A Secured Communication Model for Authenticated Data Transmission among Internet of Drones

PRITHVIRAJ.V

Vellore Institute of Technology, Vellore, Tamil Nadu, India 632014

---***---

Abstract - *The Internet of Drones (IoD) is a layered network control system primarily designed to coordinate the connectivity of unmanned aerial vehicles. We propose a cloud integrated IoD architecture and put forth a software architecture for the cloud-based management of drones linked via Internet .In this paper we focus on securing the identity or location of clients who want to get access to the drones that are connected through internet and have a common cloud database. By implementing the software architecture proposed in this paper, users can have flexible access to the stored data in a secured way .It also limits the level of access being given to the untrusted cloud service providers.*

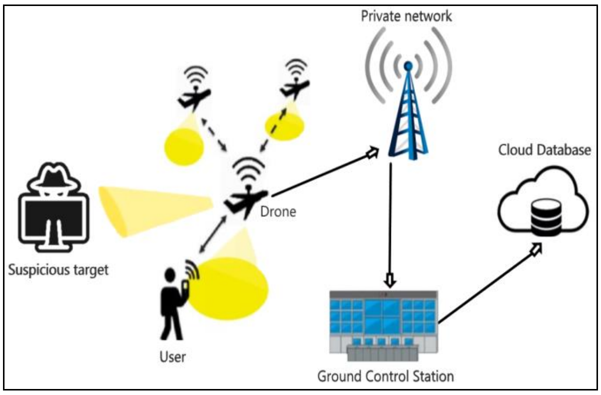

FIGURE: 1

Key Words: ***Cloud integrated IoD, Data privacy protection, Data encryption and decryption*****, zone service providers (ZSPs) , Pseudonyms , IMEI Code**

1. INTRODUCTION

Internet of drones is a fast growing concept in the modern world because of its capability of being deployed in various utilizations such as traffic monitoring, package delivery, military operations, infrastructure inspection, search and rescue, modern agriculture .A user can control and assign certain missions to the drones and collect data of interest. All the real time data are collected by the drones with the help of sensors that are present in them and it is sent to the ground base station .From there it is outsourced to the cloud where data is stored and analyzed. And only during this transfer of data between ground station and the cloud where the hackers plan to attack. This creates high security threats as the cloud contains all sensitive data regarding the user which also includes his current location. The data regarding location of the user can be misused in several ways.

We will face a number of challenges if we try protecting the IoD cloud data with existing security techniques. Nowadays even security mechanisms that include sophisticated cipher mechanisms are also easily broken by the powerful attackers of the era of cloud computing. We have also not developed that powerful drones that have high computing power and also that are capable of performing complex encryption and decryption of vast content (e.g., CCTV footage) .When personalized IOD cloud data is being stored on common cloud servers; it becomes vulnerable to attacks by other cloud tenants

2. RELATED WORKS

Preserving the user's location privacy is highly important whenever the user tries to connect with the drones .In [1], the author proposes a scheme for WSN (wireless sensor networks) that secures the privacy of source location. This paper incorporates the concept of cluster based anonymization where the cluster heads periodically generates some random identities. Therefore during the communication, the original identities of source node are anonymized by the random identities that have been already generated.

Despite several works on the concept of location privacy, researchers fail to maintain the quality of location based service (LBS) when they just emphasis more on the idea of anonymization through the concepts of Cloaking region, Dummy node, Silence period, etc. .In [2], they have combined the ideas of Cloaking region and Dummy node and have come up with a better location privacy scheme based on node density. They have also proved that the chances for an external adversary to track the target node are reduced, through the stimulation results.

In [3], the author develops the concept of cluster anonymization for location based services (LBS); the target vehicle's location is further enclosed by providing a cloaking algorithm that is based on some privacy metrics such as k-anonymity and l –diversity. In[4] ,for the users and location service providers to have mutual transformations between the pseudo location that is created to enhance location privacy and the original location, the uses a tool called function generator that periodically generates the parameter of spatial transformation.

In [5], for Vehicular Ad-Hoc Networks (VANET), the author comes up with a pseudonym scheme that provides full anonymity that is totally controlled by the users themselves

.In [6], the structured nature of spectrum databases (DBs) is surpassed by harnessing probabilistic set membership data so that location privacy can be further guaranteed as users can query DB without having to share their actual location with DB .In[7],the author uses and also considers network coding as an important technique of cloud storage as it recovers data with high reliability and very negligible repair bandwidth. But often during the transmission of data between the local datacenter and its remote backup site, the data is eavesdropped by the external adversaries. So the paper includes enhanced network coded data recovery system that includes several system nodes and precisely designed link capacity between the datacenter and the backup site.

In [8], the author proposes a new cognitive approach of developing a heterogeneous multi-server architecture that prevents the location-based service (LBS) queries from directly connecting to the query issuers. Despite several pseudonym changing strategies, the location privacy of VANET's (vehicular ad-hoc networks) users is in great threat when a pseudonym linking attack is done. Therefore in [9], various pseudonym strategies are analyzed and compared with respect to several criteria. In [10], the author sets the base for the concept of internet of drones using which several researchers later build upon using their ideas. He has given us an IoD architecture which is based on the most three vital networks like the air traffic control network, the cellular network, and the Internet.

In [11], the author has proposed a two tier light-weight network coding system based on the concept of pseudonyms. His scheme is successful against the harmful external adversaries as well as the untrusted cloud database. For a user to communicate with a drone first he has to be authenticated by that particular drone and a secret key is established between them. Therefore in [12], the author proposes a credential based anonymous lightweight user authentication mechanism known as TCALAS.

In [13], the concept of changing pseudonyms in regular intervals known as the silence period is introduced so that a malicious user fails to find his/her target. In [14], the paper focuses on a unique pseudonym technique of generating a pseudonym that cannot be linked with any other pseudonyms and also it is designed based on cryptographic method in such a way that it cannot be reversed also. In [15], Bayesian approach is initiated to rectify the problem of changing frequencies, thus improvising the pseudonym mechanism .In [16], the attacker is confused and also mislead through false location data (dummies) that are sent along with the actual location data .The paper shows that the privacy attacks can be avoided to a large extent if dummy-based techniques are combined with anonymization techniques.

3. Pseudonym-Based Location Privacy Protection:

At present, researchers who have used the concept of pseudonyms have been quite successful in enhancing the privacy and security issues of users while sharing their confidential data with drone and its cloud database. The tradeoff between originality and reliability can be radically achieved with pseudonyms. This concept of pseudonyms includes the technique of protecting the privacy of location by disconnecting a user's identity with his\her true identity .By doing so the attackers will never be able to connect to the particular user by stealing their location data .In order to avoid the attackers to distinguish the spatial difference from other members, the pseudonyms must be periodically changed.

4. CHALLENGES:

- During the authentication process, if an Outsourced Data Base (ODB) provider is able to connect a specific pseudonym to its ODB stored data, then it becomes impossible for the current pseudonym strategies to completely secure data ownership.
- And also using this technique increases the possibility of collision of drones with each other. The drones fail to identify its authenticated user because his real identity is hidden with a pseudonym and this leads to confusion among drones and collision takes place. We need better airspace management with effective real-time navigation so that diversified incidents (eg: Damages of drone arising to catastrophe of life and property)can be cleared off. For illustration, at a particular time the drones have to function and explore within a particular region without getting digressed from the endorsed fight assignment, for which the pertinent person in charge has to authorize the drones.
- Physically dynamic tracing attack is a major threat if this method is adopted. Such attacks cannot be resisted even if user's identities are hidden through pseudonyms.
- Upgrading pseudonyms and certificates regularly can result in high computing costs. For resource-constrained drones, that is not a viable option.

5. IN OUR PAPER:

Current protection and privacy technologies are typically designed to combat attacks by external adversaries. But internal attackers like a retailer and employer should not be overlooked because of their level of exposure to confidential data and collaboration with an outside attacker. For example: Approved drones or Zone Service Providers (ZSP) managers reveal information on drone navigation to an external intruder .All the above mentioned points should be under high consideration during the designing of a security model to minimize vulnerability.

So in this paper, we have come up with Authentication and data protection solutions protecting privacy which deals with both insider as well as outsider attackers. We are going to develop our security model based on the IOD architecture proposed by Gharibi, Boutaba, and Waslander. As we have discussed earlier we need to develop an architecture that ensures that the drones work in a systematic way so that they avoid collisions and utilize the airspace to the fullest so that they bring out greater productivity to the users. *Airspace is the resource that drones use.* Therefore, the airspace is divided into zones which have its own sets of nodes and intersections.

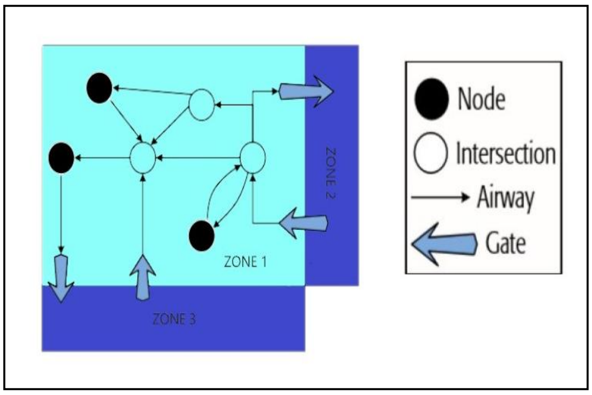

FIGURE: 2

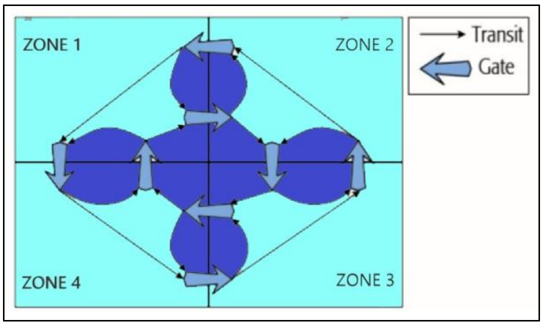

FIGURE: 3

We also have included the term known as zone service providers (ZSPs). The cloud is being linked to All ZSPs and drones. In each region, each ZSP provides the requesting drones with navigation information between any two elements in its specified area. ZSPs are the main architectural controllers, ZSPs is not only providing navigation information but also controlling a drone to hold, travel to a specific location or hang for some time at a point .For each and every drone, which is flying in a specific zone, has a corresponding ZSP that would send across the congestion detection task to get the quickest possible driving route for that specific drone in its defined area. When entering each ZSP's coverage area, the drone recovers a response from the ZSP, and finally arrives at a destination.

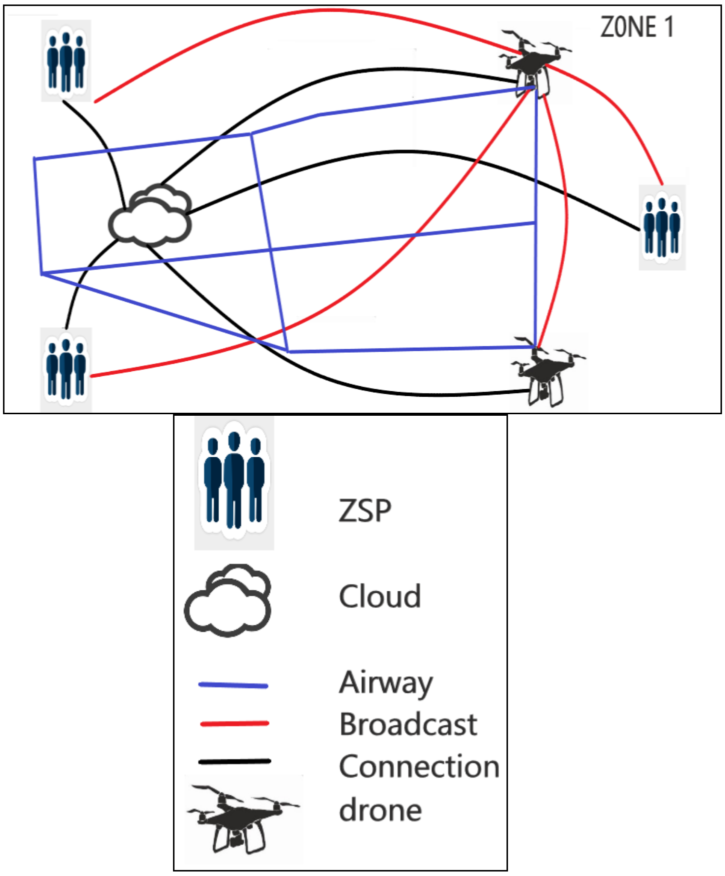

FIGURE: 4

Meanwhile, private details of the drone (e.g., original location of drones, owners or working firms, foremost route of travel) may be geographically close. A particular person may be connected with these private details and it may disclose details about once lifestyle ending up in profiling or loss of privacy, for example: location-based "spam" (i.e., companies that use location information to promote unsolicited product or service marketing). In addition, an intruder can use the location to deduce political opinions, health status or personal preferences of an individual, as well as performing a physical assault (for example, stalking or robbery). ZSPs and drones often share navigation information thus forming a vital control and feedback system; hence it becomes a loophole for attackers who try to breach the network, albeit for different reasons. In the case of successful denial of service (DoS) attacks, spoofing attacks or any other dangerous injection of data, IoD management, operation and control may crash or be disabled .Only with the help of security auditing and inspection by third parties, we will be able to detect these types of attacks.

Therefore we encrypt the navigation data of the requester in our security model (i.e., the destination and source address) along with a unique IMEI code and password created by the users who want to communicate with the drones.

5.1 SECURITY MODEL:

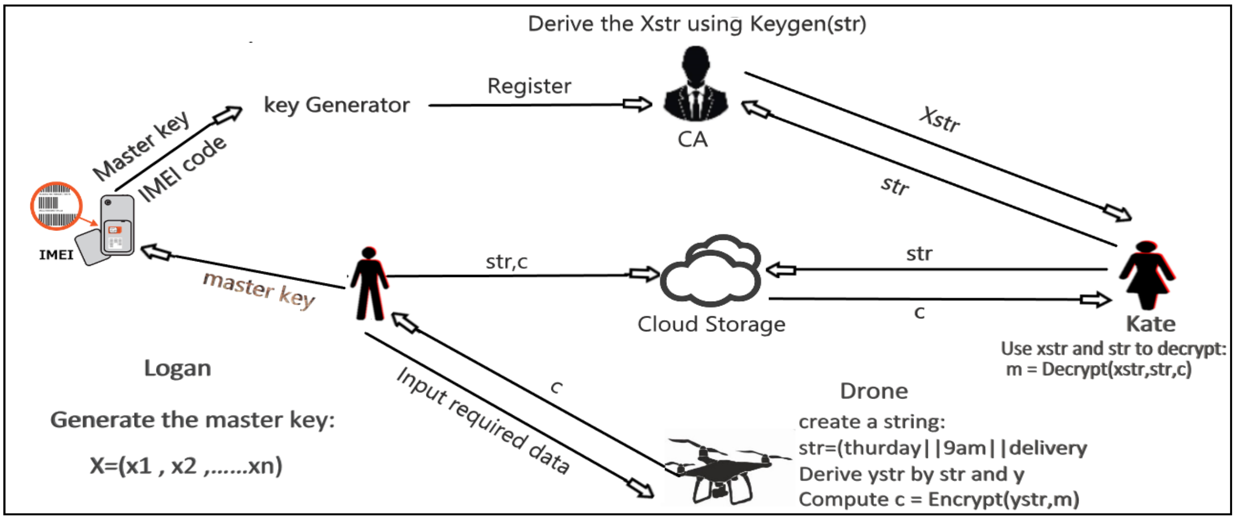

FIGURE 5:

In our model, drone-collected data is transferred to the cloud for processing and it not only guarantees data confidentiality but also provides access to the outsourced data in a flexible way. As the storage site is not reliable, only the certificate authority (CA) (i.e. acting as a trustworthy party and not colluding with others) manages the access control within the system.

Logan is the user who wants to store the shared data in the cloud and Kate is the other user who wishes to access the data shared by Logan. Logan then starts by generating the master key X = (x_1, x_2… $x_{n)}$ through the setup algorithm.

5.2 ENCRYPTION OF DATA:

First, all the important data (m) related to the task assigned to the drone (such as when, where, at what time) has to be collected .Then a string str is generated by Logan's drones according to a pre-agreed syntax such as str =(Thursday||9am||package delivery). Now, the data (m) has to be encrypted by the drones. Hence the drones make use of the above generated string and a public key $y_{str} = \sum h_i(str) \cdot y_i$ is derived by the parameter Y = (y_1, y_2, ..., y_n) to encrypt m where h(·) is a collision resistant one-way hash function .Finally the cipher text is sent to the cloud for further processing and storage by Logan. And then the master key generated by Logan is combined with his unique IMEI code and then it is passed through a key generator which ends up generating a strong unique passcode that is impossible to crack by the hackers. Then it is registered in the CA (Certified authority) with some additional instructions.

5.3 IMEI CODE:

So in our security model we have implemented the idea of IMEI code. The International Mobile Equipment Identity (IMEI) number is a special identifier or serial number that all cell phones and smartphones have. Normally fifteen digits long. You will find the IMEI number on the silver sticker at the back of our phone, under the battery pack. Or we need to just dial *#06# to get the unique IMEI code for every mobile phone. Therefore, combining the IMEI code of the user along with their usual passwords and then converting it into a string using a key generator strengthens the security level more than the concept of pseudonyms. In case even when some unauthorized people try to get access to the drone, their device can be blacklisted using its IMEI number which renders it useless to anyone else, even if they swap out the SIM.

5.4 DECRYPTION OF DATA:

If Kate wants to access the data collected under any str (received from Logan), the CA has to be contacted by her for permission. The Keygen(str) is run by the CA to extract the corresponding secret key $x_{str}= x_i(str) \cdot x_i$ via the same string as str = (Thursday||9am||package delivery) after performing the necessary tests. At last, the data which has been previously encrypted by the drones using the same string (str), is now decrypted by Kate using $x_{str.}$

6. RESULT ANALYSIS:

Now we will analyze how our security model can effectively ensure the security of data and achieve sharing. Most importantly ,all the data is being encrypted using y_{str} ,therefore the contents of a drone's data cloud could not be accessed and eventually the cloud fails to find the corresponding secret key x_{str} which is required to learn the drone's data and thereby the data of other drones can be hardly accessed by any unauthorized party . Because y_{str} which is derived from the string str encrypts every minute detail of data fetched by a drone. Even though Logan is authorized to access the data which has been encrypted using str, he is not allowed by the secret key x_{str} to decrypt the non-encrypted cipher text using y_{str}. Moreover, only the important data related to the task assigned by the user is stored by the drone's sensor. Any of the useful data from the storage site obtained by the target drone will not reach the attacker through a compromised or malicious drone. Finally, we may license any other individual or a group to access the data, using appropriate certificates.

7. CONCLUSION:

The future is not too far for it to depend on the concept of IoD. At the same time we should be constantly working to improvise the protection and privacy of data obtained from drones and to outsource data to the cloud safely and efficiently. We present a typical IoD architecture in this article and identify many private and security issues, such as privacy leakage and also make sure that data is shared in a safe and efficient way. We have developed a model that will limit both the insider as well as outsider attackers. Despite all the developments that have been made on this particular context, there is still lot many aspects that have to be looked upon In the future works.

REFERENCES:

1. A. Gurjar and A. R. B. Patil, "Cluster based anonymization for source location privacy in wireless sensor network," in Proc. Int. Conf. Commun. Syst. Netw. Technol., 2013, pp. 248–251
2. K. Miura and F. Sato, "A hybrid method of user privacy protection for location based services," in Proc. Int. Conf. Complex Intell. Softw. Intensive Syst., 2013, pp. 434–439.
3. B. Ying and D. Makrakis, "Protecting location privacy with clustering anonymization in vehicular networks," in Proc. IEEE Conf. Comput. Commun. Workshops, Toronto, ON, Canada, 2014, pp. 305–310.
4. T. Peng, Q. Liu, and G. Wang, "Enhanced location privacy preserving scheme in location-based services," IEEE Syst. J., vol. 11, no. 1, pp. 219–230, Mar. 2017.
5. D. Forster, F. Kargl, and H. Lohr, "PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-hoc Networks (VANET)," VNC, 2014, pp. 25–32.
6. M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Location privacy preservation in database-driven wireless cognitive networks through encrypted probabilistic data structures," IEEE Trans. Cogn. Commun. Netw., vol. 3, no. 2, pp. 255–266, Jun. 2017.
7. Y.-J. Chen, L.-C. Wang, and C.-H. Liao, "Eavesdropping prevention for network coding encrypted cloud storage systems," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 8, pp. 2261–2273, Aug. 2016.
8. M. Han et al., "Cognitive approach for location privacy protection," IEEE Access, vol. 6, pp. 13466–13477, 2018.
9. A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 770–790, 1st Quart., 2018
10. M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," IEEE Access, vol. 4, 2016, pp. 1148–62.
11. Yu-Jia Chen , Member, IEEE, and Li-Chun Wang , Fellow, IEEE," Privacy Protection for Internet of Drones: A Network Coding Approach,". VOL. 6, NO. 2, APRIL 2019
12. Jangirala Srinivas,Ashuk Kumar Das,Neeraj Kumar,Joel J.P.C Rodrigues."TCALAS:Temporal Credential-Based Anonymous Lightweight Envirenment",IEEE Transactions on Vechicular Technology.2019
13. R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.
14. S. Guo, D. Zeng, and Y. Xiang, "Chameleon Hashing for secure and privacy-preserving vehicular communications," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 11, pp. 2794–2803, Nov. 2014.
15. X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in Proc. IEEE Conf. Comput. Commun., 2013, pp. 2985–2993.
16. B. Niu, S. Gao, F. Li, H. Li, and Z. Lu, "Protection of location privacy in continuous LBSs against adversaries with background information," in Proc. Int. Conf. Comput. Netw. Commun. (ICNC), 2016, pp. 1–6.
17. T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," IEEE Access, vol. 4, pp. 673–687, 2016.
18. J. Lim, H. Yu, K. Kim, M. Kim, and S.-B. Lee, "Preserving location privacy of connected vehicles with highly accurate location updates," IEEE Commun. Lett., vol. 21, no. 3, pp. 540–543, Mar. 2017.
19. R. Yu et al., "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," IEEE Trans. Depend. Secure Comput., vol. 13, no. 1, pp. 93–105, Jan./Feb. 2016.
20. B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," IEEE Commun. Lett., vol. 17, no. 8, pp. 1524–1527, Aug. 2013.
21. Z. Zhu and G. Cao, "Toward privacy preserving and collusion resistance in a location proof updating system," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64, Jan. 2013
22.] Z. Montazeri, A. Houmansadr, and H. Pishro-Nik, "Achieving perfect location privacy in wireless devices using anonymization," IEEE Trans. Inf. Forensics Security, vol. 12, no. 11, pp. 2683–2698, Nov. 2017.