: Key-Aggregate Proxy Reencryption for Secure and Flexible Data Sharing in Cloud Storage. Journal of Information Security and Applications. DOI: https://doi.org/10.1016/j.jisa.2021.103009
2. Gaurav Pareek and B R Purushothama. Secure and Efficient Revocable KeyAggregate Cryptosystem for Multiple Non-Predefined Non-Disjoint Aggregate Sets. Journal of Information Security and Applications, 58: 102799. DOI: https://doi.org/ 10.1016/j.jisa.2021.102799
3. Gaurav Pareek and B R Purushothama. TP-PRE: Threshold Progressive Proxy Re-encryption, its Definitions, Construction and Applications. Journal of Ambient Intelligence and Humanized Computing, Springer, 12: 1943–1965. DOI: https://doi. org/10.1007/s12652-020-02285-4
4. Gaurav Pareek and B R Purushothama. Proxy Re-encryption for Fine-Grained Access Control: its Applicability, Security under Stronger Notions and Performance. Journal of Information Security and Applications, 54: 102453. DOI: https://doi.org/ 10.1016/j.jisa.2020.102543
5. Gaurav Pareek and B R Purushothama. Extended Hierarchical Key Assignment Scheme (E-HKAS): How to efficiently enforce explicit policy exceptions in dynamic hierarchies. Sadhana – Academy Proceedings in Engineering Sciences 44(12):235, 2019. DOI: https://doi.org/10.1007/s12046-019-1216-8
6. Gaurav Pareek and B R Purushothama. Provably secure group key management scheme based on proxy re-encryption with constant public bulletin size and key derivation time. Sadhana – Academy Proceedings in Engineering Sciences, 43(9):137, 2018. DOI: https://doi.org/10.1007/s12046-018-0917-8

7. Gaurav Pareek and B R Purushothama. Blockchain-Based Decentralized Access Control Scheme for Dynamic Hierarchies. International Journal of Information and Computer Security (IJICS), Vol.16 No.3/4, pp. 324 - 354. DOI: https://dx.doi.org/10.1504/IJICS.2021.118956

Conferences:

1. Gaurav Pareek and B R Purushothama. Flexible cryptographic access control through proxy re-encryption between groups. In Proceedings of the 20th International Conference on Distributed Computing and Networking (ICDCN'19), IISc Bangalore, India, pages 507–507. ACM, 2019.
2. Gaurav Pareek and B R Purushothama. Proxy re-encryption scheme for access control enforcement delegation on outsourced data in public cloud. In Proceedings of the 14th International Conference on Information Systems Security (ICISS'18), IISc Bangalore, India, pages 251–271. LNCS Springer, 2018. (Published by Springer LNCS)
3. Gaurav Pareek and B R Purushothama. Efficient strong key indistinguishable access control in dynamic hierarchies with constant decryption cost. In Proceedings of the 11th International Conference on Security of Information and Networks (SIN'18), Cardiff University, United Kingdom, page 10:1–10:7. ACM, 2018.
4. Gaurav Pareek and B R Purushothama, On Efficient Access Control Mechanisms in Hierarchy using Unidirectional and Transitive Proxy Re-encryption Schemes, In Proceedings of 14th International conference on Security and Cryptography (SECRYPT'17), Madrid University, Spain, July 24-26, 2017, pp. 519-524. (SCITEPRESS Digital Library)
5. Gaurav Pareek and B R Purushothama, A Proxy Visible Re-encryption Scheme with Application to Email Forwarding, In Proceedings of 10th International Conference on Security of Information and Networks, 2017 (SIN '17), Manipal University Jaipur and MNIT Jaipur, October 13-15, 2017, pp. 212-217. [Adjudged BEST PAPER of the conference]
6. Gaurav Pareek and B R Purushothama. A provably secure re-encryption-based access control in hierarchy. In 5 th International Conference on Advanced Computing, Networking, and Informatics (ICACNI '17), NIT Goa, India, pages 97–104. Springer, 2019.
7. Sarvesh V Sawant, Gaurav Pareek, and B R Purushothama. Group key management under strong active adversary model: A security analysis. In Proceedings of the 6th International Symposium on Security in Computing and Communication (SSCC'18), PES Institute of Technology, India, pages 403–418. CCIS Springer, 2018.
8. Ashwini chaudhari, Gaurav Pareek, and B R Purushothama. Security analysis of centralized group key management schemes for wireless sensor networks under strong active outsider adversary model. In Proceedings of the 7th International Conference on Advances in Computing, Communications and Informatics (ICACCI'17), Manipal University, India, pages 1576–1581. IEEE, 2017.
9. Sarvesh V Sawant, Gaurav Pareek, and B R Purushothama. A ringer-based throttling approach to mitigate ddos attacks. In Proceedings of the 5th International Symposium on Security in Computing and Communication (SSCC'17), Manipal University, India, pages 95–108. CCIS Springer, 2017.
10. Chandrasekhar K., Kethzi G., Prabhav S., Gaurav Pareek, and Purushothama B R. Outsource-secured calculation of closest pair of points. In International Symposium on Security in Computing and Communication (SSCC'16), LNM Institute of Information Technology India, pages 377–389. CCIS Springer, 2016.

11. Gaurav Pareek, Ratna Kumari, and Aitha Nagaraju. Mobile sensor localization under wormhole attacks: An analysis. In Proceedings of the 3rd International Symposium on Intelligent Informatics, Galgotias University, India, pages 129–137. Springer, 2015.
12. Gaurav Pareek, Chetanya Goyal, and Mukesh Nayal. A result verification scheme for mapreduce having untrusted participants. In Proceedings of the 3rd International Symposium on Intelligent Informatics, Galgotias University, India, pages 11–19. Springer, 2015.

Book Chapters:

1. P K D Pramanik, Gaurav Pareek, and Anand Nayyar. Security and privacy in remote healthcare: Issues, solutions, and standards. In Telemedicine Technologies, pages 201–225. Academic Press Elsevier, 2019. (Published by Elsevier, SCOPUS Indexed)
2. P K D Pramanik, Anand Nayyar and Gaurav Pareek. WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring: Architecture and Protocols. Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare, page 89–119, Academic Press Elsevier, 2019. (Published by Elsevier, SCOPUS Indexed)
3. P K D Pramanik, Saurabh Pal, Gaurav Pareek, Shubhendu Dutta, and Prasenjit Choudhury. Crowd computing: The computing revolution. In Crowdsourcing and Knowledge Management in Contemporary Business Environments, pages 166–198. IGI Global, 2019.