The Journal of Supercomputing (2025) 81:149
https://doi.org/10.1007/s11227-024-06661-1

Comment on "Efficient design of an authenticated key agreement protocol for dew-assisted IoT systems"

Zhengjun Cao[1] · **Huachen Ye**[1]

Accepted: 26 October 2024

Abstract
We show that the key agreement scheme (Rana et al. in J Supercomput 78(3):3696–3714, 2022) cannot resist impersonation attack, both for the sensor node and dew server. The adversary can use an equivalent computation to finish a core computation for the dew server and retrieve the sensor node's secret key. We also remark that it seems impossible to revise the scheme due to its simple secret key invoking mechanism.

Keywords Dew computing · Key agreement · Mutual authentication · Impersonation attack

1 Introduction

Dew computing aims to fully realize the potentials of personal computers and cloud services, which could influence the future direction of computer hardware and software, including operating systems and browsers. Its key feature is microservices in collaboration with macroservices or dew services in collaboration with cloud services. In 2020, Garg and Lee [1] presented a key agreement for multidevice home IoT environment. Chen et al. [2] put forth a blockchain-based group key agreement protocol for IoT. Wu et al. [3] designed an improved authenticated key agreement scheme for fog-driven IoT healthcare system. In 2022, Mall et al. [4] discussed some PUF-based authentication and key agreement protocols for IoT. Thakur et al. [4] investigated a privacy-preserving authenticated key agreement protocol for an IoT network. Nikooghadam et al. [6] proposed a key agreement scheme based on ECDH for RFID in IoT environment. Uppuluri and Lakshmeeswari [7] presented a user authentication and key agreement scheme for IoT device access control-based smart

✉ Zhengjun Cao
caozhj@shu.edu.cn

[1] Department of Mathematics, Newtouch Center for Mathematics, Shanghai University, Shangda Road 99, Shanghai 200444, China

Published online: 09 November 2024