JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain-Assisted Distributed and Lightweight Authentication Service for Industrial Unmanned Aerial Vehicles

[1]Thara D,[2]Bhanu Prasad D,[3]Bhavana H G
[1]Professor, Department of ISE, CIT, Gubbi, Tumakuru
[2] Student, Department of ISE, CIT, Gubbi, Tumakuru
[3] Student, Department of ISE, CIT, Gubbi, Tumakuru

Abstract: **Unmanned aerial vehicles (UAVs) have demonstrated a great deal of promise for sectors because of their advantageous characteristics, which include cheap maintenance costs and ease of deployment.Prior to the widespread use of industrial UAVs, there is still a significant obstacle in the form of the communication security issue. Untrusted communication environments can result in the loss of vital cargo that UAVs are carrying or the release of priceless industrial data. Conventional methods of communication security authentication include infrastructure-based public keys, identity-based authentication, and certificateless authentication. Some of these techniques may bring high-complexity computation, making them unsuitable for industrial drones, and they are centralized in nature. Thus, in order to address these issues, we have designed a distributed, lightweight, blockchain-assisted authentication service for industrial UAVs. The distributed and immutable storing of industrial UAV authentication data is supported by blockchain technology, and smart contracts make it easy for drones to obtain or update the relevant data. An assessment of our security shows that our plan can withstand a wide range of threats and ensure reliable communications for industrial drones. Comprehensive tests further demonstrate that our developed authentication service can be reliable even in the event that a tiny percentage of industrial UAVs are compromised, in addition to achieving minimal computing and communication costs.**

***Index Terms*–Unmanned aerial vehicles, Block Chain nodes, AIL, DP.**

I. INTRODUCTION:

The Industrial Internet of Things (IIoT), which aims to advance manufacturing and enable dependable and efficient industrial production, is predicted to be able to contribute $14.2 trillion to the global economy by 2030 [1], [2].

Drones, also known as unmanned aerial vehicles (UAVs), are considered to be among the most promising instruments for the industrial factor because of their versatility and range of functions, which include sensing, processing, delivering, and more. Compared to a single UAV system, a swarm of drones with sophisticated sensors can assist industrial operations even more, offering a higher degree of automation, durability, and a larger covering range.

The four aspects of industrial drone applications are "see," "sense," "move," and "transform," based on the physical and analytical capabilities needed for the respective industrial tasks [3].

Low analytical and practical skills are needed for visible dimension applications like visual inspection [4] and monitoring [5]. The sense dimension includes activities like remote sensing [6] and 3-D mapping [7] that require great intellectual skill but minimal physical competence. The move dimension, with delivery [8] as the typical use, denotes low analytical capability and great physical competence. Last but not least, transform applications—such as warehouse management and lifesaving—require strong analytical and physical skills [9].
Even though UAV adoption has a lot of potential for the future, secure drone communications is still a problem that needs to be resolved before widespread use. UAVs must gather data from a specific industrial region in order to perform the observe and sense aspects. Examples of such areas include transportation routes for traffic management [5], or natural gas exploration sites for industrial gas sensing [6]. They then send these data, or data that has been processed, to a central infrastructure so that more analysis and decision-making may take place.

To reach the ultimate destination in these cases, data transmission may need many hops between drones. To ensure secret interactions between drones or within a group, shared session keys or group session keys are required if valuable industrial data is involved. If a cargo is lost after it has been collected, there may be catastrophic repercussions, including financial losses for clients in last-mile logistics [8] or risks to patients' lives when transporting blood samples [3].

In order to prevent hijacking, a rudimentary authentication mechanism must be in place so that UAVs can differentiate between legitimate signals and hijacker-spoofing communications .Unquestionably, secure communications should be given top attention in transform dimension applications since UAVs must enable physical transportation and data collection simultaneously.There could be disastrous consequences if a cargo is lost after it has been picked up, such as monetary losses for customers in last-mile logistics [8] or dangers to patients' lives when transferring blood samples [3].

A basic authentication technique that allows UAVs to distinguish between genuine signals and hijacker-spoofing messages is necessary to prevent hijacking. Since UAVs need to facilitate both physical transportation and data collecting at the same time, secure communications should undoubtedly receive the utmost priority in transform dimension applications.

II RELATED WORK:

A. Applications of Blockchain in the Industrial Field

Blockchain technology has been recognized as one of the key enablers for driving the industry toward its new stage, i.e., Industry 4.0, with great potentials, such as enhancing security and facilitating data collection and storage. Alladi et al. [15] gave a comprehensive survey about current research trends of applying blockchain in Industry 4.0 as well as its successful commercial implementations.

Six main industrial sectors have been reviewed, including healthcare,logistics,power, agriculture,manufacturing, and e-commerce. In addition, blockchain technology has also been explored for realizing sustainability in businesses and industries. Leng et al. [16] reviewed the capabilities of blockchain to achieve sustainability from both the manufacturing system perspective and the product lifecycle management perspective.

B. Blockchain-Based Authentication for IoT

Due to blockchain’s special features, such as decentralization, tamper proof, traceability, etc., which perfectly suit the needs of secure authentication, many existing works haveexplored the utilization of the blockchain for the design of an authentication mechanism in the IoT field. Guo et al. [17] used the blockchain to benefit the edge computing system,where edge nodes managed authentication logs and cache of contents for terminal devices based on the blockchain, for improving the authentication efficiency toward end users. In the same scenario, Wang et al. [18] mainly focused on the mutual authentication between edge servers and end users with the help of blockchain. It can be seen that the authentication entities of these schemes, namely, servers and users, are asymmetric, so that these approaches may not suit the cases when authentication participants are peer entities, such as industrial UAVs that we concern.

Some existing research worked on authentication toward peer entities. Aiming at vehicular networks, in [19], vehicles’ certificates were stored in the blockchain as a Merkle tree; through checking the existence of the provided certificate in the Merkle tree, vehicles could authenticate each others’ messages; nevertheless, the authors did not give discussions about whether this scheme could be expanded tosupport key agreement for secret communications between vehicles.

For UAV networks, a blockchain-based key distribution scheme was proposed in [20], where the longest chain principle was exploited to ensure accurate key recovery. However, this scheme required UAVs to maintain the blockchain, which might not suit task-intensive industrial UAVs since the blockchain management could cause intolerable extra cost. Gai et al. [21] proposed to use the blockchain and smart contract for realizing a secure data transition in UAV networks, where verification and consensus of blockchain were required for each data transition. Although trustworthy communication can be guaranteed, the extra round of consensus for the confirmation of communication may cause serious latency, which might not satisfy some industrial applications with low latency requirements.

Different from these works, we take the blockchain-assisted authentication as a service to help with the authentication procedure of industrial UAVs in a lightweight way, where drones participate as peer entities. In addition to message authentication, key agreement and group key agreement with the mutual-healing feature have all been designed for guaranteeing the data integrity and trustworthy communications that are required by many industrial applications.

III. Objectives:

1) We create an industrial UAV authentication service with blockchain support. Systems pertaining to message authentication, key agreement, and group key agreement with self-healing capabilities have all been developed with the aim of ensuring reliable communications and data integrity, which are essential for numerous industrial applications.

To the best of our knowledge, we are the first to thoroughly examine the problem of industrial drone authentication while taking into account all three of the common cases mentioned above.

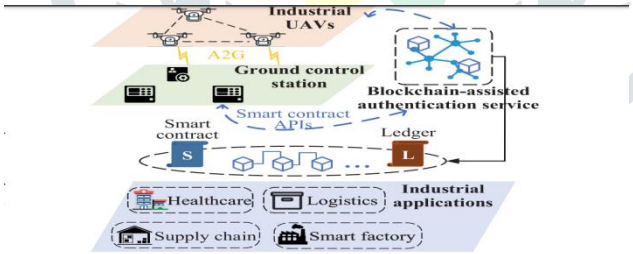
2) We provide a thorough security analysis based on the design objectives of our proposal to show that our solutions can meet all security standards.
Its logic accuracy is further demonstrated by Burrows-Abadi-Needham (BAN) logic, and its security is further confirmed by formal verification based on the automated validation of Internet security protocols and applications (AVISPA).

3) We build the blockchain network and put our plan's prototype into action using Hyperledger Fabric.The evaluation findings demonstrate that, in comparison to previous IoT authentication techniques, the computing and communication costs of UAVs in our proposal are cheaper. Additionally, we can ensure successful mutual healing even in the event that a small percentage of drones are compromised.

V1. METHODOLOGY:

A. Architecture and Design Goals

The high-level system architecture of the blockchain assisted authentication service for industrial UAVs is presented in Fig. 1. Blockchain technology is applied to decentralize the service, which is supported by a set of blockchain peer Fig. 1. System architecture of blockchain-assisted authentication service for industrial UAVs.
nodes that is deployed on the cloud server. These nodes can be accessed by base stations that cover the industrial mission area. Note that based on the ultradense network technology in 5G [22], it is reasonable to assume that there are enough base stations that can cover the industrial mission area to support the authentication service.
Each of those nodes holds a copy of a ledger and blockchain, where the ledger stores all the drones' authentication information, while the blockchain incrementally records every change of the ledger, making the authentication service unforgeable and traceable. Smart contracts are installed on all peer nodes for automatically executing operations of adding, deleting or updating the ledger records. As users, industrial drones and GCS can trigger the blockchain peer nodes' executions of smart contracts by calling smart contract APIs. Each drone can only update its own information, while GCS as drones' registrar has the permission to add or delete records of the ledger. Any change of the ledger should pass the validation of all blockchain peer nodes before finally being committed and written into the blockchain, thus ensuring a secure distributed authentication service. According to recent works [18], [23]–[25], for achieving secure and practical authentication service, the following goals should be taken into consideration. Confidentiality: Guarantee the secrecy of valuable industrial data in communications. Mutual Authentication: Allow UAVs to authenticate each other and believe that they are communicating to the one they expect.FIG1.system architecture is shown below.



Protected and pseudonyms are used during communications. These pseudonyms ought to be updated every time before a new industrial mission. However, when malicious behaviors are detected, GCS has the ability to trace the real identities of suspicions UAVs.
Perfect Forward Secrecy: Prevent an adversary from learning previous session keys, even if it is in possession of long-term secrets of other entities.
Backward Secrecy: Prevent newly joined members learning previous session keys.
Resistance to Cyberattacks: The scheme should provide resilience against common cyberattacks, such as replay attack, message tampering, spoofing, etc. Lightweight: Considering the resource-constrained feature of UAVs, the computation and communication overhead during the authentication procedure should be minimized.

B. Key Component:

1) Blockchain Nodes: Orderer nodes and validation/endorsement nodes are the two kinds of nodes that take part in overseeing the blockchain. All validation/endorsement nodes host a copy of the ledger and blockchain and have smart contracts implemented on them. As validation nodes, all blockchain peer nodes are in charge of verifying the validity of each new block before it is added to the blockchain. In contrast, endorsement nodes are chosen based on the endorsement policy and are in charge of accepting transaction proposals from UAVs or GCS, carrying out the associated smart contracts, endorsing the outcomes, and providing proposal responses to UAVs or GCS.

2) Designed Ledger and Smart Contracts: To implement the authentication service, a ledger called the Authentication Information Ledger (AIL) is created, wherein the public dynamic parameter (DP),PK, expiration period of PK, and genuine identity of legitimate UAVs are all stored. The DP described in this article can be thought of as a random component that is employed in numerous cryptographic processes to produce new shared keys or create digital signatures.

It always exists in pairs, that is, public DP, stored in AIL for public access, and private DP, kept by UAVs secretly. The former is calculated by the latter. The corresponding smart contract designed for AIL is called AuthenticationInfo, which consists of several APIs for UAVs or GCS to invoke during the authentication process, including saveInfo, deleteInfo, updateDP, queryPK, and queryDP, as introduced in the following. saveInfo can only be called by GCS to store new authentication information into AIL, and deleteInfo is the opposite API for GCS to delete records in AIL for UAVs who lose connections during the industrial mission or are detected as malicious ones.

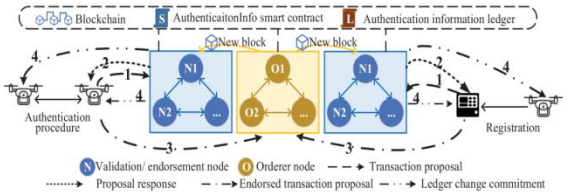
We use the permission mechanism to ensure that these two APIs are only open to the GCS and any UAVs' calling requests are refused. updateDP is designed for UAVs to update their own public DPs stored in AIL for keeping the freshness of shared keys and the security of signatures. Noted that each UAV only has permission to update its own public DP successfully, while any attempts aiming at other's information are denied. The above three APIs all involve changes of AIL, so their execution results are sent to all valid UAVs and the GCS to inform them of the latest state of AIL.

Considering the unstable wireless communications between drones, for cases that UAVs fail to receive the updated results thus leading to authentication failure, we also design two query APIs, i.e., queryPK and queryDP, for them to ask for the PK and public DP of other UAVs that they are interested in. The query results of these two APIs are only return to the requesters.

3) Smart Contract Applications: Developed based on the Software Development Kit (SDK) provided by the blockchain platform, smart contract applications are installed on all industrial UAVs and the GCS, enabling them to invoke smart contract APIs and submit transaction proposals to update authentication information stored in AIL. We define all applications in a listening mode, so that any update related to AIL can be captured by them and informed to UAVs and the GCS.

C. Working Flow:

As depicted in Fig. 2, the procedure of updating the AIL records requested by UAVs or GCS is described as follows. Assume that a UAV wants to update its DP stored in the blockchain for preparation of the subsequent authentication. First, the UAV calls updateDP through its smart contract application to send transaction proposal to endorsement nodes near it. Second, those nodes check whether this UAV has the permission to modify the corresponding DP, if so, they execute the AuthenticationInfo smart contract and endorse the result, which is returned to the UAV as proposal response. Third, after collecting enough responses, the UAV sends those endorsed transaction proposals to orderer nodes, who check the validation of the endorsements. After verification, orderer nodes package the transaction into a new block and send it to all validation nodes, who verify the correctness of the block. If it passes the checking, validation nodes add it into the blockchain and change the AIL according to the contained transactions. Finally, the changes are sent to all valid UAVs, according to which they can update their cached authentication information of others. FIG2.Work Flow is shown below.



We elaborate the detailed authentication procedure in the next section and some mainly used notations are summarized in Table I.

TABLE I
NOTATIONS AND MEANINGS

Notation	Meaning
P	A generator of the additive cyclic group $\mathbb{G}$.
SK_i	The secret key of UAV_i.
PK_i	The public key of UAV_i.
ID_i	The real identity of UAV_i.
PID_i	The pseudonym of UAV_i for an industrial mission.
d_i	The private dynamic parameter of UAV_i.
D_i	The public dynamic parameter of UAV_i and is stored in the blockchain ledger for pubic access.
T	The current timestamp.
M	The broadcast message.
key_{ij}	The shared key between UAV_i and UAV_j.
key_{group}	The group shared key of multiple UAVs.
k_i	The contributing factor of UAV_i for key_{group}.

D.AUTHENTICATION PROCEDURE

System Setup and Registration In this phase, GCS generates public parameters for subsequent authentication procedures and then all UAVs who participate in the industrial mission should register with the GCS for getting the blockchain-assisted authentication service. System Setup: GCS sets a large prime number n that defines a nonsingular elliptic curve E(n). Points in this curve form an additive cyclic group G, with P as the generator and q as the order. Then, GCS randomly selects SKG ∈ Z∗ q as its private key and the corresponding PK is calculated by PKG = SKG ·P. We define three hash functions as: H1 : {0, 1}∗ → Z∗ q, H2 : {0, 1}∗ → {0, 1}l , and H3 : {0, 1}∗ → {0, 1}k, where l is the bit length of identity and k is the key length of the symmetric encryption method.

GCS keeps SKG secretly and publishes the public parameter: (n, q, P, PKG, H1, H2, H3). Registration: Every UAV registers with the GCS to get its pseudonym and public–private key pair, after which the GCS stores all the authentication information into the blockchain network. The communication channel in this phase is assumed to be secure, in the station's Intranet, for example. Noted that this phase is only executed once for each industrial mission and all the further interactions between drones and the GCS will be encrypted with shared keys. Take UAVi as an example to illustrate the concrete process.

1)UAVi sends Registation request = to GCS, where IDi is its real identity and OtherDetails refers to information that can confirm its legal status.

2) Receiving the Registation request, GCS first verifies the real identity of UAVi. The request will be aborted if the identity verification fails. Otherwise, GCS randomly chooses nonce ∈ Z∗ q, and then calculates SKi = H1(IDi||SKG||nonce), PKi = SKi · P, PIDi = IDi ⊕ H2(SKi · PKG), where PKi and SKi are public–private key pairs for UAVi while PIDi denotes its pseudonym. Next, GCS invokes saveInfo to upload the authentication information of UAVi into AIL. Finally, it sends Response = to UAVi.

3) UAVi keeps SKi as a secret and randomly selects di ∈ Z∗ q to calculate Di = di · P as its public DP. Di is uploaded to AIL via updateDP for the preparation of future authentication or key agreement and di is kept secretly as its private DP.

4) After registration, both GCS and UAVi can calculate keyGi = H3(SKi · PKG) separately, which can be used as shared keys for subsequent secure communications. GCS stores the PIDs, PKs, and public DPs of all registered UAVs of the industrial mission and send this information to drones, who keep this as a lightweight ledger. Each time a UAV updates its DP or the GCS adds or deletes new records, other UAVs can receive blockchain peer nodes' notification.

according to which they can change their own cached ledger. B. Message Authentication When drones receive messages that are not encrypted with shared keys they know, it is necessary for them to ensure the originator's identity as well as the integrity and freshness of these messages. Assume that UAVi wants to broadcast message M to other UAVs.

1)UAVi calculates f = di +SKi ·H1(PIDi||T||M), where di is its current private DP and T is the current timestamp. Then, it sends Auth{M} = PIDi||T||M||f to others.

2) When the remaining UAVs, take UAVj as an example, receiving Auth{M} = PID i ||T ||M ||f , it first checks timestamp T to judge the freshness of message M . After verification, UAVj searches its kept lightweight ledger to obtain PKi and Di of UAVi for checking whether the equation f ·P = Di+H1(PID i ||T ||M)·PKi is satisfied. UAVj accepts M only when the validation passes. The correctness can be confirmed by f · P = di · P + H1(PIDi||T||M) · SKi · P = Di + H1(PIDi||T||M) · PKi.(1) If the validation fails, UAVj will abort message M immediately. Noted that each DP can only be used once for signing messages; otherwise, the SKs may be leaked, so UAVs should call updateDP every time after signing a message to keep the freshness of DPs.

E. Key Agreement

The shared secret keys need to be maintained between two UAVs for encrypting their communications if confidentiality is required. We elaborate in the following how this key agreement can be achieved.

1) Assume that UAVi wants to have the shared key with UAVj. It first gets Kj and Dj of UAVj in its stored ledger and then calculates the session key by keyij = H3((SKi + di) · (PKj + Dj)), and deposits it as in its cache for a subsequent session key search. Finally, it randomly selects noncei ∈ Z∗ q and sends Request = PIDi||keyij(noncei) to UAVj. We note that noncei is secretly stored temporarily for subsequent verification.

2) After receiving the Request from UAVi, UAVj also gets PKi and Di from its ledger for calculating keyij = H3((SKj + dj)) · (PKi + Di)). Then, UAVj utilizes the keyij to decrypt keyij(noncei) for acqquiring noncei. If the decryption successes, UAVj will deposit in its cache and send Responce = H2(PIDi||PIDj)||keyij(noncei +1) to UAVi.

3) Upon getting the Responce, UAVi seeks its cache and finds keyij to decrypt keyij(noncei + 1). Then, it compares the obtained noncei + 1 with the stored noncei and judges the correctness. If the validation passes, UAVi will believe that it has negotiated the same session key with UAVj and they can begin confidential communication based on the shared key.

F. UAV Revocation

GCS should use deleteInfo to get rid of the authentication tuples of related UAVs in AIL if any UAVs lose connectivity or if the PKs created during the registration phase expire. Additionally, as soon as malicious conduct is recognized, the GCS should identify the suspect UAV and utilize deleteInfo to remove its record from AIL. The all blockchain peer nodes that are valid UAVs for the industrial mission notify the change of AIL, therefore these drones can be aware of the ones that are invalid and promptly remove the matching authentication data that is kept in their ledger.

G. Logic Correctness

Proof Based on BAN Logic In the following, we use the BAN logic, a formal model widely used to analyze the security of authentication schemes [29], to prove the logic correctness of our proposal. Several used notations and logical postulates in the BAN logic are listed as follows.
1) P |≡ X: Principal P believes statement X.
2) P ✁ X: Principal P sees statement X.
3) #(X): Formula X is fresh.
4) P |⇒ X: Principal P has jurisdiction over statement X.
5) P |∼ X: Principal P once said X.
6) {X}K: Formula X is encrypted by key K
7) P K ←→ Q: Principal P and principal Q use shared key K for communication. For logic derivation, we first need to transfer our proposal into idealized protocol model form.

H. Formal Verification Based on AVISPA

In order to create a collection of comprehensive, automatic analysis tools that are standard and intended to make it easier for protocol designers to examine their protocols, AVISPA transplants mature analysis tools with various propensities into a standard carrier [30]. It consists of four backends: SAT-based model-checker (SATMC), tree automata-based protocol analyzer (TA4SP), constraint-logic-based attack searcher (Cl-AtSe), and on-the-fly model-checker (OFMC). Only OFMC and Cl-AtSe are used to test our strategy because SATMC and TA4SP are incompatible with bitwise XOR operations.

Prior to being approved by AVISPA, a protocol must be described in the High Level Protocol Specification Language (HLPSL). Roles (participants in the protocol) and composition roles (sessions and environment) are the foundation of HLPSL. In our HLPSL specification, we define U1, U2, and U3 as three UAVs that represent the protocol participants. The intruder's knowledge includes each UAV's PID, PK and all exchanged messages.

Two types of security goals are specified.For the purpose of authentication, we need all receiving UAVs to authenticate the signed message and collective critical contributing variables. We need to keep the identities of all significant group contributors private in order to achieve our secrecy aims.. Fig. 3 shows the formal verification findings of message authentication and group key agreement simulated over the OFMC backend, as the group key agreement depends on the key agreement between two UAVs. In order to prevent repetition, we remove the simulation results on the Cl-AtSe backend because they are similar.

The findings indicate that our plan is capable of meeting all the needs for industrial UAV communications and is able to withstand both aggressive and passive attacks that are common in an industrial setting.

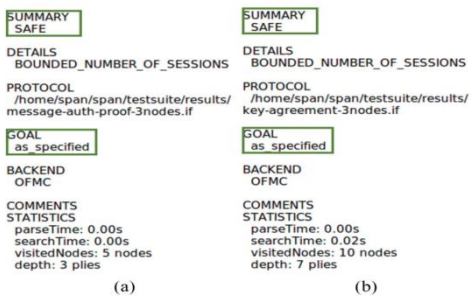


Fig. 3. AVISPA simulation results of authentication procedure for message authentication and group key agreement over OFMC. (a) Message authentication. (b) Group key agreement.

V.RESULT & DISCUSSION:

A. Security Analysis: Two hard problems, including the elliptic-curve discrete logarithm problem (ECDLP) and the computational Diffie– Hellman problem (CDHP) are the basis for our scheme, and the details can be found in [28]. Here, we give the analysis of how our scheme can meet all the security requirements mentioned in Section III.

B. Confidentiality: Shared keys generated based on the designed key agreement or group key agreement method can be used for encrypting communications, thus meeting the confidentiality requirement. Mutual Authentication: The correct calculation of

shared keys ensures that participants can verify each other's identity. Specifically, the shared key keyij = H3((SKj+dj)·(SKi+di)·P) contains private keys and private DPs of UAVi and UAVj, which are both kept secretly, ensuring the mutual authentication between participants. Conditional Anonymity: Pseudonyms are used during industrial missions and are updated before every task, preventing real identities from being revealed. Besides, when abnormal behaviors are detected, GCS can trace the real identity of the suspicious UAV by IDi = PIDi ⊕H2(SKi ·PKG), thus ensuring conditional anonymity.

C. Perfect Forward Secrecy: Part of the negotiated session keys between two UAVs are determined by their private DPs, which changes for each session key agreement. Therefore, even though the attacker has got the entities' private keys, it is impossible for him to compute the previous session keys because of the absence of private DPs. In addition, the group session keys are calculated by secret contributing factors that are randomly selected each time by all participant UAVs, so the leakage of private keys does not affect the security of previous group session keys.

D. Backward Secrecy: The group members are required to renegotiate the session key any time when new UAVs prepare to join or existing members want to leave, so new drones do not know the previous group key and those who have left cannot infer the subsequent key. Resistance to Cyberattacks: Our scheme can provide resilience against various cyberattacks as follows.

1) Impersonation Attack: Blockchain and the ECDLP hard problem prevent attackers from impersonating legitimated UAVs since they cannot get the correct associated private keys.

2) Replay Attack: The timestamp and one-way hash function can ensure the freshness of broadcast messages while the updating of DPs after each key negotiation can prevent repeated shared keys from applying.

3) Tampering Attack: Once the attacker modifies M in Auth{M}, the receiver calculates the wrong H1(PIDi||T||M) which cannot satisfy (1), thus leading to the detection of the message tampering.

4) DoS Attack: Our proposal inherits blockchain's resistance to the DoS attack. Peer nodes who maintain the AIL are organized by a distributed structure, which means that even if certain nodes are attacked, remain nodes can also support the same services to industrial UAVs. We also compare our scheme with some recent research related to IoT authentication in terms of the supported security features, as Table II shows.

Note that we only select several features that can typify the advantages of our proposal. The BPAS scheme proposed in [24] realized efficient message authentication in vehicular ad hoc networks with privacy preservation. However, the shared key agreement as the premise of confidential communication was not considered.

The key agreement scheme proposed in [18] is flexible and eliminates the management of revoked key list, but it is only limited to two entities. Guo et al. [17] and Yao et al. [25] considered confidential authentication from vehicles to the trust center but reliable interactions between vehicles were not discussed.

A certificateless group authenticated key agreement protocol for UAV networks was proposed in [12], but authors did not consider the mutual-healing feature and the revocation of UAVs. To sum up, our proposal supports the essential security properties and resists to various attacks.

VI.CONCLUSION:

We have developed a blockchain-assisted industrial UAV authentication service in this paper. Industrial drones can call smart contract APIs to access the ledger for the purpose of facilitating their authentication process.

The ledger is maintained by distributed blockchain peer nodes working together to ensure security. The ledger is implemented using elliptic-curve cryptography. BAN logic was used to demonstrate the scheme's logical correctness, and AVISPA was used for formal verification.

We implemented a prototype using the Hyperledger Fabric, and the outcomes demonstrate its efficacy for industrial UAVs in comparison to other IoT authentication techniques. Future research is being done to include anomaly detection techniques in order to improve industrial UAV system security even more.

VII.REFERENCES:

[1] "Business Guide to Industrial IoT (Industrial Internet of Things)." [Online]. Available: https://www.i-scoop.eu/internet-of-thingsiot/industrial-internet-things-iiot-saving-costs-innovation/ (accessed Sep. 2021).

[2] D. Wu, X. Han, Z. Yang, and R. Wang, "Exploiting transfer learning for emotion recognition under cloud-edge-client collaborations," IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 479–490, Feb. 2021.

[3] O. Maghazei and T. Netland, "Drones in manufacturing: Exploring opportunities for research and practice," J. Manuf. Technol. Manag., vol. 31, no. 6, pp. 1237–1259, Nov. 2020.

[4] S. Omari, P. Gohl, M. Burri, M. Achtelik, and R. Siegwart, “Visual industrial inspection using aerial robots,” in Proc. 3rd Int. Conf. Appl. Robot. Power Ind., Oct. 2014, pp. 1–5.

[5] Thara D. K., et al. "EEG Forecasting With Univariate and Multivariate Time Series Using Windowing and Baseline Method." *IJEHMC* vol.13, no.5 2022: pp.1-13. http://doi.org/10.4018/IJEHMC.315731

[6] M. Hossain, M. A. Hossain, and F. A. Sunny, “A UAV-based traffic monitoring system for smart cities,” in Proc. Int. Conf. Sustain. Technol. Ind. 4.0, Dhaka, Bangladesh, Dec. 2019, pp. 1–6.

[7] P. Tosato, D. Facinelli, M. Prada, L. Gemma, M. Rossi, and D. Brunelli, “An autonomous swarm of drones for industrial gas sensing applications,” in Proc. 20th Int. Symp. World Wireless Mobile Multimedia Netw., Washington, DC, USA, Jun. 2019, pp. 1–6.

[8] F. Nex and F. Remondino, “UAV for 3D mapping applications: A review,” Appl. Geomatics, vol. 6, no. 1, pp. 1–15, Mar. 2014.

[9] B. D. Song, K. Park, and J. Kim, “Persistent UAV delivery logistics: MILP formulation and efficient heuristic,” Comput. Ind. Eng., vol. 120, pp. 418–428, Jun. 2018.

[10] T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, and P. Fraga-Lamas, “Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management,” Sensors, vol. 19, no. 10, p. 2394, 2019.

[11] N. Shenets, “Security infrastructure of FANET based on secret sharing and authenticated encryption,” Autom. Control Comput. Sci., vol. 53, no. 8, pp. 857–864, Mar. 2020.

[11] Thara, D. K., and H. A. Vidya. "Detecting Insurance Fraud: A Study on Field Fires with Computer Vision and IoT." *International Journal of Advanced Scientific Innovation* 5.7 (2023).

[12] H. Xiong, Y. Wu, C. Jin, and S. Kumari, “Efficient and privacypreserving authentication protocol for heterogeneous systems in IIoT,” IEEE Internet Things J., vol. 7, no. 12, pp. 11713–11724, Dec. 2020.

[13] B. Semal, K. Markantonakis, and R. N. Akram, “A certificateless group authenticated key agreement protocol for secure communication in untrusted UAVs networks,” in Proc. IEEE/AIAA 37th Digit. Avionics Syst. Conf., London, U.K., Sep. 2018, pp. 1–8.

[14] P. B. G, T. D. K and T. K. N, "ML based methods XGBoost and Random Forest for Crop and Fertilizer Prediction," *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, Al-Khobar, Saudi Arabia, 2022, pp. 492-497, doi: 10.1109/CICN56167.2022.10008234.

[15] D. Wu, Z. Yang, B. Yang, R. Wang, and P. Zhang, “From centralized management to edge collaboration: A privacy-preserving task assignment framework for mobile crowdsensing,” IEEE Internet Things J., vol. 8, no. 6, pp. 4579–4589, Mar. 2021. [14] T. Jiang, H. Fang, and H. Wang.

.