scientific reports

Check for updates

OPEN

Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme

Vincent Omollo Nyangaresi[1,2], Zaid Ameen Abduljabbar[3,4,5✉], Keyan Abdul-Aziz Mutlaq[6,7], Salim Sabah Bulbul[8], Junchao Ma[4✉], Abdulla J. Y. Aldarwish[3], Dhafer G. Honi[3,9], Mustafa A. Al Sibahee[10,11] & Husam A. Neamah[12]

Advancements in cloud computing, flying ad-hoc networks, wireless sensor networks, artificial intelligence, big data, 5th generation mobile network and internet of things have led to the development of smart cities. Owing to their massive interconnectedness, high volumes of data are collected and exchanged over the public internet. Therefore, the exchanged messages are susceptible to numerous security and privacy threats across these open public channels. Although many security techniques have been designed to address this issue, most of them are still vulnerable to attacks while some deploy computationally extensive cryptographic operations such as bilinear pairings and blockchain. In this paper, we leverage on biometrics, error correction codes and fuzzy commitment schemes to develop a secure and energy efficient authentication scheme for the smart cities. This is informed by the fact that biometric data is cumbersome to reproduce and hence attacks such as side-channeling are thwarted. We formally analyze the security of our protocol using the Burrows–Abadi–Needham logic logic, which shows that our scheme achieves strong mutual authentication among the communicating entities. The semantic analysis of our protocol shows that it mitigates attacks such as de-synchronization, eavesdropping, session hijacking, forgery and side-channeling. In addition, its formal security analysis demonstrates that it is secure under the Canetti and Krawczyk attack model. In terms of performance, our scheme is shown to reduce the computation overheads by 20.7% and hence is the most efficient among the state-of-the-art protocols.

Keywords Authentication, Biometrics, Fuzzy commitment, Security, Privacy, Efficiency, Hamming distance, Smart city

A smart city refers to a geographical area where technologies such as energy production, logistics and information communication technology are amalgamated to enhance environmental quality, intelligent development, citizen well-being, participation and inclusion. As explained in[1,2], smart cities utilize data-driven technologies to boost sustainability, efficiency, quality of life of the citizens and streamline city services. In addition, the usage of smart city data and technologies facilitate efficient and optimized management of resources, urban services and assets, as well as aiding in making informed decisions[3,4]. The advancements in big data, cloud computing,

[1]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya. [2]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamilnadu, India. [3]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq. [4]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China. [5]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China. [6]IT and Communications Center, University of Basrah, Basrah 61004, Iraq. [7]School of Computer Sciences, UniversitiSains Malaysia, USM, 11800 Gelugor, Penang, Malaysia. [8]Directorate General of Education Basra, Ministry of Education, Basra 61004, Iraq. [9]Department of IT, University of Debrecen, Debrecen 4002, Hungary. [10]National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen 518060, China. [11]Computer Technology Engineering Department, Iraq University College, Basrah 61004, Iraq. [12]Mechatronics Department, Faculty of Engineering, University of Debrecen, Ótemető U. 4-5, Debrecen 4028, Hungary. ✉email: zaid.ameen@uobasrah.edu.iq; majunchao@sztu.edu.cn