sustainability

MDPI

Article

Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture

Zaid Ameen Abduljabbar [1,2,3,*], Vincent Omollo Nyangaresi [4], Hend Muslim Jasim [1], Junchao Ma [5,*], Mohammed Abdulridha Hussain [1,2], Zaid Alaa Hussien [6] and Abdulla J. Y. Aldarwish [1]

1 Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
2 Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
3 Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China
4 Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya
5 College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
6 Information Technology Department, Management Technical College, Southern Technical University, Basrah 61005, Iraq
* Correspondence: zaid.ameen@uobasrah.edu.iq (Z.A.A.); majunchao@sztu.edu.cn (J.M.)

Abstract: Precision agriculture encompasses automation and application of a wide range of information technology devices to improve farm output. In this environment, smart devices collect and exchange a massive number of messages with other devices and servers over public channels. Consequently, smart farming is exposed to diverse attacks, which can have serious consequences since the sensed data are normally processed to help determine the agricultural field status and facilitate decision-making. Although a myriad of security schemes has been presented in the literature to curb these challenges, they either have poor performance or are susceptible to attacks. In this paper, an elliptic curve cryptography-based scheme is presented, which is shown to be formally secure under the Burrows–Abadi–Needham (BAN) logic. In addition, it is semantically demonstrated to offer user privacy, anonymity, unlinkability, untraceability, robust authentication, session key agreement, and key secrecy and does not require the deployment of verifier tables. In addition, it can withstand side-channeling, physical capture, eavesdropping, password guessing, spoofing, forgery, replay, session hijacking, impersonation, de-synchronization, man-in-the-middle, privileged insider, denial of service, stolen smart device, and known session-specific temporary information attacks. In terms of performance, the proposed protocol results in 14.67% and 18% reductions in computation and communication costs, respectively, and a 35.29% improvement in supported security features.

Keywords: Agriculture 4.0; precision agriculture; privacy; smart farming; security

Citation: Abduljabbar, Z.A.; Nyangaresi, V.O.; Jasim, H.M.; Ma, J.; Hussain, M.A.; Hussien, Z.A.; Aldarwish, A.J.Y. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. *Sustainability* **2023**, *15*, 10264. https://doi.org/10.3390/su151310264

Academic Editors: Mourade Azrour, Azidine Guezzaz, Imad Zeroual, Azeem Irshad, Jamal Mabrouki, Said Benkirane and Shehzad Ashraf Chaudhry

Received: 9 May 2023
Revised: 23 June 2023
Accepted: 26 June 2023
Published: 28 June 2023

1. Introduction

Many economies in developing countries are dependent on agriculture as a source of income and contributions to gross domestic product (GDP) [1]. However, the majority of the farming practices are based on experience and ad hoc insights of the farmers. Consequently, there is little control on the agricultural produce quantity and hence financial profits. Fortunately, precision agriculture (PA) and the Internet of Things (IoT) can be deployed to address these issues [2,3]. As explained in [4], PA is part of Agriculture 3.0 in which farm yields are regularly monitored. In addition, PA involves automation and the application of information technology (IT) to improve farm output. In Agriculture 4.0, also referred to as smart agriculture or smart farming, additional technologies such as drones, artificial intelligence (AI), blockchain, big data, wireless sensor networks (WSN), and robotics are incorporated in agriculture. In PA, a number of sensors are deployed, such as radiation, air humidity, optimal, soil moisture, and ground sensors. According to