Nat. Volatiles & Essent. Oils, 2021; 8(5): 3446 - 3457

NVEO
Natural Volatiles & Essential Oils

Iot Based Authentication And Key Establishment Protocol For Modern Agriculture

[1]Venkatasamy Sureshkumar, [2]S. Mugunthan, [3]V. Senthil kumaran
[1,2,3,] Departement of Applied Mathematics and Computational Sciences
PSG College of Technology, Coimbatore

Abstract
Agriculture has been the source of raw food material and a major source of economic activity in many countries. The increase in demand for food necessitates innovative ideas to be infused into the traditional agricultural practices. Agriculture productivity can be vastly improved by the use of latest technologies such as Wireless Sensor Networks which have variety of application in agriculture field such as agriculture monitoring and control, food supply chain tracking etc., The increase in deployment of sensors results in increase in communication between the various entities in the environment and it becomes important to secure the data being communicated. Authentication protocol is one of the security mechanism to protect the communications. Moreover, the constrains in wireless sensors such as limited computation capacity and limited power source makes it essential to design authentication protocols that are both secure as well as lightweight. In this paper we have proposed an authentication scheme based on Elliptic Curve Cryptography. We also presented a comparative analysis of security features as well as performance metrics.

Keywords: Smart agriculture, Mutual authentication, WSN, Smart card, ECC.

1 Introduction

Since the early ages of the human existence, agriculture of some sort, has always been an essential part of a man's survival for it also serves him with a basic need for his thriving, food [14]. From the nomadic slash and burn agriculture or even the age-old unknown, un-named forms of cultivation, to today's tech driven smart agriculture, agriculture has evolved over the years and has been refined in accordance with human needs and human evolution [14]. The inefficiency, tiring nature, humungous labour requirement, vulnerability of crops to factors such as pests and diseases and other drawbacks of agriculture since its discovery, and the advancement of human lives and human brains that brought into existence a variety of methods to help the betterment of human lives such as the machines at present that more or less does everything as a man's substitute, has resulted in the evolution of the methods of agriculture since the inception [17].

With the growing technology, things that never could have been put into thoughts earlier, are being accomplished on a daily basis. Like-wise, agriculture without human labour required to work in fields, which probably would have been just a myth, or maybe would not have been even thought of being made possible back in the 10th or 11th century, can actually be made possible today with the new inventions and ideas that are well developed and being worked on to produce never-before-seen marvels. The usage

of IoT devices in agriculture is one way that man has made possible, to minimize human intervention into farms and fields [5].

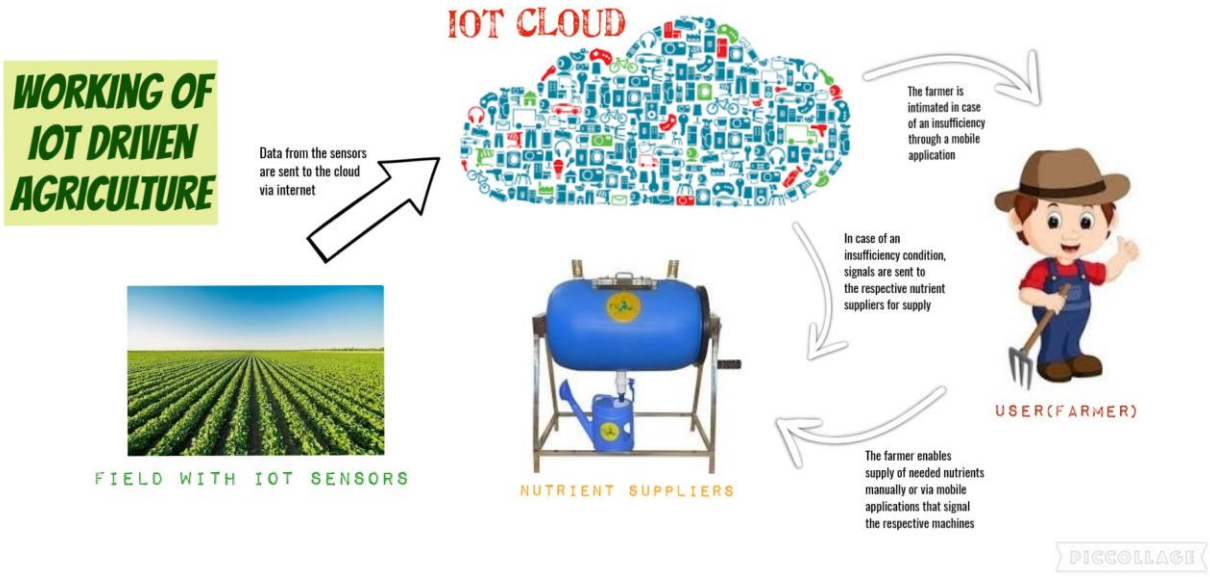

Figure 1: IoT enabled agriculture firm

Internet of Things (IoT), as described by Kevin Ashton, the person who coined the term IoT, is a standardised way for computers to understand the real world. It refers to fixed or mobile intelligent devices that can, without human intervention, communicate with each other and exchange data automatically. Devices involved in this concept turn intelligent, by obtaining unique addresses on the internet using sensors and actuators thus enabling every person to control the control the technology that is already in use, in a novel way. IoT is an implementation of hardware and software systems combined. Since its conception, it has been used extensively in various fields. Its working, simply put, is based on signals sent by various sensors. These signals are data to be analysed and they are stored in the database using the Internet as a medium. This database is monitored and any disharmony in the flow is directly intimated to the user or the manager who requests the data, through the respectively mobile application that is priorly synced with the sensors via the internet. This way tracking of any malfunction or erroneous action is immediately known and rectified [24].

1.1 Proposed architecture

Using this concept in agriculture would multiply the efficiency of agriculture manifolds and thus would result in easier production, less tedious processes in the course of production and very less, or almost no requirement of human labour. This is the exact technology needed for the agriculture sector. Various sensors are placed in the soil. These would monitor various aspects such as water availability, fertilizer levels, nutrient levels, etc.. This information is stored in the database and monitored so that whenever

there is any shortage of any of the nutrients, or an alarming situation in terms of the same, the farmer would be notified immediately via the corresponding mobile application installed. This way, the farmer just needs to play with switches, turning on and off the nutrient supplies to the plants. The overall architecture of this idea is depicted in Figure. 1.

Protruding a little more with the usage of IoT, the ups and downs, i.e. the insufficiencies and the surpluses, in the flow sensed by the sensors can be programmed to directly send signals to the respective supply machines, to minimise human intervention a little more, to manipulate the machines accordingly to increase or decrease their supply. For instance, in case of inadequate water level in a sector of the field, the sensor in the particular area signals for the water supplier to water the sector. This can be done also using the concept of trees in data structures, considering each of the sensors to be a node, the pipe to be branches, thus the sensors signalling the supplier to supply the nutrient to the particular sector by marking the path that the nutrient has to flow.

Talking about IoT sensors, they are of three major types, namely – Asynchronous, Synchronous, and Intelligent sensors. Asynchronous sensors are low powered sensors, often placed in remote places, that become active only on request for data. Synchronous sensors are permanently active one-way sensors that require a specific bandwidth for transmission. They also need suitable communication channel for data security. Intelligent sensors, are also permanently active sensors, but unlike the synchronous sensors, these are bidirectional sensors. These sensors are said to be intelligent as they modify the generated data, measured data, and security coding by themselves unlike the other sensors that require the user to do them. These sensors also perform software updates when needed automatically, but these intelligent sensors are too complex in nature and thus are mostly preferred in future IoT applications.

Considering the IoT system hardware, it generally consists of three layers, namely, device layer, gateway layer and data processing layer. In case of five layered IoT systems, 3 layers are dedicated to data processing. The device layer and the gateway layer alone though, are sufficient for necessary hardware implementations. The device layer constitutes the collection of sensors connected to a common device for easier transmission to a gateway that it belongs to. This communication ranges between 100 metres and 100 kilometres depending on the protocol.

Data procession in the IoT architecture can be achieved through any of the four methods named - On-premise IoT platform method, IoT platform in the cloud method, Edge computing, or Fog computing.

Thus, using this system for agriculture would ensure a definite minimisation in the loss of crops due to nutrient insufficiency, or disease (which is manually next to impossible), by detection via the IoT sensors. This implementation also doesn't require huge amount of human labour, thus decreasing the total investment in cultivation in a long run.

Pest management is the important part in agriculture. The occurrence of pest is inevitable in cultivation of crops. The study conducted by NCBI (National Centre for Biotechnology Information) revealed that 26 % of primary yield loss and 38 % secondary loss is due to pests. Proper identification and controlling the pest involves lot of risk. On other hand use of large quantities of pesticides for managing the pest lead to resurgence of pest and also lead to pesticides residue in harvestable products that ultimately affect human health. There is no science to avoid occurrence or eliminate the pest, the only way is the proper management of pest. The management of pest involves identifying the optimum condition for the pest outbreak each pest need certain particular condition for growth and reproduction. Pests like cotton mealy

bug infestation will be more when the temperature is 33+2◦C and pest like Rice whorl maggot infestation will be more when RH is more than 90 %, so identifying these condition and taking precautionary measures can help to control the occurrence of pest and we can reduce the yield loss. All these can't be possible by human but human invention like IoT can do. IoT are nothing but Internet of Things consists of sensors that are sensitive to change in environment conditions. These sensors accurately sense the environmental conditions favour the occurrence of pest and predict in advance which will help the farmers to take precautionary measures at best time. Nowadays IoT are gaining popularity among all levels of farmers due to its accuracy and timely information. New Era of Climate smart Agriculture highly depend on these Iot and sensors.

1.2 Major Contribution

This paper deals with how IoT work in identifying the optimum condition for pest occurrence and how it convey the information to farmers in simple way. The wireless communication is prone to many of the security attacks, to prevent such attacks a robust security scheme is needed. In this work, we propose a novel secure communication protocol with key establishment technique.

2 Related work

Open Platform Communications Unified Architecture can be used for yield monitoring system in combined harvestor [18]. This OPC UA is considered to be a potential technology for safe and secure communication. The Parameters of Combined harvestor can be accessed remotely using this technology.

A modern technology, a Private Blockchain-based secure Access Control (PBAC) for agriculture can be used to monitor the environmental parameters. Different sensors can be deployed to collect information on various weather parameters. This information can be sent to public channel (Farmers or officers) to take appropriate measures. This new private block chain can store access records and protects the smart agricultural system from variety of attacks [3].

According to the study [23] the real time monitoring, intelligent decision making is possible using Wireless Sensor Networks (WSNs). Time correlated measurements is possible by deploying sink node's clock as reference. WSN NODE can be designed by integrating the Arduino prototyping board and XBee transceivers with sensory devices.

An original decentralized system called bubbles of trust is designed to ensure robust identification and authentication of devices. It also protects the data integrity and availability. In bubbles of trust secure virtual zones are created, where devices communicate in a completely secure way [12]. It also meets the requested security requirements as well as its resiliency towards attacks.

Climate parameters such as temperature, humidity, light, carbon dioxide, soil moisture are required for growth, quality and productivity of crops [2]. By monitoring these parameters using Wireless Sensor Networks (WSNs) can help to increase the productivity of crops. The study [2] addresses on the problem of authenticity to keep away from unauthorized access in WSNs environment. This shows that it is possible to avoid passing of wrong command from the sensor by ensuring the legality before transmitting the actual data. IoT communication take place over internet it is vulnerable to various security threats. The study [8] deals with various security requirements and also presented the security protocols needed for

IoT. A taxonomy of multiple security protocols needed for IoT environment. Various techniques such as pre-distribution, user authentication, device authentication, user access control, privacy-preservation and identity management techniques are developed to ensure security to IoT services. The authors [10] surveyed state of the art of existing security and privacy solutions for green IoT based agriculture architecture. Green IoT based agriculture deals with Facility agriculture which is an industrialized agricultural production mode common in developed countries. It is four-tier system consists of Sensors layer, Fog layer, Core layer, Cloud layer. The study also suggests various attacks for IoT and developing of security protocols to ensure secure way of sharing information.

Services like object tracking, marking ownership, noting boundaries and indicating identities can be done by using Passive IoT like radio frequency tags. Authors [1] denoted that communication between reader and participating tags is vulnerable to attacks. They introduced novel dynamic authentication protocol for passive IoT systems. The proposed system saves storage resources and it is found to be more efficient than other protocols.

A system based on LoRaWAN network for long range and lower power consumption data transmission from the sensor nodes to the cloud services is developed by [9]. LoRaWAN was specially designed for IoT applications for connecting sensors, modules and applications over a large network. The system is flexible and extensible that can be integrated with other IoT platforms. With the help of drones and known weather information, the crop selection can be made. Artificial intelligence for sowing, irrigation is used in [21]. If there is any change in weather, alteration can be made in cultural operations taken by the system. But maintaining big data consisting of weather, soil information pose as great challenge.

Ali et al.'s [2] scheme cannot provide user anonymity, user traceability, session key security and is insecure against insider attacks and sensor node impersonation attacks. But the [6] proposed a system that eliminates those security weakness by four new phases of six existing phases and it is 80 times more efficient when compare with Ali et al.'s. This system is most suitable for agricultural purposes using WSNs. An energy and secure IoT based WSN framework is deployed by [13] for smart agriculture application. The proposed framework is to appoint the more suitable cluster heads based on multiple-criteria decision function. It also uses a mechanism that is based on the SNR factor to determine the strength of signal and to provide more stable network.

IoT play important role and it is successful in protected agriculture. The study [20] deals with state-of-art of IoT applications in protected agriculture and to identify the system structure and key technologies. WSN can be divided into terrestrial WSN and Wireless Underground Sensor Networks. In order to tackle the complex and changing agricultural environment the devices should be upgraded and also protected from other networks. According to the study [4] 20-40 % of yield loss is due to Pest and Diseases, for controlling them pesticides act as key but on other hand increase in usage of pesticides lead to lot of problems to both human and environment. Recent advances in Science such as wireless sensors, drones, Robots help the farmers to minimize pesticide usage and also provide real time monitoring, modeling and forecasting the occurrence of pest effectively. Integrated pest Management will be successful if we understand the observable changes in weather and Insect Ontology. This will act as basics for developing

a effective IoT. By integrating the observed weather changes and generated Ontologies, the pest occurrence can be predicted and managed in advance [7]. Sucking pests like white flies and fruit flies are detected using IoT based remote green house monitoring systems using wireless imaging and sensor nodes (WiSN). This system continuously monitor the number of pest fall on the yellow sticky traps and also environmental parameters simultaneously. If there is any significant change noticed in Temperature, Humidity and light intensity, there is abrupt increase in pest count. By understanding this relationship the system can able to provide possible information on infestation of pests on crops. Scientists suggested that this study [19] can be used as reference for future applications of early pest prediction in green house as well as open field conditions.

An automated detection system proposed by the scientists help to classify the type of pest and detect the occurrence of pest. Raspberry Pi and IR sensors are used for identification of pest and to count the number of pest respectively. Ultrasonic sensors are used for detecting the growth parameters of crops. The information collected from the sensors are processed and sent to mobiles so that the farmers can know the early occurrence of pest by this way they can minimize the use of pesticides for managing the pests, The changes in foliage of crops due to nutrient deficiency, water stress and pests can be detected using canopy reflectance (near infrared region). This helps the farmers to predict the systems even though it is invisible to human eye. In the study [11] scientists proposed pest monitoring system for sugarcane. The system uses acoustic sensors which will send the acoustic waves to detect the noise level of pest. Sound produced by the small level population of pest will affect the amplitude of the travelling acoustic waves. If it is above the threshold level it will alarm the farmers for taking precaution measures.
Most of pest occurrence depends mainly on temperature, increase or decrease of temperature from optimum level will lead to outbreak of pest. This study uses Thermistor as temperature sensor, the sensed data from the sensor is sent to arduino board which will give information about the occurrence of type of pest. Depending on type of pest the Ultrasonic sensor will generate the required amount of frequency to kill such pest.
In this scenario, the wireless communication is prone to many of the security attacks, to prevent such attacks a robust security scheme is needed. In this work, we propose a novel secure communication protocol with key establishment technique.

3 Proposed protocol

The scheme consists of setup, registration, login and mutual authentication phases with key generation feature.

3.1 Initial setup

System Administrator (SA) selects a large prime p and constructs a well defined Elliptic Curve Cryptosystem $E: y^2 = x^3 + ax + b \ (modp)$ over the finite field F_p such that $4a^3 + 27b^2 \neq 0$. SA identifies a cyclic group G of points from ECC with generator Q. Finally SA constructs a cryptographic one-way hash function $h: (0,1)^* \longrightarrow F_p$.

3.2 Gateway deployment and user registration

The gateway is deployed in the suitable place by the system administrator with its identity GW_j and

its permanent secret value g_j of size 32 bits and 160 bits respectively. In addition the gateway is equipped with its public key $C_j = g_j \cdot Q$.

The user U_k selects his/her identity UID_k, the password UPW_k and compute the bio-hashvalue $b_k = H(B_k)$, where B_k is the user bio-metric and H is a bio hash function. The user submits $\langle UID_k, UPW_k, b_k \rangle$ to the system admin through a secure channel.

Now SA computes $a_k = h(UID_k||UPW_k)$, $f_k = h(UID_k||b_k)$, $d_k = h(a_k||b_k)$, selects a random secret g_{jk} of GW_j corresponding to U_k, and computes $e_{kj} = g_{jk} \oplus a_k$. SA constructs the user smartcard $SC = \langle C_j, e_{kj}, GW_j, d_k, G(ECC), h(\cdot) \rangle$ and send it to the user through the same secure channel. At the same time, SA stores the secret value g_{jk} in the memory of GW_j corresponding to f_k.

3.3 sensor node registration

Each sensor node registers with the concern gateway node GW_j. During the registration, the node GW_j assigns an identity Sn_i, computes $R_{ij} = h(Sn_i||g_j)$ and stores $\langle Sn_i, R_{ij}, GW_j, Q \rangle$ into the memory of the sensor node.

3.4 Login and mutual authentication

When the legal user wants to login to the system, U_k inputs the user identity UID_k, the password UPW_k and bio-metric B_k. The smartcard SC computes

$$b_k = H(B_k)$$
$$a_k = h(UID_k||UPW_k)$$
$$d_k^* = h(a_k||b_k)$$

extracts d_k from the SC and checks whether the computed d_k^* is equal to the stored value d_k. Further, the SC generates the random number r_U, computes

$$L_1 = r_U Q$$
$$L_2 = r_u \cdot C_j$$
$$l_2 = h(L_2)$$
$$f_k = h(UID_k||b_k)$$
$$v_k = f_k \oplus l_2$$
$$g_{jk} = e_{kj} \oplus a_k$$
$$s = h(L_1||g_{jK})$$
$$V_1 = h(v_k||s||l_2||T_1)$$

Now SC constructs the message $M_1 = \langle L_1, v_k, V_1, Sn_i, T_1 \rangle$, where T_1 is the current timestamp at U_k and sends the message M_1 to the gateway GW_j.

Upon the receipt of the message M_1, the node GW_j verifies whether $T_2 - T_1 \leq \Delta T$, where T_2 is the timestamp at GW_j node and ΔT is the acceptable time delay. The gateway node further computes

$$L_2^* = g_j \cdot L_1$$
$$l_2^* = h(L_2^*)$$
$$f_k^* = v_k \oplus l_2^*$$

The gateway node searches for f_k in its memory, if not found aborts the connection. If found then extracts g_{jk} corresponding to f_k, computes $s^* = h(L_1||g_{jK})$, $V_1^* = h(v_k||s^*||l_2^*||T_1)$ and checks whether $V_1^* = V_1$. If it not holds, aborts the session otherwise the user U_k is authenticated and further

the node GW_j generates the random number r_G and compute the following:

$$L_3 = r_G \cdot L_1$$
$$R_{ij} = h(Sn_i||g_j)$$
$$V_2 = h(R_{ij}||Sn_i||T_2)$$
$$TC = l_2 \oplus R_{ij}$$

Finally, the node GW_j constructs the message $M_2 = \langle L_1, L_3, V_2, TC, T_2 \rangle$ and sends to the sensor node Sn_i.

After receiving the message M_2 from GW_j, The sensor node checks the time delay $T_3 - T_2 \leq \Delta T$. Further Sn_i computes $V_2^* = h(R_{ij}||Sn_i||T_2)$ and verifies whether $V_2 \stackrel{?}{=} V_2^*$. If it not holds aborts the session, otherwise generates the random number r_S and computes the following:

$$L_4 = r_S \cdot L_3$$
$$L_5 = r_S \cdot L_1$$
$$L_6 = r_S \cdot Q$$
$$l_2^* = TC \oplus R_{ij}$$
$$SK = h(L_4||l_2^*||GW_j)$$
$$V_3 = h(T_3||SK||R_{ij})$$

Finally the node Sn_i constructs the message $M_3 = \langle L_5, L_6, V_3, T_3 \rangle$ and send to the gateway node GW_j.

After receiving the message M_3 from the sensor node, GW_j checks the time delay $T_4 - T_3 \leq \Delta T$ and computes

$$L_7 = r_G \cdot L_5$$
$$SK = h(L_7||l_2^*||GW_j)$$
$$V_3^* = h(SK||R_{ij}||T_3)$$

GW_j checks $V_3^* \stackrel{?}{=} V_3$, if not holds reconstruct the message M_2 and resends to Sn_i otherwise GW_j authenticates the node Sn_i and computes

$$L_8 = r_G \cdot L_6$$
$$V_4 = h(SK||l_2||T_4)$$

GW_j constructs the message $M_4 = \langle L_1, L_8, V_4, T_4 \rangle$ and sends to the user U_k.

Upon the receipt of M_4, U_k checks the time delay $T_5 - T_4 \leq \Delta T$ and computes

$$L_9 = r_U \cdot L_8$$
$$Sk = h(L_9||l_2||GW_j)$$
$$V_4^* = h(Sk||l_2||T_4)$$

The user verifies $V_4^* \stackrel{?}{=} V_4$, if not holds reconstruct M_1 and resend to GW_j, otherwise accepts SK

4 Comparative analysis

The comparative study of the proposed scheme with the others is a suitable measure to evaluate the ability of the scheme for its practical use. The detailed study is as follows.

4.1 Computational cost comparison

Table 1. Computational cost comparison

Protocol	User / SC	BS	GWN	SN	Total (in ms)
Vaidya et al. [22]	$7T_h$	–	$6T_h$	$2T_h$	≈ 0.07761
Kumari et al. [15]	$8T_h$	–	$8T_h$	$5T_h$	≈ 0.108654
Ali et al. [2]	$1T_{fe} + 9T_h + 2T_{sym}$	$4T_h + 2T_{sym}$	$7T_h + 3T_{sym}$	$4T_h + 3T_{sym}$	≈ 0.72362
Li et al. [16]	$1T_{fe} + 9T_h + 2T_{sm}$	–	$8T_h + 1T_{sm}$	$1T_{sm}5T_h$	≈ 2.246534
Proposed	$1T_{fe} + 9T_h + 2T_{sm}$	–	$8T_h + 4T_{sm}$	$3T_h + 3T_{sm}$	≈ 4.37924

T_a : ECC point addition, T_e : exponentiation, T_{fe} : biometric fuzzy extractor computation time, T_h : hash function execution time, T_{MAC} - Message Authentication Code / HMAC, T_{sm} : ECC scalar multiplication, T_p:bilinear pairing, T_{PUF} : Physical Unclonable Function, T_{sym} : - symmetric encryption/decryption

Computation cost is the time taken by the machine to perform a single round of a cryptographic operation. Computational cost of the compared protocols is given in the table. Among the protocols, Vaidya et al. [22] has the lowest computational cost owing to the fact that the scheme uses only hash function. A considerable number of computations is reduced in the protocols Vaidya et al. [22] and Kumari et al. [15] since the protocols do not employ smart card. It is seen that only the protocol Ali et al. [2] route its messages through a base station. Li et al [16] which used Elliptic Curve Cryptography has the second highest computational cost. The proposed protocol is on the higher side due to the use of elliptic curve cryptography which provides strong security. The total computational cost for various schemes are shown in Table 1.

4.2 Communication cost comparison

Communication cost is the number of bits sent over the network during a single round of authentication. Among the protocols, Ali et al. [2] has the highest communication cost which is due to the fact that among the compared protocol, this scheme sends the highest number of hash values over the network and also employed the use of base station.The proposed protocol performs well compared to Ali et al. [2] and Li et al. [16] Also, the proposed protocol has marginally high communication cost compared to Vaidya et al. and Kumari et al. This marginal increase is justified the fact that our protocol support biometric authentication whereas the other two do not. Table 2. Shows computational cost for various schemes.

Table 2. Computational cost comparison

Protocol	No. of messages	No. of bits
Vaidya et al. [22]	4	5248
Kumari et al. [15]	4	5344
Ali et al. [2]	5	6464
Li et al. [16]	4	5888
Proposed	4	5472

4.3 Comparison of security features and threats

Table 3. Security functionality and attacks

Protocol	ASR_1	ASR_2	ASR_3	ASR_4	ASR_5	ASR_6	ASR_7
Vaidya et al. [22]	×	✓	×	✓	×	×	✓
Kumari et al. [15]	×	✓	×	✓	✓	✓	×
Ali et al. [2]	✓	✓	✓	×	×	✓	×
Li et al [16]	✓	×	×	✓	✓	✓	✓
Our	✓	✓	✓	✓	✓	✓	✓

ASR_1 : Resists the offline password guessing, ASR_2 : Withstands replay attack, ASR_3 : Supports three party authentication, ASR_4 : Withstands traceability attack, ASR_5 : Supports perfect forward secrecy, ASR_6 : Prevents insider attack, ASR_7 : Sustains user anonymity, ✓: Yes, ×: No.

Comparision of security protocols is presented in the Table 3. Vaidya et al. [22] fails to provide protection against offline password guessing attack and insider attack. Also, the scheme do not provide three factor authentication while also failed to provide perfect forward secrecy. Among the protocols compared, it is only the protocol by Ali et al. [2] that does not resist traceability attack. The scheme also fails to provide perfect forward secrecy and fails to sustain user anonymity. The scheme by Li et al. [16] fails to withstand replay attack while also does not support three-factor authentication. Our protocol fulfils all the security requirements and also provides additional security features such as three factor authentication.

5 Conclusion

Agriculture has been the backbone of many developing nations. Labour intensive fields such as

agriculture can make use of modern technology to increase productivity resulting in output with increased quantity and quality. In this article, a novel authentication protocol using Elliptic Curve Cryptosystem is proposed for the smart agriculture environment. Also, the propsed scheme is compared with other protocols in terms of security features and performance metrics. It is found that our protocol provides the security mechanisms and additional security features.

References

1. Afifi, M.H., Zhou, L., Chakrabartty, S., Ren, J.: Dynamic authentication protocol using self-powered timers for passive internet of things. IEEE Internet of Things Journal 5(4), 2927–2935 (2017)
2. 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. Future Generation Computer Systems 84, 200–215 (2018)
3. Arshad, J., Siddique, M.A.B., Zulfiqar, Z., Khokhar, A., Salim, S., Younas, T., Rehman, A.U., Asad, A.: A novel remote user authentication scheme by using private blockchainbased secure access control for agriculture monitoring. In: 2020 International Conference on Engineering and Emerging Technologies (ICEET), pp. 1–9. IEEE (2020)
4. Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., Aggoune, E.H.M.: Internet-ofthings (iot)-based smart agriculture: Toward making the fields talk. IEEE Access 7, 129551–129583 (2019)
5. Brust, G.E., Gotoh, T.: Mites: Biology, ecology, and management. In: Sustainable Management of Arthropod Pests of Tomato, pp. 111–130. Elsevier (2018)
6. Chen, M., Lee, T.F., Pan, J.I.: An enhanced lightweight dynamic pseudonym identity based authentication and key agreement scheme using wireless sensor networks for agriculture monitoring. Sensors 19(5), 1146 (2019)
7. Chougule, A., Jha, V.K., Mukhopadhyay, D.: Using iot for integrated pest management. In: 2016 International Conference on Internet of Things and Applications (IOTA), pp. 17–22. IEEE (2016)
8. Das, A.K., Zeadally, S., He, D.: Taxonomy and analysis of security protocols for internet of things. Future Generation Computer Systems 89, 110–125 (2018)
9. Davcev, D., Mitreski, K., Trajkovic, S., Nikolovski, V., Koteli, N.: Iot agriculture system based on lorawan. In: 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), pp. 1–4. IEEE (2018)
10. Ferrag, M.A., Shu, L., Yang, X., Derhab, A., Maglaras, L.: Security and privacy for green iot-based agriculture: Review, blockchain solutions, and challenges. IEEE Access 8, 32031–32053 (2020)
11. Gavaskar, S., Sumithra, A.: Design and development of pest monitoring system for implementing precision agriculture using iot. IJSTE-International Journal of Science Technology & Engineering 3(09) (2017)
12. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of trust: A decentralized blockchain-based authentication system for iot. Computers & Security 78, 126–142 (2018)
13. Haseeb, K., Ud Din, I., Almogren, A., Islam, N.: An energy efficient and secure iot-based wsn framework: An application to smart agriculture. Sensors 20(7), 2081 (2020)

14. Jing, Y., Yuzhi, Z., Dan, D., Xiao, W., Ping, Y., Lingfang, C., Yuefang, S., Zetao, L.: An early warning system of diseases and pests for blueberry based on wsn. In: 2017 36th Chinese Control Conference (CCC), pp. 8885–8889. IEEE (2017)
15. Kumari, S., Om, H.: Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Computer Networks 104, 137–154 (2016)
16. Li, X., Niu, J., Bhuiyan, M.Z.A.,Wu, F., Karuppiah, M., Kumari, S.: A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things. IEEE Transactions on Industrial Informatics 14(8), 3599–3609 (2017)
17. Meissner, H., Fritz, J., Kohl, L., Moylett, H., Moan, M., Emerine, S., Kaye, A.: Pestlens: an early-warning system supporting us safeguarding against exotic plant pests. EPPO Bulletin 45(2), 304–310 (2015)
18. Oksanen, T., Linkolehto, R., Seilonen, I.: Adapting an industrial automation protocol to remote monitoring of mobile agricultural machinery: a combine harvester with iot. IFAC-PapersOnLine 49(16), 127–131 (2016)
19. Rustia, D.J.A., Lin, T.T.: An iot-based wireless imaging and sensor node system for remote greenhouse pest monitoring. Chemical Engineering Transactions 58, 601–606 (2017)
20. 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 19(8), 1833 (2019)
21. Srilakshmi, A., Rakkini, J., Sekar, K., Manikandan, R.: A comparative study on internet of things (iot) and its applications in smart agriculture. Pharmacognosy Journal 10(2) (2018)
22. Vaidya, B., Makrakis, D., Mouftah, H.: Two-factor mutual authentication with key agreement in wireless sensor networks. Security and Communication Networks 9(2), 171–183 (2016)
23. Zervopoulos, A., Tsipis, A., Alvanou, A.G., Bezas, K., Papamichail, A., Vergis, S., Stylidou, A., Tsoumanis, G., Komianos, V., Koufoudakis, G., et al.: Wireless sensor network synchronization for precision agriculture applications. Agriculture 10(3), 89 (2020)
24. Zhuhua, H., Yaochi, Z.: Construction and application of intelligent video monitoring system for agricultural diseases and insect pests. Journal of Chinese Agricultural Mechanization (3), 42 (2016)