**Blockchain Assisted Secure Authentication Protocol for Aerial Surveillance in IoT based Smart Agriculture**

|  |  |  |
| --- | --- | --- |
| Tamizharasi GS,  Assistant Professor,  School of Engineering & Technology,  CMR University,  Bangalore-562149,  gst30091993@gmail.com | Dr. Rubini P,  Professor,  School of Engineering & Technology,  CMR University,  Bangalore-562149,  Rubini.p@cmr.edu.in | Dr. K.C. Sriharipriya,  Associate Professor,  School of Electronics Engineering,  Vellore Institute of Technology,  Vellore,  sriharipriya.kc@vit.ac.in |
| Dr. Achyut Shankar,  Department of Cyber Systems Engineering,  WMG,  University of Warwick, Coventry,  United Kingdom, CV74AL, ashankar2711@gmail.com | Bharat Bhushan,  Department of Computer Science and Engineering,  School of Engineering and Technology, Sharda University, India. | Abhay Bansal,  Bennett University,  Greater Noida,  India, abhay.bansal@bennett.edu.in |

**Abstract:**

Data acquisition, modelling and management are the three vital components of smart agriculture. Drones play a major role in this regard by capturing the detailed data using high-resolution cameras and advanced sensors. It acts as a key element driving enhancement to crop productivity, agricultural precision and many more. The data collected from the drones are at higher risk of security concerns as the process of data collection in smart agriculture involves collaboration among several entities. There is a possibility that the intruders can intentionally get in to the system and grab the data for wrong reasons. This emphasis the greater requirement for advancing the security features associated with aerial surveillance in smart agriculture. This paper presents a blockchain assisted secure two factor mutual authentication scheme for aerial surveillance security. The major contributions of this paper involve twofold: first a blockchain based secure authentication framework is provided; second, an efficient and lightweight two factor mutual authentication scheme for aerial surveillance in smart agriculture is provided. The proposed protocol is evaluated using the simulation tool called AVISPA and it is assessed for both security and performance related features. The security analysis of the proposed protocol states that this approach remains more resistant to most challenging security threats that occurs across IoT based smart agricultural systems. This protocol is also providing reduced computational cost and complexity measures in comparison the conventional approaches. A detailed comparative analysis shows that this approach provides the better results with the total computational complexity of 1.11ms.

**Keywords:** Unmanned Aerial Vehicles, smart agriculture, IoT devices, Aerial surveillance security, PUF, and Blockchain.

1. **Introduction:**

Agriculture in modern times is under technological revolution, where human involvements in farming are slowly replaced with unmanned aerial vehicles. Currently there was a great decline in soil biodiversity and productivity [1]. This is due to the reason that the resources are getting scarce and the issue of food shortage is increasing globally. Thus, now its time to provide agriculture a new look with advanced tools and technologies. Traditional method of agriculture involves greater amount of human involvement with huge efforts. This may sometimes affect the productivity of the crops. This is where exactly the role of smart agriculture comes in gaining a huge attention in recent times [2].

The term ‘smart agriculture’ refers to the application of smart technologies to enhance the crop productivity in both quantitively and qualitative aspects [3]. The prime objective of the smart agriculture is to reduce the cost and risk factors associated with growing of crops. It makes use of the most advanced technologies such as sensors, satellites, and drones to perform various activities such as soil management, light and heat control, mechanized irrigation and many more. Drones when equipped with high resolution camera captures the detailed images of the crop and assist in earlier prediction of diseases, pest infestations and nutrient deficiencies. They also assist in livestock management by effectively monitoring and manging the animal herds. It helps to track the health and location of the livestock in a more effective and simpler way [4,5,6].

In smart agriculture, it is mandate to monitor the entire process of various farming activities right from growing to harvesting of crops [7]. In order to carry out these activities effectively there involves variety of IoT devices and sensors that are connected to each other and controlled or monitored by the drones to ensure fresh and healthy productivity of crops [8.9.10]. The visualized data will be transferred between the devices for more precise management. The data collected by the drones as a result of monitoring form an important source for decision making. The data collected by the drones are then transferred to the cloud storage through satellite communication systems and internet. An overview of data collection in smart agriculture is illustrated in figure 1. Then over the cloud environment advanced analytics techniques will be applied over the datasets to predict the patterns, potential risks and trends related to smart farming. This data-driven approach imposes the need for greater security requirements across smart agriculture to process the real-time information’s in a more secure and efficient manner.

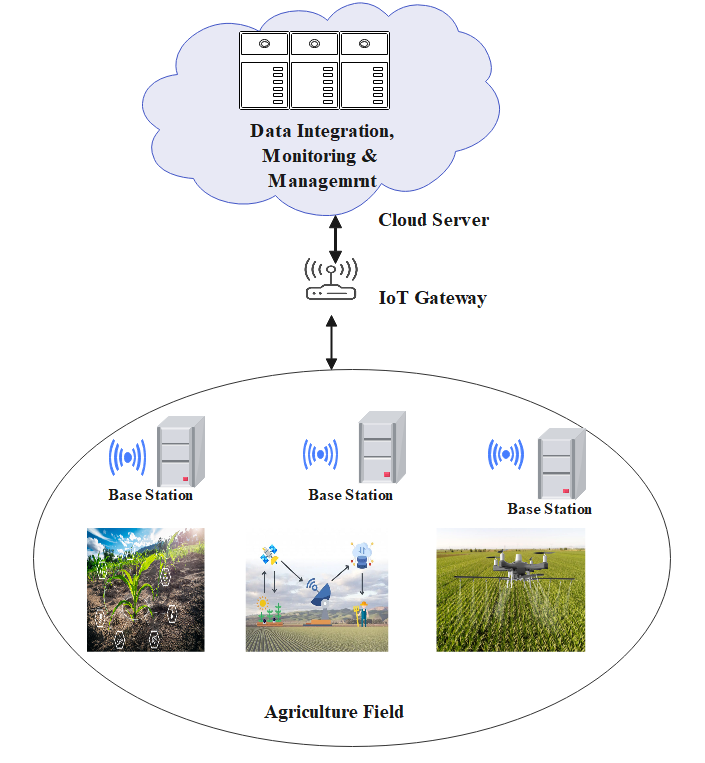


Figure 1. Overview of Smart Agriculture

In general, Unmanned Aerial Vehicles are more suspectable to greater security threats and vulnerabilities as they need to communicate with numerous IoT devices and sensors for efficient data collection. Security issues may arise at any point associated with navigational or the communicational links [11,12]. Further, protection to the drone privacy has also become an important requirement. At present, several works have been carried out to protect the security of the Unmanned aerial vehicles. But they face several challenges with respect to computational complexities and communication overheads. In addition, majority of the cyberthreats across the unmanned aerial surveillance systems will be prevented if the nodes are securely authenticated with each other before they establish a secure connection. In this context, this paper presents a blockchain based secure two factor mutual authentication scheme for secure aerial surveillance across smart agricultural systems. The proposed mutual authentication scheme is lightweight in nature and it works on the basis of the PUF parameter. A detailed description to the proposed protocol will be given in the upcoming sections.

The organization of the paper is given as follows: section provides introduction to the proposed protocol. Section 2 presents a brief literature review discussing various security threats associated with unmanned aerial surveillance systems. Detailed description of the proposed security protocol is given in section 3. Section 4 presents the results and discussions. Section 5 concludes the proposed approach.

1. **Literature Review:**

This section presents a brief summary on various security issues associated with the unmanned aerial surveillance in smart agriculture. Each approach is discussed with its advantages, disadvantages and future research directions.

Security and privacy issues greatly influences the widespread application of the drones across various systems. A detailed review on security and privacy issues associated with the drones are given in [13]. This work states that availability, confidentiality, authenticity, integrity, and privacy are some of the important security and privacy requirements for the drone systems. Further, this work states that cryptographic based authentication techniques form the most appropriate for these purposes.

Yang, Wencheng, et al. [14] presents a review on security and privacy issues associated with Internet of Drones. The author states that blockchain powered authentication schemes plays a huge role in protecting the security features across IoT powered drones. Also, this approach states that the level of security and cost efficiency remains to be the greater challenge across the existing approaches.

The challenges faced due to the use of drones in agriculture is explored in [15]. This work explores various ethics, safety and regulatory hurdles associated with implementation of drone technologies across smart agriculture.

A blockchain envisioned authentication scheme for drones in smart agriculture is presented in [16]. This approach provides blockchain based authentication and key management scheme for IoT enabled smart agricultural systems. The security and comparative study reveal that this approach offer improved security and lesser communication cost in comparison to the existing approaches.

A secure authentication framework for Internet of Drone applications is given in [17]. This approach states the significance of having integrated security mechanisms across the IoT devices. The authentication schemes applied to drone authentication should require limited resources and energy requirements. This approach presents an extended version of elliptic curve based cryptographic methods for secure authentication of drones. But however, this approach lacks in provision of efficient performance measures.

Khalid, Haqi, et al. [18] presents a secure two factor mutual authentication scheme for Internet of Drones. A light-weight anonymous two-factor authentication scheme for drones is presented based on asymptotic cryptographic method. The primary objective of this scheme is to preserve the security of the real-time information. This approach provides minimal complexity and computation cost in comparison to existing approaches. But however, the performance degrades with increasing complexity of the data.

A provably secure mutual authentication scheme using PUF is given in [19]. The use of Physically Unclonable Function (PUF) creates the system more resistant to drone stolen attacks. This scheme provides more convenient and secured wireless communication. But this approach fails to attain appropriate cost efficiency measures.

A light-weight privacy preserving mutual authentication scheme for drone environment is given in [20]. This approach provides both mutual authentication and key agreement system for Internet of Drone Environment. The security features of this system are evaluated using the AVISPA tool and it provides resilience to various security attacks. However, this approach lacks due to greater communication cost measures.

In [21], the blockchain based secured mutual authentication scheme for Drone-GSS communication is presented. This approach implements PUF based mutual authentications for drones. The formal and informal security analysis of this scheme provides more resilient towards various security threats.

In [22], an efficient mutual authentication scheme is given for edge assisted Internet of drones. This approach considers the physical security of the UAV, which forms the most important highlight of the work. It enables third-party communication, where the edge computing service providers authenticate the UAV without any compromise to its security and privacy measures. But however, this approach lacks due to higher computational complexity measures.

It has been envisioned from the literature that [23, 24, 25, 26, 27] device to device communication in aerial surveillance across smart agriculture has subject to numerous security threats. Implementing an efficient mutual authentication protocol resolve this issue in a more efficient manner. However, the major drawback with the conventional approaches is it lacks in computational complexity and communication cost measures though they preserve the security of the system. In this regard, this paper aims to present a secure mutual authentication scheme for smart agriculture with lesser communication cost and computational complexity measure. A detailed description to the protocol will be discussed in detail in the upcoming section.

1. **Proposed System:**

This section provides a brief description to the working of the proposed mutual authentication protocol. Initially, description to the working of blockchain protocol will be provided and the working of the security protocol will be given at the later part of this section.

* 1. **Overview of the Proposed Architecture:**

In recent, the growth of IoT devices in agriculture are more significant and at the same time the light-weight nature of those IoT devices makes security as a major constraint in drone based aerial surveillance. It is mandatory for the IoT devices and device controller to authenticate with each other for a secure communication. In the proposed approach, the IoT nodes and controller node makes use of the cloud environment to facilitate the authentication process. This paper presents a blockchain based secure architecture that ensures privacy and security of the IoT devices in smart agriculture. The proposed approach implements an PUF based security protocol that works in three layers. The top most layer contains the centralized blockchain node that manages the blocks of references representing which ancestor node should be queried to acquire the reference for a particular IoT device across the particular domain. Here, every ancestor PUF node in the blockchain environment maintains the reference to the distributor node that has to be processed next to provide challenge response pair (CHREP) for a particular IoT device. The blockchain associated with parent PUF node is arranged on the basis of various categories of IoT devices (smart tractors, drones, sensors, etc.). The distributor nodes are arranged depending on various service providers. An overview of the proposed architecture is given in figure 2. The proposed approach can authenticate both the mobile and stationary IoT components installed at the agricultural fields. It also authenticates both the local and the distributed controller nodes. The cloud environment associated with the proposed approach is assumed to be consist of higher storage and computing resources. Further, it includes a blockchain node, where the PUF challenge response pairs are stored and maintained.

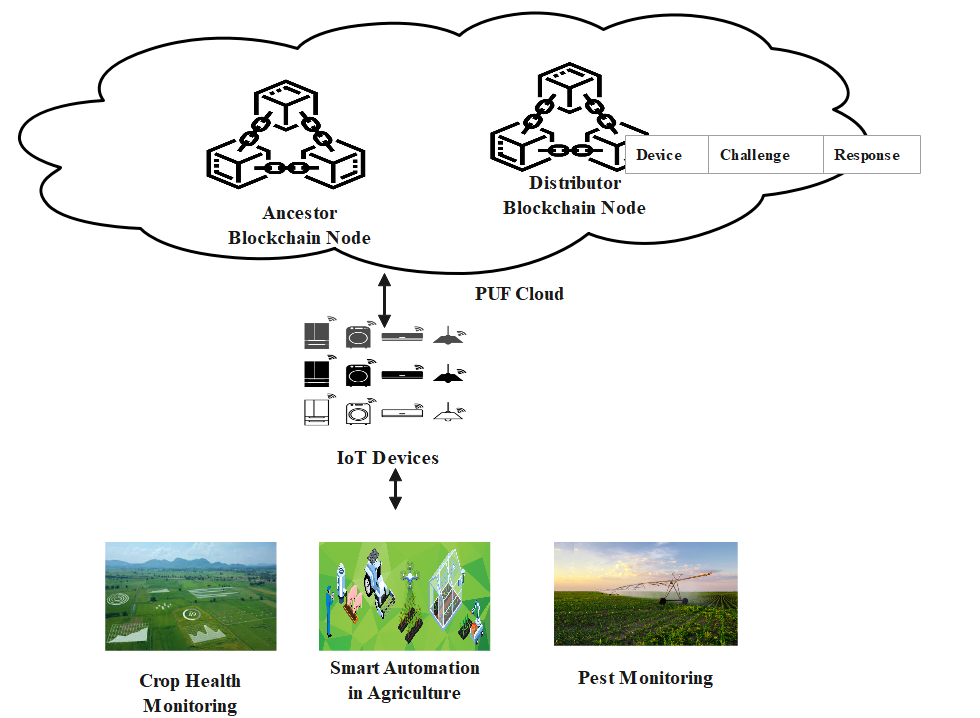


Figure 2. Overview of the Proposed Architecture

* 1. **Blockchain Assisted Secure Mutual Authentication Protocol for Aerial Surveillance in IoT based Smart Agriculture:**

Each IoT device completes their membership phase during the deployment process. At the stage of deployment every IoT device will be given an original identity. The original identity will also be given to IoT gateway. Further, the credentials such as CHREP will also be acquired for every IoT gateway and devices associated with aerial surveillance. The credentials such as CHREP will be verified and only the error-free CHREP’s are used for reference. After verification the CHREP will be loaded in to cloud and stored using blockchain.

* + 1. **Enrolment Stage:**

The major objective of this stage is to perform the registration of the IoT device. Initially the trusted authority (TA) will perform numerous operations. This includes assigning the IoT device (ID) with an false identity , type identity , and cyber domain identity . Here, the false identity is used by the IoT devices to establish communication with intermediate gateway . For every authentication process, will get changed significantly. The primary objective of using the false identity is to ensure untrace ability and unlike ability of the IoT devices. It also ensures the anonymity of every session. The trusted entity will make use of the IoT device false identity and original identity of the IoT gateway to produce three different authentication parameters . This is made with the help of XOR operations and one-way function. Next, the trusted authority TA will provide OTP using random number generator. This OTP is valid between IoT devices and . Once the IoT device registration is completed both IoT device and intermediate gateway will generate their OTP for each authentication without the involvement of any other users. In the third step, the TA will retrieve CHREO () from the cloud environment. Where the PUF blockchains are stored. Next, the TA will store . It also includes the OTP associated with the and saves the , , OTP, , , in to the IoT device memory.

The original identities of both the IoT devices and the IoT gateway are secure values that exists between the IoT devices and Intermediate gateway. Their real identities will be transmitted in a plain text format.

**Step 1:** TA provides to I

**Step 2:** TA maps the I with its suitable cyber domain and compute to I.

**Step 3:** TA computes for every I depending on its type and assign them with appropriate values.

**Step 4:** TA acquires CHREO from PUF cloud.

**Step 5:** The three security parameters will be computed.

Here, the parameters such as , are used only to compute The security parameters and is stored only with the and the IoT devices does not posses any information regarding this instant. Similarly, will only be available in database and remains unknown to the IoT devices. In such a way it is highly impossible for the intruder to find and . Further, the effective use of makes it infeasible for the intruder to impersonate the .

**Step 6:** The TA will generate OTP using random number generator.

**Step 7:** The TA stores the confidential information’s such as , and OTP across the IoT device storage.

**Step 8:** The TA updates the database with credentials such as and OTP associated with the IoT devices.

* + 1. **Mutual Authentication Stage:**

This stage involves effective implementation of two-factor authentication process over the key agreement between the IoT devices and Intermediate gateway. The session key will be used for the authentication process and it will be computed using hash function. At this stage, both the Intermediate gateway and IoT devices will establish a secret session key. The process of key exchange is illustrated as follows:

|  |  |
| --- | --- |
| I |  |
| Select  Generate | Select:  Generate: |
|  |  |

This phase is initiated by the IoT devices, it establishes the connection and request the message that is transferred to .

**Step 1:** The IoT devices generated the time stamp . This will prevent replay attack.

**Step 2:** During this step the IoT device will compute .

**Step 3:** The IoT device I choose the random parameter and compute .

**Step 4:** The IoT device then calculates

**Step 5:** Then in step 5 the request message for establishing the connection is sent by the IoT device.

The process of mutual authentication between the IoT device and the intermediate gateway is given as follows:

|  |  |
| --- | --- |
| IoT Device (I) | Intermediate Gateway |
| Produce:  Calculate: |  |
| Verify: |  Obtain:  Read:  Calculate:  RE            Verify:  SMI’= HA(  Produce:  RA  Calculate:    CHA’ =          Calculate:  =HA(      Validate:    Produce:    Calculate:      ||      Verify: |  Calculate:  OT    Validate:    Store (OTPn’, | |

The process of establishing the connection is discussed as follows:

**Step 1:** Initially the intermediate gateway verifies the acquired time stamp. The comparison is made between the time when the message is received and the maximum amount of transmission delay. The message will not be accepted if there exists any difference between the time of message received and the time stamp are greater than the estimated transmission delay.

**Step 2:** During this step the intermediate gateway acquires the original identity of the IoT devices that correspond to its false identity. The connection will be rejected if there exists no appropriate false identity.

**Step 3:** Upon the successful completion of step 2, the credentials such as along with the original identity.

Step 4: The intermediate gateway then transfers the challenge associated with the gateway to its PUF function for computing the response.

**Step 5:** The intermediate gateway make use of the response generated to compute the authentication factor through the use of one-way hash function. Through the use of authentication factor acquired from intermediate gateway Further, the other authentication parameters and will be generated in the same way and it is given as:

**Step 6:** The intermediate gateway then computes

**Step 7:** The next step is to calculate

**Step 8:** During this step the intermediate gateway make use of the computed , to produce . This is acquired using the combination of with the help of one-way hash function. The connection request is accepted by the intermediate gateway only if the computed and received value are equivalent. Otherwise, the connection will be discarded.

|  |
| --- |
| SI’=HA(  If Then  Connection request is accepted  Else  Connection request discarded |

The intermediate gateway then validates the IoT node. This is made through the communication with grand OUF node to obtain the corresponding PUF challenge ( and its response (. This is made with the help of a secure communication channel. As a result a session Id and a random value R is generated by the intermediate gateway. To differentiate one session from the another, the time stamp associated is also generated. The steps associated with establishment of connection process is given as follows:

* Initially the intermediate gateway selects a random parameter (.
* Intermediate gateway produces a new time stamp (.
* Intermediate gateway produces the session ID (.
* Intermediate gateway calculates
* Then the intermediate gateway computes CHA=
* is computed by the intermediate gateway.
* The connection response message is then sent by the intermediate gateway.

The connection response message consists of various parameters such as session ID , false identity of the intermediate gateway , CHA, , . Then the message is encrypted as follows:

}.

Upon the receipt of the connection response, the following steps will be executed consecutively:

1. First the IoT device verifies the validity of the acquired timestamp. It checks whether the time when the message is received and the timestamp are equivalent to the expected transmission delay. The message will be discarded if there is a greater transmission delay.
2. In the next step the IoT device retrieves the original identity of the intermediate gateway that corresponds to the given false identity. The connection will be discarded if there exist no appropriate matches.
3. In the next step, the IoT device computes .
4. IoT device compute .
5. The IoT device computes .
6. The IoT device then compute .
7. The random generator RA and will be retrieved to decrypt the message. The IoT device will make use of for this process.
8. Finally the IoT device computes the one-way hash function and compare the generated with the received . The message will be accepted by the IoT device, when there exists a match between both the parameters. This process is defined as follows:

The connection is established

Else

Connection rejected and message discarded

The IoT device will compute the steps given below upon the correctness validation of and validating the integrity of the sent message.

1. The IoT device generates the timestamp .
2. The IoT device computes the .
3. The IoT device compute New OTP (.
4. The IoT device then computes the new alias identity ID().
5. Then the IoT device computes
6. The IoT device select its approach to compute session key. The IoT device will transfer either the time stamp 1 or time stamp 2.
7. The IoT device transfers a message to the intermediate gateway that includes . Here, either the hash function or public key will be used to generate the session key. The message encryption will be made through the random .

Once the message transferred by the IoT device is successfully received. The intermediate gateway will perform the following steps:

1. Initially, the intermediate gateway validates . Then the validity of the acquired timestamp is verified. The message will be discarded if there exists a difference between the time when the message is received and timestamp is greater than the expected maximum transmission delay. Otherwise, the connection will be established successfully.
2. Then the intermediate gateway performs the decryption of message using PUF response
3. In the third step, the intermediate gateway compute OTP(
4. Next step involves the computation of new false identity ID(.
5. Next step involves the computation of , which is a combination of . The session will be established only if the calculated is equivalent to the received . In the other case, the session will be ended. In addition, the intermediate gateway saves the and , which is mandate for the next authentication session.

Then

* + 1. **Key Generation Stage:**

Upon the successful completion of mutual authentication process, both the IoT device and the intermediate gateway will compute a secret session (SK) based on the technique that they agree during the mutual authentication process. It could be made either with the hash function or the public key parameter. In case of any disruption with the key generation phase, the intermediate gateway and the IoT devices next to start with the entire mutual authentication process from beginning. Session key generation with the help of the hash function:

Secret Session Key

Session Key Generation with the help of public key parameter.

**Algorithm for the Process of Mutual Authentication between the IoT Devices and Intermediate Gateway:**

|  |
| --- |
| **Input:** Original and False identity of the IoT device, Original and false identity of the intermediate gateway, authentication parameters and OTP  **Output:** Mutual authentication between the IoT devices and intermediate gateway  **Start:**  **Step 1:** IoT device generate timestamp , random nonce , using which it computes ( and (SI)HA(AI, *.*  **Step 2:** The IoT device transfers message to server (.  **Step 3:** If ( then  **Step 4:**  recovers the , , , that corresponds to , which is acquired from its database. The recovers the , , , that corresponds to , which is acquired from its database. The further computes the using the and PUF function.  **Step 5:** The intermediate gateway computes the authentication parameter . Next the calculates that can be acquired from that is attained by performing XOR operation on and . Finally SI’ HA( message is computed.  **Step 6:** If (computed message in step 6 match with hash message in step 2)  Then  **Step 7:** The establish connection with grand PUF node to CHERP, computes the timestamp  .  **Step 8:**  transfers , Message that is encrypted by .  **Step 9:** Else  Go to step 2  End if  **Step 10:** The IoT device validate the timestamp compute to acquire from . Here, the IoT device will make use of the PUF to compute for . Further the will be used by the IoT device for the decryption of message and it retrieves and . The IoT device further calculates ).  **Step 11:** If (Computed hash message in step 10 matches the hash message sent in step 9)  Then  The authenticity of the intermediate gateway is validated.  **Step 12:** The IoT device computes the timestamp and it computes the appropriate public key.  **Step 13:** The IoT device computes OTP(.  **Step 14:** The IoT device computes new false identity ID(.  **Step 15:** The IoT device computes  || .  **Step 16:** The IoT device sends encrypted message by to .  **Steo 17: E**lse  Go to step 22  End if  **Step 18:** The intermediate gateway decrypts the message with the help of and , and compute (HA(||SK’||  **Step 19:** If (computed hash value in step 18 match with hash message sent at step 16 then the authenticity of the IoT device is validated.  **Step 20:** Successful mutual authentication of IoT device and server  **Step 21:** Else  Go to Step 22  End if  Stop |

1. **Results and Discussions:**

This section provides a detailed description to the security and performance analysis measures associated with the proposed approach in the context of aerial surveillance system. Further, a comparative analysis of the proposed technique with the other conventional approaches are also discussed in detail.

* 1. **Security Analysis of the Proposed Mutual Authentication Technique:**

The security analysis measure discussed in this section is a formal approach and the simulations are performed using AVISPA tool. The most widely accepted tool for evaluation of various security protocols. The results ensure that the proposed approach is more resilient to man-in-the-middle attack, replay attack, active and passive attacks. The simulation process mainly focuses on 10 different security objectives and two different authentication parameters, which are described as follows:

1. **Objective 1:** The secrecy of the original identity associated with IoT device states that the original identity associated with the IoT device is always made secret and they are known only to the IoT devices and Intermediate gateway.
2. **Objective 2:** The secrecy factor associated with the OTP states that OTP is kept confidential only between the IoT devices and intermediate gateway.
3. **Objective 3:** The secrecy of the random value generated during authentication is kept secret only between the IoT devices and intermediate gateway.
4. **Objective 4:** The random value associated with the intermediate gateway is always kept confidential only to the IoT devices and intermediate gateway.
5. **Objective 5:** The secrecy of the real identity of the intermediate gateway represent that the intermediate gateway is always made secret and is known only between the IoT devices and intermediate gateway.
6. **Objective 6:** The secrecy of the response factor is made secret only between the IoT devices and intermediate gateway.
7. **Objective 7:** The secrecy measure associated with the challenge is kept confidential only to the IoT devices and the intermediate gateway.
8. **Objective 8:** The secrecy of the private key indicates that the private key is always kept secret and is shared only between the IoT devices and intermediate gateway.
9. **Objective 9:** The secrecy of the OTP denotes that the OTP is permanently kept secret and is known only to the IoT devices and intermediate gateway.
10. **Objective 10:** The response associated with the intermediate gateway is always kept secret and it made visible only to the IoT devices and intermediate gateway.
11. **Authentication Property 1:** The authentication process associated with the random value generated by intermediate gateway represent that the IoT device acquires the random value through a message and it completes the authentication of the intermediate gateway.
12. **Authentication Property 2:** The authentication process associated with the random value generated by IoT devices indicates that the intermediate gateway acquires the random value through message and it completes the authentication of the IoT device.

In order to successfully ensure the security objectives listed above an HLSPL script is written and simulation is performed using the AVISPA tool. IoT devices (I), Intermediate gateway IGw, Session Se, and computing environment, which instantiates all the variables, agents, and functions. Initially The IoT device I is of the Intermediate gateway and IoT devices associated with the proposed protocol. It is also aware of its original and false identity. In addition, it is aware of its original identity of its own and the intermediate gateway, which has to be kept secret. The IoT device is also aware of various authentication parameters such as Tsm, A, B, hash function HA(.), and the OPT produced by the trusted entity (TE), and the message sending and receiving channels.

First the IoT device acquires the start signal to begin with the execution of the protocol. Consequently, it also generates the new random values and calculates the I1, I2, and SE. Then the IoT device transfers the parameters such as (IFID, TSM1I, I2, SEI) to the intermediate gateway. During the phase of second transition, the IoT device receives the (IGwFID, SEID, TSMIGw, {CHA, H2} RE1) message from the intermediate gateway and it is encrypted using the parameter RE1. During this transition process the IoT device authenticates the intermediate gateway if the gateway two comes as expected by the IoT device. After the successful completion of the authentication process, the IoT devices generates time stamp associated with IoT devices, random value, OTP, and new false identity for the third IoT device. Through the help of the negotiation agreement the session key is generated during this phase.

Similarly, the intermediate gateway is aware of all the agents associated with the intermediate gateway and IoT devices. It is also further aware of all the security protocols associated with the proposed system. During the first transition process, the intermediate gateway acquires the (IFID, TSmI, I2,SEIGw) message which is transferred by the IoT device. The intermediate gateway makes use of the IFID to retrieve CDID, TSmI, OTP, CHA. Upon the successful verification of the session key it calculates a new value for the IoT devices and the time stamp. The time stamp, challenge, and gateway 2 all these values are calculated based on the steps described at the proposed approach. Then the intermediate gateway will transfer the parameters such as I(IGwFID, SEID, TSmIG, CHA, {I, G2}RE1). Next, the intermediate gateway acquires the (SEID, TSeI’ {I’.exp(HA,qn’).I3’}\_RE1. The message is decrypted by the intermediate gateway through the help of Re1. The new false identity and new OTP of the IoT device are verified in accordance to the proposed protocol described at the previous section. The session entity is responsible for establishment of the mutual authentication between two entities. The computing environment role is responsible for instantiation of one or more sessions.

The proposed mutual authentication protocol is informally assessed to identify how effectively it satisfies the various security requirements. The security assessment results are briefly discussed as follows:

* 1. **Mutual Authentication:**

In the proposed approach before the message is sent, the IoT device selects a random number and calculate IA1, IA2, and SE associated with the IoT device. In the next step intermediate gateway needs to retrieve the random value and it needs to compute the authentication parameters A2 and A3 and then further it performs the computation of A1. A1 is computed with the help of the PUF function. In such a scenario, any kind of adversary will not be able to generate the authentication parameters A1 without knowledge on original identity of the IoT device, intermediate gateway and the PUF response. Further, the adversary will not be able to validate the A2 and A3 without the help of domain identity and time stamp associated with the IoT devices that are securely stored across the intermediate gateway. The intermediate gateway and the IoT devices both mutually authenticate with each other based on the correctness of and . In such a scenario, the adversary will not be able to compute H2 without the help of H1. Further, the adversary will not be able to make a guess of REIGw to obtain A1, which is an element of H1. Further, the OTP will have no information regarding the OTP, which is shared only between the IoT devices and the intermediate gateway. In short, the adversary will not be able to compute the identity of the intermediate gateway and IoT devices without knowing their real identity of intermediate gateway. As a result, the proposed approach can effectively perform the mutual authentication process.

* 1. **Forward/ Backward Security:**

In the proposed approach the session key is generated either using the public key or through the hash function values. The forward/backward security property assures that the exposure of the session key should not affect any past or future sessions. Even if a session key is exposed for a particular session, he should not be able to compute the session key for the past or future sessions. In case of the second scenario. In case of the second scenario, the random value selected for every session should not be replicated. Because the random value associated with each device is unique for each IoT devices. Through the use of PUF, the proposed approach ensures that any compromise on secret key will not impact on any future session. Thus, it ensures the forward/backward secrecy property, which states that exposure of any secret key should not affect the process of any future or past sessions. As a result, the proposed approach ensures the forward and backward security measures.

* 1. **Stolen Database Attack:**

In case of any kind of failure across the IoT device end, the adversary may able to steal the authentication parameters, original identity and OTP parameters related to the IoT device and they impersonate the IoT device. However, the unauthorized node will fail during the challenge response validation process. Similarly, if the intermediate gateway is compromised the adversary can steal the real identity of the IoT device and intermediate gateway, domain ID of the IoT device, time stamp and OTP from the Intermediate gateway and they can impersonate. But however, the compromised intermediate gateway will fail to compute its original identity. Thus, the proposed approach is more resilient to the stolen database attack.

* 1. **Replay Attack:**

The effective use of time stamp parameter prevents replay attack. The time stamp generated by the sender node is attached to the hash function this ensures that the adversary cannot compromise over the time stamp. Further the use of challenge response pair also prevents replay attack. Hence, the proposed approach is more resilient to the replay attack.

* 1. **Data Modification Attack:**

The proposed approach is more resilient to the data modification attack, because the original identity of the IoT devices, private key, time stamp, one-way has function, challenge response pairs, and random value associated with intermediate gateway and IoT device remains unknown to the adversary. Thus, in this way the data modification attack is prevented.

* 1. **Physical Attack:**

The proposed approach is more resilient to the physical attack, this is attained through the effective implementation of PUF.

Next the simulation results of the proposed protocol is compared between the conventional approaches [28,29,30] and the results are discussed appropriately in table 1.

Table 1 Comparison of the Security Measures with Conventional Approaches

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Parameter** | **Scheme I** | **Scheme II** | **Scheme III** | **Proposed Protocol** |
| Replay Attack | ✓ | ✓ | X | ✓ |
| Impersonation Attack | ✓ | X | X | ✓ |
| Data Modification Attack | X | ✓ | ✓ | ✓ |
| Device Counterfeit | ✓ | X | ✓ | ✓ |
| Anonymity and Untraceability | X | X | ✓ | ✓ |
| Modelling Attack | ✓ | ✓ | ✓ | ✓ |
| Brute Force Attack | X | ✓ | X | ✓ |
| Mutual Authentication | ✓ | ✓ | ✓ | ✓ |
| Key Storage | ✓ | ✓ | X | X |
| Physical Attacks | ✓ | ✓ | ✓ | ✓ |

It is observed from table 1 that the proposed approach fulfils the requirement of multiple essential security features and it is found to comparatively better than the conventional approaches. Further, it will highly challenging for the adversary to intrude between the aerial surveillance systems.

* 1. **Performance Analysis of the Proposed Mutual Authentication Scheme:**

This section illustrates the detailed performance analysis measures associated with the proposed mutual authentication protocol for aerial surveillance systems.

* 1. **Storage Requirements:**

In the proposed mutual authentication scheme, every IoT device saves its original and false identity, authentication parameters, on-time password, original and false identity measures. Here, SHA-256 is used for the implementation of the hash function. By applying these settings, the storage requirements associated with the IoT devices and intermediate gateway is computed and it is represented in table 2.

Table 2. Storage Cost Measures Associated with the Proposed Protocol

|  |  |
| --- | --- |
| **Node** | **Storage Cost accompanying every bits** |
| IoT Device (I) | 128 + 256 \* 2 + 8\* 2 + 256 = 912 + 64 = 976 bits |
| Intermediate Gateway (IG) | 128 + 256 + 128 + 8\*4 = 544 bits |

* 1. **Detailed Analysis of Computational Complexity Measures:**

In this subsection we make a detailed analysis of the computational complexity associated with the proposed approach. The computational complexity associated with proposed protocol is calculated using the systematic simulation of the cryptographic operations. An HP laptop with i7 processor and dual-core CPU of 2.7 GHz with 8GM RAM acts as an intermediate gateway. The IoT devices are simulated using Raspberry Pi 4 model with processors. The 128-bit arbiter is used for the PUF operations. The simulations are made using the Python libraries such as Fastecdsa library and Pycryptodome cryptographic functions. The execution time taken for the various cryptographic functions is illustrated in table 3.

Table 3. Execution Time Required to Perform Various Cryptographic Operations

|  |  |  |
| --- | --- | --- |
| **Cryptographic Operation** | **Computation Time taken by the IoT Devices** | **Computation Time taken by the Intermediate Gateway** |
| Time to execute one-way hash function operation | 0.002ms | .001 ms |
| Time to Perform ECC point multiplication | 4ms | 3ms |
| Time to execute fuzzy extraction operation | 4ms | 3ms |
| Time taken to perform modular exponentiation | 8 | 6 |
| Time to execute the Encryption Process (128 bit Encryption) | 0.16 ms | .14 ms |
| Time taken for the Decryption process | 0.16 ms | .14 ms |
| Time to execute PUF operation | 10 ms | 10 ms |

Table 4. Comparison of Computational Complexity Measures Associated with Conventional Approaches

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **System Entity** | **Scheme I** | **Scheme II** | **Scheme III** | **Proposed Scheme Implementation using Hash Function** | **Proposed Scheme Implementation using ECC** |
| IoT Devices | 8TH + 2TPUF | 6TH + 2TPUF+ 2TEM + 1TENC | 3TH + 2TMAC + 2TENC + 1TENC + 2 PUF | 6TH + 1TPUF + 1TENC + 1TDEC | 6TH + 1TENC + 1TDEC + 1TPUF + 1 TEM |
| Cost Parameter Associated with the IoT devices | 6.25 ms | 15.29 ms | 9.8 ms | .59 ms | 5.79 ms |
| Intermediate Gateway | 8TH + 2TEXP | 6TH + 1DEC + 3TEM | 3TH + 2TMAC + 1TENC | 11TH + 1TENC + 1TDEC + 1TPUF | 9TH + 1TENC + 1TDEC + 1TPUF |
| Intermediate Gateway Cost | 17.01 ms | 8.76 ms | 4.83 ms | .52 ms | .52 ms |
| Total Cost Meaures | 17.26 ms | 23.55 ms | 14.63 ms | 1.11 ms | 6.31 ms |

* 1. **Analysis of the Communication Cost:**

The communication cost associated with the proposed protocol is analysed in detail across this subsection. It is essential that the communication cost should always be lesser to prevent network congestion and to enable faster message transmission. In order to analyse the communication cost associated with the proposed protocol, the cost measures are evaluated in terms of the size of the message. Comparative analysis are also made with other conventional protocols.

Table 5. Comparison of Computational Cost Measures

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Message Number** | **Scheme I** | **Scheme II** | **Scheme III** | **Proposed scheme with hash function** | **Proposed Scheme with ECC** |
| M1: I→ SER | 256 bits | 176 bits | 256 bits | 560 bits | 560 bits |
| M2: SER → I | 520 bits | 304 bits | 640 bits | 576 bits | 576 bits |
| M3: I → SER | 680 bits | 1024 bits | 768 bits | 568 bits | 720 bits |
| M4: SER → I | 380 bits | 1024 bits | 1024 bits | ------ | ----- |
| M5: I → SER | 640 bits | -------- | --------- | --------- | --------- |
| Total | 2,476 | 2,528 | 2,688 | 1,704 | 1,856 |

It is observed from table 4 that the proposed approach has comparatively lesser communication cost when compared with the conventional approaches. When implemented using the hash function the proposed approach shows the communication cost 1704 bits and with ECC model it has the communication cost of 1856 bits. In addition, from the above experimental observations it is also identifies that the proposed approach fulfils most of the security properties with lesser communication cost and computational overhead measures. Hence, the proposed protocol provides better security features to the aerial surveillance systems in smart agriculture.

1. **Conclusion:**

The automation, navigation and smart control technologies associated with IoT assisted smart agriculture systems significantly change the way of conventional agricultural practices and at the same time they are subject to numerous security threats. In order to provide the secure communication among the drone assisted smart agriculture system, this paper presents an blockchain based light-weight two factor mutual authentication scheme for IoT based smart agricultural systems. The proposed protocol ensures the security, confidentiality, and data integrity associated with drone data. The security analysis of the proposed protocol is made both formally and informally manner and it provides comparatively better results than the conventional approaches. The protocol efficiency is also evaluated in terms computational complexity, storage requirements and communication costs. In all the aspects the proposed protocol found to be providing comparatively better results than the conventional approaches. This approach is found to be more suitable and efficient for IoT devices. In future, the blockchain based framework presented in this approach could be extended to offer better security and privacy measures.

**Conflicts of Interests:**

I confirm that there are no conflicts of interest associated with this publication. I have no financial relationships with any entities that could be perceived to influence the content of this manuscript. Furthermore, I have no personal or professional affiliations that could be considered to have influenced the research presented in the manuscript.

**References:**

1. Vangala, Anusha, et al. "Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges." Cluster Computing 26.2 (2023): 879-902.

2. Yang, Xing, et al. "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges." IEEE/CAA Journal of Automatica Sinica 8.2 (2021): 273-302.

3. Hai, Tao, et al. "A Novel & Innovative Blockchain-Empowered Federated Learning Approach for Secure Data Sharing in Smart City Applications." International Conference on Advances in Communication Technology and Computer Engineering. Cham: Springer Nature Switzerland, 2023.

4. Qureshi, Taimoor, et al. "Smart agriculture for sustainable food security using internet of things (IoT)." Wireless Communications and Mobile Computing 2022.1 (2022): 9608394.

5. Sinha, Bam Bahadur, and R. Dhanalakshmi. "Recent advancements and challenges of Internet of Things in smart agriculture: A survey." Future Generation Computer Systems 126 (2022): 169-184.

6. Baranwal, Tanmay, and Pushpendra Kumar Pateriya. "Development of IoT based smart security and monitoring devices for agriculture." 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence). IEEE, 2016.

7. Tamizharasi, G. S., B. Balamurugan, and R. Manjula. "Attribute based encryption with fine-grained access provision in cloud computing." Proceedings of the International Conference on Informatics and Analytics. 2016.

8. Chaganti, Rajasekhar, et al. "Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture." Future Internet 14.9 (2022): 250.

9. Friha, Othmane, et al. "Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies." IEEE/CAA Journal of Automatica Sinica 8.4 (2021): 718-752.

10. Tamizharasi, G. S., B. Balamurugan, and S. L. Aarthy. "Scalable and efficient attribute based encryption scheme for point to multi-point communication in cloud computing." 2016 International Conference on Inventive Computation Technologies (ICICT). Vol. 1. IEEE, 2016.

11. Tao, Wen, et al. "Review of the internet of things communication technologies in smart agriculture and challenges." Computers and Electronics in Agriculture 189 (2021): 106352.

12. Gagliardi, Gianfranco, et al. "An internet of things solution for smart agriculture." Agronomy 11.11 (2021): 2140.

13. Yahuza, Muktar, et al. "Internet of drones security and privacy issues: Taxonomy and open challenges." IEEE Access 9 (2021): 57243-57270.

14. Yang, Wencheng, et al. "A review on security issues and solutions of the internet of drones." IEEE Open Journal of the Computer Society 3 (2022): 96-110.

15. Ayamga, Matthew, Bedir Tekinerdogan, and Ayalew Kassahun. "Exploring the challenges posed by regulations for the use of drones in agriculture in the African context." Land 10.2 (2021): 164.

16. Bera, Basudeb, et al. "Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment." Computer Standards & Interfaces 80 (2022): 103567.

17. Ever, Yoney Kirsal. "A secure authentication scheme framework for mobile-sinks used in the internet of drones applications." Computer Communications 155 (2020): 143-149.

18. Khalid, Haqi, et al. "Secure real-time data access using two-factor authentication scheme for the internet of drones." 2021 IEEE 19th Student Conference on Research and Development (SCOReD). IEEE, 2021.

19. Zhang, Yunru, et al. "A lightweight authentication and key agreement scheme for Internet of Drones." Computer Communications 154 (2020): 455-464.

20. Pu, Cong, et al. "A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment." IEEE Internet of Things Journal 9.12 (2022): 9918-9933.

21. Gupta, Anvita, Ayushi Jain, and Mehak Garg. "Blockchain-Based Secure Mutual Authentication Scheme for Drone-GSS Communication in Internet of Drones Environment." International Conference on Recent Developments in Cyber Security. Singapore: Springer Nature Singapore, 2023.

22. Gope, Prosanta, and Biplab Sikdar. "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones." IEEE Transactions on Vehicular Technology 69.11 (2020): 13621-13630.

23. Vangala, Anusha, et al. "Smart contract-based blockchain-envisioned authentication scheme for smart farming." IEEE Internet of Things Journal 8.13 (2021): 10792-10806.

24. Chen, Meriske, Tian-Fu Lee, and Jiann-I. Pan. "An enhanced lightweight dynamic pseudonym identity based authentication and key agreement scheme using wireless sensor networks for agriculture monitoring." Sensors 19.5 (2019): 1146.

25. Vangala, Anusha, et al. "Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural iot networks." IEEE Transactions on Information Forensics and Security 18 (2022): 904-919.

26. Hassan, Bilal, et al. "A Cost Effective Identity‐Based Authentication Scheme for Internet of Things‐Enabled Agriculture." Wireless Communications and Mobile Computing 2022.1 (2022): 4275243.

27. Jan, Saeed Ullah, Irshad Ahmed Abbasi, and Mohammed A. Alqarni. "Lmas-shs: A lightweight mutual authentication scheme for smart home surveillance." IEEE Access 10 (2022): 52791-52803.

28. Rangwani, Diksha, et al. "An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network." Transactions on Emerging Telecommunications Technologies 32.3 (2021): e4218.

29. Gabsi, Souhir, et al. "Novel ECC-based RFID mutual authentication protocol for emerging IoT applications." IEEE access 9 (2021): 130895-130913.

30. Xu, Zisang, et al. "A lightweight mutual authentication and key agreement scheme for medical Internet of Things." IEEE Access 7 (2019): 53922-53931.