Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 5s (2025)

# UAV Based Data Access Communication Control in Distributed Hash Table Mechanism

**Shaik Mohammad Rafi[1], Dr. R Yogesh Rajkumar[2]**

[1]Research Scholar, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India. Email: shaikrafi17@gmail.com

[2]Assistant Professor, Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, India. Email: yogeshrajkumar.it@bharathuniv.ac.in

***Article History:***

***Received:*** *04-10-2024*

***Revised:*** *27-11-2024*

***Accepted:*** *04-12-2024*

**Abstract:**

The combination of Internet of Things ( IoT ) and aeronautical integration, made possible by satellite and 6G technology for communication, has led to the emergence of the World Wide Web of unmanned aerial vehicles, or UAVs, often referred to as the Internet of Drones (IoD). Using cloud-based Connectivity of Predators (IoD) is a necessary choice to reduce the heavy workload that mobile UAVs and enable the storing and exchange of massive quantities of actual time UAV data. Protecting highly sensitive UAV data in a transparent, curious, open, and decentralized environment, while operating UAVs with limited resources, is a significant challenge. In our previous research project, SPNCE'21, we introduced a system called PATLDAC that devised a method for managing and regulating access to unmanned aerial vehicle (UAV) data stored in the cloud. This scheme offers robust policy privacy protection, restricted access duration, and comprehensive user traceability. Nevertheless, there are several disadvantages associated with it, such as rigid and centralized storage and retrieval of data in the cloud, as well as unreliable information in an untrustworthy cloud environment for accessing data and tracking users. To accomplish this goal, we propose the implementation of a method known as a blockchain-based privacy-aware control of data access (BPADAC) to securely share UAV data in an internet-based Internet of Drones (IoD) setting. Expanding on the detailed, trackable, and privacy-protecting features of our prior research, we improve it by integrating blockchain and Decentralized Hash Table (DHT) technology. This enables the decentralized and dependable access and storage the UAV data, combined with a secure and limited access method. The objective is to guarantee the delivery of cloud-based Unmanned Aerial Vehicle (UAV) data sharing services. Furthermore, we provide a strong and unquestionable user tracking mechanism to protect against the abuse of user keys and denial by traitors. In the end, we conduct a thorough security study and develop a working model of the system using the smart contracts of the Ethereum blockchain. The purpose of this is to assess the system's efficacy and showcase the feasibility of BPADAC.

**Keywords**: Internet of Things (IoT), Internet of Drones (IoD) ,blockchain technology, Cipher text-Policy Attribute-Based Cryptography (CP-ABE), Disguised Access Policy, Decentralized Hash Table (DHT) Technology.

## I. INTRODUCTION

Cloud computing depends on networks within data centers to provide interconnections between storage and server systems, making use of different network equipment such as switches, routers, firewalls, and load balancers. Cloud computing is the technology that supports the hosting of many distributed applications, such as search engines, social media platforms, banking services, computationally intensive and applications for data analytics [1]. Distributed applications function over several servers to provide improved scalability, reliability, and performance, enabling them to handle bigger workloads. These apps generate a significant volume of traffic that must be efficiently handled by the servers processing the requests plus the network responsible for sending the traffic.

The proliferation of the web in the Internet of Things (IoT) and the incorporation of aeronautical technology into satellite and 6G communication networks have recently enhanced the potential applications of Unmanned Aerial Vehicles (UAVs). The extensive accessibility of 6G earth stations (GS) [3] and the substantial communication capacity among smart devices of IoT [4] facilitate the advancement of the Internet of Drone (IoD) [5]. This enables the deployment of networked Unmanned Aerial Vehicles (UAVs) in various locations to carry out duties such as monitoring traffic, responding to disasters, and delivering packages. By utilizing integrated satellite and ground communication networks [6], [7], groups of unmanned aerial vehicles (UAVs) are able to carry out their tasks in complex situations. While working on the IoD assignment, drones that have limited resources have a major obstacle in collecting and analyzing vast quantities of UAV information to perform predictive and analytical purposes [8]. Cloud-based Web of Drones (IoD) systems are especially engineered to provide an ideal platform for the exchange and delegation of UAV data, while efficiently overseeing sufficient resources. However, the information collected by unmanned aerial vehicles (UAVs) usually covers a large geographical region and includes significant amounts of sensitive data, such as location-related and GPS signals [9]. If this data is compromised on a cloud that is operated by a trustworthy but inquisitive party, there might be severe and disastrous outcomes. Hence, the security concerns related to the storage of unmanned aerial vehicle (UAV) data in a mobile, cloud-based Network of Drones (IoD) system pose a substantial and challenging undertaking.

In order to tackle the security concern of sharing UAV data in cloud-based Internet of Drones (IoD), it is advisable to employ data access control through the utilization of Cipher text-Policy Attribute-Based Encryption (CP-ABE) [10], [11], [12], [13], [14], [15], [16], [17], [18]. This technology guarantees the protection of data and exact control over who may access it by allowing data owners to establish specific access policies that dictate the privileges of data users in relation to encrypted data stored in the cloud. However, conventional CP-ABE methods face several substantial challenges when applied in mobile cloud-based Internet for Devices (IoD) systems. At first, the access restrictions in the encrypted texts of classic CP-ABE structures, which are in clear text, are vulnerable to privacy violations [19]. For instance, let's examine a situation in which an access policy is implemented for the encrypted data in an Internet of Things (IoT) system. Any anyone who obtains the policy can infer the information pertaining to the particular users using the shared UAV data. The utilization of Unmanned Aerial Vehicles (UAVs), especially in military contexts, will have a significantly negative impact. Zeng et al. [20] or Li et al. [21] have created two standard model systems for safeguarding privacy in access policy by partially concealing the access policy. Nevertheless, the efficacy of UAV data encryption and decryption in such scenarios is unsatisfactory.

Moreover, the stored in the cloud IoD system's UAV data contains a significant quantity of sensitive information, which creates a possibility for insiders to gain profit by sharing their login credentials with other individuals. This form of assault, referred to as key abusing attack, has the potential to lead to the unauthorized disclosure of Unmanned Aerial Vehicle (UAV) data, which may include classified military information. The challenge arises in cloud data access control when employing traditional CP-ABE solutions, since they lack the ability to precisely identify an unauthorized user just based on their common decryption essential which is associated with a specific set of attributes. A number of researchers have created traceable CP-ABE methods [22], [23], [24] by including traceable mechanisms into CP-ABE approaches. A commonly used technique is white-box individual tracing, where the user's identity is combined with their decryption key in a manner that simplifies the detection of a betrayer. Several existing white-box traceable CP-ABE platforms [25], [26], [27] are either computationally challenging for tracing a traitor or impose a substantial burden on a centralized user tracing authority that is responsible for maintaining a database of users for individual user tracing. Moreover, these techniques are incapable of reducing the risk of being turned down by treachery after user tracking. Hence, it is imperative to address the urgent matter of improving user monitoring and publicly exposing the betrayer in a manner that leaves no room for denial. This is particularly crucial when employing traceable CP-ABE in stored in the cloud Internet of Things (also called IoT) systems. In addition, based on the cloud Internet of Things, or IoT, networks are located in a susceptible environment that makes them susceptible to various external risks, such as replay attacks, impersonation assaults, sniffing and catching attacks, tampering attacks, as well as Denial of Service (DoS) attacks, among others [28]. The most serious of these common assaults is the Denial of Service ( or DoS ) assault which can disable the data and service delivery from the cloud to Uas data consumers. An adversarial individual possesses the ability to consistently infiltrate the data exchange system with the intention of depleting the resources for the public internet and causing disruptions in data availability. This might lead to the denial of requests from Uas data consumers, which can have potentially catastrophic effects, especially in military and rescue missions. Hence, it is imperative to consider this vital aspect while establishing access control for data in cloud-based Internet of Detectives (IoD) systems for the purpose of exchanging UAV data. Several CP-ABE approaches [29], [30], [31] have recently been used to restrict the amount and duration of data access. Nevertheless, these alterations lead to substantial computational expenses for access verification, rendering them inappropriate for stored in the cloud Internet of Drones (IoD) platforms that employ UAV devices with restricted resources. In addition, the UAV a group of IoD systems frequently function in a dynamic setting and are situated in distinct areas from the data collected by UAV recipients. This requires the use of distributed data storage and retrieval. Therefore, it is essential to ascertain the approach for deploying Internet of Drones (IoD) technologies in a decentralized environment, where access to manned aerial vehicle (UAV) data is spread out, restricted, and comprehensive, in the presence of a substantial volume of data. This is especially crucial when it comes to exchanging Unmanned Aerial Vehicle (UAV) data via cloud-based Internet of Drones (IoD) systems. Figure 1 illustrates a cloud-based application that is distributed across many locations.

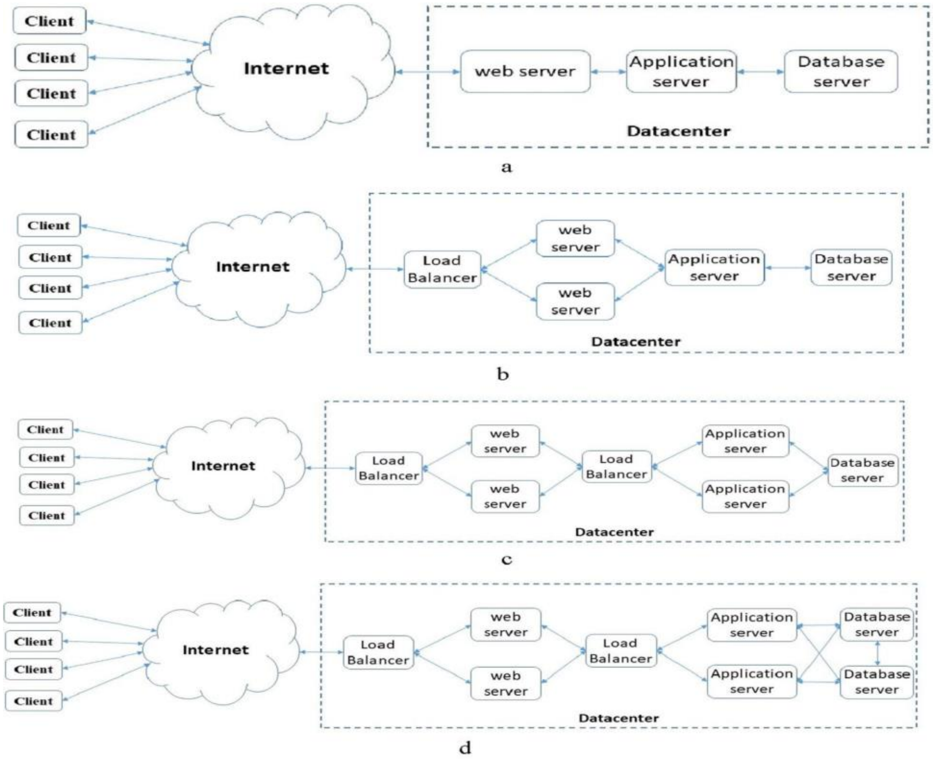

**Figure 1: Distributed Cloud-Based Application**

## II. CONTRIBUTIONS

After analyzing the listed difficulties, it is clear that they provide considerable challenges for cloud-based Network of Drones (IoD) systems for data interchange for UAVs. In our earlier study [32], we introduced a cloud-based system called PATLDAC. This system effectively deals with concerns related to privacy breaches, denial-of-service assaults, and the misuse of user keys by betrayers. PATLDAC offers robust measures for ensuring data confidentiality, precise control over access permissions, safeguarding policy privacy, restricting access duration, and maintaining user traceability. Nevertheless, it is unable to effectively manage distributed data storage, a critical need for enabling scalability in Internet of Things of Drones (IoD) systems that create substantial volumes of data. Moreover, the use of metadata for retrieving data and imposing time restrictions poses significant security vulnerabilities in the context of cloud computing. This can potentially lead to the abuse of privileges when accessing data, especially in situations where unmanned aerial vehicle ( UAV ) data is stored across multiple locations. Furthermore, the persons implicated by PATLDAC are given the opportunity to challenge and disprove their deceitful behaviors. This study presents a solution called blockchain-based privacy-aware control of information access (BPADAC) for securely sharing UAV data in cloud-based the web of Drones (IoD) systems, while considering the above problems. The BPADAC method expands on the characteristics of our prior PATLDAC work, incorporating detailed, verifiable, and privacy-preserving access to UAV data. BPADAC enhances the security of storing and exchanging data for unmanned aerial vehicles (UAVs) on the mobile cloud-based internet of Drones (IoD). It accomplishes this by integrating blockchain and Distributed Hash Tabulation (DHT) methodologies. The scheme's objective is to permit distributed access and storage of data, provide secure data sharing services, safeguard attribute integrity in access policies, enable traitor tracing, and minimize computing costs.

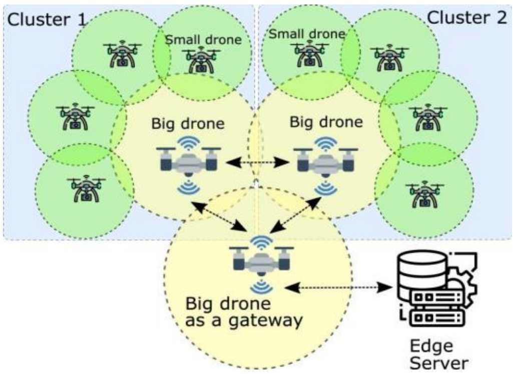

**Figure 2 illustrates the IoD Architecture incorporating the integration of Edge Computing and Blockchain.**

The distinct contributions made by this research, when contrasted with our previous work, were as follows:

Data retrieval that is decentralized, limited, and dependable. In a distributed Network of Drones (IoD) system, data collected by unmanned aircraft (UAVs) is stored in many decentralized clouds. Blockchain technology is employed to offer distributed access control, guaranteeing both security and dependability. In order to reduce the likelihood of DoS attacks on the unmanned aerial vehicle data sharing use, which can happen when unapproved individuals excessively utilize up cloud resources, new BPADAC system combines blockchain and access control mechanisms. This integration allows the system to implement a specific time restriction for authorized users to access data, resolving a constraint in our earlier efforts.

Unambiguous and easily understood identification of betrayers, with a primary emphasis on efficiency and protection. BPADAC employs a public white-box tracking mechanism to tackle the problem of key misuse. This solution enables any entity within the system to easily and effectively detect betrayers, without the need to keep a user list in a centralized certifying authority. BPADAC use blockchain systems to securely document irrefutable proof of treasonous activities, guaranteeing that traitors cannot deny their conduct. Furthermore, via a comprehensive analysis of efficiency carried out by a substantial number of experiments, BPADAC exhibits exceptional performance in both the encryption and decryption of data. This is accomplished by employing online/offline encryption and delegated decryption testing techniques. Furthermore, we offer a comprehensive security framework for BPADAC, together with the corresponding verifications, which were omitted in our previous release.

## III. METHODOLOGY

The proposed architecture involves the scattering and encoding of users' data immediately upon data transmission over diverse and varied networks. After being securely stored, the data is subsequently spread throughout a network of interconnected blocks. The recommended framework's procedural process is depicted.

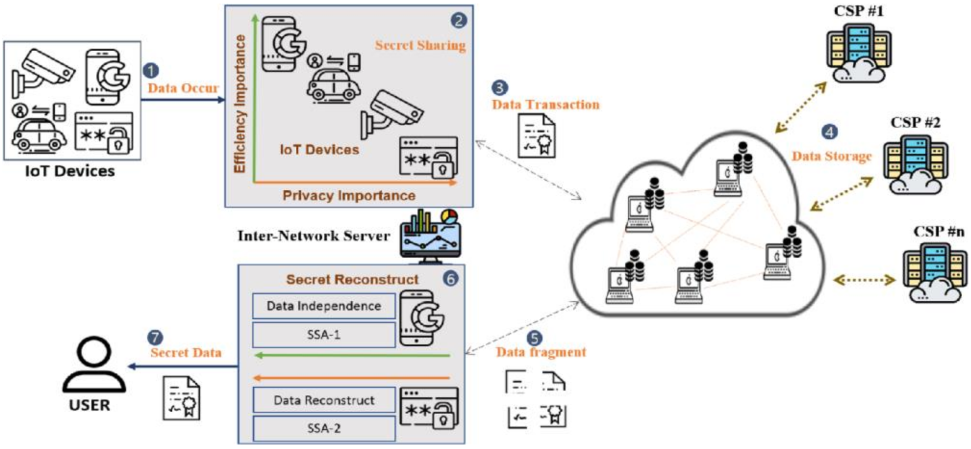

**Figure 3: The Methodological Flow of the Proposed Architecture.**

- The data gathered by the Internet of Things (IoT) devices at the Sensor Layer is transmitted to the Inter-Network Server, which is situated within the owner's Trust Domain. To ensure the security of the raw data collected from various IoT devices, it is essential to protect it during transmission between the device and the inter-network server using appropriate processing methods.

- Data analysis: The process of data processing categorizes information from IoT devices according to their level of privacy and efficiency of communication. The data is protected by the use of the Secret Sharing method. The Secret Share algorithm may be categorized into two forms, and data is disseminated using Random Value within Inter-Network Server. The Inter-Network Server generates two values, R1 and R2, in a random manner. The R1 XORs are derived by applying the exclusive Nand operation to each bit of the original encoded information S. The data is partitioned based on the value of a binary variable. If the variable is equal to 1, the data is allocated to S1. If the variable is equal to 0, the data is allocated to S2. The data is scrambled using two Secrets Sharing computations, S1 and S2, depending on the desired level of secrecy for the data.

- The Inter-Network Server may generate transactions on a consortium chain composed of cloud service providers (CSPs) by utilizing Data Transactions. These transactions employ shared knowledge S1, S2, and S3, and employ Secret Sharing techniques. The blocks included into the consortium's blockchain contain the CSPs' knowledge, including the Hash Number of the dispersed confidential data. This guarantees the accuracy and reliability of the data that is transmitted by the Inter-Network Server. Block data can be stored in chains, hence ensuring the integrity of the block data. If the user, who is the owner of the data, is unable to retrieve the secret data, the block data can be inspected to verify the credibility of the information given by a certain Cloud Services Provider (CSP).

- Secret communication: The safe distribution of secret data S to S1 and S2 in an Inter-Network Server can be accomplished by utilizing R2 of R1, R2. Presently, the Secret Sharing technique is divided into two scalable techniques that take into account the Privacy Importance in relation to the diverse system environment. The Secret Sharing Algorithmic (SSA-1) is primarily concerned with the transmission of information.

- The smart contract is the most often employed application of blockchain technology in many businesses, alongside crypto currency. A smart contract, or smart contract, is a protocol that involves a series of logical computations executed on the blockchain according to pre-established conditions. The solution is deployed on a blockchain platform, enabling automated execution of verification of results without human intervention. A smart contract is a computer program that allows for programmability over the blockchain. Smart contracts produce immutable and reliable results.

- In the next part, the system model and the experimental analysis will be presented.

- The graphic depicts the system model that we proposed BPADAC. The system consists of five essential entities: Trustworthy Authority (TA), UAV Clouds Providers (UCPs), Crypto currency (BC), Data Product (DP), and Data Consumption (DC). Their powers are elucidated in meticulous detail below.

- The TA is responsible for the implementation of the system, as well as the registration and authorization of users. During the registration procedure, the Teaching Assistant verifies the user's identification and thereafter distributes the decryption keys plus transformation keys. After completing the registration process in TA, every user is qualified to take part in the distributed ledger.

- UCP is a versatile platform that focuses on providing users with a broad selection of various and varied UAV information services, along with unlimited processing and storage capacities. The system consists of many clouds, each linked to a certain provider of services, and is given a unique address using a random allocation procedure utilizing DHT. When users share or download files, their IP address is used to locate the relevant provider of cloud services within the UCP.

- BC stands for blockchain, a technology that provides secure and immutable data storage, and it also offers an open and decentralized access method, among other characteristics. Our strategy use blockchain technology to store public parameters and limit data access time, therefore protecting UCP services from potential assaults like DDoS. Furthermore, BC acts as a mediator between users and UCP when it comes to data sourcing and access. Blockchain technology may be used in the public individual monitoring process to capture undeniable proof of a malicious user's desire to reveal their keys for illegal financial profit.

- Data Processing (DP) refers to a variety of UAVs (unmanned aerial vehicles) that have the ability to produce or gather significant quantities of temporal UAV data. To minimize storage costs for UAVs with scarce resources, it has been suggested to transfer the data to a centralized processing unit (UCP) using blockchain (BC) technology. This will involve documenting the evidence of uploading for the data that is outsourced, which includes the identification of the cloud service provider responsible for storing this data, along with their respective names and addresses.

- DC refers to UAV data consumers who want to assess and get relevant insights utilizing machine learning approaches. Authorized domain control centers (DCs) have the privilege to access the necessary UAV (unmanned aerial vehicle) data available in the universal communications platform (UCP) using a distributed blockchain (BC) system. Furthermore, BC will record proof of data transfers. Furthermore, BC will validate if the access times of the UAV data exceed its maximum threshold and record the identities of malicious DCs for the purpose of transparent and publicly available user monitoring.

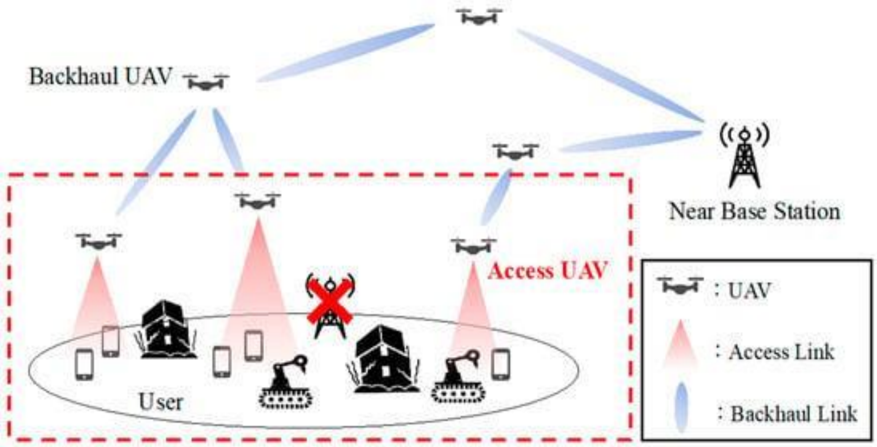

**Figure 4: A System Model**

### *Analysis of Security*

Within the system we have, the TA (trusted institution) is regarded as an entirely dependable entity. The tasks of the system include the establishment of system settings and the provision of keys to users over an encrypted way. UCP is categorized as semi-honest, which indicates that it dutifully performs data exporting and access procedures but may also participate in passive attacks. DP is highly regarded for its unwavering dependability and accountability in producing a substantial volume of unmanned aerial vehicle (UAV) data, which will thereafter be delegated to UCP. There is no motivation to begin attacks on the system. The DC is deemed untrustworthy inside the system as the UAV network structure functions in an open and intricate environment. Both individuals and organizations can freely engage in the framework to communicate UAV data without the need for any specific rights. Even a trustworthy individual who has authorized accessibility to a data center, referred to as an insider, has the ability to deliberately reveal their passwords for illegal financial profit and then deny any evidence that may prove their guilt. Hence, the next segment offers a succinct summary of the possible risks to our system.

### *Possible manifestations of assault:*

An eavesdropping attack is the illegal act of intercepting data that is being broadcast in a wireless Drone network. This enables an institution to have access to crucial information and acquire shared data in the UCP despite requiring consent or cooperation from other unlawful parties.

Data tampering attack involves the modification of decrypted results by providers according to the UCP. This attack occurs when a data center (DC) accesses unmanned aerial vehicle (UAV) data shared on the unmanned control plane (UCP), causing disruption within the local decryption procedure inside the data center (DC).

The privacy leakage attack happens when an entity gains access to the shared Uavs data in UCP and is able to infer sensitive information from an access policy associated with the encrypted text in UCP, leading to a significant data breach.

A key abuse assault may be carried out by any unlawful insider, indicating that any authorized information controller has the capability to disclose their keys to external persons for illegal financial profit.

A Distributed Denial of Service (DDoS) attack poses a substantial risk to data service providers, especially those operating in broad and intricate settings like internet-based cloud networks. Any company may utilize the UCP network to establish connections with many clouds and launch an attack against a specific cloud service provider, causing disruption to their data services.

***Prerequisites for guaranteeing security***

Exerting meticulous command over information access and guaranteeing the preservation of confidentiality: Our system must prioritize the preservation of data confidentiality in order to protect important details in UAV information and to prevent unauthorized access to the data by addressing any security breaches as early as possible.

Data integrity protection encompasses the implementation of strategies and safeguards aimed at guaranteeing the precision, coherence, and dependability of data. It is crucial to verify the correctness and integrity of the decrypted data acquired from the User Control Panel (UCP) with the Data Center (DC) in our system to reduce the potential dangers that accompany a second possible attack. Ensuring the preservation of privacy through the implementation of an access policy: When considering the third possible attack, it is crucial to assess the facts pertaining to the features of the access policy within our system. Enforcing public user tracking is crucial for detecting malicious insiders within our system. If a fourth possible assault occurs, all entities within our system should possess the capacity to reveal the real identify of these insiders as soon as their abnormal activities are detected. Meanwhile, the identified traitor is unable to deny the incontrovertible evidence.

Restrict the time periods during which authorized data centers may access data: Given the possibility of an attack, it is crucial that our system can check the data time to access before UCP provides external decryption services. The security analysis of the smart city environment is ensured by the implementation of protocols that enable the secure flow of data to the cloud in the Empowered Cloud Architecture. It places importance on factors like as privacy, honesty and effectiveness, capacity, and decentralization. The table provides a juxtaposition of the existing research investigations and the proposed architecture. Privacy: We have incorporated a confidential sharing idea into the inter-network layer of the planned smart city architecture. The 1st algorithm (SSA-1) in the recommended architecture ensures compliance with the privacy and confidentiality requirements. For example, let's consider the Secret data of devices in the Internet of Things (S), which is denoted by the decimal number 24 and its binary representation is (11000).2. The secret is divided into two halves, S1 and S2, with the quantity of k being 2. Let's choose two random integers, which we will call R1 and R2. Let R1 be equal to 7 in binary form (00111)2 and R2 be equal to 11 is binary form (01011).The number 2. We are employing two naturally occurring prime quantities for their robust security and distinctiveness.

**Algorithm1**. If the XOR procedure between S and R1, specifically (11000)2 XOR (00111)2, results in (11111)2 and not (00000)2, then it employs the S2 secret distributed sharing data. Alternatively, we employ S1. The equation expresses the polynomial function y(t).

The equation provided is a polynomial equation expressed as $y(t) = 24 + 7t + 11t^2$. Furthermore, the notation Wt—1 = (t, y(t)) is employed to represent a specific point located on the graph of the equation. The user's input is "(2)".

**Algorithm 1**: Secret Sharing (SSA)

**Input:** S, Sensitive data acquired via Internet of Things (IoT) devices.

**Outcome**: Information that is sent in a decentralized manner through the use of secret sharing Sentence 1. Sentence 2.

**Method:**

1: The Random generation () method yields a tuple (R1, R2).The process of generating random keys

The function Rotate key length (R1, R2) provides the parameters of R1 and R2.* Rotation keys following defined protocols

3: Iterate over each element s in the collection S

4: If the modulus of s divided by the length of key R1 is zero, distribute the details as S1, S2, S3, and subsequently increment the value of pos Value by 1. 4: if the modulus of the pos Value multiplied by 2 is equal to 0.

If the output of the XOR operation involving s and R1 equals true, the execute S1. 6: Alternatively, if the outcome of the exclusive OR operator among s and R1 is not true, proceed to perform S2. Terminate the loop at 7.

8: The Smart Contract executes the transaction by utilizing the aggregated values of S1 is the supply and R2, as well as the aggregated numbers of S2 and R2.

**Method 2**: Transaction Validation

The user's text: PKu denotes the publicly available key of the entity responsible for initiating the transaction, whereas T indicates the activity that has to be verified.

**Output**: A binary number representing either true or false.

1: H is the outcome of implementing the authorized signature verification technique, Ver, on the inputs PKu, T, and Sigt.

2: If H is true, then return True.

4: alternatively The statement "5" is false.

6: conclude the conditional statement

Establish a secure key exchange between the parties PK and PKu, resulting in the generation of a public key PKu and a corresponding secret key SKu. The data controller (DC) chooses a random value zu of the set ZN to serve as the secret key SKu = zu. The DC calculates the public key provided by the user PKu through setting the function h to zu, using a system-wide public key PK. Once developed, DP/DC will be integrated into the blockchain network. The system will utilize the blockchain to store information about them, access cloud data, and monitor malicious users through an exchange T = (IDu, TS, Action, Sigt) that is authenticated using their secret key. The "Sigt" in a transaction generated by DP/DC denotes the cryptographic signature of the transaction T, which is created by utilizing the secret key of DP/DC supplied by IDu.

The recommended design ensures data integrity by utilizing Blockchain technology, namely at the fog layer. Blockchain is a cryptography system that merges many blocks together. The term "hash chain" is used to describe this structure, as each block has its own hash value, along with the hash value of the previous block, a timestamp, and encrypted data underlying IoT transactions. The data is transferred from the inter-network plane and serves as a method of secret sharing to encrypt IoT data.

bT is defined as the data block that contains the Tth transaction. Here, m and n denote the hash function utilized in the blockchain network.

The equation (3) expresses the correlation between the parameter DT and the integers of hT—1 and m(YT).

The equation hT represents the product of H and DT.The user's input is the number "4".

By utilizing these techniques, we may improve the ability to scale of storing Internet of Things (IoT) data in the public internet, when compared to the traditional approach. The reason for this is that blockchain networks are capable of effectively and swiftly verifying or validating the IoT data, and then storing them in the cloud storage of the recommended architecture. The cost of holding per transaction is governed by the following factors: Equation 5:

The equation (5) may be written as F = log2q + 2log2p bits.

Hence, it can be inferred that our proposed architecture provides superior scalability as a more optimized framework for storing IoT information throughout the cloud, as compared to the previous architecture or model.

**TABLE 1: The gas cost of BPADAC**

| Operation | Size(Bytes) | GAS | Ether |
|---|---|---|---|
| Encryption | 1805 | 128451 | 0.00025498 |
| Decryption | 575 | 50121 | 0.00010021 |
| User Trace | 400 | 35792 | 0.00007154 |

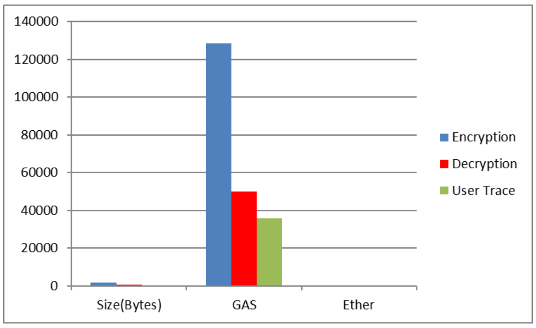

Figure 5: The gas cost of BPADAC

Area Under Curve (AUC) is a metric used to measure the performance of a classification model. It quantifies the ability of the model to distinguish between different classes by calculating the area under the receiver operating characteristic (ROC) curve.

The performance metric we use is the area under the curve (AUC), which provides a comprehensive measure of performance across all potential classification thresholds. The AUC represents the classification performance, with a higher value indicating a better classifier. When the AUC is equal to 1, the classifier achieves perfect accuracy when the threshold is appropriately selected. The below equations elucidate the methodology for computing the Area Under the Curve (AUC).

The formula for false positive rate (FPR) is calculated by dividing the number of false positives (FP) by the sum of false positives and true negatives (TN). Specificity is equal to 1 minus the false positive rate (FPR). The area under the curve (AUC) is calculated by adding the specificity and recall, and then dividing the sum by 2.

The findings depicted in Figure demonstrate that the SVM classifier has the greatest AUC, signifying its superior ability to differentiate between normal and aberrant behavior when compared to other approaches.

**Table 2: The performance of the proposed method in comparison with other techniques.**

| Performance Measure | SVM | NB | DT | LR |
|---|---|---|---|---|
| Recall | 96.21 | 88.41 | 91.54 | 80.11 |
| Precision | 95.12 | 88.77 | 93.81 | 82.2 |
| F-score | 97.01 | 93.10 | 95.3 | 84.15 |

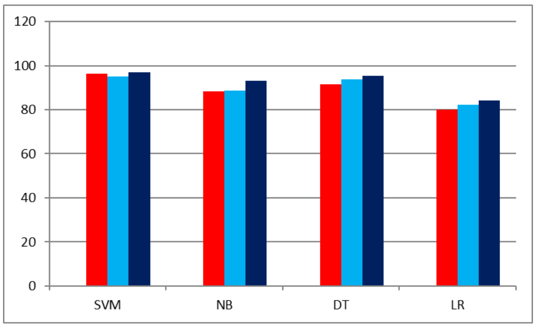

**Figure 6: The performance of the proposed method in comparison with other techniques.**

## V.CONCLUSION

This research focuses on addressing the challenges associated with sharing UAV data in cloud-based Internet of Drones (IoD) systems. We have developed a privacy-aware data management scheme called Blockchain-based Privacy-Aware Info Access Control System (BPADAC) to enable secure and distributed sharing of UAV data in large-scale mobile settings. We have also provided formal models, definitions, and detailed buildings for this scheme. BPADAC utilizes blockchain and CP-ABE methods to provide precise and decentralized data access. This allows privileged users to access UAV data over the blockchain. Meanwhile, the provision of the UAV sharing of data service may be ensured by implementing a mechanism that restricts access to certain time periods. Furthermore, the utilization of multi-cloud in conjunction with the Distributed Hash Table (DHT) technology enables the storage of vast amounts of Unmanned Aerial Vehicle (UAV) data in a distributed and scalable manner, while also eliminating the limitations associated with typical centralized cloud systems. BPADAC uses partial policy masking to safeguard the privacy of access policies for UAV data stored in cloud environments. Moreover, BPADAC effectively and openly handles traitor tracing by employing a public user tracing method without any kind of denial. Furthermore, the security and efficiency research conducted using a prototype built on the Ethereum blockchain yield compelling evidence that BPADAC is both secure and well-suited for exchanging UAV data in cloud-based Internet of Drones (IoD) systems. Our future research will focus on investigating the challenges associated with identifying the source of UAV data and managing outsourced Quadcopter data in cloud-based Internet of Drones (IoD) systems.

## REFERENCES

[1] 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 Gener. Comput. Syst., vol. 128, pp. 167–177, Mar. 2022.

[2] F. Tang, X. Chen, M. Zhao, and N. Kato, ‘‘The roadmap of communication and networking in 6G for the metaverse,’’ IEEE Wireless Commun., early access, Jun. 24, 2022, doi: 10.1109/MWC.019.2100721.

[3] M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. ywiolek, and I. Ullah, ‘‘Swarm of UAVs for network management in 6G: A technical review,’’ IEEE Trans. Netw. Service Manag., vol. 20, no. 1, pp. 741–761, Mar. 2023.

[4] 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 Things J., vol. 9, no. 17, pp. 16284–16296, Sep. 2022.

[5] 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 Trans. Veh. Technol., vol. 71, no. 10, pp. 10374–10388, Oct. 2022.

[6] W. Wang, T. Chen, R. Ding, G. Seco-Granados, L. You, and X. Gao, ‘‘Location-based timing advance estimation for 5G integrated LEO satellite communications,’’ IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6002–6017, Jun. 2021.

[7] H. Xu, Z. Chen, H. Liu, L. Chang, T. Huang, S. Ye, L. Zhang, and C. Du, ‘‘Single-fed dual-circularly polarized stacked dielectric resonator antenna for K/Ka-bandUAVsatellite communications,’’ IEEE Trans. Veh. Technol., vol. 71, no. 4, pp. 4449–4453, Apr. 2022.

[8] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, ‘‘A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks,’’ Ad Hoc Netw., vol. 133, Aug. 2022, Art. no. 102894.

[9] Y. Dang, C. Benzaid, B. Yang, T. Taleb, and Y. Shen, ‘‘Deep-ensemblelearning- based GPS spoofing detection for cellular-connected UAVs,’’ IEEE Internet Things J., vol. 9, no. 24, pp. 25068–25085, Dec. 2022.

[10] J. Zhang, J. Ma, T. Li, and Q. Jiang, ‘‘Efficient hierarchical and timesensitive data sharing with user revocation in mobile crowdsensing,’’ Secur. Commun. Netw., vol. 2021, pp. 1–17, Feb. 2021.

[11] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, ‘‘Enabling efficient data sharing with auditable user revocation for IoV systems,’’ IEEE Syst. J., vol. 16, no. 1, pp. 1355–1366, Mar. 2022.

[12] S. Das and S. Namasudra, ‘‘Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure,’’ IEEE Trans. Ind.\ Informat., vol. 19, no. 1, pp. 821–829, Jan. 2023.

[13] Q. Tong, Y. Miao, H. Li, X. Liu, and R. Deng, ‘‘Privacy-preserving ranked spatial keyword query in mobile cloud-assisted fog computing,’’ IEEE Trans. Mobile Comput., early access, Dec. 13, 2022, doi: 10.1109/TMC.2021.3134711.

[14] Y. Li, J. Ma, Y. Miao, Y. Wang, T. Yang, X. Liu, and K.-K.-R. Choo, ‘‘Traceable and controllable encrypted cloud image search in multi-user settings,’’ IEEE Trans. Cloud Comput., vol. 10, no. 4, pp. 2936–2948, Oct. 2022.

[15] Y. Guo, Z. Lu, H. Ge, and J. Li, ‘‘Revocable blockchain-aided attributebased encryption with escrow-free in cloud storage,’’ IEEE Trans. Comput., early access, Jan. 5, 2023, doi: 10.1109/TC.2023.3234210.

[16] R.Senthamil Selvan “INTEGRATING THE BIGDATA ANALYTICS AND DEEP LEARNING analysis human movement to improve the sports” by 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISSN:0018-9219,E-ISSN:1558-2256,December 2023. 10.1109/AECE59614.2023.10428236.

[17] R.Senthamil Selvan “MULTI OBJECTIVES EVALUATOR MODEL DEVELOPMENT FOR ANALYZE THE CUSTOMER BEHAVIOUS” by 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISSN:0018-9219,E-ISSN:1558-2256,December 2023. 10.1109/AECE59614.2023.10428189.

[18] R.Senthamil Selvan “Cloud Computing Based Medical Activity Supporting System” by 2024 2nd International Conference on Disruptive Technologies (ICDT) on 15th and 16th March 2024, 10.1109/ICDT61202.2024.10489245, ISSN:0018-9219,E-ISSN:1558-2256,11 April 2024

[19] I. Odun-Ayo, M. Ananya, F. Agono, and R. Goddy-Worlu, ‘‘Cloud computing architecture: A critical analysis,” 18th International Conference on Computational Science and Applications (ICCSA), Melbourne, VIC, pp. 1–7, 2018.

[20] Rath M. Resource provision and QoS support with added security for client side applications in cloud computing. Int J Inform Technol 2019;11(2):357–64.

[21] Li X, Li K, Ding Y, Wei D, Ma X. Application of autonomous monitoring method based on distributed environment deployment in network fault. J Phys ConfSer 2020;1486:022048.

[22] Deng S, Xiang Z, Taheri J, Mohammad KA, Yin J, Zomaya A, et al. Optimal application deployment in resource constrained distributed edges. IEEE Trans Mob Comput 2020.

[23] Syed HJ, Gani A, Ahmad RW, Khan MK, Ahmed AIA. Cloud monitoring: a review, taxonomy, and open research issues. J Netw Comput Appl 2017;98:11–26.

[24] M. Akter, M. M. S. Maswood, S. S. Sonia and A. G. Alharbi, ‘‘A Novel Approach to Reduce Bandwidth Cost and Balance Network and Server Level Load in Intra Data Center Network,” 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, pp. 194-198, 2020.