

A Periodic Validation in Blockchain based Mobile Edge Computing (MEC) through Key Management

Dr. S. Sandosh¹, Aditya Kumar Singh², Aditya Gupta³

Assistant Professor (Sr.), School of Computer Science and Engineering¹

Students, School of Computer Science and Engineering^{2,3}

Vellore Institute of Technology, Chennai, India

sandosh.s@vit.ac.in, adityakumar.singh2020a@vitstudent.ac.in, aditya.gupta2020b@vitstudent.ac.in

Abstract: In order to offer mobile consumers shared services and resources with high bandwidth and low latency, key management through blockchain technology is used. However, when shared resources are involved, the MEC infrastructure creates serious security risks. User sensitive and private information. This study presents a key management scheme which is generally used blockchain oriented technology for ensuring common conversation among the devices for they can able to flexibly switch between subnetworks. In the suggested method, when a mobile device joins a subnetwork, it generates compact shared key for electronic signatures and authentication when it joins a subnetwork. All of the public keys for mobile devices are combined by a block that is sent to additional users in the subnetwork by the network miner in the subnetwork. Experimental results demonstrate that the proposed strategy outperforms two baselines in respect of processing, communication, and storage.

Keywords: MEC, Blockchain, Key Management, Periodic Authentication

REFERENCES

- [1]. C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," IEEE/ACM Transactions on Networking (TON), vol. 8, no. 1, pp. 16–30, 2000.
- [2]. M.-L. Messai and H. Seba, "A survey of key management schemes in multi-phase wireless sensor networks," Computer Networks, vol. 105, pp. 60–74, 2016.
- [3]. D. Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," Tech. Rep., 1999
- [4]. S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in international conference on wireless algorithms, systems, and applications. Springer, 2015, pp. 685–695.
- [5]. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.
- [6]. M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," Computer Communications, 2018.
- [7]. W. H. D. Ng, M. Howarth, Z. Sun, and H. Cruickshank, "Dynamic balanced key tree management for secure multicast communications," IEEE Transactions on Computers, vol. 56, no. 5, 2007.
- [8]. D.-H. Je, J.-S. Lee, Y. Park, and S.-W. Seo, "Computation-and-storage-efficient key tree management protocol for secure multicast communications," Computer Communications, vol. 33, no. 2, pp. 136–148, 2010.
- [9]. Y. Sun and K. R. Liu, "Hierarchical group access control for secure multicast communications," IEEE/ACM Transactions on Networking, vol. 15, no. 6, pp. 1514–1526, 2007.
- [10]. C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed group key management for event notification confidentiality among sensors," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 566–580, 2020.

- [11]. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017. [Online].
- [12]. B. Daghighi, M. L. M. Kiah, S. Iqbal, M.
- [13]. H. U. Rehman, and K. Martin, "Host mobility key management in dynamic secure group communication," *Wireless Networks*, pp. 1–19, 2017.
- [14]. S. Hong, H.-I. Kim, and J.-W. Chang, "An efficient key management scheme for user access control in outsourced databases," *World Wide Web*, vol. 20, no. 3, pp. 467–490, 2017.
- [15]. Y. Challal, F. Z. Benhamida, and O. Nouali, "Scalable key management for elastic security domains in fog networks," in *2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2018, pp. 187–192.
- [16]. Z. Q. Lou J and Q. Z., "A blockchain- based key management scheme for named data networking," in *1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 2018, pp. 141–146.
- [17]. P. Vijayakumar, V. Chang, L. J. Deborah, and B. S. R. Kshatriya, "Key management and key distribution for secure group communication in mobile and cloud network," 2018.
- [18]. J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in *Proceedings of 1st IEEE International Conference on Hot Information-Centric Networking*, 2018, pp. 141–146.
- [19]. M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, "Multicast security (msec) group key management architecture," *Tech. Rep.*, 2005.
- [20]. A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.
- [21]. N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in *International Conference on Cryptography and Security Systems*. Springer, 2014, pp. 131–144.
- [22]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," <https://bitcoin.org/bitcoin.pdf>, 2008.
- [23]. N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in *International Conference on Cryptography and Security Systems*. Springer, 2014, pp. 131–144.
- [24]. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for iot data," in *Web Services (ICWS), 2017 IEEE International Conference on*. IEEE, 2017, pp. 468–475.
- [25]. Y. Hu, Y. Xiong, W. Huang, and X. Bao, "Keychain: Blockchainbased key distribution," in *2018 4th International Conference on Big Data Computing and Communications (BIGCOM)*. IEEE, 2018, pp. 126–131.
- [26]. N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.