Dr Mahender Kumar

Post Doctoral Research Fellow
Cyber Systems Engineering Group,
WMG, University of Warwick,
Coventry, CV47AL
United Kingdom
Email: mahender.kumar@warwick.ac.uk,
mahendjnu1989@gmail.com
Phone: +44 7880 113 010 +91 9990 460 960
: sites/mahenderkumar

Research Interest

Cryptography, Privacy Enhancing Technology, Blockchain and Artificial Intelligence

Experience

March 2021-till date	**Research Fellow** *Cyber Systems Engineering, Warwick Manufacturing Group* *University of Warwick, United Kingdom*
Jan 2018-March 2021	**Lecturer, Computer science** *Directorate of Education, Delhi, India,*
Jan2017-Dec2019	**Senior Research Fellow**, *School of Computer & Systems Sciences,* *JawaharLal Nehru University, Delhi, India* Pairing-Friendly Elliptic Curves for Cryptographic Primitives
Jan2015- Dec2017	**Junior Research Fellow**, *School of Computer & Systems Sciences,* *JawaharLal Nehru University, Delhi, India* Identity-based Cryptosystem and their Application and Challenges

Projects

RAMONA	**Responsive Additive Manufacture to Overcome Natural and Attack-based Disruption**
Oct 2021 - Feb 2024	**Funder**: ESPRC **Role**: As a research leader, responsible for conceptualising the idea, designing proof-of-concept, implementation, and reports writing.
MUTHOS 1.0	**Multi-Source Triage Horizon Scanning Phase 1**
Apr 2022 - Nov 2022	**Funders**: Dstl and Alan Turing Institute **Role**: Coordinate the team, deal with the client (Dstl), conceptualise the idea, design the proof of concept, and reports writing.
MUTHOS 2.0	**Multi-Source Triage Horizon Scanning Phase 2**
Dec 2022 - Jun 2023	**Funders**: Dstl and Alan Turing Institute **Role**: Coordinate the team, deal with the client (Dstl), conceptualise the idea, design the proof of concept, and reports writing.

funding and Grants

1. International Travel Grant of INR 100,000 by **Council of Scientific & Industrial Research**, October 2019.
2. Funding of INR 2,000,000 by **Council of Scientific & Industrial Research**, Jan 2015-December 2019.

Doctoral of Philosophy

July 2015-July 2020	Doctorate of Philosophy in Cryptography *Jawaharlal Nehru University, Delhi, India* Thesis:"Design and Analysis of Pairing-friendly elliptic curves for cryptographic primitives" Advisor: Prof. C.P. Katti (July 2015-Aug 2017) and Prof. Satish Chand (Aug 2017-July 2020)

Education

July2013-July2015	Master of Technology in Computer Science *JawaharLal Nehru University, Delhi, India* Dissertation: "An Approach to Remove Key Escrow Problem in Identity-based Encryption from Pairing" Advisor: Prof. C.P. Katti
July2012-July2013	Master of Technology in Bio-Informatics (Discontinued) *JawaharLal Nehru University, Delhi, India*
Aug2009-July2012	Bachelor of Technology in Computer Science and Engineering *Netaji Subhas University of Technology (East Campus), Delhi, India*
Aug2006-July2009	Diploma in Computer Science and Engineering *Board of Technical Education, Delhi, India*
2006	Secondary Education *Central Board of Secondary Education* *Subjects: Physics, Chemistry, Mathematics, English and Engg. Drawing*
2004	Matriculation Education *Central Board of Secondary Education* *Subjects: Science, Mathematics, English, Hindi, Social Science and Sanskrit*

Journals (Published/Accepted/Communicated)

1. **Mahender Kumar**, Ruby Rani, Gregory Epiphaniou, Carsten Maple, "Exploring the Future: A Systematic Review and Comparative Analysis of Technology Scouting Approaches for Identifying Emerging Science and Technology Trends". (**Communicated**)
2. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, "Blockchain-Based G-Code Protection with Physical-to-Digital Cryptographic Anchor in Additive Manufacturing System". (**Communicated**)
3. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, "Securing Additive Manufacturing Systems: A Threat-Centric Risk Assessment Framework", Journal of Computing and Information Science in Engineering. (**Communicated**)
4. **Mahender Kumar**, Carsten Maple and Satish Chand. *"An Efficient and Secure Identity-Based Integrity Auditing Scheme for Sensitive Data with Anti-Replacement Attack on Multi-Cloud Storage"* **Journal of King Saud University - Computer and Information Sciences** , (**Revision**).
5. **Mahender Kumar**, and Satish Chand. *"Pairing-Friendly Elliptic Curves: Classification, Recent Attacks and Their Security"* arXiv preprint arXiv:2212.01855 (2022).
6. **Mahender Kumar**, and Satish Chand. *"Provable Secure Escrow-Free Identity-Based Signature Scheme for Smart City Environment "* **wireless personal communications**, Springer.
7. **Mahender Kumar**, and Satish Chand. *"A Provable Secure and Lightweight Smart Healthcare Cyber-Physical System with Public Verifiability"* and its solutions", **IEEE Systems Journal** 16.4 (2021): 5501-5508.(**SCIE, IF: 4.462**)
8. **Mahender Kumar**, and Satish Chand. *"Pairing for Greenhorn: Survey and Future Perspective"* **arXiv preprint arXiv**:2108.12392 (2021).
9. **Mahender Kumar**, and Satish Chand. *"SAI-BA-IoMT: Secure AI-Based Blockchain-Assisted Internet of Medical Things Tool to Moderate the Outbreak of COVID-19 Crisis"*, **arXiv preprint arXiv**:2108.09539(2021).
10. **Mahender Kumar**, and Satish Chand. "MedHypChain: A Patient-Centered Interoperability Hyperledger-Based Medical Healthcare System: Regulation in COVID-19 Pandemic", **Journal of Network and Computer Applications** 179 (2021): 102975. (**SCIE, IF: 5.57**)
11. **Mahender Kumar**, and Satish Chand. *"A Secure and Efficient Cloud-Centric Internet of Medical Things-Enabled Smart Healthcare System with Public Verifiability"*, **IEEE Internet of Things Journals**. doi: 10.1109/JIOT.2020.3006523. (**SCIE, IF: 9.94**)
12. **Mahender Kumar**, and Satish Chand. *"A Lightweight Cloud-Assisted Identity-Based Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network."*, **IEEE Systems Journal** (2020), doi: 10.1109/JSYST.2020.2990749. (**SCIE, IF: 4.462**)
13. **Mahender Kumar**, Satish Chand, and C. P. Katti. *"A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature."*, **IEEE Systems Journal** (2020) 14.2 (2020): 2032-2041. (**SCIE, IF: 4.642**)

14. **Mahender Kumar**, and Satish Chand. *"SecP2PVoD: a secure peer-to-peer video-on-demand system against pollution attack and untrusted service provider."*, **Multimedia Tools and Applications** 79.9 (2020): 6163-6190. (**SCIE, IF: 2.101**)
15. **Mahender Kumar**, Satish Chand. *"Escrow-Less Identity-Based Signature Scheme with Outsourced Protection in Cloud Computing"*. **Wireless Personal Communication**, Springer (2020). https://doi.org/10.1007/s11277-020-07520-x (**SCIE, IF: 1.06**)
16. **Mahender Kumar** and Satish Chand. *"ESKI-IBE: Efficient and secure key issuing identity-based encryption with cloud privacy centers."*, **Multimedia Tools and Applications**, Springer, 78.14 (2019): 19753-19786. (**SCIE, IF: 2.101**)
17. **Mahender Kumar**, and Satish Chand. "Cryptanalysis and Improvement of Anonymous Authentication for Wireless Body Area Networks with Provable Security" **Cryptology ePrint Archive: Report 2020/936**, https://eprint.iacr.org/2020/936

Conferences/Workshop(Published/Accepted/Communicated)

1. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, "*Leveraging Semantic Relationships to Prioritise Indicators of Compromise in Additive Manufacturing Systems*", International Workshop on Critical Infrastructure and Manufacturing System Security with 21st International Conference on **Applied Cryptography and Network Security**, June 2023 (**Accepted**).
2. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, "*A Novel Intelligence and Information Acquisition System for Managing Indicators of Compromise in Distributed Responsive Manufacturing Systems*", International Conference on AI and the Digital Economy, June 2023 (**Accepted**).
3. **Mahender Kumar**, Ruby Rani, Mirko Botarelli Gregory Epiphaniou, Carsten Maple, "*Science and Technology Ontology: A Taxonomy of Emerging Topics*", Internation workshop on Knowledge Graph Generation from Text, May 2023 (**Accepted**).
4. **Mahender Kumar** and Satish Chand, *"A pairing free provable secure identity based blind signature scheme with message recovery for cloud assisted services"*, InsCrypt 2019, Springer LNCS 6-8 Dec 2019.
5. **Mahender Kumar**, and P. C. Saxena. *"One-Round Authenticated Identity-Based Tri-Partite Key Agreement Protocol for Internet of Things Based Sensors"*, 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 26-28 March 2018.
6. **Mahender Kumar**, and P. C. Saxena. *"PF-AID-2KAP: Pairing-Free Authenticated Identity-Based Two-Party Key Agreement Protocol for Resource-Constrained Devices"*, International conference on Futuristic trend in network and communication technologies, 9-10 Feb 2018.
7. **Mahender Kumar**, C.P. Katti, and P. C. Saxena, "*A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme*," in International Conference on Information Systems Security, 2017, pp. 29–49.
8. **Mahender Kumar** C. P. Katti and P.C. Saxena, "*An Untraceable Identity-Based Blind Signature Scheme without Pairing for E-cash Payment System*," in International Conference on Ubiquitous Communication and Network Computing, 2017.
9. **Mahender Kumar**, C.P. Katti, "*An Efficient ID-Based Partially Blind Signature Scheme and Application in Electronic-Cash Payment System*", National Workshop for Cryptography 2016, JNNCE Shimogga, 2016.

Talks/Presentations

1. Support Team and Dstl in Hackathon Event at Data Study Group, Alan Turing Institute, 22 May-26 May 2023.
2. Presented a poster on showcase at Dstl, Porton Down, Salisbury, 6 Feb 2023.
3. Demonstrated working Proof-of-concept to the Defence Science and Technology Laboratory team and funder at Dstl, Portsdown West, Portsdown Hill Rd, 20 September 2022.
4. Demonstrated preliminary work of Proof-of-concept to the team of Defence Science and Technology Laboratory at Dstl, Portsdown West, Portsdown Hill Rd, 15 July 2022.
5. Presented work entitled, "Secure and Efficient Cloud-Centric Internet of Medical Things-Enabled Smart Healthcare System with Public Verifiability", University of Warwick, 13 July 2022.

6. Presented paper entitled, "A pairing free provable secure identity-based blind signature scheme with message recovery for cloud-assisted services", at Inscrypt, China, 6-8 December 2019.
7. Presented paper entitled, "One-Round Authenticated Identity-Based Tri-Partite Key Agreement Protocol for Internet of Things Based Sensors", at MNIT Jaipur, India, 26-28 March 2018.
8. Presented paper entitled, "Pairing-Free Authenticated Identity-Based Two-Party Key Agreement Protocol for Resource-Constraint Devices", at JUIT Wakhnaghat, India, 9-10 Feb 2018.
9. Presented paper entitled "A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme" at IIT Bombay, 16-20 Dec 2017.
10. Presented paper entitled "An Untraceable Identity-Based Blind Signature Scheme without Pairing for E-cash Payment System" at Amrita vishwa Vidhyapeetham,Bengalore, India, 3-5 Aug 2017.
11. Presented paper entitled "A new blind signature scheme using identity-based technique", organized by SN Education Society and hosted by Jain College of Engineering, Belagavi (Near Goa) India, January 27-28, 2017.
12. Presented paper entitled "A New Protocol to Defend the Denial of Service Based on Hamiltonian Traversal", NIT, Tiruchirapalli, 27 -28 Aug 2017.
13. Presented poster on National Science Day, Jawaharlal Nehru University, 2017.
14. Presented paper entitled "An Efficient ID-Based Partially Blind Signature Scheme and Application in Electronic-Cash Payment System", National Workshop for Cryptography 2016, JNNCE Shimogga, 2016.
15. Presented poster on National Science Day, Jawaharlal Nehru University, 2016.
16. Presented poster on National Science Day, Jawaharlal Nehru University, 2015.

Reviewer (Journals/Conferences)

- IEEE Transactions on Industrial Informatics
- IEEE Transactions on Dependable and Secure Computing
- Elsevier, Journal of Network and Computer Applications
- IEEE Internet of Things.
- Elsevier, Discrete Mathematics
- Elsevier, Theoretical Computer Science
- IEEE Systems Journal
- IET Information Security
- IEEE Access
- IEEE Sensors
- Springer, International Journal of Information Security
- Springer, Wireless Personal Communication
- Springer, Journal of Cloud Computing
- Springer, Journal of Supercomputing

Certifications

1. **IBM Cybersecurity Analyst**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, Auguts 2021.
2. **IBM Cybersecurity Analyst Assessment**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, August 2021.
3. **Cybersecurity Compliance Framework & System Administration**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
4. **Introduction to Cybersecurity Tools & Cyber Attacks**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.

5. **Penetration Testing, Incident Response and Forensics**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
6. **Network Security & Database Vulnerabilities Cybersecurity Capstone: Breach Response Case Studies**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
7. **Network Security & Database Vulnerabilities**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
8. **Cybersecurity Roles, Processes & Operating System Security**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
9. **Cyber Threat Intelligence**, instructed by IBM Global Subject Matter Experts, **IBM Security Learning Services**, Jun 2021.
10. **An Introduction to Interactive Programming in Python**, instructed by John Greiner, Stephen Wong, Scott Rixner, Joe Warren, **Rice University**, Jan 2014.
11. **An Learn to Program: The Fundamentals**, instructed by Jennifer Campbell, Paul Gries, **University of Torronto**, Feb 2014.
12. **Cryptography I**, instructed by Dan Boneh, **Standford University**, Nov 2013.

Scholarships and Awards

1. Awarded Full international travel grant by **Council of Scientific & Industrial Research**, October 2019
2. Awarded Senior Research Fellow by **Council of Scientific & Industrial Research**, January 2017.
3. Score 1927 Rank among 131803 appeared candidates in **Graduate Aptitude Test in Engineering** conducted by Indian Institute Technology, 2016.
4. Awarded National Eligibility for Lecturership by **University Grant Commission**, Dec 2015
5. Awarded National Eligibility for Lecturership by **University Grant Commission**, Dec 2014
6. Awarded Junior Research Fellow by **Council of Scientific & Industrial Research**, June 2014.
7. Awarded National Eligibility for Lecturer-ship by **University Grant Commission**, June 2014

Practicle Skills

Programming Languages:	Python, Java, C, C++, Golang
Crypto tools:	PBC, RELIC, BAN logic, AVISPA
cybersecurity tools:	MITRE framework, AleinVault OTX, STIX and TAXII
Blockchain :	Hyperledger fabric
Word processing tools:	MS-word 2010, Latex, LibreOffice
Framework and libraries:	Panda, Numpy, TensorFlow, Pytorch

Languages

Hindi:	Native
English:	Fluent
Punjabi:	Basic Knowledge

Personal Profile

Mother's Name:	Mrs. Rajenderi Devi
Father's Name:	Sh. Chhittar Singh
Place | Date of Birth:	Delhi, India | 17 June 1989
Status:	Married
Sex:	Male
Status:	Indian
Permanent Address:	30 Drapers Field, Coventry, United Kingdom

References

Prof. Carsten Maple
Principal Investigator
NCSC-EPSRC Academic Centre of Excellence
Cyber Security Research
&
Professor of Cyber Systems Engineering
Warwick Manufacturing Group
University of Warwick
CM@warwick.ac.uk

Dr Gregory Epiphaniou
Associate Professor
Security Engineering
University of Warwick
United Kingdom
Gregory.Epiphaniou@warwick.ac.uk

Prof. Satish Chand
School of Computer & Systems Sciences
Jawaharlal Nehru University
Delhi 110067, India
schand@mail.jnu.ac.in
+91-9667569581

Prof. C.P. Katti
School of Computer & Systems Sciences
Jawaharlal Nehru University
Delhi 110067, India
cpkatti@yahoo.com
+91 9810 366 758

I hereby declare that, the above furnished information is true and correct to the best of my knowledge.

Place: WMG, University of Warwick, UK

Mahender Kumar