



## Dr. Mohammad Nauman

Computer Science Department

Address: Effat University, P.O. Box 34689 Jeddah 21478 Kingdom of Saudi Arabia

Phone: +966 122137897

Cell: +966 56 359 1640

Email: [mnauman@effatuniversity.edu.sa](mailto:mnauman@effatuniversity.edu.sa)

Scholar Profile: <https://scholar.google.com/citations?user=LgO11BgAAAAJ>

Scopus Profile: <https://www.scopus.com/authid/detail.uri?authorId=22234585800>

Research Gate Profile: <https://www.researchgate.net/profile/Mohammad-Nauman>

LinkedIn Profile: <https://linkedin.com/in/recluze>

### EDUCATION

---

#### **PostDoc (Applications of Machine Learning in Security and Privacy) - 2015-2017**

Fully Funded under Foreign Researcher Grant  
Max Planck Institute for Software Systems, Germany

#### **PhD in Information Technology (2011-2014)**

Universiti Kuala Lumpur, Malaysia  
Thesis title: Extending User Privacy on Virtual Machine based Smartphones through Resource Usage Control

#### **MS Software Engineering (2006-2008)**

City University, Peshawar, Pakistan  
Thesis title: Common Sense and Folksonomy: Engineering a Model for an Intelligent Search System

#### **BSc (Hons) (2001-2004)**

Specialization: IT. CGPA: 3.9

### TEACHING EXPERIENCE

---

**Assistant Professor, Computer Science Department, October 2022 – Present**  
Computer Science Department, Effat College of Engineering, Effat University, Jeddah, KSA

**Associate Professor, July 2020 – August 2022**  
Computer Science Department, FAST National University of Computer and Emerging Sciences, Peshawar, Pakistan

**Assistant Professor, July 2015 – July 2020**  
Computer Science Department, FAST National University of Computer and Emerging Sciences, Peshawar, Pakistan

### Courses Taught

- Programming Fundamentals
- Object Oriented Programming
- Data Structures
- Operating Systems
- Computer Networks
- Digital Forensics
- Computer Organization and Assembly Language
- Numerical Computing
- Probability and Statistics
- Software Engineering
- Machine Learning
- Advanced Programming
- Advanced Operating Systems (MS/PhD)
- Secure Software Systems (MS/PhD)
- Advanced Machine Learning (MS/PhD)
- Advanced Reinforcement Learning (MS/PhD)

### RESEARCH EXPERIENCE

**Fields of specialization:** Security, Privacy

**Current research areas:** Applications of Machine Learning in Security and Privacy

**Conferences Chaired:** Member, Program Committee - 6<sup>th</sup> International Conference on Trust & Trustworthy Computing, London, UK (2013)

**hIndex:** 20

**i10-index:** 31

**Total Citations:** 1940

### PRESENTATIONS

**Ireland – 2007** – For presentation of a paper at 20th International Conference on Software Engineering Education and Training (CSEE&T)  
Sponsored by CSEE&T and Dublin City University, Ireland

**USA – 2009** – For presentation of a paper at the 4th International Workshop on Scalable Trusted Computing  
Held in conjunction with 16th ACM Conference on Computers and Communication Security (CCS'09). Sponsored by Higher Education Commission of Pakistan

**United Kingdom -2009** – For presentation of a paper at International Conference on Technical and Socio-Economic Aspects of Trusted Computing (Trust 2009)  
Sponsored by ICT R&D Fund, Ministry of IT, Pakistan

**Germany -2015** – For an invited talk at Universitat des Saarlandes, Saarbrucken, Germany  
Funded by Center for IT-Security, Privacy and Accountability (CISPA) at Universitat des Saarlandes

**France - 2016** – For a talk at the 2nd IEEE European Symposium on Security and Privacy (Euro S&P '17), Paris, France.  
Funded by the Max-Planck Institute for Software Systems Germany

**Japan - 2019** – For a talk at the 7th International Symposium on Computing and Networking  
Nagasaki, Japan. Best paper award.

## THESIS SUPERVISIONS

---

**PhD Thesis supervised:** Musadaq Mansoor (2022)

**Thesis title:** Generative Adversarial Learning from Protein Sequence Data

**PhD Thesis supervised:** Waqas Ali (2022)

**Thesis title:** A Three-way Decision Model for Anonymization of Attributes using Differential Privacy

## PUBLICATIONS

---

### Books, Book Chapters and Journal Papers

M Mansoor, M Nauman, HU Rehman, M Omar. Gene Ontology Capsule GAN: an improved architecture for protein function prediction. PeerJ Computer Science 8, e1014. Impact factor: 2.41. 2022.

KN Khan, N Ullah, S Ali, MS Khan, M Nauman, A Ghani. Op2Vec: An Opcode Embedding Technique and Dataset Design for End-to-End Detection of Android Malware. Security and Communication Networks. Impact factor: 1.791. 2022.

W Ali, M Nauman, N Azam. A privacy enhancing model for Internet of Things using three-way decisions and differential privacy. Computers and Electrical Engineering 100, 107894. Impact factor: 3.818. 2022.

M Mansoor, M Nauman, H Ur Rehman, A Benso. Gene Ontology GAN (GOGAN): a novel architecture for protein function prediction. Soft Computing, 1-15. Impact factor: 2.587. 2022.



S Khan, M Nauman, SA Alsaif, TA Syed, HA Eleraky. Using Capsule Networks for Android Malware Detection Through Orientation-Based Features. *Expert Systems* 38 (4), e12611. Impact factor: 2022.

Nauman, M. , Ali, T., Khan, S., Syed, T. A. Deep Neural Architectures for Large Scale Android Malware Analysis. In *Cluster Computing*. Accepted. pp n–n. Indexed ISI. Impact factor: 1.514. Springer. May, 2017.

Ali, T., Nauman, M. , Jan, S. Trust in IoT: dynamic remote attestation through efficient behavior capture. In *Cluster Computing*. Early Access. pp 1–13. Indexed ISI. Impact factor: 1.514. Springer. April, 2017.

Ali, T., Ismail, R., Musa, S., Nauman, M. , Khan, S. Design and implementation of an attestation protocol for measured dynamic behavior. In *Journal of Supercomputing*. Vol. 73. No. 4. pp 1–28. Indexed ISI. Impact factor: 1.088. Springer. April, 2017.

Nauman, M. , Azam, N., Yao, J.T. A three-way decision making approach to malware analysis using probabilistic rough sets. In *Information Sciences*. Vol. 374 pp 193–209. Indexed ISI. Impact factor: 3.364. Elsevier. December, 2016.

Khan, S., Nauman, M. , Othman, A.T., Musa, S., Ali, T. TSSDroid: realization of an efficient and usable TSS API for the Android software stack. In *Security and Communication Networks*. 9(11) pp 1553–1576. Indexed ISI. Impact factor: 0.806. Wiley. July, 2016.

Nauman, M. Khan, S., Othman, A.T., Musa, S. Realization of a User-Centric, Privacy Preserving Permission Framework for Android. In *Security and Communication Networks*. Indexed ISI. Impact factor: 0.806. Wiley. February, 2015.

Toegl, R. , Winkler, T., Nauman, M. , Hong, T.W., Winter, J., Gissing, M. Programming Interfaces for the TPM. [Book Chapter] in *Trusted Computing for Embedded Systems*. pp 3-32. Springer. November, 2014.

Toegl, R., Winkler, T., Nauman, M. Hong, T. Specification and Standardization of a Java Trusted Computing API. In *Software: Practice and Experience*. Indexed ISI. Impact factor: 0.652. Wiley. July, 2011.

Alam, M., Ali, T., Khan, S., Khan, S., Ali, M., Nauman, M. , Hayat, A., Khan, M.K., Alghathbar, K. Analysis of existing remote attestation techniques. In *Security and Communication Networks*. Indexed ISI. Impact factor: 0.806. Wiley. 2011.

Alam, M., Zhang X., Nauman, M. Ali, T., Ali, M., Anwar, S., and Alam, Q. Behavioral Attestation for Web Services using access policies. In *Multimedia Tools and Applications*. Indexed ISI. Impact factor: 1.331. Volume 53. No. 1. Springer. May, 2011.

Nauman, M. Tamleek Ali and Azhar Rauf. Using Trusted Computing for Privacy Preserving Keystroke-based Authentication in Smartphones. In *Telecommunications Systems Journal*. Indexed ISI. Impact factor: 0.822. Springer. July, 2011.



Tamleek Ali, Masoom Alam, Nauman, M , Toqeer Ali, Muhammad Ali and Sajid Anwar. A Scalable and Privacy Preserving Remote Attestation. Journal of Information. Indexed ISI. Impact factor: 0.099. Accepted October, 2010.

Nauman, M , Tamleek Ali, Muhammad Khurram Khan and Khaled Alghathbar. Information Flow Analysis of UCON. International Journal of Physical Sciences. June 2010 Vol. 5, Num. 6. pp 865 – 875. Indexed ISI. Impact Factor: 0.554

Masoom Alam, Xinwen Zhang, Nauman, M , Tamleek Ali and Patrick C.K. Hung. Behavioral Attestation for Web Services Based Business Processes. International Journal of Web Services Research. Indexed ISI/SCI-E, Impact factor: 1.200. Vol. 7. Num 3. pp 52-72. 2010.

Nauman, M and Sohail Khan. Design and Implementation of a Fine-grained Resource Usage Model for the Android Platform. International Arab Journal of Information Technology. Indexed ISI/SCI-E. Impact Factor: 0.519. Vol. 8, No. 4 October 2011.

### Conference Papers

Backes, M., Nauman, M. LUNA: Quantifying and Leveraging Uncertainty in Android Malware Analysis through Bayesian Machine Learning. April, 2017. Proceedings of the IEEE European Symposium on Security and Privacy (Euro S&P '17). Paris, France.

Ali, T., Ali, J., Ali, T., Nauman, M. , Musa, S. Efficient, Scalable and Privacy Preserving Application Attestation in a Multi Stakeholder Scenario. 16th International Conference on Computer Science and its Applications (ICCSA'2016). July 2016. LNCS Vol. 9789, pp 407-421. Beijing, China.

Nauman, M. , Azam, N. A Three-way Decision Making Approach to Malware Analysis. 2015 International Joint Conference on Rough Sets. December, 2015. Tianjin, China.

Nauman, M. , Khan, S., Othman, A.T., Musa, S., Najeeb-ur-Rehman. POAuth: Privacy-aware Open Authorization for Native Apps on Smartphone Platforms. 6th ACM International Conference on Ubiquitous Information Management and Communication (ACM ICUIMC 2012). February, 2012. Kuala Lumpur, Malaysia.

Syed, T.A., Ismail, R., Musa, S., Nauman, M. , Khan, S. A Sense of Others: Behavioral Attestation of Unix Processes on Remote Platforms. 6th ACM International Conference on Ubiquitous Information Management and Communication (ACM ICUIMC 2012). February, 2012. Kuala Lumpur, Malaysia.

Khan, S., Nauman, M. , Othman, A.T., Musa, M. How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms. 8th IEEE International Conference on Networked Computing and Advanced Information Management (NCM 2012). April, 2012. Seoul, Korea.

Tamleek Ali, Nauman, M and Xinwen Zhang. On Leveraging Stochastic Models for Remote Attestation. 2nd International Conference on Trusted Systems (InTrust2010). December 2010. Beijing, China.



Nauman, M. , Sohail Khan, Xinwen Zhang and Jean-Pierre Seifert. Beyond Kernel-level Integrity Measurement: Enabling Remote Attestation for the Android Platform. 3rd International Conference on Trust and Trustworthy Computing (Trust 2010). June, 2010. Berlin, Germany.

Alam, M., Zhang, X., Nauman, M , Khan, S., Alam, Q. MAuth: A Fine-Grained and User-centric Permission Delegation Framework for Multi-mashup Web Services. 6th World Congress on Services, SERVICES 2010. July 2010. Florida, USA.

Nauman, M. and Ali, T. TOKEN: Trustable Keystroke-based Authentication for Web-based Applications on Smartphones. International Workshop on Wireless and Network Security (WSN'10) in conjunction with International Conference on Information Security and Assurance (ISA'10). June, 2010. Miyazaki, Japan.

Tamleek Ali, Nauman, M. Fazl-e-Hadi, Fahad bin Muhaya. On Usage Control of Multimedia Content in and through Cloud Computing Paradigm. 5th International Conference on Future Information Technology (FutureTech2010). May 2010. Busan, Korea.

Tamleek Ali, Nauman, M. , Muhammad Amin, Masoom Alam . Scalable, Privacy-preserving Remote Attestation in and through Federated Identity Management Frameworks. International Conference on Information Science and Applications (ICISA 2010). April 2010. Seoul, Korea.

Nauman, M. , Sohail Khan and Xinwen Zhang. Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints.(Full version\_) 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS2010). April 2010. Beijing, China.

Tamleek Ali, Nauman, M. and Masoom Alam. Scalable, Privacy-preserving Remote Attestation. International Conference on Trusted Systems (Intrust09). December 2009. Beijing, China.

Imran Khan, Nauman, M. , Masoom Alam and Furqan Aziz. SAuthMash: Mobile Agent based Self Authorization in Mashups. International ACM Conference on Frontiers of Information Technology (FIT'09). 2009. ACM. Abottabad, Pakistan.

Shahbaz Khan, Sanullah Khan, Nauman, M. , Tamleek Ali and Masoom Alam. Realizing Dynamic Behavior Attestation for Mobile. International ACM Conference on Frontiers of Information Technology (FIT'09). 2009. ACM. Abottabad, Pakistan.

Ronald Toegl, Thomas Winkler, Nauman, M. and Theordore Hong. Towards Platform Independent Trusted Computing. Proceedings of the Fourth Annual Workshop on Scalable Trusted Computing (STC'09) at the 16th International ACM Conference on Computers and Communication Security (CCS'09). 2009. ACM. Chicago, Illinois, USA.

Tamleek Ali and Nauman, M. Incorporating Remote Attestation for End-to-End Protection in Web Communications Paradigm. International Conference on Internet Technologies and Applications (ITA'09). September 2009. Wrexham, UK.



Masoom Alam, Nauman, M. , Xinwen Zhang, Tamleek Ali and Patrick Hung. Behavioral Attestation for Business Processes (BA4BP). 7th IEEE International Conference on Web Services (ICWS'09). IEEE. July, 2009. Los Angeles, USA.

Nauman, M. , Masoom Alam, Xinwen Zhang and Tamleek Ali. Remote Attestation of Information Flows and Attribute Updates in a UCON System. 2nd International Conference on Technical and Socio-Economic Aspects of Trusted Computing (Trust2009). Springer. April, 2009. Oxford, UK. [PPTX] Talk Sponsored by the ICT R&D Fund, Pakistan.

Nauman M. and Tamleek Ali. HUE: A Hardware UCON Engine for Fine-grained, Continuous Usage Control. 12th International IEEE Multitopic Conference (INMIC 2008). December, 2008. Karachi, Pakistan.

Masoom Alam, Xinwen Zhang, Nauman, M. , and Tamleek Ali. Behavioral Attestation for Web Services (BA4WS). In Proceedings of International Workshop on Secure Web Services (SWS'08.) at the 15th International ACM Conference on Computers and Communication Security (CCS'08). 2008. ACM. Fairfax, Virginia, USA.

Nauman, M. , Khan, S., Amin, M. and Hussain, F. Resolving Lexical Ambiguities in Folksonomy Based Search Systems through Common Sense and Personalization. in Proceedings of the Semantic Search 2008 Workshop. (SemSearch 2008): located at the 5th European Semantic Web Conference (ESWC2008), Tenerife, Spain.

Masoom Alam, Zhang, X., Nauman, M. , Ali, T., and Seifert, J. Model-based Behavioral Attestation. In Proceedings of the 13th ACM Symposium on Access Control Models and Technologies. SACMAT '08. ACM, New York, NY, 175-184. Estes Park, CO, USA.

Khan S., Amin, M and Nauman, M. A Comprehensive Analysis of MAC Enhancements for Leveraging Distributed MAC. In Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS 08), Hong Kong.

Ali, T. Nauman, M. and Alam M. An Accessible Formal Specification of UML and OCL Meta-Model in Isabelle/HOL. In Proceedings of the International Multitopic Conference 2007 (INMIC'07). Lahore, Pakistan.

Nauman, M. and Khan, S. Using Personalized Web Search for Enhancing Common Sense and Folksonomy Based Intelligent Search Systems. In Proceedings of the IEEE/WIC/ACM international Conference on Web intelligence (November 02 – 05, 2007). Web Intelligence. IEEE Computer Society, Washington, DC, 423-426. Silicon Valley, USA.

Nauman, M. and Hussain, F. "Common Sense and Folksonomy: Engineering an Intelligent Search System," in Proceedings of ICIET'07: International Conference on Information and Emerging Technologies. ICET. IEEE. Karachi, Pakistan. 2007.

Nauman, M. and Uzair, M. 2007. SE and CS Collaboration: Training Students for Engineering Large, Complex Systems. In Proceedings of the 20th Conference on Software Engineering Education & Training (July 03 – 05, 2007). CSEET. IEEE Computer Society. Dublin, Ireland