IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An optimal Fuzzy and Secure Data Encryption in Cloud

Deephika siva S
Information Technology
National Engineering college
Kovilpatti, India

Mathumitha A
Information Technology
National Engineering College
Kovilpatti, India

Jerart Julus L
Information Technology
National Engineering College
Kovilpatti, India

***Abstract*—In the cloud-assisted internet of things, it presents a flexible privacy-preserving data sharing (FPDS) approach (IoT). An IoT user can encrypt data and send it to a receiver using the FPDS scheme, which uses identity-based encryption. A data owner can use identity based encryption (IBE) to restrict access to his data by encrypting it with the intended recipient's public identification address. As a result, only the authorized user with his own secret key may access the outsourced data. In particular, the data owner can create an access policy to generate a delegation credential, which the cloud can use to turn any encrypted data that meets the access policy into cypher text accessible by a new receiver. The purpose of the FPDS scheme is to secure under the IBE scheme's security. Informally, unless the associated private keys are accessible, an attacker cannot identify the (original or converted) cypher texts of two equal-length messages. As a result, the confidentiality of data that is outsourced is effectively secured. The FPDS system accomplishes delegation security while maintaining security. Informally, an attacker possessing delegation credentials and private keys can collude with customer service representatives and data users. The attacker cannot convert any cypher text unless it knows the associated delegation credential or the private key to the cypher text, according to the FPDS scheme. Based on the foregoing studies, the suggested FPDS method provides an efficient data sharing conversion mechanism. Without conducting costly decryption and encryption operations, a data owner can encrypt his data with numerous keywords and then share it with a data consumer by establishing an access policy.**

Keywords— cloud,IoT, FPDS, cipher,IBE

I. INTRODUCTION

Cloud-based IoT has become increasingly popular technology, as the performance of IoT applications can be greatly improved by sending a cloud to handle large IoT data. To protect the confidentiality of data extracted from IoT devices to the cloud, cryptographic methods are often used to encrypt data in such a way that only the user selected by the data owner can decrypt the data. However, in an area with high IoT users, encrypted data may also need to be shared to more users than previously mentioned. In this paper, we propose a flexible cloud-based data sharing system (FPDS) on cloud-assisted IoT. With the FPDS system, an IoT user can encrypt data to recipients using proprietary-based encryption. More importantly, an IoT user can specify a fine-grained access policy to create a unique identifier, and then send this certificate to the cloud so that it can convert all encrypted data satisfying the access policy into readable new scripts. In this way, IoT users can share cloud-based data in a flexible and secure manner. With the rapid development of wireless communication technology, Internet of Things (IoT) has become a promising paradigm that greatly facilitates Internet communication and real-world virtual reality. In IoT, all everyday objects ("objects") can be connected to the Internet, creating a network of connected objects everywhere, in order to trade and transmit information and data. The integration of all of these factors will contribute to automation analysis, machine intelligence and decision-making ability, and support a wide range of applications in various areas such as health care, pollution monitoring, logistics, home security, and so on. It uses an effective proxy re-encryption system in the IBE framework to help reduce overhead on the user side while ensuring flexible data sharing between subscribers and even partners. Generates an access control policy for registered users, and assigns this policy to a set of subscribers who can access content, and encrypts the content object using IBE, that is, generates an encrypted power block, and sends the power block to the storage route. We are investigating how we can adapt and securely exported IoT data to the cloud. Like the above-mentioned solutions, we protect the privacy of external data with encryption-based encryption.

A. Cloud Architecture

Multiple cloud components communicate with one another using application programming interfaces (APIs), which are often web services. The front end and the back end are the two most important components of cloud computing architecture. The component that the customer sees is called the front end. This comprises the client network or computer, as well as the apps that employ a user interface like a web browser to reach the cloud. The cloud, which consists of multiple computers, servers, and data storage devices, is the back end of the cloud computing architecture.

From the lowest layer to the top layer, cloud services can be supplied in a variety of ways, with each layer representing a different service model. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are the three main cloud delivery types (IaaS). IaaS is provided at the lowest layer, where resources are pooled and controlled either physically (e.g., Emu lab) or virtually (e.g., Amazon EC2), and services are delivered based on storage (e.g., GoogleFS), network (e.g., Open flow), or processing capabilities (e.g., Hadoop Map Reduce). Platform as a Service (PaaS) is supplied by the intermediate layer, where services are given as an environment for programming (e.g., Django) or software execution (e.g., Google App Engine).

Software as a Service (SaaS) is a top-layer service in which a cloud provider restricts client freedom by only providing software applications as a service. In order to administer a big cloud system, the cloud provider maintains a suite of management tools and facilities (for example, service instance life-cycle management, metering and billing, and dynamic configuration).

Cloud stack refers to the overall architecture of a cloud platform. From the lowest layer to the top layer, cloud services can be supplied in a variety of ways, with each layer representing a different service model. Software as a service, platform as a service, and infrastructure as a service are the three main cloud delivery methods.

B. Cloud Security

Cloud computing has gotten a lot of attention in this modern era and has become a new computation paradigm. Microsoft, IBM, Amazon, Huawei, Alibaba, and other IT businesses have been quickly expanding. They made a difference by establishing a cloud computing server for themselves as well as the rest of the globe. Saving data locally is more expensive than storing significant amounts of data on a cloud storage server. After then, the payment for the service's rent will be made. Previously, they had to purchase and maintain IT infrastructure, which was fairly costly. As a result, storing data on a cloud storage server has become a new trend for everyone.

Furthermore, the cloud server is untrustworthy as well. Data that is only utilised once in a while is erased without the data owner's awareness to make room for the storage resource. There's a danger the data might be tampered with without the data owner's awareness. As a result, the customer should demand a practical method of ensuring data security.

To see if the data on a remote cloud server is being stored appropriately without having to download it. It employs a method called provable data possession. Even though different PDP schemes for different situations have been proposed after the information has been received, the cloud server calculates the evidence for the data's safety and a set of data that describes and gives information about the other data, if the evidence passes the formal verification support, the data is proven to be complete or not damaged.

Data integrity auditing is performed by a third-party auditor who is trusted by both the cloud server and the data owner to ensure that the results are accurate. Checking the data's integrity is beneficial to the data owner. When data is destroyed, the data owner loses all of his or her data. To strengthen the data's capacity to survive damage and availability, data owners will be able to produce and keep numerous copies on cloud servers. If one of the copies of the data is tampered with, the data owner may be able to obtain other copies of the data. To mitigate the risk, the data owner distributed several copies of the data to separate cloud storage servers. They could always recover their data from any of the other cloud storage servers, even if the data copies kept on one server were destroyed.

C. SystemModel ofCloudServiceProvide

A typical data sharing scenario in a cloud-assisted IoT scenario, which primarily consists of four categories of entities: authenticationcenters (AC), cloudserviceproviders (CSP), dataowners, and data consumers.

- Authentication centre (AC): a vital institution in charge of setting up the system and responding to user registration requests (including data owners and dataconsumers).
- Cloud service provider (CSP): an entity that holds encrypted data (i.e., data in ciphertext format) that is outsourced from data owners and answers to data owners' conversion requests.
- Data owners: users who encrypt data gathered from IoT devices and then outsource the cypher texts to CSP; they may also set access policies and delegate CSP to convert the ciphertexts fulfilling the access regulations so that specified data consumers can access the underlying data.
- Data owners: users who encrypt data gathered from IoT devices and then outsource the cypher texts to CSP; they may also set access policies and delegate CSP to convert the ciphertexts fulfilling the access regulations so that specified data consumers can access the underlying data.

AC It initializes the system by publishing system public parameters; it creates and provides private keys for users in response to user registration requests. A data owner uses mobile/wearable smart devices to capture real-time data such as pulse rate and blood pressure in the system. The data is sent from the devices to the gateway, which encrypts it with the target user's identity ID (e.g., e-mail address, IP address) and sends the ciphertexts to CSP.

As a result, only the userID has access to the data encrypted in the cypher texts. When selecting to share some out sourced data with a data consumer ID, the data owner (or user ID) creates a delegation credential DC with the identity ID and the access policy A. The data owner then delivers this credential to CSP, who will use it to transform the data owner's ciphertexts that comply with the access policy into new ciphertexts for the data consumer ID. The data consumer can now access data that had previously been encrypted by the data owner.

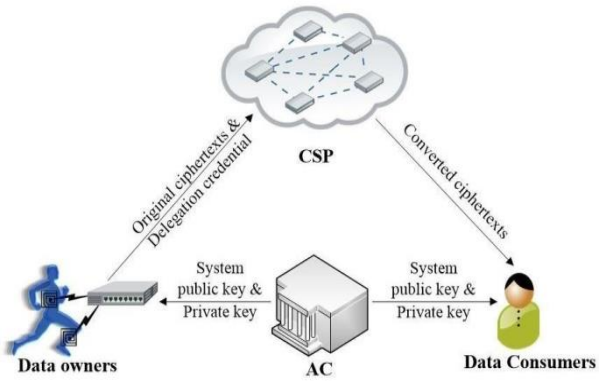


Fig. 1 Data sharing in cloud-assisted IoT

II. LITERATURE REVIEW

Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Consumer iot protection in a smart home: structures, challenges, and counter measures," IEEE Wireless Communications, vol. 25, no. 6, pages 53–59, 2018. In this paper, we introduce a new privacy protection framework for communication platforms

based on two key concepts: cloud computing and the Attribute-Based Encryption system (ABE). Cloud computing is used to store data from a third party company. However, management issues for these external companies that lose data control arise. Thus, one does not know where the data is stored. In the proposed framework we propose the use of a more authoritative ABE scheme, which provides flexible access to confidential data, and only users with the right keys can access it. Performance tests are performed with simulation with different parameters including number of attributes, encryption time and privacy removal time. The results obtained and the security analysis show that our solution exceeds the traditional solutions in terms of safety and durability.

K. E. Psannis, C. Stergiou, and B. B. Gupta, "Advanced media-based smart big data on intelligent cloud systems," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 77-87, 2018. Advanced modern media technology preaches a happy time that will be very useful in everyday life. In addition the rapid rise of wireless communication and communication will ultimately bring improved media to our lives anytime, anywhere, and any device. According to the National Institute of Standards and Technology (NIST), Cloud Computing (CC) is a system that allows easy, highly demanded network access to configurable computing ports (for example networks, applications, storage, servers and services) that can be detected quickly and delivered with minimal effort to manage or collaborate with service providers. This paper has developed an efficient MediabasedSmart Big Data (3D, Ultra HD) advanced data algorithm for Intelligent Cloud Computing systems. In order to approve the proposed approach in addition, a related study has been conducted. The proposed method can be used and integrated into HEVC, such as Smart Big Data, without compromising quality.

S. Chaudhry, "A secure framework based on encryption of iot data transfer," at the 7th 2018 International Conference on Integrity, Infocom Technology and Development (Future Trends and Guidelines) (ICRITO). IEEE, 2018, pages 743-747. Currently installed frames, IoT devices and portable frames are presented separately on security issues. These devices should be protected from unauthorized access keeping in mind the ultimate goal of verifying information about the services involved. A high-density environment with high-density, dynamic time-display, increased computer-aided use is an important driver for the introduction of security attacks, errors, risks, and security bargaining clauses. Organizations should be concerned about security, including burglary or loss of cell phones, suspected contamination, unauthorized disruption and more. Similarly, IoT devices allow a much larger number of people, servers, and systems to communicate more frequently and share data. As the use of these devices expanded, the tendency for security attacks has increased. IoT devices require privacy, authentication, control, reliability remembering the ultimate goal of keeping a few attacks. In this paper, we briefly present current security challenges on mobile phones and IoT devices. We have introduced a variety of security attacks and your prevention methods in detail for their advantages and disadvantages after the introduction of the proposed encryption algorithm.

K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, and E. Djaba, "Encryption protocol for compressed iot-based device applications using simultaneous pads," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3925–3933, 2019. Using fog allows data to be processed on the edge of the network without access to cloud infrastructure to reduce network latency and bandwidth. However, it does not have its own security challenges as existing security systems, used in fog, do not fully address the movement and variability of fog, especially on fog-blocked nodes. Thus, this increases the delay and the maximum of those touch and fog nodes. This paper investigates whether it is possible to create an encrypted protocol based on OneTime Pad without packet loss; less time and energy than compared with the agreements proposed by the available research. The protocol will be tested on wireless sensors, with devices connected, and the result monitored. One-time pads will be generated using Random Number Generator between nodes. The results are good and can be applied to fog nodes pressed by resources.

Y. Yahiatene, D. E. Menacer, M. A. Riahla, A. Rachedi, and T. B. Tebibel, "Focuses on a distributed path based on abe to protect privacy on social networks," at the 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019, pages 1–7. In this paper, we introduce a new privacy protection framework for communication platforms based on two key concepts: cloud computing and the Attribute-Based Encryption system (ABE). Cloud computing is used to store data from a third party company. However, management issues for these external companies that lose data control arise. Thus, one does not know where the data is stored. In the proposed framework we propose the use of a more authoritative ABE scheme, which provides flexible access to confidential data, and only users with the right keys can access it. Performance tests are performed with simulation with different parameters including number of attributes, encryption time and privacy removal time. Findings and security analysis show that our solution works better than traditional solutions in terms of safety and durability.

Mobile Internet - Air Pollution Monitoring System (IoT-Mobair) The Internet of Things (IoT) is a global system of "smart devices" that can detect and connect to its location and interact with users and other systems. Air pollution is one of the major concerns of our era. Existing monitoring systems have low accuracy, low sensitivity, and require laboratory analysis. Therefore, advanced monitoring systems are required. To overcome the problems of existing systems, we propose a three-phase air pollution monitoring system. The IoT kit was developed using gas sensors, an integrated Arduino development (IDE), and a Wi-Fi module. This kit can be physically installed in various cities to monitor air pollution. Gas sensors collect data in the air and transfer data to Arduino IDE. Arduino IDE transfers data to the cloud via a Wi-Fi module. We've also built an Android app called IoT-Mobair, so users can access the right air quality data from the cloud. When a user goes to an area, the pollution level of the entire route is predicted, and a warning is displayed if the pollution level is too high. The proposed system is similar to Google Traffic or the Google Maps navigation

application. In addition, air quality data can be used to predict future levels of air quality indicator (AQI).

Easy Searchable Encryption Key for the Community Network of Aided by the Cloud-Based Nerve Network The Internet of Commerce is thriving, driven in an unprecedented way by the rapid development of wireless sensory networks (WSNs) with the help of cloud computing. A new wave of technologies will create new threats to Internet security, especially the confidentiality of data on cloud-based WSNs (CWSNs). Searchable key encryption (SPE) is a promising way to deal with this problem. In theory, it allows sensors to load public key ciphertexts into the cloud, and the owner of these sensors can securely send keyword searches to the cloud and retrieve targeted data while maintaining data privacy. However, all existing and statistically protected SPE schemes have costly costs in terms of producing ciphertexts and search keywords. Therefore, this paper proposes a lightweight SPE system (LSPE) with semantic security on CWSNs. LSPE reduces the number of calculation tasks used in previous operations; therefore, LSPE has a similar search function to other searchable symmetric encryption schemes. In addition, LSPE saves a lot of time and energy on nerves to form ciphertexts. Finally, we evaluate LSPE and compare the results with other previous activities to maximize the benefits.

WSN Data Protocol for Receiving / Transferring WSN Data to IoT Using Cryptography Flexible Storage based on Information. Safety is one of the most important things in life, and it plays a vital role in every aspect of human life. Wireless Sensor Node (WSN) is connected via Internet of Things (IoT). IoT is very committed to the field of security research. In our work, we discuss explicitly the concept of data transfer to IoT devices or IoT systems. When data is transferred from the sensor node to the client it can be stealing other attackers there is a lack of security. To overcome this problem, the concept of encryption security based on reusable storage ownership is described and used here. Sensor nodes are used here and online to transmit data and there is a law to prevent interference. We have developed a system called revocable storage identitybased encryption technique which provides a valid secret key to transfer data from the sensor area to the client during a particular session. The great advantage of using this concept is that it will reduce the complexity of the recording process for both the sensor node and the client. With the help of this process, the system is secure and a high level of security is improved.

A conditional representative based on ownership also encrypts the tne character policy. The IBD CPRE system allows the less trustworthy representative to convert ciphertext that satisfies one condition, set by the sender, under one ownership to another without the need to produce a basic message. ICISC 2012, Liang, Liu, Tan, Wong and Tang proposed the IB-CPRE program, and left the unknown problem of how to create an IB-CPRE secure encryption that supports OR gates in the terms. In this work, we address the above-mentioned problem by creating a conditional patent re-enactment system based on the protocol for the ne-characters (IB-CPRE-FG). In the anIB-CPRE-FG system, each cipher text is labeled with a set of descriptive characters and each encryption key is associated with a tree accessing which type of ciphertexts the proxy can encrypt. In addition, our system may appear to be protected against dynamic accesstree and adaptive identity select-ciphertext attack.

IoT device security based on proxy reset. It seems that the interest in the Internet of Things (IoT) has recently reached a climax, with a strong focus on both the private and public sectors. IoT, a technology that allows data exchange through connections between all objects around the user, can create new resources. Data communication between objects is not limited to personal information, but can also bring in a variety of data types, such as sensory information collected locally. If such data is collected and used by a malicious attacker, it is more vulnerable to threats than to a normal network environment. The security of all data transmitted to the IoT environment is therefore important in preventing attacks. However, it is difficult to use a common cipher algorithm for lightweight devices. Therefore, we propose a way to share and manage data using a common cipher algorithm for heavyweight devices in a variety of situations. This method uses proxy encryption to manage data with multiple encryption, and provides data sharing functionality to increase the maximum network capacity of a lightweight device.

A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta, “Iot transaction processing through cooperative concurrency control on fog – cloud computing environment,” Soft Computing, vol. 24, no. 8, pp. 5695– 5711, 2020 In the case of cloud-fog, the opportunity to avoid using a stream that flows up and down the river from customers to a cloud server is always possible by switching to standard cash management agreements. With the current paper, the researcher aims to introduce a separate protocol for managing reliable financial compliance. With the use of an extended component authentication protocol, only readable IoT functions can be processed in a fog area. For final confirmation, only performance updates are sent to the cloud. In addition, the update transaction goes through partial verification in the fog area which makes them more likely to be committed to the cloud. This protocol reduces network connectivity and computing as much as possible while supporting the performance of the services required by applications running in such environments. Based on numerical studies, the researcher examined the partial verification process under three co-operation agreements. The research results show that using the proposed method will generate benefits for IoT users. These benefits come from in-service services. We assessed the impact of partial verification feeds in the fog zone of three mutual funds, namely AOCCRBSC, AOCCRB and STUBcast. We did a comprehensive set of tests to compare three protocols with and without such submissions. The result reported a reduction in the missed rate, a restart rate and a communication delay throughout. The researcher found that the proposed method reduces communication delays significantly. They found that the proposed method would allow low-density computer applications for IoT applications that are sensitive to delays. "Security, privacy and trust of the various categories in the Internet of Things (iots)", Internet of Things (IoT) plays an important role after its emergence, ranging from traditional to common household items such as WSN and RFID. With the great power of IoT, all kinds of

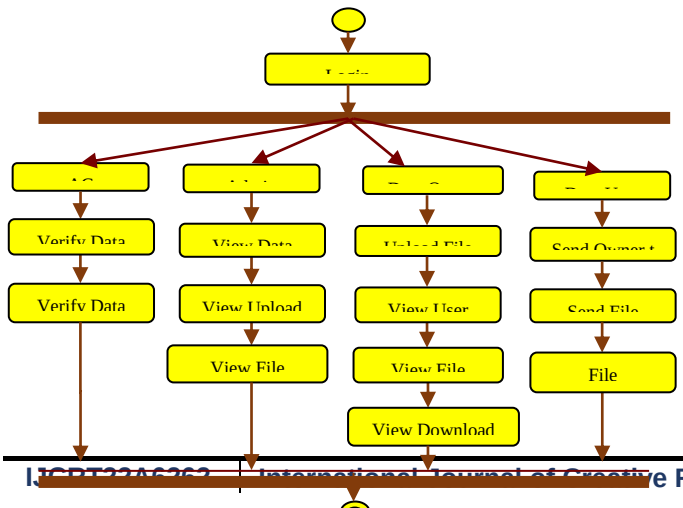
challenges come. This paper focuses on security issues among all other challenges. Since IoT is built on an Internet foundation, Internet security issues will also arise from IoT. In addition, since IoT consists of three layers: the vision layer, the transport layer and the application layer, this paper will analyze the security issues of each layer separately and try to find new problems and solutions. This paper also analyzes various integration issues and security issues in detail and discusses IoT security issues as a whole and tries to find solutions to them. Finally, this paper compares security issues between IoT and traditional networks, and discusses opening IoT security issues. "An encrypted protocol for blockchain iot-based devices using simultaneous pads" Fog computing allows data to be processed on the edge of the network without access to cloud infrastructure to reduce network latency and bandwidth. However, it does not have its own security challenges as existing security systems, used in fog, do not fully address the movement and variability of fog, especially on fog-blocked nodes. Thus, this increases the delay and the maximum of those touch and fog nodes. This paper investigates whether it is possible to create a one-time (OTP) -based encryption protocol without packet loss; less time and energy than compared with the agreements proposed by the available research. The protocol will be tested on wireless sensors, with devices connected, and the result monitored. OTPs will be generated using a random number generator between nodes. The results are good and can be applied to fog nodes pressed by resources.

III. EXISTING SYSTEM

In an existing system, they have used traditional encryption technology, but these solutions present high value on the client side and have a high demand for end-user memory and computer power. Networks handle all kinds of information, even including personal data or important business confidential information. In many cases, the removal of sensitive data may result in significant losses. It also leads to major security issues during content conversion.

IV. PROPOSED SYSTEM

In the proposed program, the Representative Reinstallation system in the IBE framework to solve the problem of security issues during content conversion and detection of flexible access control. At the same time, the PRE program also incorporates Shamir's secret sharing and Publish / Subscribe Network Content Distribution Service to transfer content efficiently and reduce the calculation burden on the user side. Proprietary-based proxy authentication is a great way to share IBE encrypted data without requiring an authorized user to share his or her private key.



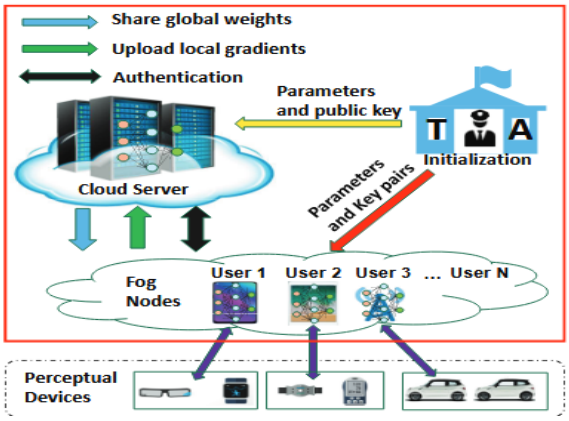


Fig. 2 Proposed System

V. RESULTS

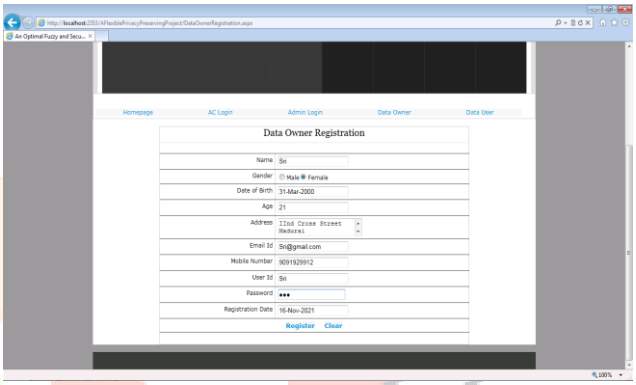


Fig. 3 Data Owner Registration

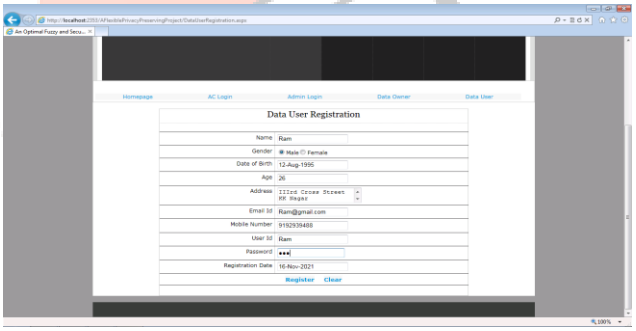


Fig. 4 Data User Registration

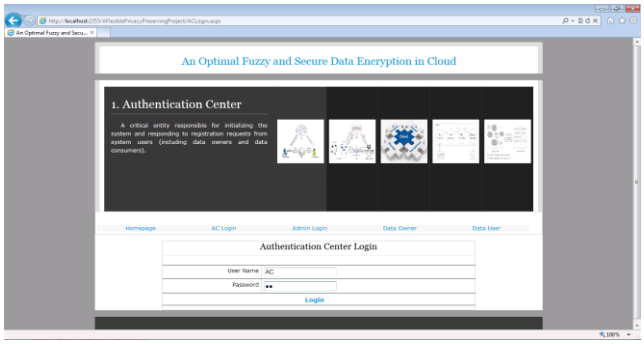


Fig. 5 Authentication Center Login

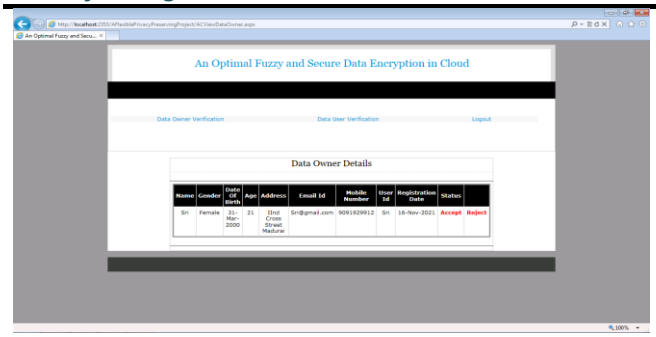


Fig. 6 Verification

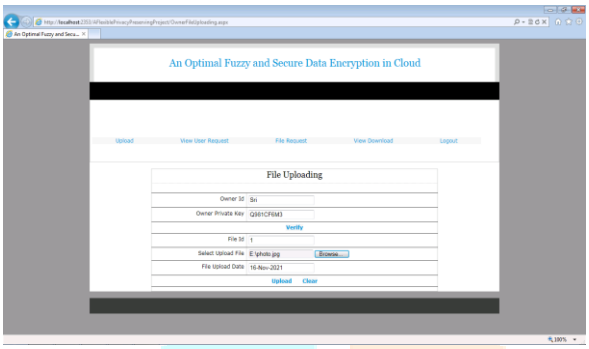


Fig. 7 File Uploading

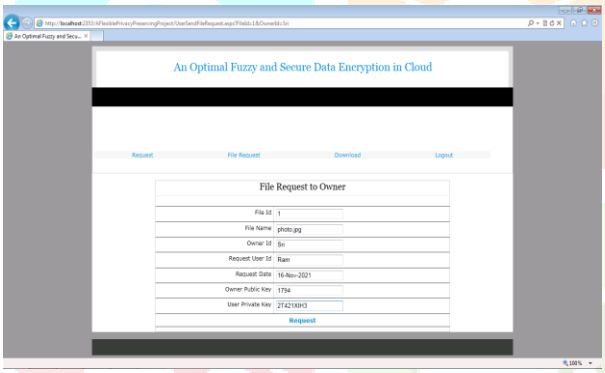


Fig. 8: Request File

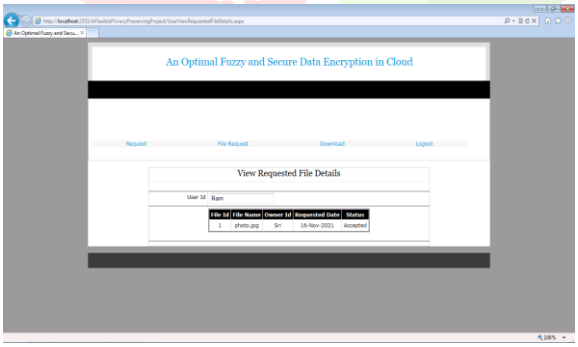


Fig. 9 View Request Status

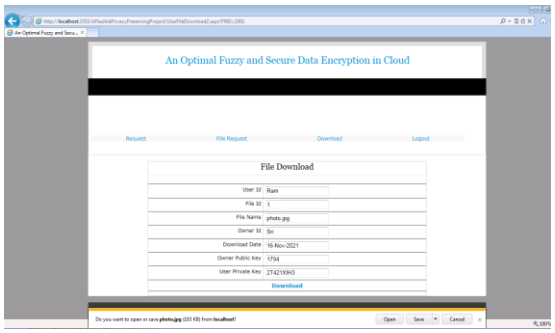


Fig. 10 Download File

VI. CONCLUSION

The FPDS system is characterized by the use of an encryption-based encryption and a secure sharing system to not only maintain the confidentiality of the extracted data but also to facilitate compliant sharing of encrypted data. A detailed security analysis shows that the FPDS system is protected against less trusted cloud and malicious users. A complete performance test shows the high efficiency of the system. The FPDS system allows encryption of data with any visible identifier and thus avoids complicated public key certificates in standard secure secure systems. Similar to proprietary-based encryption, however, the FPDS system only allows data sharing on a single recipient, making it difficult to share data with a group of users. This results in a light weight calculation for customers, and the overall function in the information-based network is relevant. The implementation of this program also shows that the system works well compared to the calculation costs and complex communication features.

REFERENCES

[1] S. Dhingra, R. B. Madda, A. H. Gandomi, R. Patan and M. Daneshmand, "Internet of Things mobile-air pollution monitoring system (IoT-Mobair)", IEEE Internet Things J., vol. 6, no. 3, 5577-5584, Jun. 2019.

[2] Tewari and B. B. Gupta, Future Gener. Comput. Syst., vol. 108, pp. 909-920, Jul. 2020.

[3] Al-Qerem, M. Alauthman, A. Almomani and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog–cloud computing environment", Soft Comput., vol. 24, no. 8, pp. 5695-5711, 2020.

[4] J. A. Guerrero-Ibanez, S. Zeadally and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle cloud computing and Internet of Things technologies", *IEEE Wireless Commun.*, vol. 22, no. 6,122-128, Dec. 2016.

[5] J. Shao, G. Wei, Y. Ling and M. Xie, "Identity-based conditional proxy re-encryption", *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 1-5, 2011.

[6] B. Gupta, "IoT transaction processing through cooperative concurrency control on fog–cloud computing environment", *Soft Comput.*, vol. 24, no. 8, pp. 5695-5711, 2020.

[7] Chamaeshika, Vasanthi and J. Julus, "Provable data possession based Multi-Cloud Storage Security with Auditing," 2022 International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), 2022, pp. 1-6, doi: 10.1109/ICSTSN53084.2022.9761315.

[8] S. Sudha, L. Jerart Julus and S. Vimal, "Performance of CE-MSK-OFDM for long haul optical transmission," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], 2014, pp. 1146-1152, doi: 10.1109/ICCPCT.2014.7054832.

[9] M. R. Palattella et al., "Internet of Things in the 5G era: Enablers architecture and business models", IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510-527, Mar. 2016.

[10] D. Boneh and M. Franklin, "Identity-based

encryption from the weil pairing", *CRYPTO*, pp. 213-229, 2001.

[11] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3712–3723, 2018.