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

Profile

Researcher in Cybersecurity and AI, specialising in applied cryptography, secure autonomous systems, and privacy-preserving technologies. My work bridges theoretical rigor with deployable solutions for critical infrastructure, evidenced by publications in IEEE IoT-J and Elsevier Computers & Security. As an educator, I employ research-led teaching to connect formal methods with industry frameworks (NIST, MITRE ATT&CK), fostering critical thinking through case-based learning. Committed to mentoring early-career researchers and advancing trustworthy AI through interdisciplinary collaboration.

Research Interest

Cybersecurity, Public key Cryptography, AI-driven security solutions and Trustworthy AI

Teaching Interest & Portfolio

- **Core Modules Delivered**: Computer and Network security, Java programming, Database management system cryptography.
- **Course Development**: Designed modules in *Network Security* and *Cryptography*, integrating NIST frameworks.
- **Innovative Pedagogy**: Implemented flipped classrooms and research-led case studies (e.g., MITRE ATT&CK). Mentored 20+ projects.

Education

July 2015- July 2020	**Doctorate of Philosophy in Computer Science**, (*Jawaharlal Nehru University, Delhi, India*) *Thesis*:"Design and Analysis of Pairing-friendly elliptic curves for cryptographic primitives" *Contribution*: Studied and developed novel Pairing-Based Cryptosystems (PBC) and Escrow-Free Identity-Based schemes (EF-IBE, EF-IBS) to enhance security in cloud, e-voting, and healthcare systems. Proposed lightweight ECC/PBC solutions for IoT/WBANs, including OR-3PID-KAP and IBAAKA, ensuring anonymity and integrity in resource-constrained environments. *Advisor*: Prof. C.P. Katti (July 2015-Aug 2017) and Prof. Satish Chand (Aug 2017-July 2020) *Skills*: Elliptic Curve Cryptography, Key Exchange/Authentication protocol, Internet of Things, Cloud Security
July 2013- July 2015	**Master of Technology in Computer Science** (*JawaharLal Nehru University, Delhi, India* **|** 77.1%) *Dissertation*: "An Approach to Remove Key Escrow Problem in Identity-based Encryption from Pairing" *Contribution*: Presents a democratic identity-based encryption model that divides key escrow between two entities (PKG and PKPO) to balance government surveillance needs with user privacy. Proves security against adversarial attacks while optimising efficiency for low-power devices, making it practical for wireless networks and email systems. *Advisor*: Prof. C.P. Katti *Skills*: Identity-Based Encryption, Key escrow problem, threshold cryptography
July 2012- July 2013	**Master of Technology in Bio-Informatics** (Discontinued) *JawaharLal Nehru University, Delhi, India* **|** 81.1%
Aug 2009- July 2012	**Bachelor of Technology in Computer Science and Engineering** *Netaji Subhas University of Technology (East Campus), Delhi, India* **|** 73.2%

Funding and Grants

1. **Follow-on Funding (Project: Muthos)** – Co-author and Lead Contributor
   Secured 6-month funded extension (supporting 1 full-time, 2 part-time researchers) and 6-month no-cost extension. **Funding Body: Dstl, UK Government**, December 2022.
2. **International Travel Grant** – INR 100,000 Council of Scientific & Industrial Research (CSIR), October 2019.
3. **Research Fellowship** – INR 2,000,000 **|** CSIR **|** January 2015 – December 2019.
4. **PhD Supervision**:
   - Mentored 2 PhD candidates (JNU, 2019-2022) in cryptography and cybersecurity
   - Mentored 2 MSc students (Coventry, 2022 & Warwick Universities, 2023) on projects in secure systems design
   - Provided academic guidance on thesis structuring, methodology, and publication strategies

5. **Research Team Leadership**: Lead 3+ RAs and 10+ across DSTL and Medsecurance projects.

Projects

MedSecurance	**Advanced Security-for-safety Assurance for Medical Device IoT**
Jan 2025 - Till date	**Funder**: Horizon Europe *Technical Lead*: Designing a Threat, Vulnerability, and Risk Assessment (TVRA) toolbox for medical IoT, ensuring compliance with ISO 27001 and EU MDR. *Collaboration*: Coordinating 12+ European partners (industry: Doccla, Hygeia Hospital; academia: UPC Barcelona; standards: The Open Group) to align cybersecurity with safety-critical healthcare systems.
Cyber Skill framework	**Harmonizing Cybersecurity Qualifications and Frameworks Across Nations**
Aug 2024- Dec 2024	**Funder**: DSIT UK GOV *Lead Analyst*: Conducted comparative analysis of cybersecurity frameworks in 5 nations (India, Ghana, Japan, Dubai, EU), identifying gaps for mutual qualification recognition. *Partnership*: Collaborated with the University of Southampton and Rudge University to deliver policy recommendations for the UK DSIT's international skills strategy.
UK NACE	**Intelligent Risk Quantification and Verification Framework for in-vehicle Incidents and Indicators of Compromise**
Feb 2024 - Jan 2025	**Funder**: UK NACE *Key Contribution*: Developed a real-time risk-scoring engine using explainable AI (SHAP, LIME), reducing false positives by 22% while maintaining 98% detection accuracy for automotive IoCs. *Outcome*: Aligned framework with ISO/SAE 21434 standards for cybersecurity-compliant autonomous vehicles.
RAMONA	**Responsive Additive Manufacture to Overcome Natural and Attack-based Disruption**
Oct 2021 - Till date	**Funder**: ESPRC *Technical Leadership*: Designed and implemented Meta4API (96.7% accuracy) for detecting hidden attack paths in AM supply chains. Developed a dual-lock integrity auditing system using blockchain for 3D object authentication, and engineered a privacy-preserving threat intelligence sharing framework using homomorphic encryption. *Cross-Institutional Collaboration*: Led integration of cybersecurity tools with partner institutions (Surrey, Bristol, Reading).
TDI	**Trustworthiness in Digital Identity**
July 2023 - Dec 2023	**Funder**: Bill & Melinda Gate foundation
MUTHOS 1.0	**Multi-Source Triage Horizon Scanning Phase 1**
Apr 2022 - Nov 2022	**Funders**: Dstl and Alan Turing Institute
MUTHOS 2.0	**Multi-Source Triage Horizon Scanning Phase 2**
Dec 2022 - Jun 2023	**Funders**: Dstl and Alan Turing Institute *Ontology Development*: Built a Science & Technology Topic Ontology (5,153 topics) using BERTopic, enabling semi-automated early topic identifications for UK defence. *Funding Success*: Secured 12-month extension through evidence-based impact demonstration.

Impact and Knowledge Exchange

Industry Collaboration

Partnered with 12+ EU institutions across healthcare, biotech, and academia for the Medsecurance Project.

- *Healthcare*: Doccla (Sweden), Hygeia Hospital (Greece), EFMI (Switzerland)
- *Biotech*: BioAssist CEA (France), STAB VIDA (Portugal)
- *Academia*: University of Birmingham, UPC Barcelona, European Uni Cyprus
- *Tech Standards*: The Open Group (Belgium), Unparallel Innovation (Portugal)
- *Focus Areas*: Secure health systems, biomedical AI, EU-funded research

Policy Impact & Regulatory Contributions

- *UK DSIT Cyber Skills Framework*: Conducted comparative analysis of cybersecurity qualifications across 10 countries (Ghana, India, Japan, EU and more), supporting the development of mutual recognition frameworks for international workforce standards.
- *EU Medical Device Regulation*: Performed gap analysis of MDCG requirements and co-developed recommendations to strengthen regulatory alignment for medical device cybersecurity.

Invited Collaboration

- Invited expert contributor for University of Surrey/Bristol study on AM supply chains (July 2025), delivering technical insights from the RAMONA project—covering objectives, challenges, and industrial applications of double-lock integrating systems for an industry audience.

Experience

Research Experience

Mar 2021 - Present

Research Fellow
Secure Cyber Systems Research Group, Warwick Manufacturing Group
University of Warwick, United Kingdom
Leadership & Collaboration Skills: *Cross-functional team leadership | Stakeholder engagement & client feedback integration | Project lifecycle management (from design to compliance assurance) | Funded project extensions & resource mobilization*
Technical Skills: *Threat & Vulnerability Risk Assessment| ISO 27001/21434 compliance frameworks | Intrusion Prevention Systems (IPS) | Post-quantum cryptography | Deep Reinforcement Learning | Explainable AI (SHAP) | Fuzzy logic–based risk assessment*
Tools and Technologies: *Python | Pentesting (OpenVAS, SpyderRisk) | AI/ML (TensorFlow, SHAP, BERT, Reinforcement Learning) | Cybersecurity Tools (Splunk, Neo4j, NLTK) | Compliance Standards (ISO 27001, ISO/SAE 21434)*

Key Contributions and Achievements:

- *MedSecurance*: Designed and managed TVRA infrastructure for medical device cybersecurity; developed ISO 27001-aligned assurance framework; conducted risk assessments using OpenVas and SpyderRisk.
- *UK NACE*: Developed a real-time Intrusion Prevention System (IPS) for automotive networks using Deep Reinforcement Learning, achieving 98.2% detection accuracy with 22% fewer false positives. Enhanced incident response efficiency by 31.2% through SHAP-based explainable AI, supporting transparent and interpretable threat triage. Engineered adaptive threat response mechanisms using Splunk and machine learning tools, improving operational efficiency by 42.1%. Additionally, implemented a fuzzy logic–based risk assessment model aligned with ISO/SAE 21434 standards to ensure cybersecurity compliance in AV systems.
- *RAMONA*: Led development of Meta4API (96.7% accuracy) for detecting hidden attack paths in AM supply chains; designed Dual-Lock Integrity Auditing for 3D object authentication using blockchain; implemented Threat Severity Pattern Matching with post-quantum cryptography (+3.2% throughput, -9.14% delay); engineered secure cloud architecture solutions, ensuring compliance with security protocols and quality standards.
- *MUTHOS 1.0 and 2.0*: Led cross-functional team of NLP engineers and developers, designing an ontology-based AI tool for topic identification in cybersecurity (using NLTK, BERT, Neo4j); conducted client meetings for feedback and progress; developed AI-driven tools for semi-automating early technology detection; Secured 6-month funded extension (supporting 1 full-time, 2 part-time researchers) and 6-month no-cost extension.

Aug 2024 - Dec 2024

Voluntary Contributor
Department for Science, Innovation and Technology (DSIT), UK
Leadership & Collaboration Skills: *Cross-national research collaboration | Cyber Skill framework | Comparative analysis leadership*
Technical Skills: *Cybersecurity skills standardization | Regulatory & compliance research | Policy informatics*

Key Contributions and Achievements:

- *Cyber Skill framework*: Contributed to and collaborated on comparative research and analysis of cyber skills frameworks in Ghana, India, Japan, Dubai, and the EU to support mutual recognition of cybersecurity qualifications and inform a universal framework.

July 2023 -Dec 2023

Research Associate
The Alan Turing Institute, London, United Kingdom
Technical Skills: *Privacy-enhancing technologies (Zero-knowledge proofs and Homomorphic encryption) | AI/Data Engineering | GDPR compliance*
Tools and Technologies: *Python | Cryptography (Microsoft SEAL, OpenMined) | Privacy-Preserving AI (FHE/ZKP-integrated models)*

Key Contributions and Achievements:

- *Trustworthy Digital Identity*: Designed privacy-preserving AI models using zero-knowledge proofs and homomorphic encryption (96.7% anonymisation); integrated encrypted data processing into financial workflows, improving matching rates to 98.6% while ensuring GDPR compliance using OpenMined and Microsoft SEAL/FHE.

Jan 2017 -Jun 2018

Senior Research Fellow,
Council of Scientific & Industrial Research, Delhi, India
Skills: *ECC | Pairing-Based Crypto (Weil/Tate) | Post-Quantum Security | Secure e-voting | Privacy-preserving e-cash | HIPAA/GDPR-compliant healthcare systems*

Key Contributions and Achievements:

- Studied the mathematics of elliptic curves for pairing-based cryptography, identifying pairing-friendly curves optimised for low-resource devices, balancing computational efficiency with high security.
- Developed cryptographic models for healthcare, electronic voting, and electronic cash payment systems based on the identified elliptic curves, published in Q1 journals.

Jan 2015 - Dec 2016

Junior Research Fellow,
Council of Scientific & Industrial Research, Delhi, India
Skills: *ECC | Identity-Based Crypto (Weil/Tate) | Authentication | Key exchange protocol*

Key Contributions and Achievements:

- Researched identity-based cryptosystems and associated challenges, such as the key escrow problem,
- Developed a privacy-preserving approach that balances security and user privacy, published in Q1 journal.

Teaching Experience

June 2018 -Mar 2021

Lecturer, Computer Science
Directorate of Education, Delhi, India
Teaching Skills: *Curriculum Design and Coordination | Assessment Development | Student Mentoring | Active Learning | Quality Assurance*

Key Contributions and Achievements:

- Designed and updated course curricula to align with programme learning outcomes, integrating current research and professional standards, ensuring academic rigour and relevance.
- Developed assessments and marking rubrics for written exams, coursework, and practical tasks, ensuring consistency, transparency, and compliance with institutional academic regulations.
- Conducted formative and summative student evaluations, offering constructive feedback and tailored academic support to enhance student progression and achievement.
- Mentored undergraduate students on academic performance and career planning, supporting personal development and employability.
- Organised extracurricular workshops on cybersecurity awareness and digital safety, contributing to digital citizenship and outreach within the university community.
- Motivated students through real-world examples, industry guest talks, and collaborative mini-projects, helping them connect classroom learning with practical applications and career pathways.
- Actively participated in quality assurance processes, including internal moderation and student feedback analysis, to continuously enhance teaching effectiveness.

Aug 2016 -July 2017

Assistant Professor (Guest)
Delhi University, Delhi, India
Module Tutor / Lab Coordinator – Java Programming
Key Contributions and Achievements:

- Delivered lectures and tutorials on Java programming, covering OOP concepts, multithreading, and data structures.
- Designed and maintained practical lab sessions, including hands-on programming exercises, debugging clinics, and formative assessments.
- Developed and graded coursework and coding assignments aligned with learning outcomes.
- Provided academic support to postgraduate students through office hours, revision sessions, and 1:1 supervision.
- Integrated Java-based software engineering tools (e.g., Eclipse) into lab environments to reflect real-world practices.
- Received positive feedback from students and peer review through internal module evaluation processes.

Publications

Selected Top Publications

1. **Mahender Kumar**, Carsten Maple, *Secure and Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs*" IEEE transaction on intelligent transport system, (2025). **REF Rating:** ★ ★★★ (4*)
   - *Originality*: First to address anonymous batch authentication in 6G-VANETs.
   - *Significance*: Direct relevance to future ITS infrastructure and transport security policy.
   - *Rigour*: Formal security proofs and simulations in a top-tier IEEE journal.

   Contribution: Identifies vulnerabilities in existing 6G-VANET authentication protocols (e.g., MITM, impersonation) and proposes a secure, anonymous batch authentication scheme with formal security proofs and practical feasibility.
2. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *Security of Cyber-Physical Additive Manufacturing Supply Chain: Survey, Attack Taxonomy and Solutions,* Elsevier Computers and Security (2025). **REF Rating:** ★ ★★★ (4*)
   - *Originality*: First attack taxonomy covering end-to-end AM supply chains.
   - *Significance*: Influences both academic research and industrial AM risk planning.
   - *Rigour*: Strong literature base and methodological analysis.

   Contribution: Expands cybersecurity frameworks with a novel AM-specific threat taxonomy, covering cyber and cyber-physical risks across the supply chain. Proposes mitigation strategies to protect intellectual property, prevent design manipulation, and enhance AM ecosystem security.
3. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *SPM-SeCTIS: Severity Pattern Matching for Secure Computable Threat Information Sharing in Additive Manufacturing*, Elsevier Internet of Things 28 (2024): 101334. **REF Rating:** ★ ★★★ (4*)
   - *Originality*: Introduced a severity-weighted CTI sharing model.
   - *Significance*: Improves SOC operations and AM system resilience.
   - *Rigour*: Validated with real-time datasets and stakeholder feedback.

   Contribution: Proposes SPM-SeCTIS, a privacy-preserving CTI sharing system for IAM, using homomorphic encryption to enable secure threat pattern matching on encrypted data. Ensures confidentiality and scalability, preventing exposure of sensitive threat details while maintaining efficient performance for large-scale deployments.
4. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *"Comprehensive Threat Analysis in Additive Manufacturing Supply Chain: A Hybrid Qualitative and Quantitative Risk Assessment Framework"*, Springer Production Engineering (2024): 1-19. **REF Rating:** ★ ★★ (3*)
   - *Originality*: Combines qualitative and quantitative threat modelling in AM.
   - *Significance*: Used to support ISO/SAE 21434 alignment.
   - *Rigour*: Evidence-based design, field-tested.

   Contribution: Introduces a holistic risk assessment framework for AM that integrates both cyber and physical threats, enabling quantitative and qualitative evaluation of vulnerabilities. Validates effectiveness using MITRE CVEs, providing actionable insights to prioritise risks and strengthen AM supply chain security.
5. **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. **REF Rating:** ★ ★★ (3*)

- *Originality*: First semantic-based IoC prioritisation for AM using HINs with meta-path modelling and domain-aware recognition.
- *Significance*: Empowers proactive AM cybersecurity by automating and ranking IoCs based on attack frequency, lifetime, and vulnerabilities.
- *Rigour*: Combines NLP, HINs, and quantifiable scoring, validated across organisational and regional threat contexts.

Contribution: Automates IoC extraction & ranking using semantic HINs to model threat relationships. Prioritises risks by domain (org/region) via attack frequency, IoC lifetime, and vulnerabilities.

6. **Mahender Kumar**, Ruby Rani, Mirko Botarelli, Gregory Epiphaniou, Carsten Maple, *"Science and Technology Ontology: A Taxonomy of Emerging Topics"*, International workshop on Knowledge Graph Generation from Text, May 2023 (**Accepted**). **REF Rating:** ★ ★★ (3*)
   - *Originality*: First ontology of its kind for UK defence and innovation scanning.
   - *Significance*: Used in semi-automated horizon scanning tools.
   - *Rigour*: Technical novelty with stakeholder integration.

   Contribution: Introduces S&TO, the first automated multidisciplinary Science & Technology Ontology using BERTopic, covering 5,153 unconventional topics.Enables cross-domain research discovery with 13,155 semantic relations, dynamically updatable for evolving knowledge.

Journals (Published/Accepted/Communicated)

1. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *SHIELD-CAN: A Self-Healing Edge-AI Intrusion Detection System for Automotive CAN Gateways*, IEEE Transaction on Dependable and Secure Computing. (**Under Review**).
2. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *MAGD-Fraud: Multi-Evidence Assurance-Guided Deferral as Knowledge-Based Decision Support for Financial Fraud Review*, Elsevier Knowledge-Based System. (**Under Review**).
3. **Mahender Kumar**, Ruby Rani, Gregory Epiphaniou, Carsten Maple, *ATA-SOC-HAT: Adaptive Trust-Aware Human-AI Teaming Framework for Resilient and Compliance-Aligned SOC Operations*" Computers & Security (2026): 104971.
4. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *metA4API: Meta-Path and Meta-Graph Analysis for Attack Pattern Identification in Additive Manufacturing Supply Chain*, Elsevier Computer Eginerring and Industrial Applications (**Revision**).
5. **Mahender Kumar**, Mark Hooper, Gregory Epiphaniou, Carsten Maple, *Privacy-Preserving and Secure Analysis for Detecting Gender Disparity in a Microfinance Loan System*, Elsevier Journal of Information Security Applications, (**Revision**).
6. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *AutoIPS: Real-Time, Explainable Intrusion Prevention for Automotive Networks Using Deep Reinforcement Learning*" IEEE transaction on intelligent transport system, (**Under review**).
7. **Mahender Kumar**, Ruby Rani, Gregory Epiphaniou, Carsten Maple, *" ICSThreatQA: A Knowledge-Graph Enhanced Question Answering Model for Industrial Control System Threat Intelligence"*. Expert Systems with Applications, 130180.
8. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, *"Securing additive manufacturing with blockchain-based cryptographic anchoring and dual-lock integrity auditing*. Computers in Industry, 173, 104395.
9. **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**)
10. **Mahender Kumar** "Cryptanalysis of Secure and Lightweight Conditional Privacy-Preserving Authentication for Securing Traffic Emergency Messages in VANETs." Cryptology ePrint Archive (2024).
11. **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** , 35.9 (2023): 101745.
12. **Mahender Kumar**, and Satish Chand. *"Pairing-Friendly Elliptic Curves: Classification, Recent Attacks and Their Security"* arXiv preprint arXiv:2212.01855 (2022).
13. **Mahender Kumar**, and Satish Chand. *"Provable Secure Escrow-Free Identity-Based Signature Scheme for Smart City Environment "* **wireless personal communications**, Springer.
14. **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**)
15. **Mahender Kumar**, and Satish Chand. *"Pairing for Greenhorn: Survey and Future Perspective"* **arXiv preprint arXiv**:2108.12392 (2021).
16. **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).

17. **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**)

18. **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**)

19. **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**)

20. **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**)

21. **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**)

22. **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**)

23. **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**)

24. **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, "*FinAgent-Reliance: A Human-in-the-Loop Reliability Benchmark for Financial LLM Agents*", (**Under progress**).

2. **Mahender Kumar**, Gregory Epiphaniou, Carsten Maple, "*FairDefer: Fairness-Aware Defer-and-Route with Multi-Level Constraints*", International Joint Conference on Artificial Intelligence , (**Under review**).

3. **Mahender Kumar**, SU Islam, C Maple, P Kumar, A Lambert, *A Corridor-Agnostic RSU Handover–Aware Authentication and Key Agreement Scheme for Internet of Vehicles*, IEEE International Conference on Consumer Electronics (ICCE), 1-6, 2026.

4. SU Islam, **Mahender Kumar**, C Maple, P Kumar, A Lambert, *Severity-First Risk Prioritization for AI Poisoning in Edge-Integrated Internet of Vehicles*, IEEE International Conference on Consumer Electronics (ICCE), 1-6, 2026.

5. **Mahender Kumar**, Ruby Rani, Gregory Epiphaniou, Carsten Maple, "*Securing Connected and Autonomous Vehicles: Analysing Attack Methods, Mitigation Strategies, and the Role of Large Language Models*", International Conference on AI and the Digital Economy.

6. **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.

7. **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.

8. **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.

9. **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.

10. **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.

11. **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.

12. **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.

Book Chapter

1. **Mahender Kumar**. "AOR-ID-KAP: An authenticated one-round identity-based key agreement protocol for wireless sensor networks." Computational Intelligence in Sensor Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018. 427-454.

Talks/Presentations/Dissemination

1. Presented Threat, Vulnerability, and Risk Assessment (TVRA) progress at the Half-Yearly Review Meeting with European partners, Hygeia Hospital, Athens (June 2025).
2. Showcased MedSecurance research at the EU Pavilion, HIMSS 2025, engaging global healthcare leaders (June 2025).
3. Delivered a talk supporting EU cybersecurity collaboration at the European Clustering Workshop (June 2025).
4. Presented TVRA progress at the Half-Yearly Review Meeting, University of Warwick (November 2025).
5. Delivered a talk and demonstration on "Securing Connected Medical Devices" for the 1st MedSecurance Webinar (December 2025).
6. Designed and led Assurance Toolkit Integration Workshops (Feb–June 2025) to enable cross-partner adoption and technical alignment.
7. Attended and also visited the NCSC exhibit at the National Cyber Security Show at the NEC Birmingham, April 2025.
8. Delivered an invited lecture on "Private Threat Intelligence Sharing in Additive Manufacturing" at the University of Warwick, March 2025.
9. Delivered a guidance lecture on "Doctoral and Postdoctoral Research Opportunities in the UK" for PhD and Master's students at the Central University of Haryana, India, November 2024.
10. Gave a technical talk on "Threat Analysis and Risk Assessment of Cyber-Physical Attacks in Additive Manufacturing" at RITICS, London, September 2024.
11. Collaborated with the Defence Science and Technology Laboratory (Dstl) and provided expert support during the Hackathon Event at the Data Study Group, Alan Turing Institute, 22–26 May 2023.
12. Presented a research poster during the showcase event at Dstl, Porton Down, Salisbury, 6 February 2023.
13. Demonstrated a working proof-of-concept to the Dstl research team and funding representatives at Portsdown West, Portsdown Hill Road, 20 September 2022.
14. Presented the preliminary design and implementation of a proof-of-concept solution to Dstl researchers at Portsdown West, 15 July 2022.
15. Presented research titled "Secure and Efficient Cloud-Centric Internet of Medical Things-Enabled Smart Healthcare System with Public Verifiability" at the University of Warwick, 13 July 2022.
16. 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.
17. 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.
18. 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.
19. Presented paper entitled "A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme" at IIT Bombay, 16-20 Dec 2017.
20. 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.
21. Presented paper entitled "A new blind signature scheme using identity-based technique", organised by SN Education Society and hosted by Jain College of Engineering, Belagavi (Near Goa), India, January 27-28, 2017.
22. Presented paper entitled "A New Protocol to Defend the Denial of Service Based on Hamiltonian Traversal", NIT, Tiruchirapalli, 27 -28 Aug 2017.
23. Presented poster on National Science Day, Jawaharlal Nehru University, 2017.
24. Presented paper entitled "An Efficient ID-Based Partially Blind Signature Scheme and Application in Electronic-Cash Payment System", National Workshop for Cryptography 2016, JNNCE Shimoga, 2016.
25. Presented poster on National Science Day, Jawaharlal Nehru University, 2016.
26. Presented poster on National Science Day, Jawaharlal Nehru University, 2015.

Reviewer (Journals/Conferences)

IEEE Transactions on Information Forensics and Security | IEEE Transactions on Dependable and Secure Computing | IEEE Transactions on Computers | IEEE Transactions on Networking | IEEE Transactions on Mobile Computing | IEEE Transactions on Industrial Informatics | IEEE Transactions on Knowledge and Data Engineering | IEEE Transactions on Network Science and Engineering | ACM Computing Survey | 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

Professional / Academic Service

Editorial Roles

- Associate Editor, IEEE Internet of Things Journal (2024–2025)

Conference Leadership

- Area Chair, International Conference on System Safety and Security (ICSSS 2025)
- Programme Committee, International Conference on Computational Performance Evaluation 2021

College Service

- **Exam Board Member**: CS Programme Assessment Committee, Directorate of Education (2019–2021).
- **EDI Lead**: Co-founded ABHYAAS NGO (2007–), providing free STEM education to 2,000+ low-income students through partnerships with 5+ local NGOs.

Licenses & Certifications

1. **ISC2 Certified Cybersecurity**, March 2025
2. **IBM Cybersecurity Analyst**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, August 2021.
3. **IBM Cybersecurity Analyst Assessment**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, August 2021.
4. **Cybersecurity Compliance Framework & System Administration**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
5. **Introduction to Cybersecurity Tools & Cyber Attacks**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
6. **Penetration Testing, Incident Response and Forensics**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
7. **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.
8. **Network Security & Database Vulnerabilities**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
9. **Cybersecurity Roles, Processes & Operating System Security**, instructed by Coreen Ryskamp, IBM Global Subject Matter Experts, **IBM Security Learning Services**, July 2021.
10. **Cyber Threat Intelligence**, instructed by IBM Global Subject Matter Experts, **IBM Security Learning Services**, Jun 2021.
11. **An Introduction to Interactive Programming in Python**, instructed by John Greiner, Stephen Wong, Scott Rixner, Joe Warren, **Rice University**, Jan 2014.
12. **An Learn to Program: The Fundamentals**, instructed by Jennifer Campbell, Paul Gries, **University of Torronto**, Feb 2014.
13. **Cryptography I**, instructed by Dan Boneh, **Standford University**, Nov 2013.

International Exchange programme

1. Selected for a 6-month academic exchange program with the **University of Bern**, Switzerland (2017–18), under the Jawaharlal Nehru University exchange scheme with the DAAD program; unable to participate due to financial constraints.
2. Received research interest and informal acceptance from **Prof. Marian Margraf, Freie Universität Berlin**, for collaboration on Lightweight Cryptography for Iot; the opportunity could not be pursued due to a lack of DAAD funding.

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

Humanitarian Work

Sep 2007 - Jul 2009 — **President (co-founder)**
ABHYAAS, Non-Governmental Organization, Delhi, India

1. Led the ABHYAAS organisation, overseeing initiatives aimed at providing free education to underprivileged students unable to afford fees.

Apr 2019 — **Presiding Officer (Election Duty)**
17th Lok Sabha Elections, West Delhi, India

1. Volunteered as Presiding Officer, responsible for ensuring the lawful, smooth, and fair conduct of polling operations at a West Delhi polling station, with full compliance to electoral guidelines and voter protocols.

Feb 2020 — **Presiding Officer (Election Duty)**
Delhi Legislative Assembly Elections, West Delhi, India

1. Volunteered as Presiding Officer, overseeing the lawful and smooth conduct of polling at a West Delhi voting station, ensuring compliance with electoral procedures and voter safety protocols.

Feb 2020 -Mar 2020 — **Cybersecurity Awareness Program Coordinator**
In collaboration with Delhi Zonal Officer, Delhi, India

1. Coordinated and conducted a cybersecurity awareness program in 20 Colleges, educating over 20,000 students on how to safely navigate the digital world and interact responsibly while using the internet.
2. Delivered key messages about online safety, including best practices for protecting personal information and avoiding cyber threats.

Apr 2020 - Feb 2021 — **COVID-19 Relief Volunteer**
Delhi, India

1. Worked with the Food Corporation of India for 2 months (Apr–May 2020), coordinating food distribution and assisting in the creation of ration cards and entitlement certificates for underserved communities.
2. Served as a Contact Tracer at Delhi Hospital for 3 months (Jun–Aug 2020), supporting COVID-19 containment by managing positive cases and reporting updates to the Delhi Health Ministry.
3. Acted as Field Supervisor with District Migration Support for 6 months (Sep 2020–Feb 2021), leading a local team to support migrant populations in West Delhi (Moti Nagar) during the pandemic, including aid coordination and public health outreach.

Memberships

1. IEEE membership
2. (ISC)2 Membership
3. Cryptology Research Society of India

Technical Skills & Tools

Programming:	Python, Golang, Java, C & C++
AI/ML:	TensorFlow, PyTorch, TenSeal, spaCy, Numpy, Panda
Compliance & Framework:	GDPR, ISO27001, ISO/SAE 21434, NIST, HIPPA, MITRE ATT&CK
Security Tools:	SIEM (Splunk, QRadar), IDS & IPS (Snort, Suricata), Firewalls (Palo Alto)
Privacy Tools:	TenSEAL, zksk

Languages

Hindi:	Native
English:	Fluent

Personal Profile

Place | Date of Birth:	Delhi, India | 17 June 1989
Status | Sex | Nationality:	Married | Male | Indian
Permanent Address:	32 Haynestone Road, Coventry, United Kingdom
Immigration Status:	Indefinite Leave to Remain
Driving License:	Yes

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

Dr Pradeep Kumar
Associate Professor
Security Engineering
University of Warwick
United Kingdom
pradeep.kumar.1@warwick.ac.uk

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

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