Methods for Enhancing Security of Precision Agriculture

Subjects: Computer Science, Cybernetics

Contributor: Zaid Ameen Abduljabbar , Vincent Omollo Nyangaresi , Hend Muslim Jasim , Junchao Ma , Mohammed Abdulridha Hussain , Zaid Alaa Hussien , Abdulla J. Y. Aldarwish

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. Many schemes have been developed to enhance security in the smart farm environment.

precision agriculture security

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 [5], intelligent precision agriculture (IPA) encompasses the deployment of numerous IoT devices and drones to monitor agricultural surroundings. To boost productivity in the face of limited resources and protection from disasters, traditional agronomy needs to be replaced with smart agronomy [6]. As discussed in [7], there are fraud risks in the agricultural sector, especially concerning beverage and food packaging. Therefore, agricultural organizations require ideal certification of their products since these risks can impact negatively on the health of their consumers.

The smart devices deployed in PA and IPA exchange a massive number of messages. Therefore, insecure communication channels among IoT devices, unmanned aerial vehicles (UAVs), or drones can expose smart farming to diverse attacks [5][8]. For instance, Wi-Fi de-authentication and denial of dervice (DoS) can be launched on Raspberry Pi-based smart farms [9]. This can have serious consequences as the sensed data are normally

processed to help determine the agricultural field status and facilitate decision-making, which may involve taking measures to maintain or enhance the farm status [10]. These attacks can also target drones deployed to monitor field conditions such as irrigation, spraying of pesticides, pollination, and planting of seeds [11]. On their part, WSNs offer monitoring, sensing, and a continuous supply of information regarding climatic conditions such as the chemical content of the soil, air humidity, temperature, light, water quality, and soil moisture. These parameters are then utilized to boost productivity, both qualitatively and quantitatively. According to [12], WSNs facilitate monitoring, data collection, and control of agricultural systems and hence ensure efficiency, minimal packet losses and economic overheads, better network control, and increased scalability and flexibility. However, threats such as interference, masquerading, interception, and message alteration can compromise these networks and harm crop production and other monitored agricultural practices [6]. The authors in [13] pointed out that issues such as sufficient energy resource utilization and secure data transmission are yet to be solved in WSN. This is because of the usage of open wireless networks during data transfers [14], which can potentially compromise the integrity, confidentiality, and authenticity of the exchanged data.

2. Enhancing Security of Precision Agriculture

Many schemes have been developed to enhance security in the smart farm environment. For example, a novel private blockchain-based authentication scheme is presented in [5]. However, this protocol fails to protect against de-synchronization and session hijacking attacks. Similarly, blockchain-based schemes were developed in [15][16][17][18][19]. Although blockchain offers traceability, integrity protection, and shareability in the agricultural environment, such as agri-food supply chains, it has high storage and computation overheads [20]. Based on signatures, the authors of [21] present a three-factor user authentication protocol. Unfortunately, this scheme cannot prevent attacks such as eavesdropping and session hijacking. On the other hand, an identity-based scheme was introduced in [22]. Nevertheless, this technique is vulnerable to stolen smart cards, sensor node spoofing, impersonation, and stolen verifier attacks [23]. In addition, it cannot provide backward key secrecy. To address these challenges, two protocols were developed in [23]. Unfortunately, the authentication and password change phases of these schemes are inefficient [24]. To offer privacy protection, a remote user authentication protocol was presented in [6]. However, this scheme cannot withstand attacks such as eavesdropping, de-synchronization, and spoofing.

Based on a public-key-based cryptosystem, an authentication scheme was developed in [25]. Although this approach protects against MitM and replay attacks, it cannot withstand privileged insider, user impersonation, and ephemeral secret leakage (ESL) attacks [5]. In addition, it does not include biometric change and user device revocation phases. The signature-based privacy-preserving protocol in [26] can address some of these issues. However, it is still susceptible to ESL attacks and cannot assure the untraceability and anonymity of the communicating parties [5]. Similarly, the protocol in [27] does not provide user and device anonymity since their internet protocol (IP) addresses incorporated in messages are exchanged publicly. In addition, it has high computation overheads due to the utilization of public key cryptography for its digital signatures and certificates [28]. Moreover, it is prone to replay, physical device capture, MitM, user and device impersonation, and attacks. On its

part, the scheme in [29] cannot protect against user anonymity violation, user impersonation, and smart card loss attacks. Similarly, the protocol in [30] is vulnerable to physical sensing device capture, untraceability violation, and smart card loss attacks [5]. Using some bilinear pairing operations, authentication and key establishment protocols were introduced in [31][32]. However, the utilization of pairing operations increased the computation costs of these protocols [33]. Since the trusted authority in [32] has access to user identity and password, it is susceptible to privileged insider attacks. In addition, it cannot withstand replay, disclosure of sensor data, offline password guessing, and stolen smart card and verifier attacks [34]. As such, an improved elliptic curve cryptography (ECC)-based scheme was developed in [34]. However, this protocol has an inefficient and delayed authentication phase. In addition, it is not robust against DoS and replay attacks [35]. Although the protocol in [36] addresses some of these issues, its bilinear pairing operations result in high computation costs [37].

To offer security in a heterogeneous IoT environment, an authentication technique was presented in [38]. Unfortunately, this protocol is vulnerable to physical device capture, privileged insider, and ESL attacks. In addition, it cannot preserve untraceability and anonymity [5]. Similarly, a remote user authentication protocol was developed in [39], which was shown to be lightweight. However, it failed to protect against ESL and privileged insider attacks. It also failed to support untraceability and anonymity [5]. On its part, the scheme in [39] was not resilient against privileged insider and sensor node capture attacks. It also failed to preserve forward key secrecy [6]. The authors in [40][41] designed identity-based signature protocols to protect message exchanges in mobile devices. However, identity-based schemes have key escrow problems [42]. Based on ECC and symmetric key encryption, a security technique was presented in [43]. Although it was shown to be robust against MitM and replay attacks, it was vulnerable to ESL, privileged insider, and user impersonation attacks. It also failed to incorporate device revocation, node addition, and password and user biometric change phases [5]. Similarly, the biometric-based scheme in [44] did not include device revocation, user passwords, and biometric update phases. It was also vulnerable to privileged insider, user impersonation, ESL, DoS, and stolen smart card attacks [45]. On its part, the protocol in [46] was susceptible to DoS attacks and could not offer forward key secrecy [47]. Similarly, the scheme in [48] did not support forward key secrecy and was prone to stolen verifier attacks [49]. As such, an enhanced ECC-based protocol was introduced in [49], while a privacy-preserving scheme was developed in [50]. The scheme in [50] was demonstrated to be resilient against eavesdropping, DoS, masquerade, privileged insider, and forgery attacks. It also supports secret key updates, traceability, and anonymity. However, it cannot withstand MitM attacks [15].

References

1. Vangala, A.; Das, A.K.; Mitra, A.; Das, S.K.; Park, Y. Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks. IEEE Trans. Inf. Forensics Secur. 2022, 18, 904–919.
2. Shafi, U.; Mumtaz, R.; García-Nieto, J.; Hassan, S.A.; Zaidi, S.A.R.; Iqbal, N. Precision Agriculture Techniques and Practices: From Considerations to Applications. Sensors 2019, 19, 3796.

3. Shi, X.; An, X.; Zhao, Q.; Liu, H.; Xia, L.; Sun, X.; Guo, Y. State-of-the-Art Internet of Things in Protected Agriculture. Sensors 2019, 19, 1833.
4. Vangala, A.; Das, A.K.; Chamola, V.; Korotaev, V.; Rodrigues, J.J. Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges. Cluster Comput. 2022, 26, 879–902.
5. Bera, B.; Vangala, A.; Das, A.K.; Lorenz, P.; Khan, M.K. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. Comput. Stand. Interfaces 2022, 80, 103567.
6. Rangwani, D.; Sadhukhan, D.; Ray, S.; Khan, M.K.; Dasgupta, M. An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network. Trans. Emerg. Telecommun. Technol. 2021, 32, e4218.
7. Lan, G.; Brewster, C.; Spek, J.; Smeenk, A.; Top, J. Blockchain for Agriculture and Food; Findings from the Pilot Study, Report; Wageningen Economic Research: Wageningen, The Netherlands, 2017; p. 34.
8. Nyangaresi, V.O.; Ibrahim, A.; Abduljabbar, Z.A.; Hussain, M.A.; Al Sibahee, M.A.; Hussien, Z.A.; Ghrabat, M.J.J. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021; pp. 1–6.
9. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber attacks on smart farming infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020; pp. 135–143.
10. Khanna, A.; Kaur, S. Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Comput. Electron. Agric. 2019, 157, 218–231.
11. Van der Merwe, D.; Burchfield, D.R.; Witt, T.D.; Price, K.P.; Sharda, A. Drones in agriculture. Adv. Agron. 2020, 162, 1–30.
12. Dagar, R.; Som, S.; Khatri, S.K. Smart farming–IoT in agriculture. In Proceedings of the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018; pp. 1052–1056.
13. Sanjeevi, P.; Prasanna, S.; Kumar, B.S.; Gunasekaran, G.; Alagiri, I.; Anand, R.V. Precision agriculture and farming using Internet of Things based on wireless sensor network. Trans. Emerg. Telecommun. Technol. 2020, 31, e3978.
14. Nyangaresi, V.O.; Abduljabbar, Z.A.; Refish, S.H.A.; Al Sibahee, M.A.; Abood, E.W.; Lu, S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In Cognitive Radio Oriented Wireless Networks and Wireless Internet, Proceedings of the 16th EAI International Conference, CROWNCOM 2021, Virtual Event, 11 December 2021, and 14th EAI

International Conference, WiCON 2021, Virtual Event, 9 November 2021; Springer International Publishing: Cham, Switzerland, 2022; pp. 325–340.

15. Vangala, A.; Sutrala, A.K.; Das, A.K.; Jo, M. Smart Contract-Based Blockchain-Envisioned Authentication Scheme for Smart Farming. IEEE Internet Things J. 2021, 8, 10792–10806.
16. Akram, S.V.; Malik, P.K.; Singh, R.; Anita, G.; Tanwar, S. Adoption of blockchain technology in various realms: Opportunities and challenges. Secur. Priv. 2020, 3, e109.
17. Lin, Y.-P.; Petway, J.R.; Anthony, J.; Mukhtar, H.; Liao, S.-W.; Chou, C.-F.; Ho, Y.-F. Blockchain: The Evolutionary Next Step for ICT E-Agriculture. Environments 2017, 4, 50.
18. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In Proceedings of the 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.
19. Wang, L.; Xu, L.; Zheng, Z.; Liu, S.; Li, X.; Cao, L.; Li, J.; Sun, C. Smart Contract-Based Agricultural Food Supply Chain Traceability. IEEE Access 2021, 9, 9296–9307.
20. Al Sibahee, M.A.; Nyangaresi, V.O.; Ma, J.; Abduljabbar, Z.A. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In IoT as a Service, Proceedings of the 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, 13–14 December 2021; Springer International Publishing: Cham, Switzerland, 2022; pp. 3–18.
21. Vangala, A.; Das, A.K.; Lee, J. Provably secure signature-based anonymous user authentication protocol in an Internet of Things-enabled intelligent precision agricultural environment. Concurr. Comput. Prac. Exp. 2021, 35, e6187.
22. Turkanović, M.; Brumen, B.; Hölbl, M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Netw. 2014, 20, 96–112.
23. Chang, C.-C.; Le, H.-D. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. IEEE Trans. Wirel. Commun. 2015, 15, 357–366.
24. Das, A.K.; Kumari, S.; Odelu, V.; Li, X.; Wu, F.; Huang, X. Provably secure user authentication and key agreement scheme for wireless sensor networks. Secur. Commun. Netw. 2016, 9, 3670–3687.
25. Shuai, M.; Xiong, L.; Wang, C.; Yu, N. A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem. Comput. Commun. 2020, 160, 215–227.
26. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. J. Inf. Secur. Appl. 2019, 48, 102354.

27. Chae, C.-J.; Cho, H.-J. Enhanced secure device authentication algorithm in P2P-based smart farm system. Peer-to-Peer Netw. Appl. 2018, 11, 1230–1239.
28. Nyangaresi, V.O.; Abduljabbar, Z.A.; Mutlaq, K.A.-A.; Ma, J.; Honi, D.G.; Aldarwish, A.J.Y.; Abduljaleel, I.Q. Energy Efficient Dynamic Symmetric Key Based Protocol for Secure Traffic Exchanges in Smart Homes. Appl. Sci. 2022, 12, 12688.
29. Wu, F.; Xu, L.; Kumari, S.; Li, X. A new and secure authentication scheme for wireless sensor networks with formal proof. Peer-to-Peer Netw. Appl. 2015, 10, 16–30.
30. Srinivas, J.; Mukhopadhyay, S.; Mishra, D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Netw. 2017, 54, 147–169.
31. Zeng, X.; Xu, G.; Zheng, X.; Xiang, Y.; Zhou, W. E-AUA: An Efficient Anonymous User Authentication Protocol for Mobile IoT. IEEE Internet Things J. 2018, 6, 1506–1519.
32. Liu, C.-H.; Chung, Y.-F. Secure user authentication scheme for wireless healthcare sensor networks. Comput. Electr. Eng. 2017, 59, 250–261.
33. Nyangaresi, V.O.; Abduljabbar, Z.A.; Ma, J.; Al Sibahee, M.A. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Cappadocia, Turkey, 14–17 June 2022; pp. 569–574.
34. Challa, S.; Das, A.K.; Odelu, V.; Kumar, N.; Kumari, S.; Khan, M.K.; Vasilakos, A.V. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Comput. Electr. Eng. 2018, 69, 534–554.
35. Ali, Z.; Ghani, A.; Khan, I.; Chaudhry, S.A.; Islam, S.H.; Giri, D. A robust authentication and access control protocol for securing wireless healthcare sensor networks. J. Inf. Secur. Appl. 2020, 52, 102502.
36. Wu, H.-T.; Tsai, C.-W. An intelligent agriculture network security system based on private blockchains. J. Commun. Netw. 2019, 21, 503–508.
37. Abduljaleel, I.Q.; Abduljabbar, Z.A.; Al Sibahee, M.A.; Ghrabat, M.J.J.; Ma, J.; Nyangaresi, V.O. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. J. Sens. Actuator Netw. 2022, 11, 66.
38. Tai, W.-L.; Chang, Y.-F.; Li, W.-H. An IoT notion–based authentication and key agreement scheme ensuring user anonymity for heterogeneous ad hoc wireless sensor networks. J. Inf. Secur. Appl. 2017, 34, 133–141.
39. Ali, R.; Pal, A.K.; Kumari, S.; Karuppiah, M.; Conti, M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Futur. Gener. Comput. Syst. 2018, 84, 200–215.

40. He, D.; Zhang, Y.; Wang, D.; Choo, K.-K.R. Secure and Efficient Two-Party Signing Protocol for the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography. IEEE Trans. Dependable Secur. Comput. 2018, 17, 1124–1132.
41. Feng, Q.; He, D.; Liu, Z.; Wang, D.; Choo, K.K.R. Multi-party signing protocol for the identity-based signature scheme in IEEE P1363 standard. IET Inf. Secur. 2020, 1, 1–10.
42. Nyangaresi, V.O. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array 2022, 15, 100210.
43. Sadhukhan, D.; Ray, S.; Biswas, G.P.; Khan, M.K.; Dasgupta, M. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. J. Supercomput. 2020, 77, 1114–1151.
44. Dhillon, P.K.; Kalra, S. A lightweight biometrics based remote user authentication scheme for IoT services. J. Inf. Secur. Appl. 2017, 34, 255–270.
45. Chang, C.-C.; Nguyen, N.-T. An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation. Wirel. Pers. Commun. 2016, 90, 1695–1715.
46. Amin, R.; Islam, S.H.; Kumar, N.; Choo, K.-K.R. An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. J. Netw. Comput. Appl. 2018, 104, 133–144.
47. Li, X.; Niu, J.; Alam Bhuiyan, Z.; Wu, F.; Karuppiah, M.; Kumari, S. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. IEEE Trans. Ind. Inform. 2017, 14, 3599–3609.
48. Alotaibi, M. An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN. IEEE Access 2018, 6, 70072–70087.
49. Moghadam, M.F.; Nikooghadam, M.; Al Jabban, M.A.B.; Alishahi, M.; Mortazavi, L.; Mohajerzadeh, A. An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network. IEEE Access 2020, 8, 73182–73192.
50. Fadi, A.T.; Deebak, B.D. Seamless authentication: For IoT-big data technologies in smart industrial application systems. IEEE Trans. Ind. Inform. 2020, 17, 2919–2927.