

Curriculum Vitæ

Mehmet Tahir SANDIKKAYA

November 26, 2024

Career Highlights

Dr. Mehmet Tahir Sandikkaya received his BS degree in Electrical Engineering from Istanbul Technical University (ITU) in 2002, his MS degree in 2005 and his PhD in 2015 in Computer Science from Informatics Institute of the same university. He contributed research efforts on several projects at Katholieke Universiteit Leuven (KU Leuven) Technologicampus Gent in Belgium from 2008 to 2010. From 2002 to 2016, he served as a research assistant in Istanbul Technical University. He visited Drakkar Research group during 2018 till 2019 at Grenoble Informatics Laboratory (LIG) of Grenoble Institute of Technology (Grenoble INP) in University of Grenoble-Alpes (UGA) as an invited research fellow. Currently, he holds an Assistant Professorship position in Computer Engineering Department of Istanbul Technical University. His research contributions include publication on computer security, privacy, electronic voting systems, computer networks and electronic health systems. His recent activities focus on cloud computing security, security measurements on the global network, security protocols and IoT security.

Academic Experience

Assistant Professor Istanbul Technical University, 2018–

Visiting Researcher Grenoble Institute of Technology, 2018–2019

Lecturer Istanbul Technical University, 2016–2018

Research & Teaching Assistant Istanbul Technical University, 2010–2016

Researcher Katholieke Universiteit Leuven Technologicampus Gent, 2008–2010

Research & Teaching Assistant Istanbul Technical University, 2002–2008

Education

Bachelor of Arts Sociology, Anadolu University, 2024

Philosophiæ Doctor Computer Science, Istanbul Technical University, 2015

Master of Science Computer Science, Istanbul Technical University, 2005

Bachelor of Science Electrical Engineering, Istanbul Technical University, 2002

Publications

- [2024] Ayşe Sayın and Mehmet Tahir Sandıkkaya. Turkey’s contact tracing infrastructure from security and privacy perspective. *Journal of Polytechnic*, 27(4):1417–1426, December 2024. ISSN 1302-0900. URL <https://doi.org/10.2339/politeknik.1118577>. (WOS:001192387300001)
- [2024] Mustafa Evcil, Zaliha Yüce Tok, and Mehmet Tahir Sandıkkaya. Unsupervised attack detection on mil-std-1553 bus for avionic platforms. In Gulchohra Mammadova, Telman Aliev, and Kamil Aidazade, editors, *Information Technologies and Their Applications*, volume 2225 of *Communications in Computer and Information Science*, pages 28–43, Cham, October 2024. Second International Conference on Information Technologies and Their Applications, ITTA 2024, Baku, Azerbaijan, 23 Apr. 2024 – 25 Apr. 2024, Springer Nature Switzerland. doi: 10.1007/978-3-031-73417-5_3. URL https://doi.org/10.1007/978-3-031-73417-5_3
- [2024] Serra Uysal and Mehmet Tahir Sandıkkaya. Obstacles to the widespread use of connected and automated vehicles. *Journal of Ambient Intelligence and Smart Environments*, To be published, March 2024. ISSN 1876-1364. URL <https://doi.org/10.3233/AIS-230232>
- [2024] Kağan Özgün, Ayşe Tosun, and Mehmet Tahir Sandıkkaya. A recommender system to detect distributed denial of service attacks with network and transport layer features. In *Proceedings of the 10th International Conference on Information Systems Security and Privacy ICISSP*, volume 1, pages 390–397. Rome, Italy, 26 Feb. 2024 – 28 Feb. 2024, SciTePress, February 2024. ISBN 978-989-758-683-5. URL <https://doi.org/10.5220/0012350100003648>
- [2023] Nazanin Moarref and Mehmet Tahir Sandıkkaya. MC-MLDCNN: Multichannel Multilayer Dilated Convolutional Neural Networks for Web Attack Detection. *Security and Communication Networks*, 2023(1):2415288, December 2023. ISSN 1939-0114
- [2023] Sabtain Ahmad, Halit Uyanık, Tolga Ovatman, Mehmet Tahir Sandıkkaya, Vincenzo De Maio, Ivona Brandić, and Atakan Aral. Sustainable environmental monitoring via energy and information efficient multi-node placement. *IEEE Internet of Things Journal*, 10(24):22065–22079, December 2023. ISSN 2327-4662. URL <https://doi.org/10.1109/JIOT.2023.3303124>. (WOS:001163472700079)
- [2023] Gizemnur Taşkın and Mehmet Tahir Sandıkkaya. Comparison of security frameworks for SMEs. In *2023 14th International Conference on Electrical and Electronics Engineering (ELECO)*, pages 1–5. Bursa, Turkey, 30 Nov. 2023 – 2 Dec. 2023, IEEE, December 2023. URL <https://doi.org/10.1109/ELECO60389.2023.10416030>
- [2023a] Dilek Yılmaz Demirel and Mehmet Tahir Sandıkkaya. MASD: Malicious Web Session Detection Using ML-Based Classifier. In *Proceedings of the 15th International Joint Conference on Computational Intelligence - NCTA*, pages 487–495. Rome, Italy, 13 Nov. 2023 – 15 Nov. 2023, SciTePress, November 2023a. ISBN 978-989-758-674-3. URL <https://doi.org/10.5220/0012174800003595>
- [2023a] Işıl Çetintav and Mehmet Tahir Sandıkkaya. A lightweight authentication and management method for internet of things. *Internet of Things*, 23:100842, October 2023a. ISSN 2543-1536. URL <https://doi.org/10.1016/j.iot.2023.100842>. (WOS:001055899100001)
- [2023] Ayşe Sayın and Mehmet Tahir Sandıkkaya. A reasoning method to interpret fate of pollutants on a cyber-physical river model. In *2023 8th International Conference on Computer Science and Engineering (UBMK)*, pages 324–329. Burdur, Turkey, 13 Sep. 2023 – 15 Sep. 2023, IEEE, September 2023. URL <https://doi.org/10.1109/UBMK59864.2023.10286674>
- [2023b] Dilek Yılmaz Demirel and Mehmet Tahir Sandıkkaya. ACUM: An Approach to Combining Unsupervised Methods for Detecting Malicious Web Sessions. In *2023 8th International Conference on Computer Science and Engineering (UBMK)*, pages 288–293. Burdur, Turkey, 13 Sep. 2023 – 15 Sep. 2023, IEEE, September 2023b. URL <https://doi.org/10.1109/UBMK59864.2023.10286727>
- [2023c] Dilek Yılmaz Demirel and Mehmet Tahir Sandıkkaya. Web Based Anomaly Detection Using Zero-Shot Learning With CNN. *IEEE Access*, 11:91511–91525, August 2023c. URL <https://doi.org/10.1109/ACCESS.2023.3303845>. (WOS:001060260600001)
- [2023] Eren Kılıç and Mehmet Tahir Sandıkkaya. Obfuscated JavaScript Code Detection using Machine Learning with AST-based Syntactic and Lexical Analysis. In *2023 8th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–6. Split/Bol, Croatia, 6 Jun. 2023 – 10 Jun. 2023, IEEE, June 2023. URL <https://doi.org/10.23919/SpliTech58164.2023.10193211>

- [2023b] Işıl Çetintav and Mehmet Tahir Sandıkkaya. LAKE: A Low-cost, Lightweight Authentication, Key Exchange, and Data Transfer Scheme for IoT. In *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–4. Budva, Montenegro, 6 Jun. 2023 – 10 Jun. 2023, IEEE, June 2023b. URL <https://doi.org/10.1109/MECO58584.2023.10155057>
- [2023] Ayşe Sayın, Mostafa Mohammadpourfard, and Mehmet Tahir Sandıkkaya. Identifying concept drift with supervised algorithms in smart grids. In *2023 IEEE PES GTD International Conference and Exposition (GTD)*, pages 263–267. Istanbul, Turkey, 22 May 2023 – 25 May 2023, IEEE, May 2023. URL <https://doi.org/10.1109/GTD49768.2023.00076>
- [2022] Mohammed Khudhair Abbas and Mehmet Tahir Sandıkkaya. An efficient VoLTE covert timing channel for 5G networks: RDCTC. *Optik*, 270:170076, November 2022. ISSN 0030-4026. URL <https://doi.org/10.1016/j.ijleo.2022.170076>. (WOS:000875639300003)
- [2022] Mostafa Mohammadpourfard, Fateme Ghanaatpishe, Yang Weng, Istemihan Genc, and Mehmet Tahir Sandıkkaya. Real-Time Detection of Cyber-Attacks in Modern Power Grids with Uncertainty using Deep Learning. In *2022 International Conference on Smart Energy Systems and Technologies (SEST)*, pages 1–6. Eindhoven, Netherlands, 5 Sep. 2022 – 7 Sep. 2022, IEEE, September 2022. URL <https://doi.org/10.1109/SEST53650.2022.9898413>
- [2022] Berkan Ufuk and Mehmet Tahir Sandıkkaya. Moving Target Defense Router: MaTaDoR. In Sabrina De Capitani di Vimercati and Pierangela Samarati, editors, *Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT*, volume 1, pages 649–654. Lisbon, Portugal, 11 Jul. 2022 – 13 Jul. 2022, SciTePress, July 2022. ISBN 978-989-758-590-6. URL <https://doi.org/10.5220/0011306500003283>
- [2020] Mehmet Tahir Sandıkkaya, Yusuf Yaslan, and Cemile Diler Özdemir. DeMETER in clouds: detection of malicious external thread execution in runtime with machine learning in PaaS clouds. *Cluster Computing*, 23(4):2565–2578, October 2020. ISSN 1386-7857. URL <https://doi.org/10.1007/s10586-019-03027-8>. (WOS:000541817300001)
- [2020] Mehmet Özkur and Mehmet Tahir Sandıkkaya. A Survey on Security & Privacy Design in e-Health. In *2020 5th International Conference on Computer Science and Engineering (UBMK)*, pages 208–213. Diyarbakır, Turkey, 9 Sep. 2020 – 11 Sep. 2020, IEEE, September 2020. URL <https://doi.org/10.1109/UBMK50275.2020.9219372>
- [2020] Tolga Bilbey and Mehmet Tahir Sandıkkaya. The Effects of Gamification to Private Data Collection. *Journal of Computational Design*, 1(3):133–154, September 2020. URL <https://dergipark.org.tr/tr/pub/jcode/issue/57045/764526>
- [2020] Gökay Şimşek and Mehmet Tahir Sandıkkaya. Parking IoT: An IoT Architecture to Collect Availability Data from Parking Lots. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–5. Budva, Montenegro, Montenegro, 8 Jun. 2020 – 11 Jun. 2020, IEEE, June 2020. URL <https://doi.org/10.1109/MECO49872.2020.9134335>
- [2019] Cemile Diler Özdemir, Mehmet Tahir Sandıkkaya, and Yusuf Yaslan. Malicious Behavior Classification in PaaS. In Víctor Méndez Muñoz, Donald Ferguson, Markus Helfert, and Claus Pahl, editors, *CLOSER 2018: Cloud Computing and Services Science*, volume 1073 of *Communications in Computer and Information Science (CCIS)*, pages 215–232. Springer International Publishing, August 2019. ISBN 978-3-030-29192-1. URL https://doi.org/10.1007/978-3-030-29193-8_11
- [2019] Mustafa Özbek and Mehmet Tahir Sandıkkaya. Detecting Malicious Behavior in Microservice Based Web Applications. In *2019 27th Signal Processing and Communications Applications Conference (SIU)*, pages 1–4. Sivas, Turkey, 24 Apr. 2019 – 26 Apr. 2019, IEEE, April 2019. ISBN 978-1-7281-1904-5. URL <https://doi.org/10.1109/SIU.2019.8806294>
- [2019] Emir Erdem and Mehmet Tahir Sandıkkaya. OTPaaS —One Time Password as a Service. *IEEE Transactions on Information Forensics and Security*, 14(3):743–756, March 2019. ISSN 1556-6013. URL <https://doi.org/10.1109/TIFS.2018.2866025>. (WOS:000444795500005)
- [2018] Cemile Diler Özdemir, Mehmet Tahir Sandıkkaya, and Yusuf Yaslan. Classifying Malicious Thread Behavior in PaaS Web Services. In *Proceedings of the 8th International Conference on Cloud Computing and Services Science (CLOSER)*, volume 1, pages 418–425. Funchal, Madeira, Portugal, 19 Mar. 2018 – 21 Mar. 2018, SciTePress, March 2018. ISBN 978-989-758-295-0. URL <https://doi.org/10.5220/0006688204180425>

- [2017] Aşkın Okkalı and Mehmet Tahir Sandikkaya. Preserving privacy using visual cryptography in surveillance systems. In *2017 International Conference on Computer Science and Engineering (UBMK)*, pages 1141–1144. Antalya, Turkey, 5 Oct. 2017 – 8 Oct. 2017, IEEE, October 2017. ISBN 978-1-5386-0931-6. URL <https://doi.org/10.1109/UBMK.2017.8093534>
- [2016] Mehmet Tahir Sandikkaya, Tolga Ovatman, and Ali Emre Harmancı. Design and formal verification of a cloud compliant secure logging mechanism. *IET Information Security*, 10(4):203–214, July 2016. ISSN 1751-8709. URL <https://doi.org/10.1049/iet-ifs.2014.0625>. (WOS:000378417900006)
- [2015] Mehmet Tahir Sandikkaya. *Bilgişlem Ortamı Sunan Bulut için Güvenlik Düzenekleri*. PhD thesis, Istanbul Technical University, Istanbul, Turkey, 2015. URL http://www.sandikkaya.name.tr/pub/DrTez_SANDIKKAYA,MT_TR.pdf. (Turkish. English title: Security Mechanisms for PaaS Cloud)
- [2015] Mehmet Tahir Sandikkaya and Ali Emre Harmancı. A Security Paradigm for PaaS Clouds. *Proceedings of the Romanian Academy Series A: Mathematics, Physics, Technical Sciences, Information Science*, 16(Special Issue: Cryptology):345–356, September 2015. ISSN 1454-9069. URL <http://www.academiaromana.ro/sectii2002/proceedings/doc2015-3s/10-Sandikkaya.pdf>. (WOS:000362155300010)
- [2014] Mehmet Tahir Sandikkaya, Bahadır Ödevci, and Tolga Ovatman. Practical runtime security mechanisms for an aPaaS cloud. In *2014 IEEE Globecom Workshops*, pages 53–58. Austin, TX, USA, 08 Dec. 2014 – 12 Dec. 2014, IEEE, December 2014. ISBN 978-1-4799-7470-2. URL <https://doi.org/10.1109/GLOCOMW.2014.7063385>
- [2012] Mehmet Tahir Sandikkaya and Ali Emre Harmancı. Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems. In *2012 IEEE 31st Symposium on Reliable Distributed Systems (SRDS)*, pages 463–468. Irvine, CA, USA, 08 Oct. 2012 – 11 Oct. 2012, IEEE, October 2012. ISBN 978-1-4673-2397-0. URL <https://doi.org/10.1109/SRDS.2012.84>
- [2010] Mehmet Tahir Sandikkaya, Bart De Decker, and Vincent Naessens. Privacy in Commercial Medical Storage Systems. In Martin Szomszor and Patty Kostkova, editors, *Electronic Healthcare (eHealth 2010)*, volume 69 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST)*, pages 247–258. Casablanca, Morocco, 13 Dec. 2010 – 15 Dec. 2010, Springer Berlin Heidelberg, December 2010. ISBN 978-3-642-23634-1. URL https://doi.org/10.1007/978-3-642-23635-8_32
- [2009] Mohamed Layouni, Kristof Verslype, Mehmet Tahir Sandikkaya, Bart De Decker, and Hans Vangheluwe. Privacy-Preserving Telemonitoring for eHealth. In Ehud Gudes and Jaideep Vaidya, editors, *Data and Applications Security XXIII (DBSec 2009)*, volume 5645 of *Lecture Notes in Computer Science*, pages 95–110. 23rd Annual IFIP WG 11.3 Working Conference, Montreal, Canada, 12 Jul. 2009 – 15 Jul. 2009, Springer Berlin Heidelberg, July 2009. ISBN 978-3-642-03006-2. URL https://doi.org/10.1007/978-3-642-03007-9_7
- [2009] Vincent Naessens, Mehmet Tahir Sandikkaya, Jorn Lapon, Kristof Verslype, Pieter Verhaeghe, Girma Nigusse, and Bart De Decker. Privacy Policies, Tools and Mechanisms of the Future. In Jan Camenisch and Dogan Kesdogan, editors, *iNetSec 2009 – Open Research Problems in Network Security*, volume 309 of *IFIP Advances in Information and Communication Technology (IFIP AICT)*, pages 125–138. IFIP WG 11, Zurich, Switzerland, 23 Apr. 2009 – 24 Apr. 2009, Springer Berlin Heidelberg, April 2009. ISBN 978-3-642-05436-5. URL https://doi.org/10.1007/978-3-642-05437-2_12
- [2007] Burak Kantarcı, Mehmet Tahir Sandikkaya, Aysegül Gençata, and Sema Oktuğ. Prudent Creditization Polling (PCP): A Novel Adaptive Polling Service for an EPON. In Ioannis Tomkos, Fabio Neri, Josep Solé Pareta, Xavier Masip Bruin, and Sergi Sánchez Lopez, editors, *Optical Network Design and Modeling (ONDM)*, volume 4534 of *Lecture Notes in Computer Science*, pages 388–397. Athens, Greece, 29 May 2007 – 31 May 2007, Springer Berlin Heidelberg, May 2007. ISBN 978-3-540-72729-3. URL https://doi.org/10.1007/978-3-540-72731-6_42
- [2006] Mehmet Tahir Sandikkaya and Mehmet Bülent Örencik. Agent-Based Offline Electronic Voting. In *30th Annual International Computer Software and Applications Conference (COMPSAC'06)*, volume 2, pages 333–340. Chicago, IL, USA., 17 Sep. 2006 – 21 Sep. 2006, IEEE, September 2006. ISBN 0-7695-2655-1. URL <https://doi.org/10.1109/COMPSAC.2006.107>
- [2005] Mehmet Tahir Sandikkaya. Etmenlerle Elektronik Oylama. Master's thesis, Istanbul Technical University, Istanbul, Turkey, 2005. URL http://www.sandikkaya.name.tr/pub/YLTez_SANDIKKAYA,MT_TR.pdf. (Turkish. English title: Electronic Voting with Agents)

Projects

- SWAIN. Sustainable Watershed Management Through IoT-Driven Artificial Intelligence. CHIST-ERA of EU, 2021. Mar. 2021–Jun. 2024
- NİCASGÜZED. A Mechanism to Mitigate Security Weaknesses Encountered During Authentication of IoT Devices. Istanbul Technical University, 2021. Jun. 2021–Mar. 2024
- SMOC. Improving the Performance of Distributed State Machine Performance on Cloud Systems. The Scientific and Technological Research Council of Turkey, 2019. Dec. 2019–Dec. 2021
- NİÇEHA. Multi-Factor Lightweight Authentication for IoT. Istanbul Technical University, 2018. Oct. 2018–Jul. 2021
- HoneyWalt. Building an Extendable IoT Honeypot. Embassy of France in Ankara & Istanbul Technical University, 2018. Aug. 2018–Feb. 2019
- FEnCY. Pollutant Fingerprint Detection based Functional Integrated Geographic Information Management Software for Ergene Basin. The Scientific and Technological Research Council of Turkey, 2016. Jan. 2016–Jun. 2019
- Cloud Fortification. Operational Optimization of a Cloud System Serving Software Development Platform. Republic of Turkey - Ministry of Science, Industry and Technology, 2013. Oct. 2013–Jun. 2015
- Secure Cloud. Developing a Secure Cloud Computing Structure. Istanbul Technical University, 2011. Apr. 2011–Apr. 2013
- DiCoMas. DiCoMas –Distributed Collaboration using Multi-Agent System Architectures. IWT (Kingdom of Belgium - Institute for Innovation through Science and Technology in Flanders), 2007. Oct. 2007–Sep. 2011

Consultancy¹

- Cyber-Physical Systems Security in Avionics. Avionics cyber-security frontier r&d laboratory. *Establishment of Frontier R&D Laboratory*, 2023. TÜBİTAK –The Scientific and Technological Research Council of Turkey, Oct. 2023–Oct. 2024
- Security Analysis of Smart Grid. Analysis of weaknesses in current smart grid communication and management protocols. *Provided data is used for further smart grid security mechanism designs*, 2022. TÜBİTAK –The Scientific and Technological Research Council of Turkey, Jan. 2022–Jan. 2023
- Continuous Assessment of Critical IT Systems. Design & application of a continuous security assessment procedure for critical information technologies systems of e-services companies. *The continuous assessment methodology is widely adopted among legal betting companies of Turkey*, 2021. Investor-funded, Jan. 2022–Sep. 2022
- Decofinder. Design & implementation of an AI-based chipboard & edge band decor search and matching engine. *The edge band search and matching engine is adopted in the furniture industry*, 2021. Investor-funded, Jul. 2021–Mar. 2022
- Certification of Critical IT Systems. Design & application of a generic performance & security certification procedure for critical information technologies systems of e-services companies. *The certification is widely adopted among legal betting companies of Turkey*, 2020. Investor-funded, Oct. 2020–Dec. 2021
- Smart Billboard. Design of a smart, scalable, multi-source data synchronization enabled digital billboard management software. *The smart billboards are widely adopted in many retail chain companies in Turkey and abroad*, 2020. TÜBİTAK –The Scientific and Technological Research Council of Turkey, Jul. 2020–Oct. 2020
- Smart City Privacy. Design of privacy-enhancing technologies for a semantic smart-city platform. *The platform is in use in many metropolitan municipalities of Turkey*, 2016. TÜBİTAK –The Scientific and Technological Research Council of Turkey, Jul. 2016–Jun. 2018

¹Details are omitted with respect to non-disclosure agreements.

- e-invoice. Design of an e-invoice archive system. *The infrastructure has been approved and used by state financial bodies in Turkey*, 2015. İTÜ ARI Teknokent Proje Geliştirme Planlama A.Ş., Apr. 2015–Dec. 2015
- Mobile Payment. Design of a mobile money transfer and payment system. *The protocols & infrastructure is widely adopted among retail sector and many major banks of Turkey.*, 2013. TÜBİTAK –The Scientific and Technological Research Council of Turkey, Jul. 2013–Dec. 2016
- Mobile OTP. Design of a generic mobile OTP application & password manager. *The application is widely adopted among Fortune 500 companies.*, 2011. Investor-funded, Dec. 2010–Dec. 2014