

# Secure and Privacy -Preserving Data Access Management IOD Systems in Distributed Cloud Networks

<sup>1</sup> Chivukula Venkata Sai Saketh Ram

PG Scholar, Department of Computer Science & Engineering, Siddhartha Institute of Technology and Sciences, Hyderabad, India.

<sup>2</sup> Mr. S. Ramesh

Assistant Professor, Department of Computer Science & Engineering, Siddhartha Institute of Technology and Sciences,

## ABSTRACT

The emerging combination of Internet of Things (IoT) and 6G communication techniques has stimulated the Internet of Unmanned Aerial Vehicles (UAVs), i.e., Internet of Drones (IoD). To accommodate and share the enormous real-time UAV data, Cloud-based IoD is an inevitable choice to lower the heavy burden of mobile UAVs. Nevertheless, how to protect highly sensitive UAV data in such a honest-but-curious, open and distributed environment with resource-limited UAVs is a significant challenge. Although our previous work (PATLDAC) in SPNCE'21 devises a cloud-based UAV data access control scheme with policy privacy protection, limited access time and user traceability, it incurs inflexible and centralized cloud data storage and access as well as untrustworthy metadata in untrusted cloud environment for data access and user tracing. To this end, we further propose a blockchain-based privacy-aware data access control (BPADAC) scheme for distributed and secure UAV data sharing in Cloud-based IoD. Based on fine-grained, traceable and privacy-preserving UAV data access characteristic of our previous work, we extend it by leveraging blockchain and Distributed Hash Table (DHT) for distributed and trustful UAV data access and storage, together with reliable and limited access mechanism to guarantee cloud UAV data sharing service provision. We also design public and undeniable user tracing mechanism to prevent user key abuse with traitor denial.

## 1. INTRODUCTION

The fast growth of Internet of Things (IoT) and 6G communication techniques recently have promoted the promising Unmanned Aerial Vehicles (UAVs) applications. The massive ubiquitous access provided by 6G

ground stations (GS) and powerful connection capacity among smart devices of IoT facilitate the emerging Internet of Drone (IoD) which enables interconnected UAVs to be deployed in various fields for task execution involving traffic

supervision, disastrous rescue, good delivery and so on. Especially, with the help of the integrated networks of satellite communications, and ground communications, UAV groups are qualified for their tasks in more complex environment. During the IoD task completion process, collecting and tackling enormous UAV data for analysis and prediction is a heavy burden for drones with limited resources.

## 2. LITERATURE SURVEY

The study aims to conduct big data analysis (BDA) on the massive data generated in the smart city Internet of things (IoT), make the smart city change to the direction of fine governance and efficient and safe data processing. Aiming at the multi-source data collected in the smart city, the study introduces the deep learning (DL) algorithm while using BDA, and puts forward the distributed parallelism strategy of convolutional neural network (CNN). Meantime, the digital twins (DTs) and multi-hop transmission technology are introduced to construct the smart city DTs multi-hop transmission IoT- BDA system based on DL, and further simulate and analyze the performance of the system. The results reveal that in the energy efficiency analysis of model data transmission, the energy efficiency first increases and then

decrease as the minimum energy collected  $\alpha_0$  increases. But a more suitable power diversion factor  $\rho$  is crucial to the signal transmission energy efficiency of the IoT-BDA system. The prediction accuracy of the model is analyzed and it suggests that the accuracy of the constructed system reaches 97.80%, which is at least 2.24% higher than the DL algorithm adopted by other scholars. Regarding the data transmission performance of the constructed system, it is found that when the successful transmission probability is 100% and the exponential distribution parameters  $\lambda$  is valued 0.01 ~0.05, it is the closest to the actual result, and the

data delay is the smallest, which is maintained at the ms level. To sum up, improving the smart city's IoT-BDA system using the DL approach can reduce data transmission delay, improve data forecasting accuracy, and offer actual efficacy, providing experimental references for the digital development of smart cities in the future.

## 3. SYSTEM ANALYSIS

### 3.1 EXISTING SYSTEM:

The new combination of Internet of Things (IoT) and 6G communication technology Internet of Unmanned Aerial Vehicles (UAV), i.e. Internet of Drones (IoD).To

accommodate and share large amounts of real-time UAV data, cloud-based IoD is an inevitable choice. It relieves the heavy burden on mobile UAVs. Nevertheless, collecting highly sensitive UAV data in one is a big challenge. To protect such an honest, yet curious, open and distributed environment with resource-constrained UAVs.

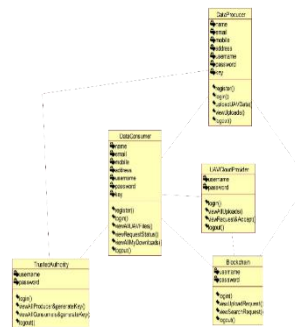
### 3.2 PROPOSED SYSTEM:

We present a block chain-based privacy-aware data access control (BPADAC) scheme for distributed and secure UAV data sharing in Cloud-based IoD setting based on the block chain and DHT-based distributed storage and data access as well as public and undeniable traceability together with trustworthy access time limitation and attribute privacy protection technique.

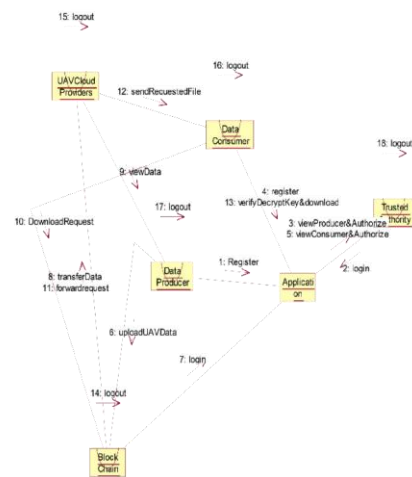
The system model of our proposed BPADAC. The system involves five generic entities, that is, Trusted Authority (TA), UAV Cloud Providers (UCPs), Block chain (BC), Data Producer (DP) and Data Consumer (DC).

## 4. SYSTEM DESIGN

### 4.1 CLASS DIAGRAM



### 4.2 COLLABORATION DIAGRAM



## 5. IMPLEMENTATION

### Module description

#### TRUSTED AUTHORITY

Here trusted authority is a module can directly login with the application, after successful login he can view all consumer, producer details and generate appropriate keys then send to their mail id.

#### Data Producer

Here data producer is a module, should register with the application and should be authorized by the trusted authority by

generating transformation key and send to mail, after successful authorization , producer can login into his/her account then can have chance to upload UAVData to block chain and view Uploaded data.

**BLOCKCHAIN**

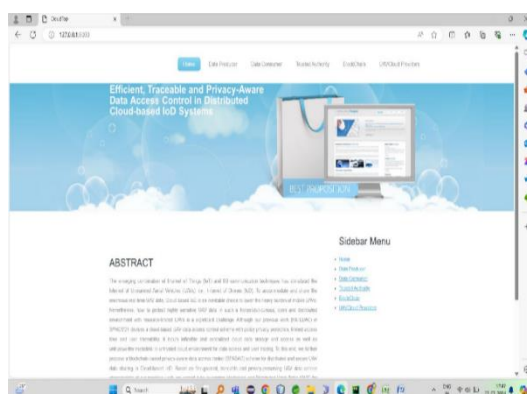
Here blockchain is a module can directly login with the application, after successful login he can view UAV data sent by the producer and transfer to cloud.

And also this module can view download request from data consumer and send to cloud.

**UAVCLOUDPROVIDER**

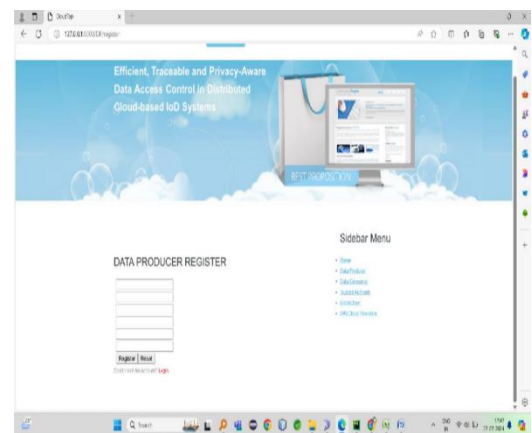
Here cloud provider is a module can directly login with the application, after successful login he can view UAV data sent by the blockcain And also this module can view file request from blockcain and send to consumer.

**6. SCREENSHOTS**



**7. CONCLUSION**

In this paper, after deeply analyzing the problems of UAV data sharing in Cloud-based IoD systems, we proposed a blockchain-based privacy-aware data access control (BPADAC) scheme for distributed and secure UAV data sharing in



such a mobile and distributed large-scale environment and gave its formal models and definitions with detailed constructions. With the help of blockchain and CP-ABE techniques, BPADAC achieves fine-grained and distributed data access such that any privileged data user has the ability to access UAV data through blockchain. In the meantime, the UAV data sharing service can be guaranteed through the mechanism of limited access times. Moreover, multi-cloud combining with DHT technique can store large-scale UAV data in a distributed and scalable way, and eliminate the drawbacks of traditional centralized cloud. Partial policy hiding is

employed by BPADAC to provide access policy privacy protection for outsourced UAV data in clouds. Furthermore, BPADAC is able to deal with traitor tracing efficiently and publicly by utilizing public user tracing approach without any denial. In addition, the security and performance analysis with a prototype implemented on Ethereum blockchain provide strong evidences that BPADAC is secure and suitable for UAV data sharing in Cloud-based IoD systems. Our future work will be devoted to study the identification problems of UAV data source and outsourced UAV data in Cloud-based IoD systems

## 8. REFERENCES

- I. X. Li, H. Liu, W. Wang, Y. Zheng, H. Lv, and Z. Lv, "Big data analysis of the internet of things in the digital twins of smart city based on deep learning," *Future Generation Computer Systems*, vol. 128, pp. 167–177, 2022.
- II. F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6g for the metaverse," *IEEE Wireless Communications*, 2022, doi:10.1109/MWC.019.2100721.
- III. M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywiólek, and I. Ullah, "Swarm of uavs for network management in 6g: A technical review," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 1–761, 2022.
- IV. Z. Na, C. Ji, B. Lin, and N. Zhang, "Joint optimization of trajectory and resource allocation in secure uav relaying communications for internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16 284–16 296, 2022.
- V. S. Yu, A. K. Das, Y. Park, and P. Lorenz, "Slap-iod: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments," *IEEE Transactions on Vehicular Technology*, vol. 71, no.