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

Fortifying Cloud Security: Unveiling an Identity-Based Authenticated Data Sharing Protocol

[1]Adepu Rajesh*, [2]Sannella Prabhaker , [3]Narla Sai Shreya, [4]Madhuri Tumula, [5]Jakku Praveen Reddy

[1]Associate Professor, [2]Assistant Professor, [3,4,5]Student
[1,2.3.4.5] Department of Computer Science and Engineering,
[1,2,3,4,5] Guru Nanak Institute of Technology , Ibrahimpatnam, RR District ,Telangana State, India

Abstract : In the complex landscape of cyber-physical cloud environments, achieving secure and efficient file storage and seamless sharing, especially with authenticated physical devices, is an ongoing challenge. This complexity is compounded by the variety of devices accessing these services and data, each with their own security considerations. To address this challenge, this paper presents a new lightweight identity-based authenticated data sharing protocol. This protocol has been carefully designed to facilitate secure data sharing between physically distributed devices and clients, bridging geographic gaps without compromising security. Through rigorous analysis, the proposed protocol is robust against Chosen Cryptographic Attacks (CCA), enhanced by the hardness of the decision-based and robust Diffie-Hellman (SDH) problem. In addition, the performance of the protocol is fully evaluated against existing data sharing protocols considering computational overhead, data transmission cost and response time to provide a comprehensive understanding of its performance in real-world scenarios.

IndexTerms **- Cloud, Diffie-Hellman, Geographic gaps, Cryptographic Attacks**

I. INTRODUCTION

Cloud-enabled Cyber-Physical Systems (Cloud-CPS; also known as Cyber-Physical Cloud Systems) have a wide range of applications, from healthcare to smart power grids, smart cities and battlefields to military, etc. [1], [2]]. In such systems, client devices (e.g. Android and iOS devices or devices with limited resources such as sensors) can be used to access relevant services (e.g. in the context of a smart grid, this can include analyzed usage data and stored in the cloud) from/through the cloud. However, client devices typically have less computing capabilities, so they are unlikely to have adequate (technical) security measures compared to conventional personal computers (PCs) [3]. Based on the Home Agent (HA) and mobile subscribers stored in relevant databases, mobile operators can decide whether to allow or deny access requests to certain services (ie Authentication, Authorization and Accounting - AAA). Once the mobile subscriber is authenticated, the mobile user's request(s) are forwarded to the Cloud Controllers (CC). The latter processes requests and provides the necessary services. In recent years, several studies have been conducted on the security of CPS [4], [5], [6]. For example, in 2012, Rajkumar [7] presented several technical/scientific challenges related to CPS. Rajhans et al. [8] proposed an architectural framework for CPS using structural and semantic mappings for consistency.

II. LITERATURE STUDY

[1] As companies offer ever-wider access to customers and employees, software functionality and continuous improvement in supply chain management capabilities, this increases the risk of cyber-physical attacks on cyber-physical cloud systems (CPCS). In this paper, the authors discuss the challenges of a CPCS attack and emphasize the need for forensic engineering before presenting their conceptual CPCS forensics model. Six elements of the framework are addressed, viz. risk management principles and practices, forensic preparation principles and practices, incident management principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements. Future research topics were also identified.

[2] As the use of cyber-physical systems such as Internet of Things (IoT) devices increases, so does the potential attack footprint for personal and business users. In this paper, we explore the possibilities of using information obtained from two IoT devices that are unlikely to store significant amounts of data. We focus mainly on visible smart home devices whose purpose is to obtain dangerous information. We conduct a collection and analysis process constrained by three types of adversarial constraints: passive forensics, active forensics and real-time active. The

previous two adversaries aim to meet forensic reliability requirements, while the real-time active adversary does not have these limitations and therefore more accurately models a malicious real attacker. The results show that even a passive adversary has access to various device data that can be used to determine a person's activity and/or presence at a given time based on how they interact with an IoT device. These interactions can be either user-initiated (such as turning a switch or light on or off) or device-initiated (such as a background request).

[3] Due to the explosive growth of mobile applications and the development of the concept of cloud computing, mobile cloud computing (MCC) has been introduced as a potential technology for mobile communication services. MCC integrates cloud computing into the mobile environment and overcomes barriers related to the discussed performance (e.g. battery life, storage and bandwidth), environment (e.g. heterogeneity, scalability and availability) and security (e.g. reliability and privacy). in mobile computing. This article contains a My Customer Center survey to help general readers gain an overview of My Customer Center, including its definition, architecture, and applications. Problems, existing solutions and approaches are presented. In addition, the future research directions of MCC are discussed.

[4] Thanks to recent advances in wireless sensor networks, big data, mobile and cloud technologies, cyber-physical systems (CPS) can connect cyberspace with the physical world better than ever. Cloud-based systems can also provide massive storage resources and cheap computing, as well as the flexibility to adapt the operating environment to complex industrial applications (CIA). In our view, Cloud Integrated CPS (CCPS) opens the door to efficiently build, deploy, manage and manage application scenarios that were previously unattainable. In this paper, we propose a new CCPS architecture (called CCPSA) and describe the technologies that enable CIA. We then explore three potential challenges and provide solutions from a CIA perspective, including virtualized resource management techniques, cloud resource scheduling, and lifecycle management. We hope that this article can provide insight and a roadmap for future research in the emerging field of CCPS.

[5] Cloud computing is an emerging technology that has been used to provide better healthcare to users due to its convenient and economical features. It has been found that healthcare services require fast and reliable sharing of information anytime, anywhere to better monitor medical requirements and make decisions. However, the privacy and integrity of electronic health data becomes an important issue during data sharing and cloud outsourcing. Protection of customer/patient data is important in healthcare where data exposure to unauthorized persons is exceptional. To address this security gap, this paper introduces a cloud-based Secure Healthcare Framework (SecHS), which provides secure access to healthcare and medical information. In particular, this paper improves CP-ABE (Ciphertext Policy Attribute Based Encryption) by adding two modules that aim to provide fine-grained access control and ensure data privacy and integrity. It facilitates cryptographic and decentralized systems. The proposed framework is compared with existing frameworks that used the CP-ABE system. This indicates that SecHS provides better features to protect health data. Optimistically, data security requirements such as privacy, integrity and strict access control are necessary to provide an effective proposition for securing data in a cloud environment.

[6] Secure cloud storage solutions such as Trust Store, Sec Cloud, HPI Secure and Twin Cloud primarily focus on protecting persistent data while it is stored in public cloud services. Although data sharing is considered an important security feature, these storage solutions mostly focus on three main functions: confidentiality, integrity and availability. Modern business applications require data to be shared within or across organizations. The challenge is how to securely share information in public clouds without increasing data transmission and processing costs. This problem has recently been addressed by exploiting or developing new data encryption techniques such as identity-based encryption, attribute-based encryption, and proxy re-encryption. However, these techniques have scalability and flexibility issues when dealing with large data and supporting dynamic access rules. This article introduces a new architecture and corresponding protocols for secure sharing of documents in public cloud services: Cloud Docs. This system uses AES to encrypt data for scalability and supports identity-based access control rules using private and public key pairs for flexibility.

III. METHODOLOGY

The architecture of our data sharing protocol project is designed to provide a robust, scalable and secure framework for seamless data exchange in the cloud environment. The architecture consists of several key components that work together to ensure data integrity, confidentiality and effective communication.

A. ID-Based Encryption, or Identity-Based Encryption (IBE) Technique :

An Intrusion-Based Encryption (IBE) scheme is comprised of four distinct algorithms, namely Setup, Extract, Encrypt, and Decrypt.

Setup: This initial algorithm operates by accepting a security parameter denoted as 'k' and subsequently generates 'params', which are universally accessible to all users, and 'MSK', which remains exclusively known to the Private Key Generator (PKG).

Extract: This subsequent algorithm undertakes the task of extracting user identity 'ID', 'params', and 'MSK' as inputs, yielding a private key 'SKID' tailored specifically for the user's identity, which may manifest as either a string or an integer based on the system's specifications.

Encrypt: The encryption procedure entails the utilization of 'params', a designated message 'M', and the recipient's identity 'ID' as inputs, culminating in the production of a ciphertext denoted as 'CT'.

Decrypt: The final algorithm, decryption, operates by receiving 'CT' and 'SKID' as inputs. It then proceeds to decipher the ciphertext, yielding either the original message 'M' if the supplied 'SKID' and 'CT' are authenticated, or a null output indicative of invalid inputs.

B. Adaptive security model for IBE scheme:

In the adaptive security model for an Identity-Based Encryption (IBE) scheme under the chosen-ciphertext attack (IND-CCA), the Challenger (Ch) engages with Adversary (A) challenges to tackle the underlying computational complexities. This model encompasses five distinct phases delineated as follows:

Setup: Initialization of the system occurs as the Challenger executes this algorithm, contingent upon the security parameter 'k', which yields the Master Secret Key (MSK) and 'params'. The Challenger retains the MSK secret and forwards 'params' to the Adversary.

Phase 1: During this stage, the Adversary is granted the liberty to issue a series of queries denoted as 'fq1, q2, …..qng' to the Challenger. Each query, 'qi', falls under one of two categories:

Key extraction queries ('IDi'): If no previous inquiry for 'IDi' has been made, the Challenger responds by invoking the Extract(MSK; IDi) algorithm, furnishing the private key 'SKID' to the Adversary.

Decryption queries ('IDj, CT'): In the absence of prior inquiries for 'IDj' and 'CT', the Challenger executes the Extract(MSK, IDj) algorithm to derive the private key 'SKIDj' for 'IDj'. Subsequently, it employs the Decrypt(CT, SKIDj) algorithm to decipher the ciphertext 'CT' using 'SKIDj', ultimately returning the plaintext output.

Challenge: A pivotal juncture ensues as the Adversary furnishes two messages of equal length, 'M0' and 'M1', alongside two distinct identities, 'ID0' and 'ID1', to the Challenger. Notably, 'ID0' and 'ID1' have not been subject to any key extraction query in Phase 1. Here, the Challenger randomly selects 'b' and 'c' from the binary set ({0, 1})^2, subsequently encrypting the message 'Mc' using the designated identity 'IDb'. The resultant ciphertext is then dispatched to the Adversary.

Phase 2: Continuation of Phase 1 unfolds adaptively, with the caveat that the Adversary abstains from querying for 'ID0' and 'ID1'.

Guess: Culmination arrives as the Adversary submits two conjectures ('b1, c1') regarding the originally selected binary values ('b, c') from the set ({0, 1})^2.

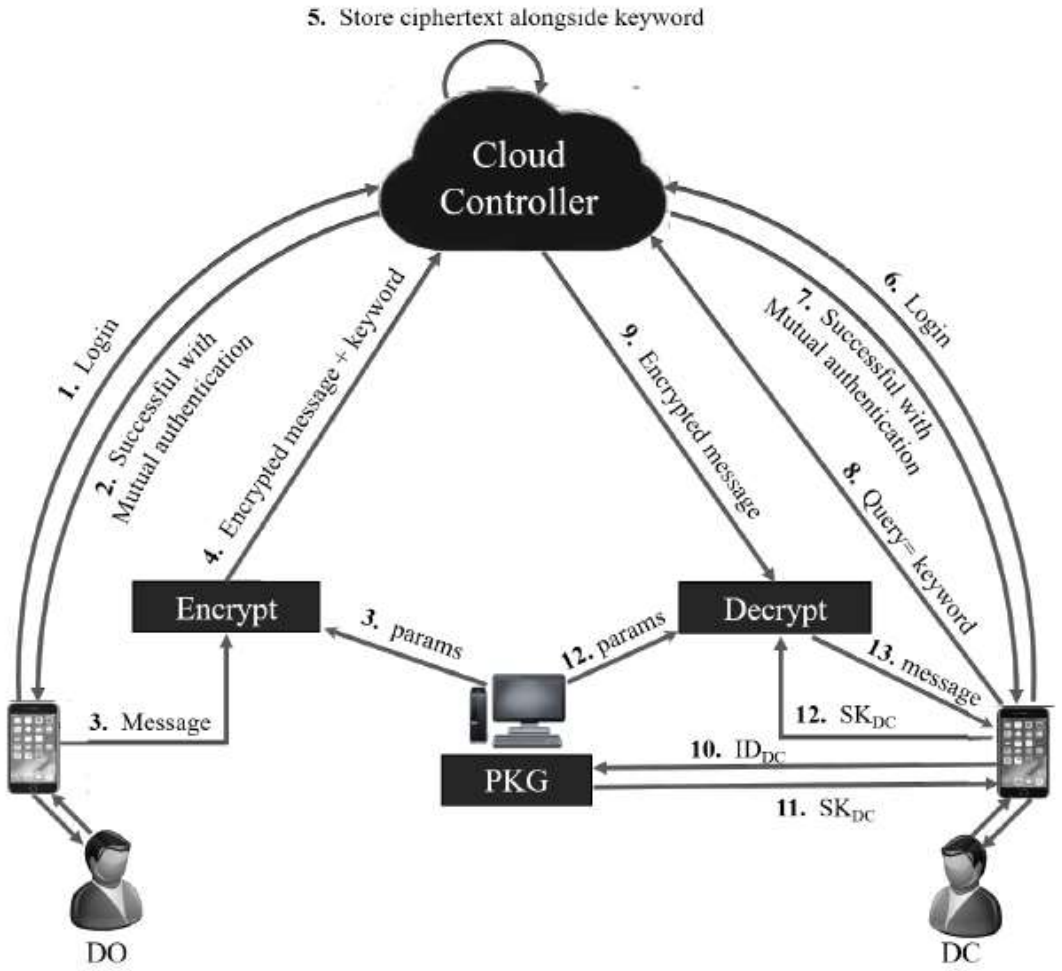

Fig:1 Network model for assuring cloud data security by the proposed IBADS protocol

C. Design

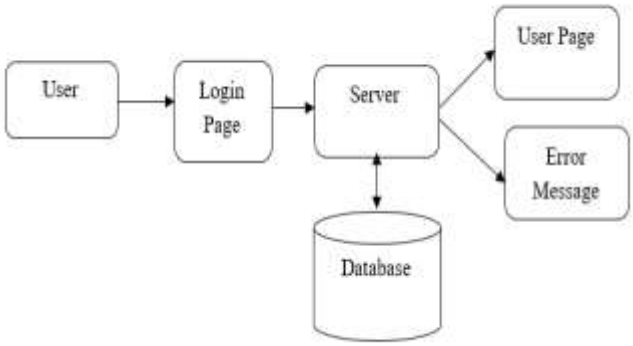

Fig:2 User Interface

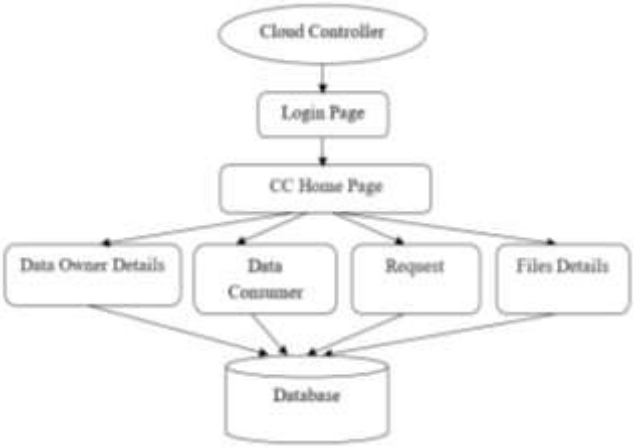

Fig 3: Cloud Controller

User Interface - To connect to the server, the user must enter a username and password so that only he can connect to the server. The database creates an account for all users to maintain upload and download speeds. The name is set as the user ID. Login is usually used to go to a specific page. It searches for the survey and displays the survey

Cloud Controller - The user (DO and DC) registers with a mobile phone. It is responsible for data processing, such as computing and data storage on behalf of cloud users.

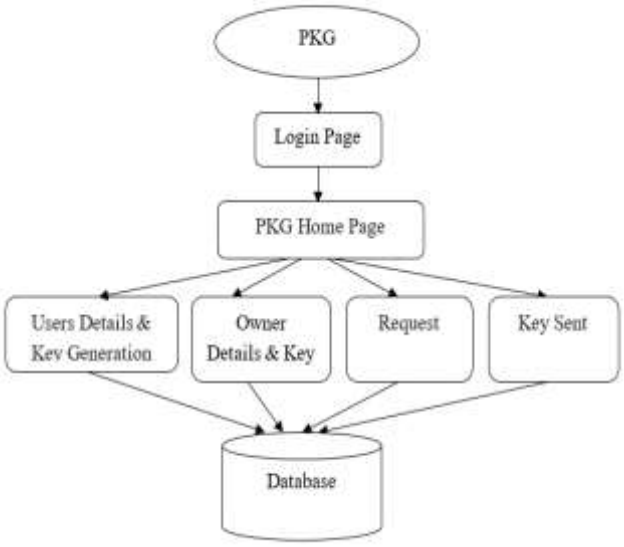

Fig: 4 Private Key Generator

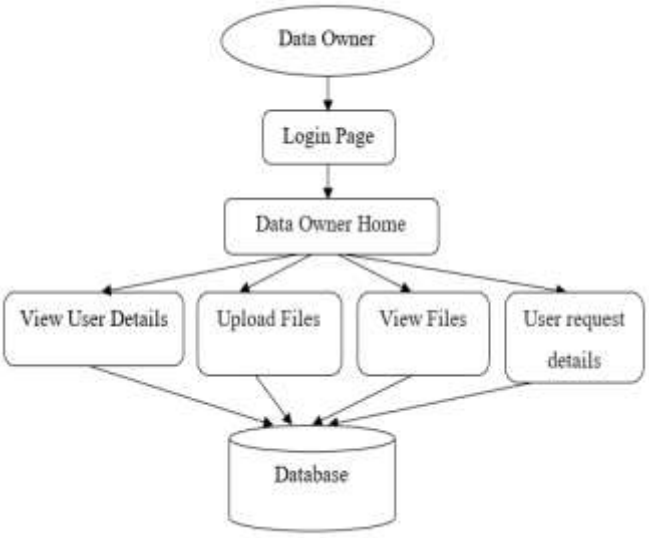

Fig: 5 Data Owner

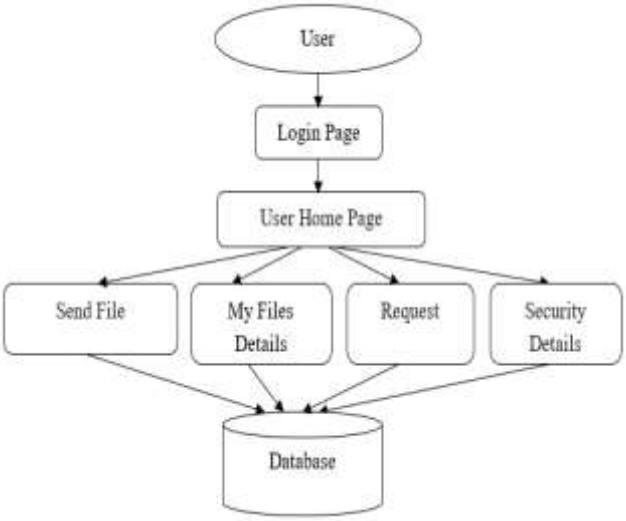

Fig: 6 Data Consumer

Private Key Generator - For decryption, the DC contacts the PKG and receives the private key associated with its unique identity, and then proceeds to decrypt the encrypted data using that private key. It is responsible for generating system global parameters and private keys for DO and DC. Any registered user acting as a DC who wishes to access stored data must log in and submit a request to the CC

Data Owner - uses a mobile device to access or send encrypted data. After successful completion of this operation, data encrypted with CC keyword can be saved to cloud storage.

Data Consumer - Only after successful login will CC send encrypted data to DC. The DO, which receives its private key from the PKG, was allowed to decrypt with the encrypted data

IV. RESULTS DISCUSSION

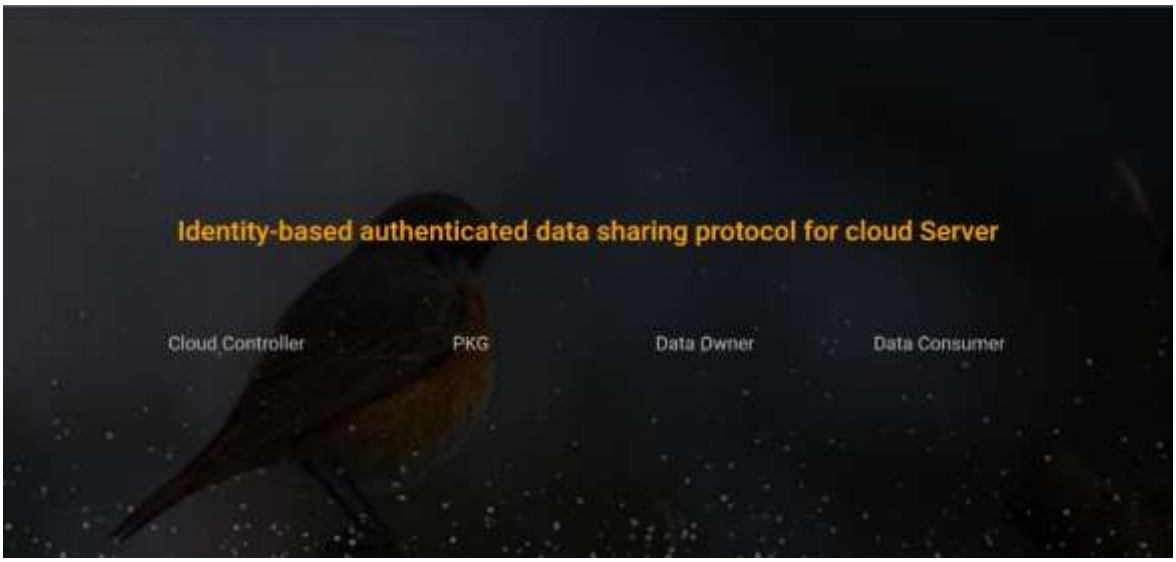

Fig:7 Home Layout

Engage with the pivotal hub of system administration through the "Cloud Controller" button, granting entry to the system's

control center. Upon activation, users are presented with a secure login interface, facilitating the input of their Cloud Controller email and password credentials. This gateway serves as a robust checkpoint, permitting authorized individuals with requisite credentials to wield comprehensive control over diverse facets of the cloud-based infrastructure. Immerse yourself in a seamless and safeguarded pathway to the system's core functionality through the invocation of the Cloud Controller login button

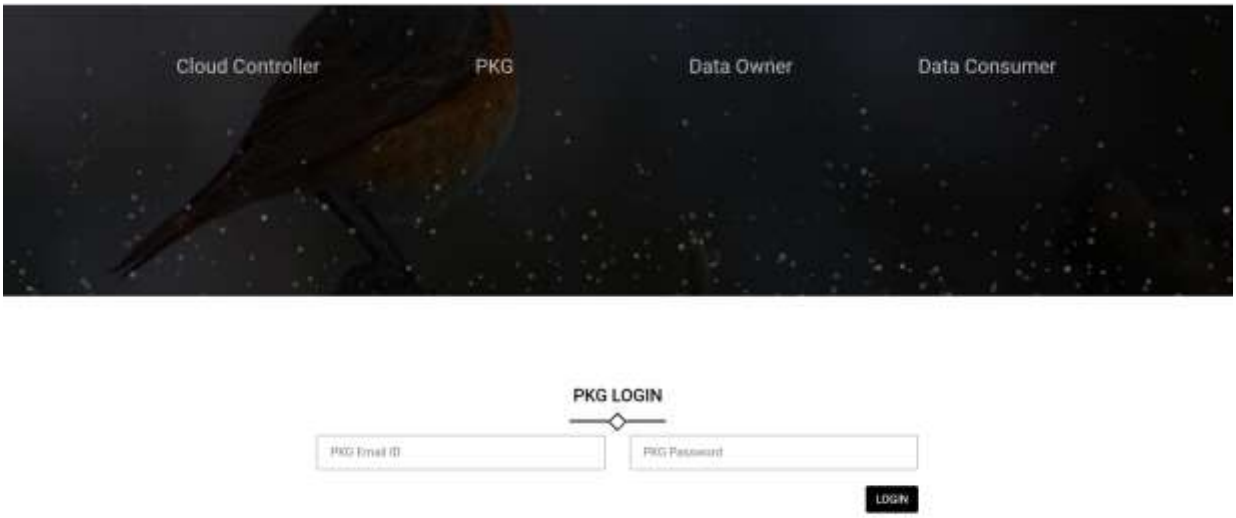

Fig:8 PKG Login Layout

Access the comprehensive packaging capabilities of the system by engaging with the "Package (pkg)" button. A simple click unveils a login interface, prompting users to input their Package credentials, conventionally comprising a designated email and password. This secure authentication mechanism serves as a robust barrier, permitting solely authorized individuals to harness the packaging functionalities embedded within the system. Effortlessly navigate and oversee packaging operations by leveraging the Package button for login, thereby upholding the integrity and security of your valuable data assets

.

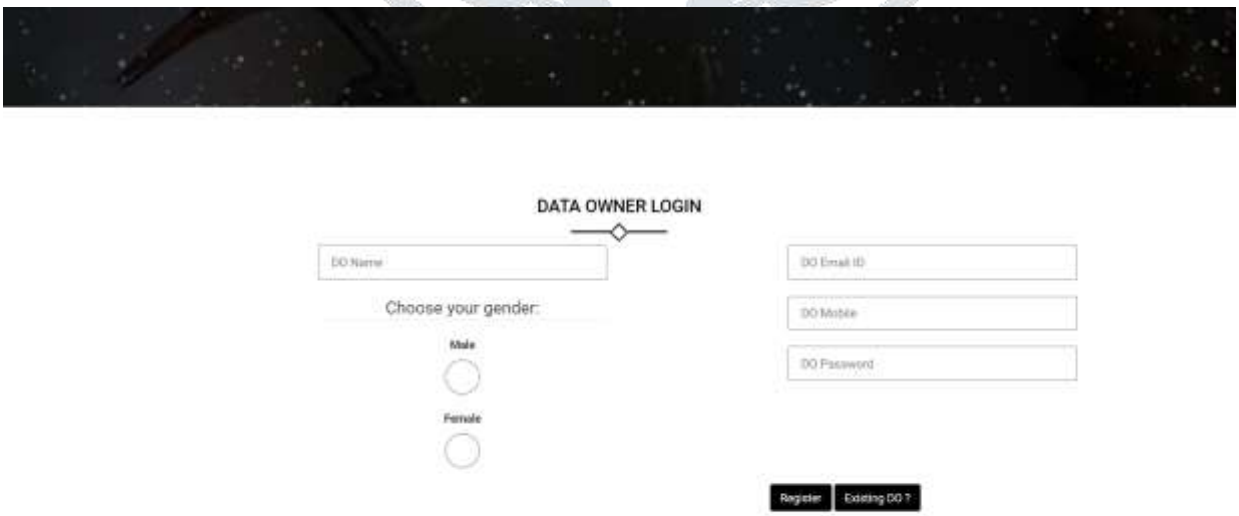

Fig: 9 Data Owner Layout

Embark on your journey as a new user through the welcoming confines of the "Data Owner" page, where a user-friendly registration process awaits. For those venturing here for the first time, simply furnish the requisite details to complete your registration and unlock access to the platform. Returning users, on the other hand, are granted direct entry through a streamlined login option. Effortlessly traverse the virtual landscape by entering your registered credentials, ensuring swift and efficient access to the platform's offerings. Whether you're a newcomer or a familiar face, rest assured that the Data Owner page is dedicated to providing a tailored, user-centric experience that aligns seamlessly with your individual requirements

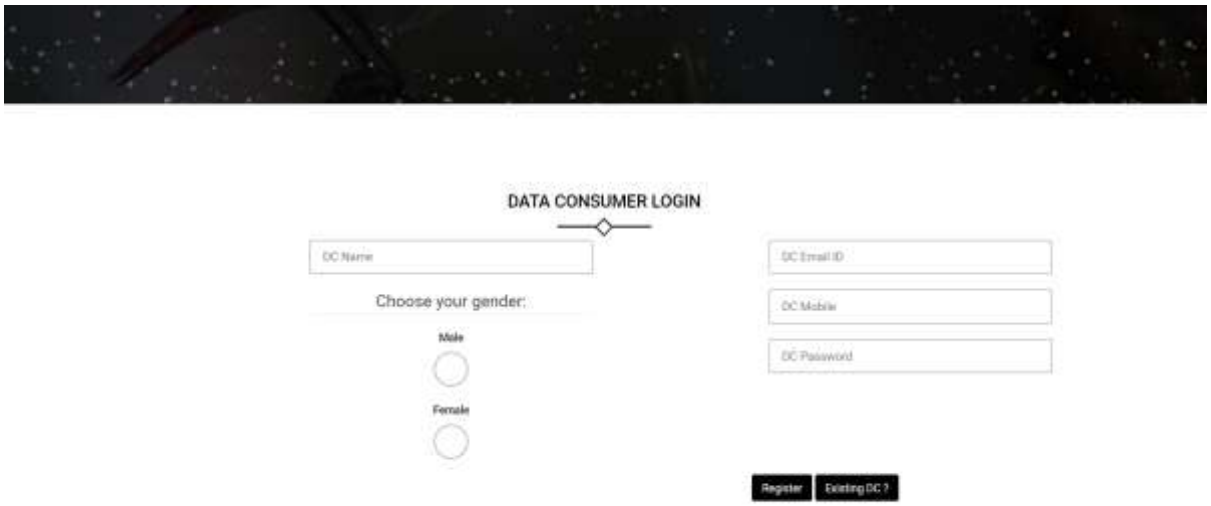

Fig: 10 Data Consumer Layout

Step into the realm of data consumption through the meticulously crafted "Data Consumer" page, meticulously tailored to accommodate both newcomers and returning visitors alike. If you find yourself venturing here for the first time, registration is a breeze – simply furnish the requisite details to initiate your journey. Alternatively, for those who have traversed these virtual corridors before, a direct login option stands ready at your disposal. Effortlessly gain access to the system by inputting your credentials, bypassing the rigors of a protracted registration process. Within the Data Consumer page, rest assured of a seamless experience meticulously engineered to cater to the needs of both novices and seasoned users, epitomizing efficiency and convenience at every turn

.

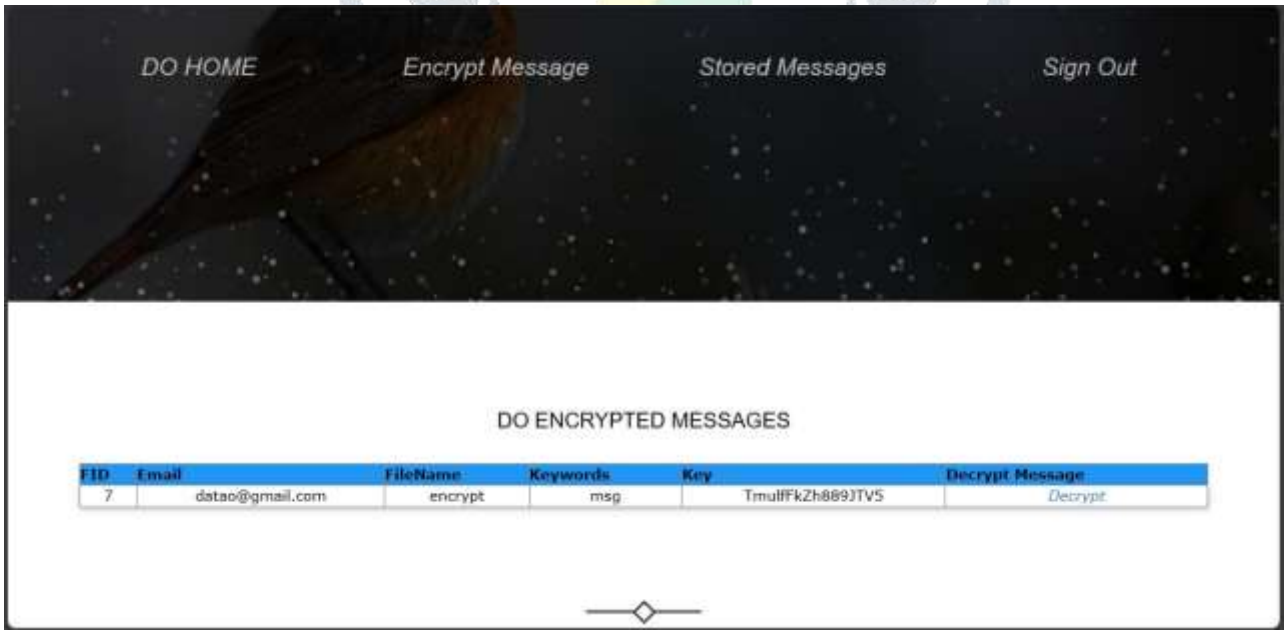

Fig: 11 Encryption Source

Enter the fortified domain of the "Data Owner" page, where users are bestowed with a suite of cutting-edge security provisions. Whether you're a novice embarking on your inaugural visit or a seasoned user returning to familiar grounds, the pathway to access remains seamless. Upon authentication, immerse yourself in the functionality of our platform, effortlessly encrypting your messages with unparalleled ease. Our system boasts the capability to generate distinct encryption keys for each message, erecting an impregnable fortress of security around your communications. Delve into the intuitive interface, where the convenience of storing and managing encrypted messages is at your fingertips, each safeguarded by its own cryptographic key. The Data Owner page stands as your premier portal to a messaging realm characterized by both security and efficiency, underpinned by automatic key generation to fortify your data against potential threats.

Fig: 12 Encryption Layout

Experience a paradigm shift in data security through the innovative interface of the "Data Owner" page. Here, users are empowered to tailor their encryption journey with unparalleled dynamism. Simply input a file name, cryptographic key, and personalized message to embark on a bespoke encryption experience. Upon submission, our cutting-edge system orchestrates the intelligent generation of unique keys and encrypts your designated message, fortifying it with an impenetrable shield of security. Traverse the platform with seamless precision to effortlessly oversee and store your encrypted files, each meticulously safeguarded by its own individually generated key. The Data Owner page stands as a beacon of user-centric design, offering a solution that seamlessly integrates customization and convenience, empowering you to navigate the encryption process with unparalleled ease and unwavering confidence.

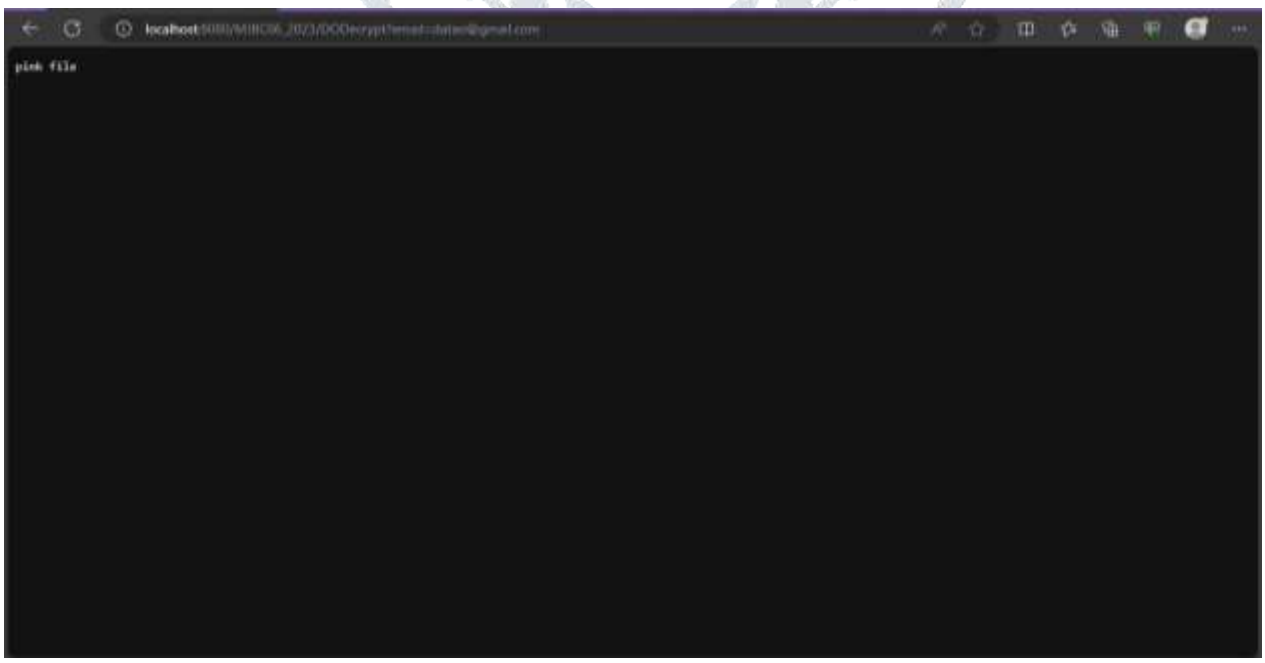

Fig: 13 Decryption Source Message

Through the streamlined decryption process orchestrated by the "Data Consumer" page. Users engage by inputting essential details, including the Data Owner ID, Data Consumer ID, Master Key (MK), and Public Key (PK). With these critical identifiers in place, the platform effortlessly embarks on the decryption journey, unveiling the original content hidden within the encrypted message. Seamlessly, the decrypted message takes center stage, ensuring users can readily access and comprehend the secure information within. At the heart of the Data Consumer page lies a commitment to both security and user-friendliness, epitomized by an intuitive interface that mandates only the essential identification inputs, fostering a secure and efficient decryption experience for all users.
Experience an advancement in data security

V. CONCLUSION

The deployment of the Identity-Based Authenticated Data Sharing (IBADS) protocol in cyber-physical cloud systems, leveraging bilinear pairing, represents a significant stride towards enhancing data sharing security and efficiency. By streamlining registration and enabling secure message transmission, IBADS ensures a robust framework for data owners. This study rigorously examined IBADS, affirming its resilience through cryptographic analysis and bolstering its strength with bilinear pairing. Its successful validation contributes substantially to secure data sharing, with future prospects for optimization and extension. IBADS stands as a beacon of progress, paving the way for more sophisticated protocols in cloud environments.

In the domain of Identity-Based Authenticated Data Sharing (IBADS), forthcoming advancements promise substantial protocol refinement. A pivotal focal point is scalability optimization to adeptly manage expanding datasets amidst growing user bases. Integration of advanced cryptographic methodologies, notably post-quantum cryptography, stands poised to fortify IBADS against evolving security paradigms. Embracing multi-cloud compatibility facilitates seamless data sharing across varied cloud providers, heightening system adaptability. User interface enhancements for both data owners and consumers, prioritizing simplicity and intuitiveness, can spur wider adoption. The exploration of dynamic key management mechanisms, facilitating periodic cryptographic key updates, is essential for bolstering long-term security. Ensuring robust defenses against malicious attacks and embracing cross-device compatibility measures are vital considerations. Moreover, an expanded evaluation of quantitative performance metrics enriches our understanding of IBADS efficacy. Through sustained research efforts in these arenas, IBADS evolves to confront emerging challenges, ensuring its enduring relevance in our dynamic technological milieu.

VI. REFERENCES

[1] Nurul Hidayah Ab Rahman, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Computing, 3(1):50–59, 2016.

[2] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. Cyber-physical systems information gathering: A smart home case study. Computer Networks, 138:1–12, 2018.

[3] Hoang T Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18):1587–1611, 2013.

[4] Qiang Liu, Jiafu Wan, and Keliang Zhou. Cloud manufacturing service system for industrial-cluster-oriented application. 15(3):373–380, 2014.

[5] Daqiang Zhang, Jiafu Wan, Qiang Liu, Xin Guan, and Xuedong Liang. A taxonomy of agent technologies for ubiquitous computing environments. KSII Transactions on Internet and Information Systems (TIIS), 6(2):547–565, 2012.

[6] Jiafu Wan, Hehua Yan, Di Li, Keliang Zhou, and Lu Zeng. Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle. The Computer Journal, 56(8):947–956, 2013.

[7] Ragunathan Rajkumar. A cyber–physical future. Proceedings of the IEEE, 100(Special Centennial Issue):1309–1312, 2012.

[8] Akshay Rajhans, Ajinkya Bhave, Ivan Ruchkin, Bruce H Krogh, David Garlan, Andr´e Platzer, and Bradley Schmerl. Supporting heterogeneity in cyber-physical systems architectures. IEEE Transactions on Automatic Control, 59(12):3178–3193, 2014.

[9] Burak Demirel, Zhenhua Zou, Pablo Soldati, and Mikael Johansson. Modular design of jointly optimal controllers and forwarding policies for wireless control. IEEE Transactions on Automatic Control, 59(12):3252–3265, 2014.

[10] Zhaogang Shu, Jiafu Wan, Daqiang Zhang, and Di Li. Cloud-integrated cyber-physical systems for complex industrial applications. Mobile Networks and Applications, 21(5):865–878, 2016.

[11] I NARSIMHA RAO, M SUPRIYA MENON, and S VIVEKA. Cloud based secure health care system using multi authority. 2015.

[12] Catherine Wise, Carsten Friedrich, Surya Nepal, Shiping Chen, and Richard O Sinnott. Cloud docs: Secure scalable document sharing on public clouds. In 2015 IEEE 8th International Conference on Cloud Computing, pages 532–539. IEEE, 2015.

[13] Deng-Guo Feng, Min Zhang, Yan Zhang, and Zhen Xu. Study on cloud computing security. Journal of software, 22(1):71–83, 2011.

[14] Tsz Hon Yuen, Ye Zhang, Siu Ming Yiu, and Joseph K Liu. Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks. In European Symposium on Research in Computer Security, pages 130–147. Springer, 2014.

[15] Yanjiang Yang, Haibing Lu, and Jian Weng. Multi-user private keyword search for cloud computing. In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, pages 264–271. IEEE, 2011.

[16] Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang. Identity-based authentication for cloud computing. In IEEE International Conference on Cloud Computing, pages 157–166. Springer, 2009.

[17] Hongbing Cheng, Chunming Rong, Zhenghua Tan, and Qingkai Zeng. Identity based encryption and biometric authentication scheme for secure data access in cloud computing. Chinese Journal of Electronics, 21(2):254–259, 2012.

[18] Jinguang Han, Willy Susilo, and Yi Mu. Identity-based data storage in cloud computing. Future Generation Computer Systems, 29(3):673–681, 2013.

[19] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou. Identity-based encryption with outsourced revocation in cloud computing. Ieee Transactions on computers, 64(2):425–437, 2015.

[20] Christian Schridde, Tim D¨ornemann, Ernst Juhnke, Bernd Freisleben, and Matthew Smith. An identity-based security infrastructure for cloud environments. In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, pages 644–649. IEEE, 2010.

[21] Nathalie Mitton, Symeon Papavassiliou, Antonio Puliafito, and Kishor S Trivedi. Combining cloud and sensors in a smart city environment. EURASIP journal on Wireless Communications and Networking, 2012(1):1, 2012.

[22] Adel S Elmaghraby and Michael M Losavio. Cyber security challenges in smart cities: Safety, security and privacy. Journal of advanced research, 5(4):491–497, 2014.

[23] Hans Schaffers, Nicos Komninos, Marc Pallot, Brigitte Trousse, Michael Nilsson, and Alvaro Oliveira. Smart cities and the future internet: Towards cooperation frameworks for open innovation. In The Future Internet Assembly, pages 431–446. Springer, 2011.

[24] Sotiris Zygiaris. Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. Journal of the Knowledge Economy, 4(2):217–231, 2013.

[25] Milind Naphade, Guruduth Banavar, Colin Harrison, Jurij Paraszczak, and Robert Morris. Smarter cities and their innovation challenges. Computer, 44(6):32–39, 2011.

[26] Jungwoo Lee, Songhoon Baik, and Choonhwa Lee. Building an integrated service management platform for ubiquitous ecological cities. Computer, 44(6):56–63, 2011.

[27] Jos´e M Hern´andez-Mu˜noz, Jes´us Bernat Vercher, Luis Mu˜noz, Jos´e A Galache, Mirko Presser, Luis A Hern´andez G´omez, and Jan Pettersson. Smart cities at the forefront of the future internet. In The Future Internet Assembly, pages 447–462. Springer, 2011.

[28] J Vercher, Santiago Perez Marin, Agustin Gonzalez Lucas, Rafael Sorribas Mollon, Luis Villarrubia Grande, Luis M Campoy Cervera, and L Hern´andez G´omez. Ubiquitous sensor networks in ims: an ambient intelligence telco platform. ICT Mobile Summit, 2008.