Assistant Professor
Department of CSE
IIIT Kalyani, West Bengal
☎ : +91-8797369160
✉ : *hafi786@gmail.com*

Dr. SK Hafizul Islam

Ph.D (IIT(ISM) Dhanbad) & M.Tech (IIT(ISM) Dhanbad)

Google Scholar Citation of My Research Paper is 827

About Myself

I received **Ph.D** in **Computer Science and Engineering** from **Indian Institute of Technology (ISM), Dhanbad, India**, under the **INSPIRE Fellowship Ph.D Program**, funded by **DST, Govt. of India**. I did **M.Tech (CA)** from **IIT(ISM) Dhanbad** in 2009. Presently, I am working as an **Assistant Professor** in Computer Science and Engineering in **Indian Institute of Information Technology, Kalyani**, West Bengal, India. Before joining IIIT Kalyani, I worked as an **Assistant Professor** in the **Department of Computer Science and Information Systems, Birla Institute of Technology and Science (BITS Pilani), Pilani Campus, Rajasthan, India**. I received **University Gold Medal**, **S.D. Singha Memorial Endowment Gold Medal** and **Sabitri Parya Memorial Endowment Gold Medal** from **Vidyasagar University**, West Bengal, India in 2006. I worked as a **Project Associate** in the project **Information Security Education and Awareness (ISEA)**, No.: MIT(2)/2006-08/189/CSE, funded by **Ministry of Communication and Information Technology, Govt. of India**. I also received **University Gold Medal** from **IIT(ISM) Dhanbad** in 2009. I received **OPERA award** from **BITS Pilani** in 2015. **I have 04 Yrs. and 10 Months (03 Yrs. and 10 months Post-Ph.D, and 01 Yr. Pre-Ph.D) teaching and research experiences**, and **published sixty five research papers** in Journals and Conference proceedings of international reputes. **I have forty SCI-E and seven SCOPUS indexed International Journals**. Presently, I am serving as an **Associate Editor** of well-reputed journal **"International journal of Communication System"** published by **Wiley**. I also served as a reviewer in many reputed International Journals and Conferences. My research interest includes Cryptography and Information Security. My personal homepage can be visited at **https://sites.google.com/site/hafi786/**.

Objective

To excel in the field of teaching with the help of providing consistently improved skills and updated knowledge, and performing Research & Development activities in the field of Computer Science and Engineering where Mathematics is an integral part.

Specialization

Cryptography and Information Security

Research Interests

Elliptic Curve Cryptography (ECC), Certificateless Public Key Cryptography (CL-PKC), Identity-based Cryptosystem/Encryption (IBC/IBE), Self-certified Public Key Cryptography (SC-PKC), Authenticated Key Agreement (AKA) Protocol, Digital Signature Scheme (DSS), Remote User Mutual Authentication Scheme (RUMA).

Ph.D Guidance

- **Somen Mondal**, Assistant Professor, Department of Computer Science and Engineering, Elite College of Engineering, Kolkata
  Title: Big Data and Data Access Control
  Guide: Dr. SK Hafizul Islam (IIIT Kalyani) & Dr. Avik Chatterjee (Calcutta University)
  Status: Not yet registered

International Journal [SCIE]

1. **SK Hafizul Islam**, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, M.K.C. Reddy, "A Robust and Efficient Password-based Conditional Privacy Preserving Authentication and Group-Key Agreement Protocol for VANETs", **Future Generation Computer Systems (Elsevier)[SCIE], IF: 3.997(Accepted on 2nd July, 2017)**.
2. R. Amin, R. S. Sherratt, D. Giri, **SK Hafizul Islam**, M. K. Khan, "A Software Agent Enabled Biometric Security Algorithm for Secure File Access in Consumer Storage Devices", **IEEE Transaction on Consumer Electronics [SCIE], Vol. 63, No. 1, pp. 53-61, 2017. IF: 1.12**.
3. R. Amin, **SK Hafizul Islam**, P. Vijayakumar, M. K. Khan, V. Chang, "A Robust and Efficient Bilinear Pairing Based Mutual Authentication and Session Key Verification Scheme Over Insecure Communication", **Multimedia Tools and Applications (Springer)[SCIE], 2017. IF: 1.530DOI: 10.1007/s11042-017-4996-z**.
4. P. Gope, R. Amin, **SK Hafizul Islam**, N. Kumar, V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for

distributed IoT infrastructure with secure localization services for smart city environment", **Future Generation Computer Systems (Elsevier)[SCIE], IF: 3.997(Accepted on 20th June, 2017)**.

5. R. Amin, **SK Hafizul Islam**, M. K. Khan, A. Karati, D. Giri, S. Kumari, "An Efficient and Robust Smartcard-based Multi-Server Authentication Scheme using RSA Cryptosystem", **Security and Communication Networks (Hindwai)[SCIE], IF: 0.806(Accepted on 18th May, 2017)**.
6. S. Kumari, A. K. Das, X. Li, F. Wu, M. K. Khan, Q. Jiang, **SK Hafizul Islam**, "A Provably Secure Biometrics-based Authenticated Key Agreement Scheme for Multi-server Environments", **Multimedia Tools and Applications (Springer)[SCIE], 2017.IF: 1.530 DOI: 10.1007/s11042-017-4390-x**.
7. T. Maitra, M. S. Obaidat, R. Amin, **SK Hafizul Islam**, S. A. Chaudhry, D. Giri, "A robust ElGamal based password authentication protocol using smart-card for client-server communication", **International Journal of Communication Systems (Wiley) [SCIE], 2016. DOI: 10.1002/dac.3242. IF: 1.066**.
8. P. Vijayakumara, R. Naresh, **SK Hafizul Islam**, L. J. Deborah, "An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies", **Security and Communication Networks (Wiley)[SCIE], 2016. DOI: 10.1002/sec.1680. IF: 0.806**.
9. T. Maitra, R. Amin, **SK Hafizul Islam**, D. Giri, M. K. Khan, N. Kumar, "An enhanced multi-server authentication protocol using password and smart card: Cryptanalysis and Design", **Security and Communication Networks (Wiley)[SCIE], Vol. 9, pp. 4615-4638, 2016. IF: 0.806**.
10. R. Amin, **SK Hafizul Islam**, G. P. Biswas, D. Giri, M. K. Khan, N. Kumar, "A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments", **Security and Communication Networks (Wiley)[SCIE], Vol. 9, pp. 4650-4666, 2016.IF:0.806**.
11. T. Maitra, M. S. Obaidat, **SK Hafizul Islam**, D. Giri, R. Amin, "Security Analysis and Design of An Efficient ECC-based Two-Factor Password Authentication Scheme", **Security and Communication Networks (Wiley)[SCIE], Vol. 9, pp. 4166-4181, 2016. IF:0.806**.
12. P. Vijayakumara, R. Naresh, L. J. Deborah, **SK Hafizul Islam**, "An efficient group key agreement protocol for secure P2P communication", **Security and Communication Networks (Wiley)[SCIE], Vol. 9, pp. 3952-3965, 2016. IF: 0.806**.
13. X. Li, K. Wang, J. Shen, S. Kumari, F. Wu, **SK Hafizul Islam**, "Secure Data Access and Sharing Scheme for Cloud Storage", **Wireless Personal Communications (Springer) [SCIE], 2016. DOI: 10.1007/s11277-016-3293-x. IF: 0.951**.
14. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, N. Kumar, 'A robust and anonymous patient monitoring system using wireless medical sensor networks", **Future Generation Computer Systems (Elsevier)[SCIE], 2016. DOI:10.1016/j.future.2016.05.032. IF: 3.997**.
15. **SK Hafizul Islam**, R. Amin, G. P. Biswas, M. S. Obaidat, M.K. Khan, "Provably secure pairing-free identity-based partially blind signature scheme and its application in online e-cash system", **Arabian Journal for Science and Engineering (Springer)[SCIE], 2016. DOI: 10.1007/s13369-016-2115-5. IF: 0.865**.
16. **SK Hafizul Islam**, A. K. Das, M. K. Khan, "Design of a provably secure identity-based digital multi-signature scheme using biometrics and fuzzy extractor", **Security and Communication Networks (Wiley) [SCIE], Vol. 9, No. 16, pp.3229-3238, 2016. IF: 0.806**.
17. **SK Hafizul Islam**, M.S. Obaidat, R. Amin, "An Anonymous and Provably Secure Authentication Scheme for Mobile User", **International Journal of Communication Systems (Wiley)[SCIE], vol. 29, No. 09, pp. 1529-1544, 2016. IF: 1.066**.
18. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, L. Leng, N. Kumar, "Design of Anonymity-Preserving, Three-Factor Authenticated Key Exchange Protocol for Wireless Sensor Networks", **Computer Networks (Elsevier) [SCIE], vol. 101, No. 04, pp. 42-62, 2016. IF:2.516**.
19. X. Li, J. Niu, S. Kumari, **SK Hafizul Islam**, F. Wu, M. K. Khan, A. K. Das, "A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security", **Wireless Personal Communications (Springer) [SCIE], Vol. 89, No. 2, pp. 569-597, 2016. IF: 0.951**.
20. S. A. Chaudhry, M. S. Farash, H. Naqvi, **SK Hafizul Islam**, T. Shon, "A robust and efficient privacy aware handover authentication scheme for wireless networks', **Wireless Personal Communications (Springer) [SCIE], 2015. IF: 0.951. DOI: 10.1007/s11277-015-3139-y**.
21. **SK Hafizul Islam**, A. K. Das, M. K. Khan, "An efficient biometric-based password authentication scheme for client-server environment using ECC and fuzzy extractor", **International Journal of Ad Hoc and Ubiquitous Computing [SCIE] (Accepted on 02 November, 2015), IF:0.66. DOI: 10.1504/IJAHUC.2015.10001794**
22. **SK Hafizul Islam**, "Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps", **Information Sciences (Elsevier)[SCIE], vol. 312, pp. 104-130, 2015. IF: 4.832**.
23. **SK Hafizul Islam**, G. P. Biswas, "Provably secure and pairing-based strong designated verifier signature scheme with message recovery", **Arabian Journal for Science and Engineering (Springer)[SCIE], vol. 40, no. 04, pp. 1069-1080, 2015. IF:0.865**.
24. **SK Hafizul Islam**, G. P. Biswas, "Design of two-party authenticated key agreement protocol based on ECC and self-certified public keys", **Wireless Personal Communications (Springer) [SCIE], Vol. 82, No. 4, pp. 2727-2750, 2015. IF:0.951**.
25. **SK Hafizul Islam**, A. Singh, "Provably secure one-round certificateless authenticated group key agreement protocol for secure communications", **Wireless Personal Communications (Springer) [SCIE], Vol. 85, No. 3, pp. 879-898, 2015. IF:0.951**.
26. **SK Hafizul Islam**, M. S. Obaidat, "Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing", **Security and Communication Networks [SCIE], Vol. 8, No. 18, pp. 4319-4332, 2015. IF: 0.806**.
27. **SK Hafizul Islam**, M. K. Khan, X. Li, "Security analysis and improvement of 'a more secure anonymous user authentication scheme for the integrated EPR information system' ", **PLOS ONE [SCIE], 10 (8): e0131368, 2015. DOI: 10.1371/journal.pone.01313682015 IF: 3.54**.
28. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, M. S. Obaidat, "Design and Analysis of an Enhanced Patient-Server Mutual Authentication Protocol for Telecare Medical Information System", **Journal of Medical Systems (Springer)[SCIE], 39 (11), 2015. DOI: 10.1007/s10916-015-0307-2. IF:2.456**.
29. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, X. Li, "Cryptanalysis and Enhancement of Anonymity Preserving Remote User Mutual Authentication and Session Key Agreement Scheme for E-Health Care Systems", **Journal of Medical Systems (Springer)[SCIE], 39 (11), 2015. DOI: 10.1007/s10916-015-0318-z. IF:2.456**.
30. **SK Hafizul Islam**, M. S. Farash, G. P. Biswas, M. K. Khan, M. S. Obaidat, "Provably secure and pairing-free certificateless digital multisignature scheme using elliptic curve cryptography", **International Journal of Computer Mathematics (Taylor & Francis)**

[SCIE], 2015. DOI: 10.1080/00207160.2015.1088148. IF:0.577.

31. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, N. Kumar, "An Efficient and Practical Smart Card Based Anonymity Preserving User Authentication Scheme for TMIS using Elliptic Curve Cryptography", **Journal of Medical Systems (Springer)[SCIE], 39 (11) 180, 2015. DOI: 10.1007/s10916-015-0351-y. IF:2.456**.
32. M. S. Farash, **SK Hafizul Islam**, M. S. Obaidat, "A provably secure and efficient two-party password-based explicit authenticated key exchange protocol", **Concurrency and Computation: Practice and Experience (Wiley) [SCIE], 2015. DOI: 10.1002/cpe.3477. IF: 1.133**.
33. **SK Hafizul Islam**, M. K. Khan, M. S. Obaidat, F. T. B. Muhaya, "Provably secure and anonymous password authentication protocol for roaming service in global mobility networks using extended chaotic maps", **Wireless Personal Communications (Springer)[SCIE], vol. 84, no. 3, pp. 2013-2034, 2015. IF:0.951**.
34. **SK Hafizul Islam**, F. Li, "Leakage-free and provably secure certificateless signcryption scheme using bilinear pairings", **The Computer Journal [SCIE], OXFORD University Press, The British Computer Society (BCS), 2015. DOI: 10.1093/comjnl/bxv002.IF:1.000**.
35. **SK Hafizul Islam**, "Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps", **Nonlinear Dynamics (Springer)[SCIE], vol. 78, no. 3, pp. 2261-2276, 2014. IF:3.464**.
36. **SK Hafizul Islam**, "Design and analysis of an improved smartcard based remote user password authentication scheme", **International Journal of Communication Systems (Wiley)[SCIE], Vol. 29, pp. 1708-1719, 2016. IF: 1.066**.
37. **SK Hafizul Islam**, "A provably secure ID-based mutual authentication and key agreement scheme for mobile multi-server environment without ESL attack", **Wireless Personal Communications (Springer)[SCIE], vol. 79, pp. 1975-1991, 2014. IF:0.951**.
38. **SK Hafizul Islam**, M. K. Khan, "Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems", **Journal of Medical Systems (Springer)[SCIE], vol. 38, no. 10, pp. 1-16, 2014. IF:2.456**.
39. **SK Hafizul Islam**, M. K. Khan, A. M. Al-Khouri, "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing", **Security and Communication Networks (Wiley) [SCIE], 2014. DOI: 10.1002/sec.1165. IF:0.806**.
40. **SK Hafizul Islam**, M. K. Khan, "Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks", **International Journal of Communication Systems (Wiley) [SCIE], Vol. 29, pp. 2442-2456, 2016. IF:1.066**.
41. **SK Hafizul Islam**, G. P. Biswas, "Design of Improved Password Authentication and Update Scheme based on Elliptic Curve Cryptography", **Mathematical and Computer Modelling (Elsevier)[SCIE], vol. 57, no. 11-12, pp. 2703-2717, 2013. IF:1.412**.
42. **SK Hafizul Islam**, G. P. Biswas, "Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography", **International Journal of Computer Mathematics (Taylor & Francis)[SCIE], vol. 90, no. 11, pp. 2244-2258, 2013. IF:0.577**
43. **SK Hafizul Islam**, G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile network", **Annals of Telecommunications (Springer)[SCIE], vol. 67, no. 11-12, pp. 547-558, 2012. IF:1.412**.
44. **SK Hafizul Islam**, G. P. Biswas, "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem", **Journal of Systems and Software (Elsevier)[SCIE], vol. 84, no. 11, pp. 1892-1898, 2011**. **[Most Downloaded article, December 2011] IF:2.444**.

International Journal [SCOPUS]

1. **SK Hafizul Islam**, G. P. Biswas, "Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system", **Journal of King Saud University - Computer and Information Sciences (Elsevier)[SCOPUS], Vol. 27, No. 2, pp. 211-221, 2015**.
2. **SK Hafizul Islam**, G. P. Biswas, "A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication", **Journal of King Saud University - Computer and Information Sciences (Elsevier)[SCOPUS], Vol. 29, No. 1, pp. 6373, 2017**.
3. **SK Hafizul Islam**, R. Amin, G. P. Biswas, M. S. Faras, X. Li, S. Kumari."An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments", **Journal of King Saud University - Computer and Information Sciences (Elsevier)[SCOPUS], Vol. 29, No. 3, pp. 311-324, 2017.**.
4. **SK Hafizul Islam**, G. P. Biswas, "A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings", **Journal of King Saud University - Computer and Information Sciences (Elsevier) [SCOPUS], vol. 26, no. 1, pp. 55-67, 2014, [One of the top 20 most downloaded articles, May 2013]**.
5. **SK Hafizul Islam**, G. P. Biswas, "Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings" **Journal of King Saud University - Computer and Information Sciences (Elsevier) [SCOPUS], vol. 26, no. 1, pp. 89-97, 2014**.
6. **SK Hafizul Islam**, G. P. Biswas, "Dynamic ID-based remote user authentication scheme with smartcard using elliptic curve cryptography", **Journal of Electronics (Springer)[SCOPUS], vol. 31, no. 5, pp. 473-488, 2014.**
7. **SK Hafizul Islam**, G. P. Biswas, "Provably secure certificateless strong designated verifier signature scheme based on elliptic curve bilinear pairings", **Journal of King Saud University - Computer and Information Sciences (Elsevier) [SCOPUS], vol. 25, pp. 51-61, 2013, One of the top 25 most downloaded articles, May 2013]**.

International Journal [Non-SCI and Non-SCOPUS]

1. **SK Hafizul Islam**, G. P. Biswas, K-K. R. Choo, "Cryptanalysis of an Improved Smartcard-based Remote Password Authentication Scheme", **Information Sciences Letter, vol. 3, no. 1, pp. 35-40, 2014. IF:1.739**
2. **SK Hafizul Islam**, G. P. Biswas, "Cryptanalysis of Lin et al.'s digital multi-signature scheme on the generalized conic curve over Z_n" **Information Sciences Letter, vol. 3, no. 2, pp. 63-68, 2014. IF:1.739**
3. **SK Hafizul Islam**, G. P. Biswas, "An efficient and secure strong designated verifier signature scheme without bilinear pairings", **Journal of Applied Mathematics and Informatics (Korea), vol. 31, no. 3-4, pp. 425 - 441, 2013**.
4. **SK Hafizul Islam**, G. P. Biswas, "An efficient and provably-secure digital signature scheme based on elliptic curve bilinear pairings",

Theoretical and Applied Informatics (Polish Academy of Science), vol. 24, no. 2, pp. 109-118, 2012. **[Most Downloaded article, 2012]**.

5. **SK Hafizul Islam**, G. P. Biswas, "An improved ID-based client authentication with key agreement scheme on ECC for mobile client-server environments", **Theoretical and Applied Informatics (Polish Academy of Science)**, vol. 24, no. 4, pp. 293-312, 2012. **[One of the top 20 most downloaded articles, May 2013]**.

International Conference

1. **SK Hafizul Islam**, V. Rajeev, R. Amin, "A Robust and Efficient Three-Factor Authentication and Session Key Agreement Mechanism for SIP", **Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM17)**, February 3-4, 2017 at University College of Engineering Tindivanam, Melpakkam, Tindivanam, Tamil Nadu 604001, India.
2. **SK Hafizul Islam**, M. S. Obaidat, V. Rajeev, R. Amin, "Design of a certificateless designated server based searchable public key encryption scheme", **Third International Conference on Mathematics and Computing (ICMC 2017)**, pp. 3-15, DOI: 10.1007/978-981-10-4642-1_1. January 17-21, 2017 at Haldia Institute of Technology, India.
3. R. Amin, **SK Hafizul Islam**, A. Karati, G.P. Biswas, "Design of an Enhanced Authentication Protocol and Its Verification using AVISPA", **In: Proceedings of the 3rd IEEE International Conference on Recent Advances in Information Technology (RAIT 2016)** DOI: 10.1109/RAIT.2016.7507936. ISM Dhanbad, March 03-05, 2016.
4. R. Garg, K. Patel, M. Gupta, **SK Hafizul Islam**, R. Amin, G.P. Biswas, "Design of Secure Authentication Protocol in SOCKS V5 for VPN using Mobile Phone", **In: Proceedings of the IEEE International Conference on Trends in Automation, Communication and Computing Technologies (ITACT 2015)**, pp. 1-6, 2016, Bangalore, India. DOI: 10.1109/ITACT.2015.7492654.
5. A. Thakur, Nikhil S. R. Chware, **SK Hafizul Islam**, "A Reading Oriented Overlapping Text Based CAPTCHA", **In: Proceedings of the IEEE International Conference on Trends in Automation, Communication and Computing Technologies (ITACT 2015)**, pp. 1-6, 2016, Bangalore, India. DOI: 10.1109/ITACT.2015.7492651.
6. R. Amin, **SK Hafizul Islam**, G. P. Biswas, M. K. Khan, "An Efficient Remote Mutual Authentication Scheme using Smart Mobile Phone over Insecure Networks", **In: Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)**, pp. 1-7, June 8-9, 2015, London, UK.
7. M. K. Mishra, **SK Hafizul Islam**, G. P. Biswas, "Design of ECC-based ElGamal Encryption Scheme using CL-PKC", In: Proceedings of the International Conference in Recent Advances in Information Technology (RAIT 2014), **Advances in Intelligent Systems and Computing (Springer)**, vol. 266, pp. 27-34, 2014. Dhanbad, India.
8. **SK Hafizul Islam**, G. P. Biswas, "Comments on ID-based client authentication with key agreement protocol on ECC for mobile client-server environment", In: Proceedings of the International Conference on Advanced in Computing and Communications (ACC 2011), **CCIS, Springer-Verlag**, Part II, vol. 191, pp. 628-635, 2011. Kochi, Kerala, India.
9. **SK Hafizul Islam**, G. P. Biswas, "Improved remote login scheme based on ECC", In: Proceedings of the International Conference on Recent Trends in Information Technology (ICRTIT 2011), pp. 1221-1226, 2011. Chennai, Tamilnadu, India.
10. **SK Hafizul Islam**, G. P. Biswas, "Design of an efficient ID-based short designated verifier proxy signature scheme", In: Proceedings of the International Conference in Recent Advances in Information Technology (RAIT 2012), pp. 48-53, 2012, Dhanbad, India.
11. **SK Hafizul Islam**, G. P. Biswas, "Certificateless strong designated verifier multisignature scheme using bilinear pairings", In: Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI 2012), pp. 540-546, 2012, Chennai, Tamilnadu, India.
12. **SK Hafizul Islam**, G. P. Biswas, "An improved pairing-free identity-based authenticated key agreement protocol based on ECC", In: Proceedings of the International Conference on Communication Technology and System Design (ICCTSD 2011), **Procedia Engineering (Elsevier)**, vol. 30, pp. 499-507, 2012. Coimbatore, Tamilnadu, India.

Technical Report (Cryptology ePrint Archive)

1. **SK Hafizul Islam**, "Design of identity-based digital signature schemes using extended chaotic maps", Cryptology ePrint Archive, Report 2014/276. Google Scholar Citation: 01
2. **SK Hafizul Islam**, "Identity-based encryption and digital signature schemes using extended chaotic maps", Cryptology ePrint Archive, Report 2014/275.Google Scholar Citation: 01

Teaching Interests

Cryptography, Information/Network Security, Computer Networks, Data Structure, Design & Analysis of Algorithms, Operating Systems, Computer Programming (C, C++, Matlab), Discrete Mathematics, Computational Number Theory, Information & Coding Theory, Machine Learning.

Subject Taught

Course Title	UG/PG	Year	Institute
Programming Languages	UG	2009	BITM, WB
Data Structure	UG	2009	BITM, WB
Operating Systems	UG	2010	BITM, WB
Prolog & LISP (Pract.)	UG	2010	BITM, WB
Cryptography & Network security	UG	2009	BITM, WB
Programming Languages	UG	2008, 2010, 2011, 2012	IIT(ISM) Dhanbad
Computer Networks	PG	2013	BITS Pilani
Operating Systems & Tutorials	UG & PG	2013, 2014	BITS Pilani
Network Security	PG & UG	2013, 2015, 2016	BITS Pilani
Cryptography	UG	2014	BITS Pilani
Machine Learning	PG	2015, 2015, 2016	BITS Pilani
Discrete Math.	UG	2015	BITS Pilani
Networking	UG	2016	IIIT Kalyani
Discrete Math.	UG	2016	IIIT Kalyani
Advanced Programming (C, C++)	UG	2017	IIIT Kalyani

Student Guided

On-campus Thesis

- **Mrigendra Kumar (tabsrahi@gmail.com), B.Tech**
  Ankit Kumar (kumarroushan197@gmail.com), B.Tech
  Ravinder Mehla (kumarroushan197@gmail.com), B.Tech
  Rahul Singh (rahul.libra1928@gmail.com), B.Tech
  Title: Study of Data Clustering Algorithms
  Institute: IIIT Kalyani
  Guide: SK Hafizul Islam
  Status: Going On

- **Olive Chakraborty, M.Tech**
  Title: Design and Analysis of Anonymous User Authentication Scheme for Wireless Sensor Networks
  Institute: BITS Pilani, Rajasthan
  Status: Completed in 2015

- **Abhishek Singh, B.Tech & M.Sc.**
  Title: Provably Secure Authenticated Group Key Agreement Protocol
  Institute: BITS Pilani, Rajasthan
  Status: Completed in 2014

- **Krishna Chaitanya, B.Tech**
  Title: Design of an Authentication Scheme for Vehicular Ad Hoc Network
  Institute: BITS Pilani
  Guide: SK Hafizul Islam
  Status: Completed in 2016

- **Olive Chakraborty, M.Tech**
  Title: Design and Analysis of Anonymous User Authentication Scheme for Wireless Sensor Networks
  Institute: BITS Pilani, Rajasthan
  Status: Completed in 2015

- **Abhishek Singh, B.Tech & M.Sc.**
  Title: Provably Secure Authenticated Group Key Agreement Protocol
  Institute: BITS Pilani, Rajasthan
  Status: Completed in 2014

Off-campus Thesis

- **C. Sneha, B.Tech**
  Title: Email Search
  Institute: Microsoft Research Center, Banglore
  Guide: Suresh Parthasarathy **Co-Guide:** SK Hafizul Islam
  Status: Completed in 2016

- **Ayush Jain, B.Tech**

Title: Development of a secure virtual filesystem in Linux to prevent malicious OS attacks
Institute: School of Computing, National University of Singapore
Guide: Prateek Saxena **Co-Guide:** SK Hafizul Islam
Status: Completed in 2015

- **Vaibhav Agarwal, B.Tech**
  Title: Optimizing HTML5 Web Performance for the Mobile
  Institute: School of Computing, National University of Singapore
  Guide: Prateek Saxena **Co-Guide:** SK Hafizul Islam
  Status: Completed in 2015

- **Pooja Garg, B.Tech**
  Title: Elliptic Curve Discrete Logarithm Problem (ECDLP)
  Institute: Theoretical Statistics and Mathematics Unit, ISI Delhi, India
  Guide: Shanta Laishram **Co-Guide:** SK Hafizul Islam
  Status: Completed in 2015

RP Project

- **Sobhit Sinha, M.Tech**
  Title: Study and Analysis on Pseudo Random Number Generator, **Institute:** IIIT Kalyani, West Bengal, **Status:** Going on

- **Aditya Ray, M.Tech**
  Title: Digital Rights Management, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2016

- **Kota Bhagyanath, M.Tech**
  Title: Hybrid Approach in Intrusion Detection System, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2016

- **Deepak Israni, M.Tech**
  Title: Hybrid Approach in Intrusion Detection System, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2016

- **P. K. Gupta, M.Tech**
  Title: SET Protocol in CL-PKC, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **S.S. Vivek, M.Tech**
  Title: SET Protocol in CL-PKC, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

SAT Project

- **P. K. Gupta, M.Tech**
  Title: SET Protocol in CL-PKC, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **S.S. Vivek, M.Tech**
  Title: SET Protocol in CL-PKC, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

SOP Project

- **Varun Rajeev M, B.Tech**
  Title: Certificateless Remote Authentication for WBANs, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2016

- **P. R. Manoj, B.Tech**
  Title: Image Encryption, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2015

- **Varun Rajeev M, B.Tech**
  Title: Design of Provably Secure Digital Signature Scheme, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2015

- **Mayank Juneja, B.Tech**
  Title: Application of Chaotic Maps in Cryptography, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2015

- **Harsh Kumar, B.Tech**
  Title: Determining fetus development using automated feature extraction from 2-D fetal anomacy scan, **Institute:** CEERI, Pilani, Rajasthan & BITS Pilani, Rajasthan, **Guide:** J. L. Raheja **Co-Guide:** SK Hafizul Islam
  Status: Completed in 2015

- **Kartik Pitale, B.Tech**
  Title: Determining fetus development using automated feature extraction from 2-D fetal anomacy scan, **Institute:** CEERI,

Pilani, Rajasthan & BITS Pilani, Rajasthan, **Guide:** J. L. Raheja **Co-Guide:** SK Hafizul Islam
Status: Completed in 2015

- **Rohit Pathak, B.Tech**
  Title: Remote Login System, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Aashish Agarwal, B.Tech**
  Title: Remote Login System, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Mayank Jha, B.Tech**
  Title: Remote Login System, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Abhishek Veeraraghavan, B.Tech**
  Title: Authentication System for GLOMONET, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Chirag Goyel, B.Tech**
  Title: Authentication System for GLOMONET, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Shiuli Das, B.Tech**
  Title: Visual Cryptography, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

- **Puneet Jolly, B.Tech**
  Title: Lottery Scheme Using Time Stamped Signature, **Institute:** BITS Pilani, Rajasthan, **Status:** Completed in 2014

Educational Qualification

Doctor of Philosophy (Ph.D)

I did my Ph.D under the INSPIRE Fellowship from the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.

Completed:	**June, 2013**
Discipline:	Computer Science and Engineering
Thesis Title:	Elliptic Curve Cryptography based Techniques for Information and Network Security
Guide:	Prof. G. P. Biswas, Professor, Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.
Funded by:	INSPIRE Fellowship, (Grant. No.-IF10247), DST, Govt. of India

Master of Technology (M.Tech)

Department:	Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.
Discipline:	Computer Application
Completed:	2009
Funded by:	MHRD, Govt. of India
OGPA:	8.68 out of 10
Position:	**1st class 1st Ranked**
Dissertation:	Study and analysis of some collision resolution protocols for multi-access channel
Mini Project:	Generation of orthogonal chip sequences using m-sequence on application of Hadamard-like operation
Guide:	Prof. G. P. Biswas, Professor, Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.

Master of Science (M.Sc)

Department:	Department of Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University, West Bengal, India
Discipline:	Applied Mathematics
Completed:	2006
Marks:	79.20%
Position:	**1st class 1st Ranked**

Bachelor of Science (B.Sc)

Institute: Tamralipta Mahavidayalay, Tamluk, Purba Medinipore, West Bengal, India
University: Vidyasagar University, West Bengal, India
Discipline: Mathematics(Honors)
Completed: 2004
Marks: 64.00%
Position: **1st class 4th Ranked**

Higher Secondary (12th class)

Institute: Shyampur High School, Howrah, West Bengal
Board: West Bengal Council of Higher Secondary Education, India
Discipline: Science (Mathematics, Physics, Chemistry, Biology)
Completed: 2000
Marks: 58.20% (2nd Class)

Secondary (10th class)

Institute: Dehimondalghat High School, Howrah, West Bengal
Board: West Bengal Board of Secondary Education, India
Discipline: General
Completed: 1998
Marks: 76.125% (1st Class)
Position: **1st Ranked in the School**

Honors and Awards

1. I have received ***Outstanding Potential for Excellence in Research and Academics (OPERA)*** award (A grant of Rs. 3 lakhs/year for 5 years) from **BITS Pilani, India**, 2015.
2. Selected for ***INSPIRE Fellowship***, funded by Department of Science and Technology (DST), Ministry of Science and Technology, Govt. of India, to pursue Ph.D up to five years in Engineering Science field, 2010.
3. Selected for ***Project Associate (Tech./Adm.)*** in the project titled as "Information Security Education and Awareness (ISEA)", (No.-MIT (2)/2006-08/189/CSE, Funded by Ministry of Communication and Information Technology, Govt. of India) in the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.
4. ***Gold Medal*** for achieving the top rank in the Department of Computer Science and Engineering from IIT(ISM) Dhanbad, Jharkhand 826004, India.
5. ***Gold Medal*** for achieving the top rank in Department of Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University, West Bengal, India, 2006 .
6. ***Gold Medal (S.D. Singha Memorial Endowment Medal)*** for achieving the top rank in Department of Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University, W.B, India, 2006 .
7. ***Gold Medal (Sabitri Parya Memorial Endowment Medal)*** for obtaining highest marks among the successful candidate in M.Sc. Examination in Applied Mathematics with Oceanology and Computer Programming, Vidyasagar University, West Bengal, India, 2006 .
8. ***1st class 4th in B.Sc.*** (Applied Mathematics), Vidyasagar University, West Bengal, India, 2004.
9. All India ***Ranked 164 and Score-396 (Percentile:- 93.68)*** in the subject MATHEMATICS in all India "***Graduate Aptitude Test in Engineering (GATE)***" Examination, conducted by Indian Institute of Technology, Kharagpur, 2007.

Editorial Board Member

1. **Associate Editor**, International Journal of Communication Systems (Wiley), SCI-E Indexed Journal, Impact Factor: 1.099 , ISSN No. 1099-1131, 2015 to Present.
2. **Associate Editor**, Security and Privacy (Wiley), International Journal, ISSN No. 2475-6725, 2017 to Present.

Society Member

1. International Association of Engineers (IAENG) (MID: 114663)
2. International Association of Computer Science and Information Technology (IACSIT) (MID: 80342364)
3. Computer Science Teachers Association (CSTA) (MID: 4283880)
4. Academy & Industry Research Collaboration Center (AIRCC), Australia, (MID: 128820)

Keynote speech

1. I delivered a keynote speech on "**Public Key Cryptography: Challenges and Recent Advances**" at the "**International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM 2017)**", February 3-4, 2017, organized by the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tamilnadu, India.
2. I delivered a lecture on "**Identity-based Cryptography (IBC)**" at the **TEQIP-II sponsored Faculty Development Program** approved

by **All India Council of Technical Education (AICTE)** on "**Image and Data Security**", February 20 - 24, 2017, organized by the Department of Computer Science and Engineering, Government College of Engineering Textile Technology, Berhampore, West Bengal 742101, India.

3. I delivered a lecture on "**Certificateless Public Key Cryptography (CL-PKC)**" at the **TEQIP-II sponsored Faculty Development Program** approved by **All India Council of Technical Education (AICTE)** on "**Image and Data Security**", February 20 - 24, 2017, organized by the Department of Computer Science and Engineering, Government College of Engineering Textile Technology, Berhampore, West Bengal 742101, India.

Session chair

1. I served as a session chair at the "International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM 2017), February 3-4, 2017, organized by the Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tamilnadu, India.

Reviewer of the Journals

1. IEEE Access, **SCI-E**.
2. IEEE Communication Letters, **SCI-E**.
3. IEEE Systems Journal, **SCI-E**.
4. IEEE Transactions on Emerging Topics in Computing, **SCI-E**.
5. IEEE Transactions on Industrial Electronics, **SCI-E**.
6. Arabian Journal for Science and Engineering (Springer), **SCI-E**.
7. Transactions on Emerging Telecommunications Technologies, **SCI-E**.
8. Future Generation Computer Systems (Elsevier), **SCI-E**.
9. SCIENCE CHINA Information Science (Springer), **SCI-E**.
10. Computer and Electrical Engineering (Elsevier), **SCI-E**.
11. Information Sciences (Elsevier), **SCI-E**.
12. Computer Methods and Programs in Biomedicine (Elsevier), **SCI-E**.
13. Soft Computing (Springer), **SCI-E**.
14. Wireless Personal Communications (Springer), **SCI-E**.
15. The Computer Journal (OXFORD University), **SCI-E**.
16. IETE Journal of Research, **SCI-E**.
17. Mathematical and Computer Modelling (Elsevier), **SCI-E**.
18. International Journal of Computer Mathematics (Taylor & Francis), **SCI-E**.
19. International Journal of Computer Mathematics: Computer Systems Theory (Taylor & Francis), **SCI-E**.
20. Annals of Telecommunications (Springer), **SCI-E**.
21. International Journal of Communication Systems (Wiley), **SCI-E**.
22. Security and Communication Networks (Wiley), **SCI-E**.
23. Computer Standard & Interfaces (Elsevier), **SCI-E**.
24. Computer Networks (Elsevier), **SCI-E**
25. Journal of Medical Systems (Springer), **SCI-E**.
26. IET Computers & Digital Techniques, **SCI-E**.
27. IET Information Security, **SCI-E**.
28. KIIS Transactions on Internet and Information Systems (Korea), **SCI-E**.
29. PLOS ONE, **SCI-E**.
30. Telecommunication Systems (Springer), **SCI-E**.
31. Multimedia Tools and Applications (Springer), **SCI-E**.
32. Frontiers of Information Technology & Electronic Engineering (Springer), **SCI-E**.
33. International Journal of Distributed Sensor Networks (SAGE), **SCI-E**.
34. International Journal of Distributed Sensor Networks (Hindawi), **SCI-E**.
35. International Journal of Trust Management in Computing and Communications (Inderscience) **DBLP**.
36. International Journal of Electronic Security and Digital Forensics (Inderscience)**SCOPUS**
37. International Journal of Information and Computer Security (Inderscience) **SCOPUS**.
38. International Journal of Internet Technology and Secured Transactions (Inderscience)**SCOPUS**.
39. International Journal of Network Security (China).
40. Information Sciences Letter (Natural Sciences Publishing, USA).
41. Journal of Information Science and Engineering (EI Compendex) .
42. International Journal of Distributed Sensor Networks (**SCOPUS** & Ei Compendex) .
43. International Journal of Information Security and Privacy (**DBLP**) .

International/National Advisory Board Member

1. **Advisory Committee Member**, National Conference on "Digital Forensic and Cyber Security (NDFCS)" December 10-11, 2016, Govt. Women Engineering College, Ajmer, Rajasthan, India.
2. **Advisory Committee Member**, IEEE, International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15), 21-22 December, 2015, Acharya Institute of Technology, Bangalore, India.

3. **Advisory Committee Member**, Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM'17), 03-04 February, 2017, Department of Computer Science and Engineering, University College of Engineering, Tindivanam, Chennai, Tamilnadu.
4. **Advisory Committee Member**, 2nd International conference on Data Engineering & Communication Technology (ICDECT-17), 20-22 January, 2017, Vignan University, Vadlamudi, Guntur, Andhra Pradesh.

Program Committee Member/Reviewer

1. **Reviewer**, 2017 IEEE Global Communications Conference: Selected Areas in Communications: E-Health, December 4-8, 2017, Singapore.
2. **Reviewer**, The 2nd International Conference on Computational Mathematics and Engineering Sciences (CMES2017), May 20 -22, 2017 Istanbul, Turkey.
3. **TPC**, 4th International Conference on Mathematics and Computing (ICMC 2018), January 09-11, 2018, at Indian Institute of Technology (BHU), Varanasi, India.
4. **TPC**, International Conference on Information Technology and Applied Mathematics (ICITAM 2017), October 30-Nvember 01, 2017 at Haldia Institute of Technology, India.
5. **TPC**, 2017 Conference on Information & Communication Technology (CICT-2017), November 3-5, 2017, ABV IIITM, Gwalior, Madhya Pradesh, India.
6. **TPC**, International Conference on Computational Intelligence, CyberSecurity and Computational Models (ICC3), December 14 - 16, 2017, PSG College of Technology, Coimbatore, India.
7. **TPC**, International Conference on Electronics, Communications and Network Engineering (ECNE2017), June 23 - 24, 2017, Hong Kong, China.
8. **TPC**, First International Conference on Innovations in Electrical, Information and Communication Engineering (ICIEICE'17), March 24 - 25, 2017, Vienna, Austria.
9. **TPC**, Fourth International Conference on Bioinformatics and Bioscience (ICBB 2017), May 27-28, 2017 at Kongunadu College of Engineering and Technology, Thottiam, Trichy, Tamilnadu, India.
10. **TPC**, International Conference on Advances in Computing, Communications and Informatics (ICACCI'17), September 13-16, 2017 at Manipal Institute of Technology, Manipal University, Manipal, India.
11. **TPC**, The Third International Conference on Mathematics and Computing (ICMC 2017), January 17-21, 2017 at Haldia Institute of Technology, India.
12. **TPC**, International Conference on Advanced Computing and Intelligent Engineering (ICACIE 2016), December 21 to 32, 2016, C V Raman College of Engineering (Autonomous), Bhubaneswar, Odisha, India.
13. **TPC**, IEEE, 3rd International Conference on Recent Advances in Information Technology (RAIT-2016), March 03 to 05, 2016, IIT(ISM) Dhanbad, Jharkhand 826004, India.
14. **TPC**, International Conference on Advance Computing and Communication Models (ICACCM-2016), April 9-10, 2016, Govt. Women Engineering College, Ajmer, Rajasthan, India.
15. **TPC**, IEEE, 2nd Conference on Number Theory and Cryptography (NTC 2016), January 14 to 16, 2016, Bangkok, Thailand.
16. **TPC**, The 2nd Internet and Digital Economics Conference (IDEC 2016), May 29 to 31, 2016, Nanjing, China.
17. **TPC**, Fourth International Conference on Advances in Computing, Communications and Informatics (ICACCI-2015), August 10-13, 2015, SCMS School of Engineering and Technology, Aluva, Kochi, India.
18. **TPC**, First Conference on on Number Theory and Cryptography (NTC2015), 29-31 January, 2015, Shanghai, China.
19. **TPC**, 2nd Spring Conference on Wireless Communications and Networks (CWCN-S 2015), 18-20 March, 2015, Suzhou, China.
20. **TPC**, 2015 Internet and Digital Economics Conference (IDEC 2015), 24-26 May, 2015, Beijing, China.
21. **TPC**, IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (IEEE SPICES 2015), 19-21 February 2015, National Institute of Technology, Kozhikode, Calicut, India.
22. **TPC**, IEEE International Conference on Computing, Communication & Automation on May 15-16, 2015, School of Computer Science and Engineering, Golgotia University.
23. **TPC**, IEEE International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT - 2015), 29-31 October, 2015, Bapuji Institute of Engineering & Technology (BIET), Davangere, Karnataka, India.
24. **TPC**, Third IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI-2014), September 24-27, 2014, Galgotias College of Engineering & Technology, New Delhi, India.
25. **TPC**, International Conference on Artificial Intelligence and Communication Engineering(AICE-2014),May 20-21, 2014 in Macao, China.
26. TPC, First IEEE International Conference on Networks & Soft Computing (ICNSC-14), 19-20 August 2014, Vignan University, Guntur, Andhra Pradesh, India.
27. **TPC**, First International Conference on Secure Knowledge Management on Big-Data era, 8-9 December 2014, BITS Pilani, Dubai Campus, Saudi Arabia.
28. **TPC**, 4th International Conference on Electronics, Communications and Networks (CECNet2014), 12-15 December, 2014, Beijing, China.
29. **TPC**, Fifth IEEE International Conference on Computer and Communication Technology (ICCCT-2014), 26-28 September 2014, MNNIT Allahabad, India.

Administrative Responsibilities

1. In-Charge, Student Welfare, IIIT Kalyani, 2017 to present

2. In-Charge, Sports Committee, IIIT Kalyani, 2016 to present
3. Member, Anti-Ragging Committee, IIIT Kalyani, 2016 to present
4. Member, Hostel Mess Committee, IIIT Kalyani, 2016 to present
5. Member, Departmental Purchase Committee (DPC), IIIT Kalyani, 2016 to present
6. Warden, Boys' Hostel, IIIT Kalyani, 2016 to present
7. Professor-In-Charge, 2nd Year CSE Students, IIIT Kalyani, 2016 to present
8. Professor-In-Charge, Firefox Student Community, BITS Pilani, 2014 to 2016

Teaching and Research Experiences

Assistant Professor **From:** 01.07.2016 **To:** till date

Presently, I am working as an Assistant Professor in the the Department of Computer Science and Engineering, Indian Institute of Information Technology, Kalyani 741235 West Bengal, India.

Assistant Professor **From:** 21.06.2013 **To:** 30.06.2016

I worked as an Assistant Professor in the the Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani (BITS Pilani), Rajasthan 333031, India

SRF and DST INSPIRE Fellow **From:** 08.07.2012 **To:** 15.05.2013

I worked as a SRF and DST INSPIRE Fellow in the the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.

Name of Fellowship: INSPIRE Fellowship.

Funding Source: Department of Science and Technology, (DST), Govt. of India.

JRF and DST INSPIRE Fellow **From:** 02.09.2010 **To:** 07.07.2012

I worked as JRF and DST INSPIRE Fellow in the the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.

Name of Fellowship: INSPIRE Fellowship.

Funding Source: Department of Science and Technology, (DST), Govt. of India.

JRF and ISEA Project Associate **From:** 19.05.2010 **To:** 01.09.2010

I worked as JRF and ISEA Project Associate in the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India.

Name of the Project: Information Security Education and Awareness (ISEA).

PI of the Project: Prof. G. P. Biswas.

Funding Source: Department of Information Technology (DIT), Ministry of Communication and Information Technology (MIT), Govt. of India.

Lecturer **From:** 17.05.2009 **To:** 17.05.2010

I worked as a Lecturer in the Department of Computer Science and Engineering.

Institute Name: Bengal Institute of Technology and Management (BITM), Santiniketan, Bolpur, Birbhum - 731246, West Bengal, India.

Affiliation: Approved by All India Council of Technical Education (AICTE) and affiliated to West Bengal University of Technology (WBUT), India.

Paper Presentation

1. I presented a paper titled as "***Comments on ID-based Client authentication with key agreement protocol on ECC for mobile client-server environment***" in the International Conference on Advanced in Computing and Communications (ACC - 2011), held at Kochi, Kerala, India, during 22 - 24 July, 2011.
2. I presented a paper titled as "***An improved pairing-free identity-based authenticated key agreement protocol based on ECC***" in the International Conference on Communication Technology and System Design (ICCTSD - 2011), held at Amrita Vishwa Vidyapeetham, Coimbatore, Tamilnadu, India, during 7 - 9 December, 2011.
3. I presented a paper titled as "***Design of an Efficient ID-based Short Designated Verifier Proxy Signature Scheme***" in the International conference in Recent Advances in Information Technology (RAIT - 2012), held at Indian School of Mines, Dhanbad, India, during 15 - 17 March, 2012.
4. I presented a paper titled as "***Certificateless Strong Designated Verifier Multisignature Scheme using Bilinear Pairings***" in the International Conference on Advances in Computing, Communications and Informatics (ICACCI - 2012), held at RMK engineering college, Chennai, India, on 3 - 5 August, 2012.
5. I presented a paper titled as "***Design of an Enhanced Authentication Protocol and Its Verification using AVISPA***" in the 3rd IEEE International Conference on Recent Advances in Information Technology (RAIT-2016), IIT(ISM) Dhanbad, March 03-05, 2016.
6. I presented a paper titled as "***Design of a certificateless designated server based searchable public key encryption scheme***" in the Third International Conference on Mathematics and Computing (ICMC 2017), January 17-21, 2017 at Haldia Institute of Technology, India.

Workshop and Seminar Attended

1. I attended a Workshop entitled "***Information and Cyber Security***" at IIT(ISM) Dhanbad, Jharkhand 826004, India, on 28 - 30 January, 2015. This workshop is jointly organized by **ISM Dhanbad** & **C-DAC Kolkata** .
2. I delivered a lecture on the topic "***Recent Advances in Cryptography and Information Security***" in Faculty Research Showcase, organized by Computer Science Association(CSA), BITS pilani, Rajasthan, on 16 - 18 January, 2015.
3. I attended a Workshop entitled "***IBM Faculty Residence Program***" at IBM, Bangalore, India, on 4 - 6 June, 2014.
4. I attended a short-term course on "***System Administration for Unix Professionals and Software Development***", Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India, on 04 - 08 July, 2011.
5. I participated in a staff development program on "***Information and Network Security***" held at Bengal Institute of Technology and Management (approved by AICTE and affiliated to WBUT), Santiniketan, Bolpur, Birbhum, India, from 05 - 16 April 2010, sponsored by AICTE.
6. I attended a workshop on "***1st Workshop on Parallel & Distributed Computing***" at the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India, on March 28, 2008.
7. I attended a national conference "***Recent Advances on Information Technology (RAIT-09)***" at the Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India, on 6 - 7 February, 2009.

Computer Skills

OS:	Windows, UNIX and Linux
Programming:	C/C++, Fortran 77, MatLab, Shell Scripting, HLPSL, AVISPA
Database:	FoxBase, MS-SQL Server
Documentation:	LaTeX

Current Address

Position:	Assistant Professor
Affiliation:	Department of Computer Science and Engineering, Indian Institute of Information Technology, Kalyani 741235, West Bengal, India.
SkypeID:	hafizul.ism
Email:	hafi786@gmail.com,hafi786@iiitkalyani.ac.in

Personal Information

DOB:	28/01/1982 at P/S - Shyampur, Dist. - Howrah, State - West Bengal, India
Status:	Married
Spouse:	Sabina Yasmin
Citizenship:	India
Religion:	Muslim
Father:	Shaik Apser Ali
Mother:	Shaik Hasina Begam
Permanent Address:	Vill. & Post.- Dehimondalghat, P/S - Shyampur, District - Howrah, State - West Bengal, India, PIN - 711301
Category:	GENERAL

Passport Details

Issued from:	Ranchi, Jharkhand, India
Date:	20/02/2009
No:	H3611668
Valid up to:	19/02/2019

List of Referees

- **Prof. Mohammad S. Obaidat**
  IEEE Fellow and SCS Fellow
  Chair and Professor
  Department of Computer and Information Science, Fordham University, East Fordham Road, Bronx NY 10458, USA
  Phone: 718-817-5280/4480 **Email:** msobaidat@gmail.com **Homepage:** http://www.theobaidat.com/

- **Prof. Muhammad Khurram Khan**
  Professor

Center of Excellence in Information Assurance (CoEIA), King Saud University, P.O. Box 92144, Riyadh 11653, Kingdom of Saudi Arabia
Email: mkhurram@ksu.edu.sa **Homepage:** http://faculty.ksu.edu.sa/khurram/default.aspx

- **Prof. Gosta Pada Biswas**

Professor
Department of Computer Science and Engineering, IIT(ISM) Dhanbad, Jharkhand 826004, India
Phone: +91-9431124198 **Fax:** +91-326-2296563 **Email:** gpbiswas@gmail.com
Homepage: http://www.ismdhanbad.ac.in/computer-science-engineering/faculty-list/

Declaration

I hereby declare that all statements made in this Curriculum Vitae, are true, complete and correct to the best of my knowledge and belief.

Date: 04/05/2017
Place: IIIT Kalyani, West Bengal, India .....
(SK Hafizul Islam)