Understanding Ephemeral Secret Leakage Attacks in Password-based Multi-factor Authentication for Mobile Devices (Appendix File)

Ding Wang, Meijia Xu, Qingxuan Wang

Abstract

This appendix file consists of one part. Appendix A shows the 120 references listed in Fig. 2 of the main text.

Index Terms

Appendix file.

APPENDIX A: THE 120 REFERENCES LISTED IN FIG.2 OF THE MAIN TEXT

This figure shows a brief history of multi-factor authentication schemes. Most of the listed schemes are analyzed in our previous works. According to this figure, we can see the tough development of multi-factor authentication schemes.

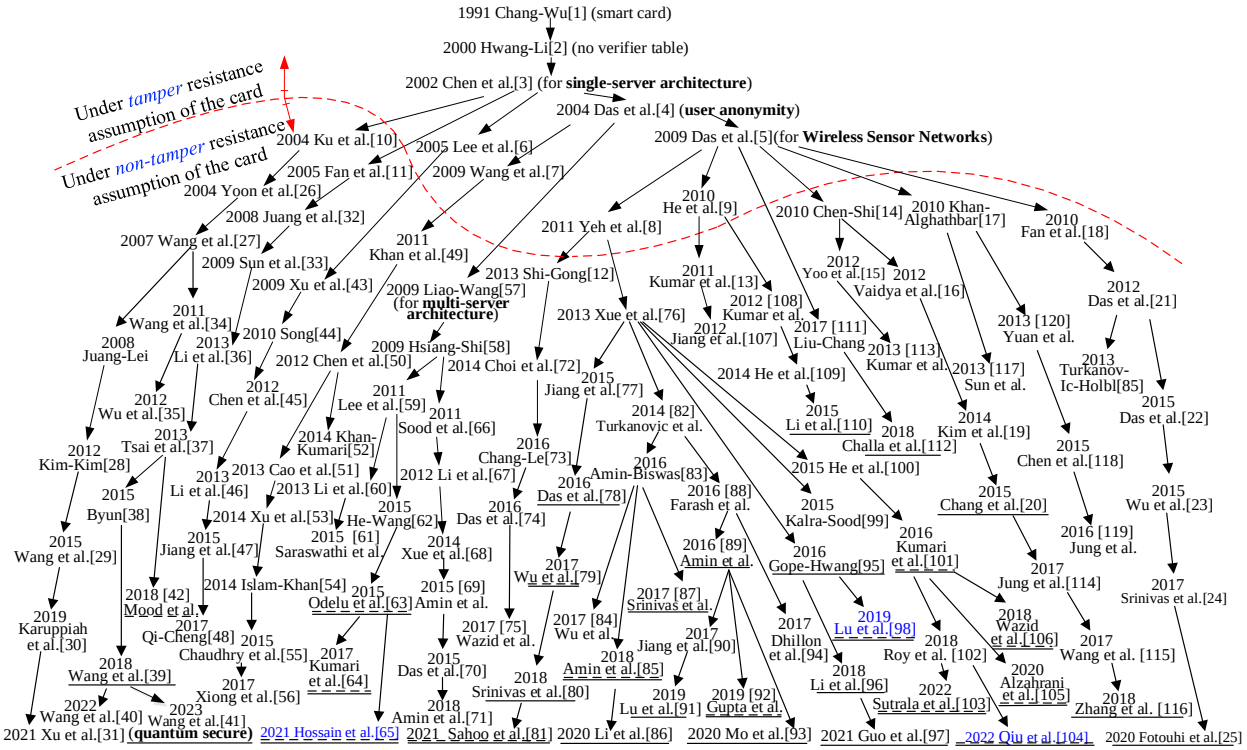

Fig. 1. A brief history of multi-factor authentication schemes. Each child node claims to be an improved scheme of its parent node but is found insecure by its child nodes. Schemes with a dashed line are claimed to be able to resist ephemeral secret leakage (ESL) attacks, and these underlined with a solid line are (actually) vulnerable to ESL attacks. Three schemes in blue are cryptanalyzed/exemplified in this work.

- *Ding Wang, Meijia Xu, and Qingxuan Wang are with the College of Cryptology and Cyber Science, Nankai University, Tianjin 300350, China, and Key Laboratory of Data and Intelligent System Security (Ministry of Education), Nankai University, Tianjin 300350, China, and also with Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China. (Email: {wangding, wangqingxuan}@nankai.edu.cn; xumeijia@mail.nankai.edu.cn;)*
- *Corresponding author is Qingxuan Wang.*

REFERENCES

[1] C. Chang and T. Wu, "Remote password authentication with smart cards," *IEE Comput. Digital Tech.*, vol. 138, no. 3, pp. 165–168, 1991.
[2] M. Hwang and L. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 46, no. 1, pp. 28–30, 2000.
[3] H. Chien, J. Jan, and Y. Tseng, "An efficient and practical solution to remote authentication: Smart card," *Comput. Secur.*, vol. 21, no. 4, pp. 372–375, 2002. [Online]. Available: https://doi.org/10.1016/S0167-4048(02)00415-7
[4] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE Trans. Consumer Electron.*, vol. 50, no. 2, pp. 629–631, 2004.
[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 8, no. 3, pp. 1086–1090, 2009.
[6] S. Lee, H. Kim, and K. Yoo, "Improvement of chien et al.'s remote user authentication scheme using smart cards," *Comput. Stand. Interfaces*, vol. 27, no. 2, pp. 181–183, 2005.
[7] Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic id-based remote user authentication scheme," *Comput. Commun.*, vol. 32, no. 4, pp. 583–585, 2009.
[8] H. Yeh, T. Chen, P. Liu *et al.*, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–79, 2011.
[9] D. He, Y. Gao, S. Chan *et al.*, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sens. Wirel. Networks*, vol. 10, no. 4, pp. 361–371, 2010.
[10] W. Ku and S. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 50, no. 1, pp. 204–207, 2004.
[11] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," *Comput. Secur.*, vol. 24, no. 8, pp. 619–628, 2005.
[12] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Int. J. Distributed Sens. Networks*, vol. 9, 2013.
[13] P. Kumar, A. J. Choudhury, M. Sain, S. Lee, and H. Lee, "RUASN: A robust user authentication framework for wireless sensor networks," *Sensors*, vol. 11, no. 5, pp. 5020–5046, 2011.
[14] T.-H. Chen and W.-K. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI journal*, vol. 32, no. 5, pp. 704–712, 2010.
[15] S. G. Yoo, K. Park, and J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *Int. J. Distributed Sens. Networks*, vol. 8, 2012.
[16] B. Vaidya, D. Makrakis, and H. Mouftah, "Two-factor mutual authentication with key agreement in wireless sensor networks," *Secur. Commun. Networks*, vol. 9, no. 2, pp. 171–183, 2016.
[17] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.
[18] R. Fan, L.-D. Ping, J.-Q. Fu, and X.-Z. Pan, "A secure and efficient user authentication protocol for two-tiered wireless sensor networks," in *PACCS 2010*, vol. 1, pp. 425–428.
[19] J. Kim, D. Lee, W. Jeon *et al.*, "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," *Sensors*, vol. 14, no. 4, pp. 6443–6462, 2014.
[20] I. Chang, T. Lee *et al.*, "Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks," *Sensors*, vol. 15, no. 12, pp. 29 841–29 854, 2015.
[21] A. Das, S. Sharma, P.and Chatterjee *et al.*, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, 2012.
[22] A. K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377–1404, 2015.
[23] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multim. Syst.*, vol. 23, no. 2, pp. 195–205, 2017.
[24] J. Srinivas, D. Mishra, and S. Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks," *J. Medical Syst.*, vol. 41, no. 5, pp. 80:1–80:19, 2017.
[25] M. Fotouhi, M. Bayat *et al.*, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot," *Comput. Networks*, vol. 177, p. 107333, 2020.
[26] E. Yoon, E. Ryu, and K. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 50, no. 2, pp. 612–614, 2004.
[27] X. Wang, W. Zhang, J. Zhang, and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," *Comput. Stand. Interfaces*, vol. 29, no. 5, pp. 507–512, 2007.
[28] T. H. Kim, C. Kim, and I. Park, "Side channel analysis attacks using AM demodulation on commercial smart cards with SEED," *J. Syst. Softw.*, vol. 85, no. 12, pp. 2899–2908, 2012.
[29] D. Wang, D. He, P. Wang, and C. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secur. Comput.*, vol. 12, no. 4, pp. 428–442, 2015.
[30] M. Karuppiah, A. K. Das, X. Li, S. Kumari, F. Wu, S. A. Chaudhry, and N. Radhakrishnan, "Secure remote user mutual authentication scheme with key agreement for cloud environment," *Mob. Networks Appl.*, vol. 24, no. 3, pp. 1046–1062, 2019.
[31] M. Xu, D. Wang, Q. Wang, and Q. Jia, "Understanding security failures of anonymous authentication schemes for cloud environments," *J. Syst. Archit.*, vol. 118, p. 102206, 2021.
[32] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551–2556, 2008.
[33] D.-Z. Sun, J.-P. Huai, J.-Z. Sun, J.-X. Li, J.-W. Zhang, and Z.-Y. Feng, "Improvements of juang's password-authenticated key agreement scheme using smart cards," *IEEE Trans. Ind. Electron.*, vol. 56, no. 6, pp. 2284–2291, 2009.
[34] R. Wang, W. Juang, and C. Lei, "Robust authentication and key agreement scheme preserving the privacy of secret key," *Comput. Commun.*, vol. 34, no. 3, pp. 274–280, 2011.
[35] S. Wu, Y. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," *Secur. Commun. Networks*, vol. 5, no. 2, pp. 236–248, 2012.
[36] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, 2010.
[37] J. Tsai, N. Lo, and T. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informatics*, vol. 9, no. 4, pp. 2004–2013, 2013.
[38] J. W. Byun, "Privacy preserving smartcard-based authentication system with provable security," *Secur. Commun. Networks*, vol. 8, no. 17, pp. 3028–3044, 2015.
[39] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 4, pp. 708–722, 2018.

[40] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 1, pp. 507–523, 2022.

[41] Q. Wang, D. Wang, C. Cheng, and D. He, "Quantum2fa: Efficient quantum-resistant two-factor authentication scheme for mobile devices," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 1, pp. 193–208, 2023.

[42] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps," *IEEE Trans. Ind. Informatics*, vol. 14, no. 11, pp. 4815–4828, 2018.

[43] J. Xu, W. T. Zhu, and D. Feng, "An improved smart card based password authentication scheme with provable security," *Comput. Stand. Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[44] R. Song, "Advanced smart card based password authentication protocol," *Comput. Stand. Interfaces*, vol. 32, no. 5-6, pp. 321–325, 2010.

[45] B. Chen, W. Kuo, and L. Wuu, "Robust smart-card-based remote user password authentication scheme," *Int. J. Commun. Syst.*, vol. 27, no. 2, pp. 377–389, 2014.

[46] X. Li, J. Niu, M. K. Khan, and J. Liao, "An enhanced smart card based remote user password authentication scheme," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1365–1371, 2013.

[47] Q. Jiang, J. Ma, G. Li, and X. Li, "Improvement of robust smart-card-based password authentication scheme," *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 383–393, 2015.

[48] M. Qi and J. Chen, "An efficient two-party authentication key exchange protocol for mobile environment," *Int. J. Commun. Syst.*, vol. 30, no. 16, 2017.

[49] M. K. Khan, S. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a 'more efficient & secure dynamic id-based remote user authentication scheme'," *Comput. Commun.*, vol. 34, no. 3, pp. 305–309, 2011.

[50] H. Chen, J. Lo, and C. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems," *J. Medical Syst.*, vol. 36, no. 6, pp. 3907–3915, 2012.

[51] T. Cao and J. Zhai, "Improved dynamic id-based authentication scheme for telecare medical information systems," *J. Medical Syst.*, vol. 37, no. 2, p. 9912, 2013.

[52] M. K. Khan and S. Kumari, "Cryptanalysis and improvement of "an efficient and secure dynamic id-based authentication scheme for telecare medical information systems"," *Secur. Commun. Networks*, vol. 7, no. 2, pp. 399–408, 2014.

[53] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *J. Medical Syst.*, vol. 39, no. 2, p. 10, 2015.

[54] S. H. Islam and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," *J. Medical Syst.*, vol. 38, no. 10, p. 135, 2014.

[55] S. A. Chaudhry, K. Mahmood, H. Naqvi, and M. K. Khan, "An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography," *J. Medical Syst.*, vol. 39, no. 11, p. 175, 2015.

[56] H. Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," *IEEE Access*, vol. 5, pp. 5648–5661, 2017.

[57] Y. Liao and S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Comput. Stand. Interfaces*, vol. 31, no. 1, pp. 24–29, 2009.

[58] H. Hsiang and W. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," *Comput. Stand. Interfaces*, vol. 31, no. 6, pp. 1118–1123, 2009.

[59] C. Lee, T. Lin, and R. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards," *Expert Syst. Appl.*, vol. 38, no. 11, pp. 13 863–13 870, 2011.

[60] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments," *Math. Comput. Model.*, vol. 58, no. 1-2, pp. 85–95, 2013.

[61] S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy, "Secure and efficient smart-card-based remote user authentication scheme for multiserver environment," *Canadian Journal of Electrical and Computer Engineering*, vol. 38, no. 1, pp. 20–30, 2015.

[62] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, 2015.

[63] V. Odelu, A. K. Das *et al.*, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1953–1966, 2015.

[64] S. Kumari, X. Li, F. Wu *et al.*, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, 2017.

[65] M. J. Hossain, C. Xu, C. Li *et al.*, "ICAS: two-factor identity-concealed authentication scheme for remote-servers," *J. Syst. Archit.*, vol. 117, p. 102077, 2021.

[66] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," *J. Netw. Comput. Appl.*, vol. 34, no. 2, pp. 609–618, 2011.

[67] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 763–769, 2012.

[68] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *J. Comput. Syst. Sci.*, vol. 80, no. 1, pp. 195–206, 2014.

[69] R. Amin and G. P. Biswas, "A novel user authentication and key agreement protocol for accessing multi-medical server usable in TMIS," *J. Medical Syst.*, vol. 39, no. 3, p. 33, 2015.

[70] A. K. Das, V. Odelu, and A. Goswami, "A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS," *J. Medical Syst.*, vol. 39, no. 9, pp. 92:1–92:24, 2015.

[71] R. Amin, S. H. Islam, P. Gope, K. R. Choo, and N. Tapas, "Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system," *IEEE J. Biomed. Health Informatics*, vol. 23, no. 4, pp. 1749–1759, 2019.

[72] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10 081–10 106, 2014.

[73] C. Chang and H. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 1, pp. 357–366, 2016.

[74] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3670–3687, 2016.

[75] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 2, pp. 391–406, 2020.

[76] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, 2013.

[77] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1070–1081, 2015.

[78] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 1, pp. 223–244, 2016.

[79] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 16–30, 2017.

[80] J. Srinivas, D. Mishra, S. Mukhopadhyay, and S. Kumari, "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 4, pp. 875–895, 2018.

[81] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using iot enabled devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 1, pp. 1419–1434, 2021.

[82] M. Turkanovic, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[83] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.

[84] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K. R. Choo, M. Wazid, and A. K. Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, 2017.

[85] R. Amin, S. K. H. Islam, N. Kumar *et al.*, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks," *J Netw. Comput. Appl.*, vol. 104, pp. 133–144, 2018.

[86] X. Li, J. Peng *et al.*, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 39–50, 2020.

[87] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Networks*, vol. 54, pp. 147–169, 2017.

[88] M. S. Farash, M. Turkanovic, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[89] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Networks*, vol. 101, pp. 42–62, 2016.

[90] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[91] Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wirel. Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[92] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Comput. Networks*, vol. 149, pp. 29–42, 2019.

[93] J. Mo, W. Shen, and W. Pan, "An improved anonymous authentication protocol for wearable health monitoring systems," *Wirel. Commun. Mob. Comput.*, vol. 2020, pp. 5 686 498:1–5 686 498:13, 2020.

[94] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for internet of things environments," *Int. J. Commun. Syst.*, vol. 30, no. 16, 2017.

[95] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, 2016.

[96] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Trans. Ind. Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[97] Y. Guo, Z. Zhang, and Y. Guo, "Anonymous authenticated key agreement and group proof protocol for wearable computing," *IEEE Trans. Mob. Comput.*, 2021, doi: 10.1109/TMC.2020.3048703.

[98] Y. Lu, G. Xu, L. Li, and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1454–1465, 2019.

[99] S. Kalra and S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *J. Inf. Secur. Appl.*, vol. 20, pp. 37–46, 2015.

[100] D. He, N. Kumar, and N. K. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, 2015.

[101] S. Kumari, X. Li, F. Wu *et al.*, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Sys.*, vol. 63, pp. 56–75, 2016.

[102] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2884–2895, 2018.

[103] A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5g-enabled softwarized industrial cyber-physical systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2316–2330, 2022.

[104] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 2, pp. 1338–1351, 2022.

[105] B. A. Alzahrani, S. A. Chaudhry *et al.*, "A privacy preserving authentication scheme for roaming in iot-based wireless mobile networks," *Symmetry*, vol. 12, no. 2, p. 287, 2020.

[106] M. Wazid, A. K. Das *et al.*, "Design of secure user authenticated key management protocol for generic iot networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, 2018.

[107] J. Qi, M. Zhuo, M. Jianfeng, and L. Guangsong, "Security enhancement of robust user authentication framework for wireless sensor networks," *China Communications*, vol. 9, no. 10, pp. 103–111, 2012.

[108] P. Kumar, S. Lee, and H. Lee, "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks," *Sensors*, vol. 12, no. 2, pp. 1625–1647, 2012.

[109] D. He, N. Kumar, J. Chen, C. Lee, N. K. Chilamkurti, and S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multim. Syst.*, vol. 21, no. 1, pp. 49–60, 2015.

[110] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Networks*, vol. 9, no. 15, pp. 2643–2655, 2016.

[111] C. Liu and Y. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 59, pp. 250–261, 2017.

[112] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ecc-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, 2018.

[113] P. Kumar, A. Gurtov, M. Ylianttila, S.-G. Lee, and H. Lee, "A strong authentication scheme with user privacy for wireless sensor networks," *ETRI journal*, vol. 35, no. 5, pp. 889–899, 2013.

[114] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," *Sensors*, vol. 17, no. 3, p. 644, 2017.

[115] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, 2017.

[116] K. Zhang, K. Xu, and F. Wei, "A provably secure anonymous authenticated key exchange protocol based on ECC for wireless sensor networks," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 2 484 268:1–2 484 268:9, 2018.
[117] D. Sun, J. Li, Z. Feng, Z. Cao, and G. Xu, "On the security and improvement of a two-factor user authentication scheme in wireless sensor networks," *Pers. Ubiquitous Comput.*, vol. 17, no. 5, pp. 895–905, 2013.
[118] L. Chen, F. Wei, and C. Ma, "A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques," *Int. J. Distributed Sens. Networks*, vol. 11, pp. 704 502:1–704 502:10, 2015.
[119] J. Jung, J. Kim, Y. Choi, and D. Won, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 8, p. 1299, 2016.
[120] J. Yuan, "An enhanced two-factor user authentication in wireless sensor networks," *Telecommun. Syst.*, vol. 55, no. 1, pp. 105–113, 2014.