Journal of
Telecommunications System & Management

Abstract

A Privacy-Preserving Authentication and Key Agreement Scheme with Deniability for IoT.

Tinashe Magara

Chongqing University of Posts and Telecommunications, Chongqing, China, Nigeria

Abstract:

User authentication for the Internet of Things (IoT) is a vital measure as it consists of numerous unattended connected devices and sensors. For security, only the user authenticated by the gateway node can access the real-time data gathered by sensor nodes. We present an efficient privacy-preserving authentication and key agreement scheme for IoT, which enables the user, the gateway node and sensor nodes to authenticate with each other. Only the trusted gateway node can determine the real identity of the user; however, no other entities can get information about user' identity by just intercepting all exchanged Cyber threats are a global risk that governments, the private sector, non-governmental organizations – and the global community as a whole – must deal with. Chatham House focuses on building cyber capacity and expertise among policymakers, investigating key issues through publishing in-depth policy research, conducting cyber simulation exercises, and convening high-level meetings with a wide group of stakeholders. messages during authentication phase. The gateway cannot prove the received messages from the sender to a third party, and thus preserving the privacy of the sender. The correctness of the proposed scheme is proved to be feasible by using BAN logic, and its security is proved under the random oracle model. The execution time of the proposed scheme is evaluated and compared with existing similar schemes, and the results demonstrate that our proposed scheme is more efficient and applicable for IoT applications. The economic and social benefits of digital technology have transformed the world as we know it, but have introduced high risks through its malicious use by both state and non-state actors. These risks affecting economies, societies and livelihoods, and are threatening international peace and security.

Biography:

Magara Tinashe is currently persuing a PhD degree with the Chongqing University of Posts and Telecommunica-

tions, China. (College of Computer Science and Technology). He worked as a researcher and a teaching assistant in the department of Mathematics, Physics and Information Technology, Zhejiang Normal University in China. Magara graduated with a Masters of Software Engineering in 2018. His research interests include Cryptography, Big Data analysis, Artificial Intelligence, Mobile security and the IoT security.

Publication of speakers:

1. Sundmaeker, H, Guillemin, P, Friess, P. Vision and challenges for realising the Internet of Things. Clust. Eur. Res. Proj. Internet Things Eur. Commis. 2010.
2. Lo, N.W.; Tsai, J.L. An efficient conditional priva- cy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. 2016, 17, 1319–1328.
3. He, D.; Kumar, N.; Chen, J. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimed. Syst. 2015, 21, 49–60.
4. Li, X.; Niu, J.; Kumari, S.; Liao, J.; Liang, W.; Khan, M.K. A new authentication protocol for healthcare-applications using wireless medical sensor networks with user anonymity. Secur. Commun. Netw. 2016, 9, 2643–2655. [CrossRef]
5. Wu, F.; Xu, L.; Kumari, S. An improved and anonymous two-factor authentication protocol for healthcare applications with wireless medical sensor networks. Multimed. Syst. 2017, 23, 195–205. [CrossRef]

International Conference on Cloud Computing and Virtualization | May 21, 2020 | London, UK

Citation: Tinashe Magara; A Privacy-Preserving Authentication and Key Agreement Scheme with Deniability for IoT; Cloud Computing 2020; May 21, 2020; London, UK