e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

REVOCABLE IDENTITY-BASED BROADCAST PROXY RE-ENCRYPTION FOR DATA SHARING IN CLOUDS

Aniyarasi. E*1

*1Student, Computer Science Engineering, Avs Engineering College,
Salem, Tamilnadu, India.

ABSTRACT

Cloud computing has become prevalent due to its nature of massive storage and vast computing capabilities. Ensuring a secure data sharing is critical to cloud applications. Recently, a number of identity-based broadcast proxy re-encryption (IB-BPRE) schemes have been proposed to resolve the problem. However, the IB-BPRE requires a cloud user (Alice) who wants to share data with a bunch of other users (e.g. colleagues) to participate the group shared key renewal process because Alice's private key is a prerequisite for shared key generation. This, however, does not leverage the benefit of cloud computing and causes the inconvenience for cloud users. Therefore, a novel security notion named revocable identity-based broadcast proxy re-encryption (RIB-BPRE) is presented to address the issue of key revocation in this work. Adopting k-TAA schemes to PAYG model, the access bound k is decided by the prepayment amount and the service usage is tracked by the number of access times. However, this approach is impractical, since existing k-TAA schemes only allow an one-time access in an authentication. This work aims to bridge this gap in the literature by designing an efficient and secure authentication system for PAYG cloud computing, supporting flexible access controllability, user anonymity and public traceability. To achieve this, we propose new k-TAA primitive, called k-times anonymous pay-as-you-go authentication (k-TAA-PAYG), that allows users to access services for multiple times in an authentication as long as the number of their access times does not exceed k. We first formalize the definition and security model for k-TAA-PAYG scheme. Subsequently, we present a concrete construction of k-TAA-PAYG scheme, with the computational complexity as O(1) and the constant communicational cost. In a RIB-BPRE scheme, a proxy can revoke a set of delegates, designated by the delegator, from the re-encryption key. The performance evaluation reveals that the proposed scheme is efficient and practical.

I. INTRODUCTION

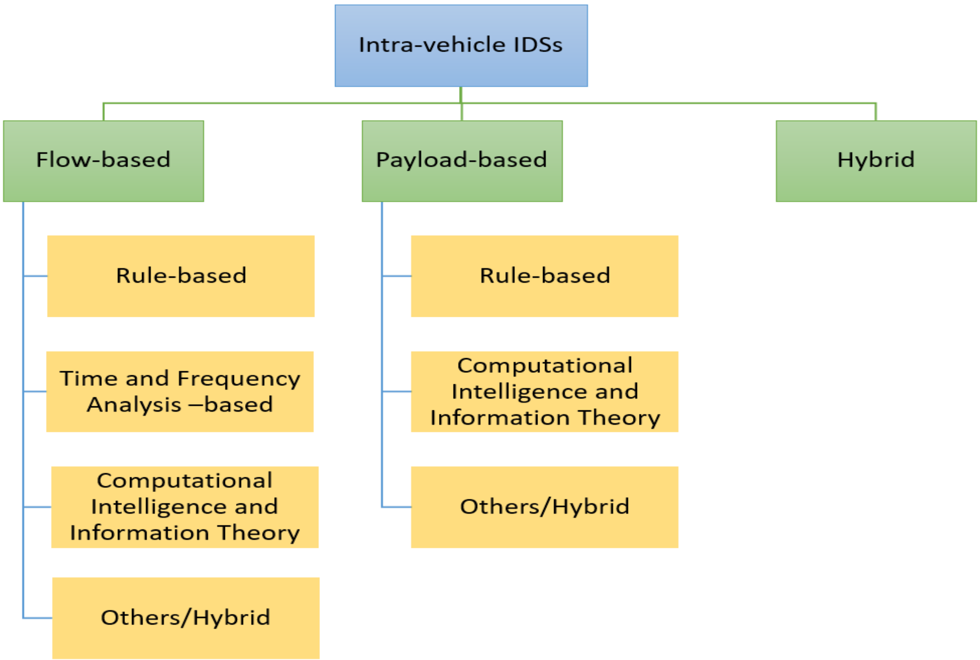
The rapid development of information technology, social media, data collection capacity, and data storage, the field of big data analytics is now rapidly expanding into all science and engineering domains. Real-world applications such as telecommunications, health care, pharmaceuticals, and finance generate massive amounts of data round the clock [1]. Taking online social media alone, for instance, today's customer base is estimated to generate 2.5 quintillion bytes of data per day in the form of tweets, likes, comments, blogs, videos, and images [2]. These big data streams contain abundant information stored in the form of hidden patterns and unknown correlations. Analyzing big data streams that were previously untapped or inaccessible will enable new insights resulting in better and faster decisions. The process of examining big data to uncover hidden patterns, unknown correlations, and other insights is referred to as big data analytics. The origin of big data analytics can be traced back to the 1970s or before, when research communities in computer science (CS) and statistics, working in fields such as machine learning and statistical computing, began to play a major role in data mining. In the following decade, the scale and volume of data grew dramatically due to the increasing capability of computing power and automation. To distinguish these large datasets from conventional data, they were referred to as "very large databases" (VLDBs) or "massive data" (MD) sets among the CS and statistics communities. The 1990s witnessed an unprecedentedly fast development and maturation of the methodology and theoretical foundations of data analytics across various disciplines from data mining, statistical learning, to knowledge discovery in databases (KDD), and we will label this as the first wave of big data analytics. In this period, the development of data analytics fell primarily in the realm of academia. Humanity has never stopped pushing the boundary of knowledge. After the first wave, the huge success in methodological and theoretical development of data analytics quickly spread to every corner of the research world, and even industry. The value of big data was increasingly recognized as its potential to change and improve society.

II. METHODOLOGY

Identity-Based Proxy Re-Encryption (IB-PRE)

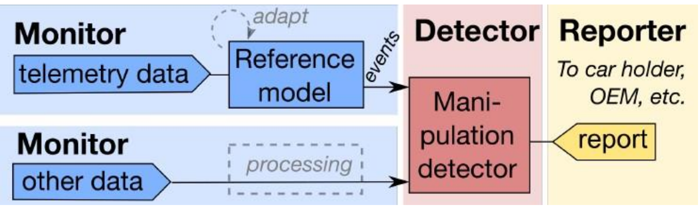
Proxy reencryption was proposed to enable a semi-trust proxy to convert a ciphertext with one's identity to a new ciphertext under a different identity [5]. Later on, the notion of IB-PRE [6] was introduced to simplify PKI (Public Key Infrastructure) since the user's identity can be considered as a replacement of the

public key in an IB-PRE scheme. One might think the IB-PRE can be a trivial solution to partially address the IBE drawback described in above application in a cloud environment. For example, Alice, with identity id, can generate a reencryption key rkid→ idi,.... rkid→idn for each colleague in the delegation list S = {idl, id2,..., idn} then she forwards these re-encryption keys to the cloud server. As soon as the server receives the keys, it has the flexibility to re-encrypt the ciphertext for each delegatee accordingly. Moreover, with IBPRE, it is convenient to revoke the individual's re-encryption by simply removing the user from the delegation/revocation list. However, similar to IBE, this solution is very inefficient as Alice is required to compute a re-encryption key for every delegate, in which the number of re-encryption keys is linear to the total counts of delegates (O(n)). Consequent in a group.


Intra-vehicle IDSs
Flow-based
Payload-based
Hybrid
Rule-based
Time and Frequency Analysis –based
Computational Intelligence and Information Theory
Others/Hybrid
Rule-based
Computational Intelligence and Information Theory
Others/Hybrid

We categorise intra-vehicle IDSs into: flow-based, pay load based, and hybrid IDSs. A flow-based IDS monitors the internal network of a vehicle, typically the CAN bus, and extracts distinct features (e.g., message frequency and interval) from the messages transmitted on the network. It then uses the extracted features to identify intrusions or abnormal behaviours without inspecting the payload/content of the messages.

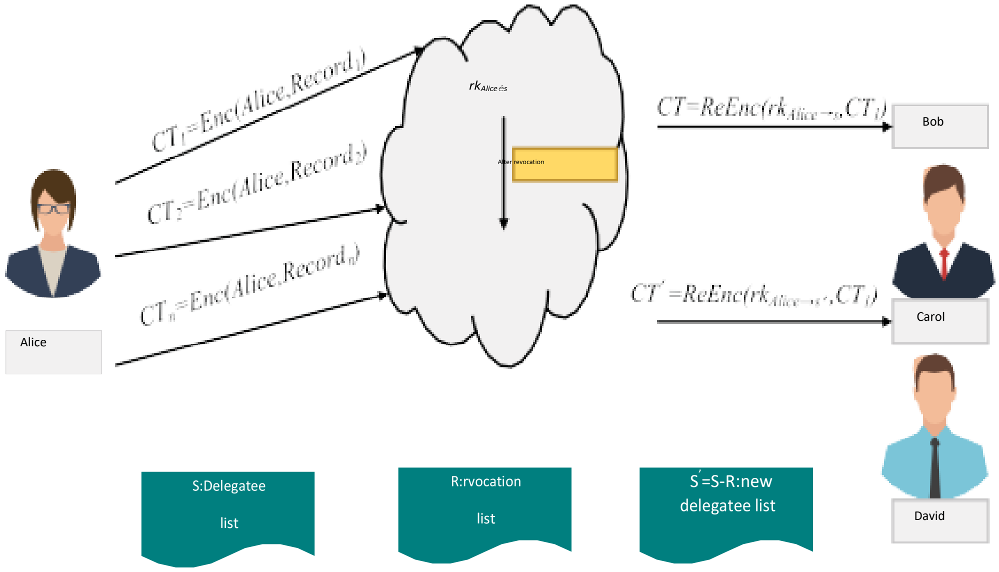
Ling and Feng [21] presented an algorithm for intrusion detection in CAN. The concept is based on combining the IDs of messages transmitted on the CAN bus with their interruptible occurrence frequency. For a given input ID, the algorithm counts the number of continuous messages that belong to the given message type (i.e., ID). If the count of messages in the interruptible sequence is greater than a predefined threshold, the algorithm raises an alarm of a possible attack. Although its simplicity, the proposed algorithm has limited capability in detecting attacks that manipulate the content of messages while maintaining their frequency



Rule-based IDSS: Bezemskij et al. [35] developed a detection mechanism that monitors real-time cyber and physical features from different on-board sources (e.g., sensors, networks, and processing) of a robot vehicle. In the learning phase, the vehicle learns the normal value range of the features (i.e., normal behaviour profile). The normal behaviour profile is based on signature characteristics of each data source. If an observed value of a feature is out of its normal range, the detection mechanism reports an attack. The tolerance of the proposed mechanism towards false positives and false negatives is controlled by a sensitivity index and individual weights for features are used to fine tune their importance in detecting anomalies, resulting in an improved detection accuracy. The proposed mechanism was evaluated on three types of attack: compass manipulation, MI and rouge node attack. The proposed method achieved an AUC of 1, 1, and 0.875 for the three attacks, respectively. However, the performance of the proposed mechanism on other attacks was not presented. In addition, the proposed mechanism was evaluated on a robot vehicle with a limited mobility capability, which might not be a good representative of the real-world where vehicles are more capable and various driving conditions exist.

Identity-Based Broadcast Proxy Re-Encryption (IBBPRE)

The notion of broadcast proxy re-encryption (BPRE) [7] has been proposed to eliminate the linear computation for re-encryption key generation. Doing so can also resolve the heavy computation issue of IBE. Instead of generating re-encryption key for every single delegatee in the group, a proxy (e.g. a cloud server) only needs to have a broadcast reencryption key in a BPRE scheme to transform a delegator's ciphertext to a set of delegatees' ciphertext without revealing plaintext to the proxy. Since then, some researchers introduced the notion of identity-based broadcast proxy re-encryption where the user's identity is used as its public key [8]. Despite the potential heavy communication of re-encryption key is resolved by IB-BPRE, key revocation problem still exists in IB-BPRE. Some may argue that Alice can generate a new broadcast re-encryption key as soon as each revocation occurs. As we pointed out earlier, this brings inconvenience to the user Alice since she has to show and present her private key to produce the broadcast re-encryption key. Such a process violates the original intention of cloud computing which is leaving the heavy computing task to the cloud not the user. Moreover, if re-encryption key is leaked in existing IB-BPRE schemes, anybody who obtained the key can re-encrypt the ciphertext. Hence, Alice needs to establish a secure channel to transmit the re-encryption key for each re-encryption key update.


CT_1=Enc(Alice,Record$_1$)
CT_2=Enc(Alice,Record$_2$)
CT_n=Enc(Alice,Record$_n$)
Alice
$rk_{Alice\, s}$
After revocation
CT=ReEnc($rk_{Alice\to s}$,CT_i)
Bob
CT′ =ReEnc($rk_{Alice\to s'}$,CT_i)
Carol
David
S:Delegatee list
R:rvocation list
S′=S-R:new delegatee list

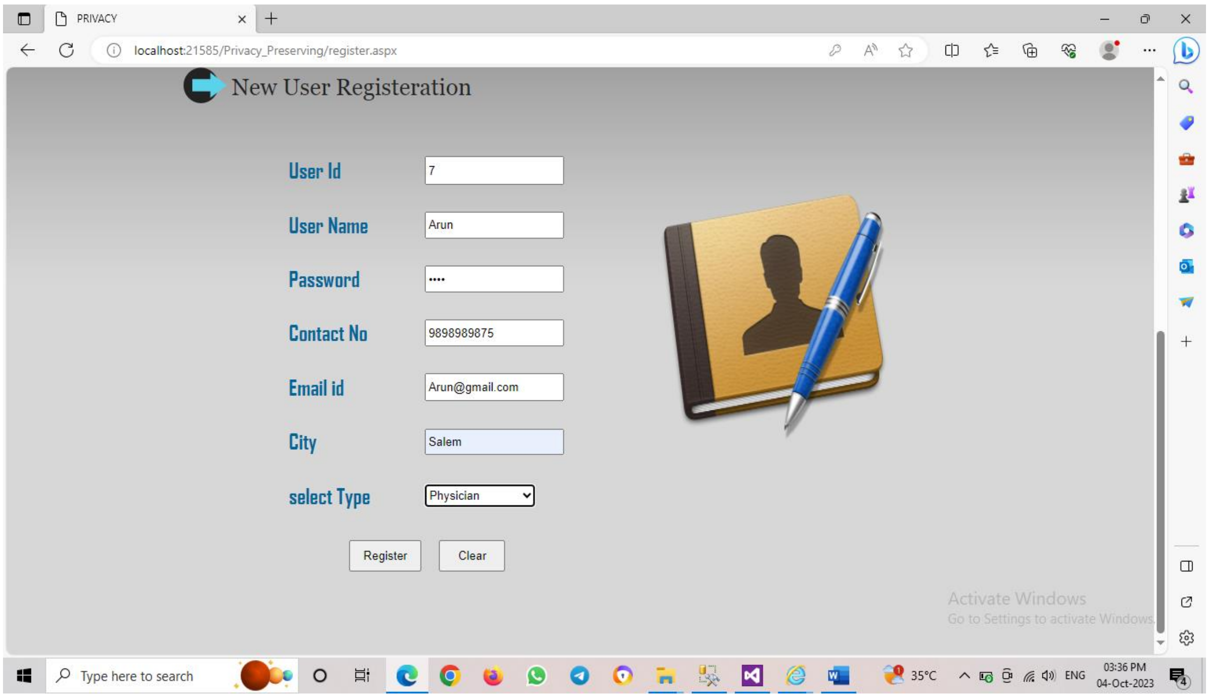
This section describes the definition of revocable identity based broadcast proxy re-encryption and the semantic security model. A. RIB-BPRE A RIB-BPRE system consists of a delegator, a proxy and a set of delegatees. In the system, the delegator outsources his encrypted data to the proxy. The delegator first generates a broadcast re-encryption key which will be used to transform his ciphertext to the delegatees' ciphertext. Then he sends the re-encryption key to the proxy so that the proxy can reencrypt the delegator's ciphertext on his behalf. Whenever the delegator wants to revoke a set of identities R from the sharing list S, he needs to update the revocation list and sync the new Computational Intelligence and Information Theory based IDSs: Theissler [39] proposed an OCSVM-based model that is capable of dealing with multivariate timeseries data to detect errors or faults. Experimental results on a real dataset showed that the proposed model can detect anomalies/faults with Training Time (TTT)between 20843 and 63631 sec, Testing Time (TST) between 4845 and 24145 sec, False Negative (FN) between 0.0/h and 10.5/h, True Negative (TN) between 9/h and 45/h, True Negative Rate (TNR) between 42.9% and 76.9%, and precision between 32.3% and 100%. Although the proposed model was evaluated on a real dataset that contains errors or faults, the performance of the proposed model on a dataset that contains cyberattacks was not presented. In addition, in term of computational complexity, the SVM is considered demanding, especially when dealing with big datasets, as it has a complexity of O(N3) [40]. This might hinder the applicability of the proposed in real-world.

Definition 1 (RIB-BPRE)

A revocable identity-based broadcast proxy re-encryption scheme consists of the following algorithms: Setup(2, N) -> (mpk, msk): The Setup algorithm is run by a trusted party, on input a security parameter 2 and the maximum number N of receivers in one encryption. Outputs the master public parameters mpk and a master secret key msk. Extract(msk, id) → skid: The Extract algorithm is run by the trusted party to generate a private key for each identity. It takes as input the master secret key msk, and an identity id, outputs a private key skid. Enc(id, M) → C: The encryption algorithm Enc is run by anyone who encrypts the message with the delegator's identity. It takes as input a message M, an identity id, outputs the original ciphertext C that can be further reencrypted. • RKeyGen(id, skid, S, k) → rk: The RKeyGen algorithm is run by the delegator to generate a re-encryption key. It takes as input an identity id, private key skid, a set of delegates' identities S = {idl,", idn} and a maximum revocation number k, where id/E S and k≤ n ≤N. Outputs the re-encryption key rk. The re-encryption key rk can be used to convert an original ciphertext C under id to a new broadcast ciphertext CT under S. Revoke(rk, S, R) →rk0: The Revoke algorithm is run by a proxy to generate a new re-encryption key that revokes identities from the sharing list. It takes as input a re-encryption key rk y set S, a revocation identity set R, where RCS and /R/≤K. Outputs a new for identityre-encryption key rk0. The re-encryption key rk0 can be used to convert an original ciphertext C under id to a new ciphertext CT under S - R. ReEnc(C, rk) → CT/1: The re-encryption algorithm ReEnc is run the proxy to transform the delegator's ciphertext to the delegatees' ciphertext. It takes as input an original ciphertext C, a re-encryption key rk, outputs the re-encrypted ciphertext CT or an error symbol 1.. Dec(skid, C/CT) → m/1: The Dec algorithm is run by the delegator (or a delegatee) to decrypt the original ciphertext (or re-encrypted ciphertext). It takes as input a private key skid, an original/re-encrypted ciphertext C/CT. Outputs the plaintext M if the ciphertext is a valid ciphertext or an error symbol 1 otherwise.

III. RESULTS AND DISCUSSION

New User Registeration:



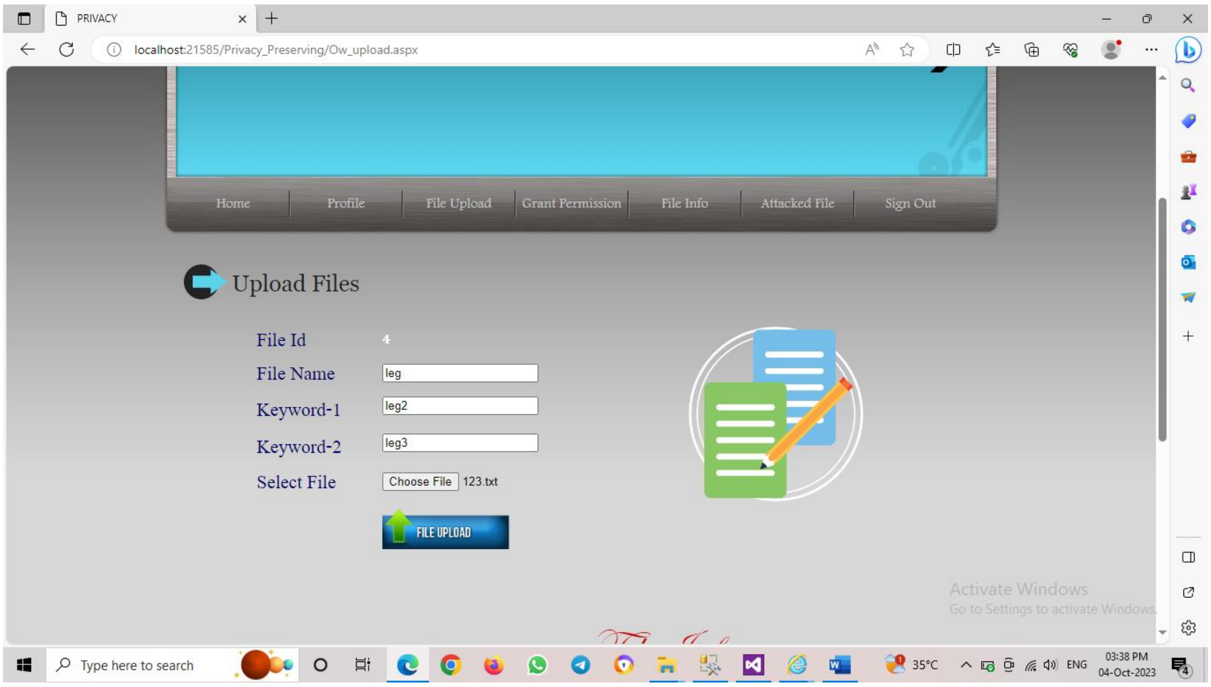
PRIVACY
localhost:21585/Privacy_Preserving/register.aspx

New User Registeration

User Id	7
User Name	Arun
Password	••••
Contact No	9898989875
Email id	Arun@gmail.com
City	Salem
select Type	Physician

Register Clear

Upload File:



Upload Files

File Id 4

File Name leg

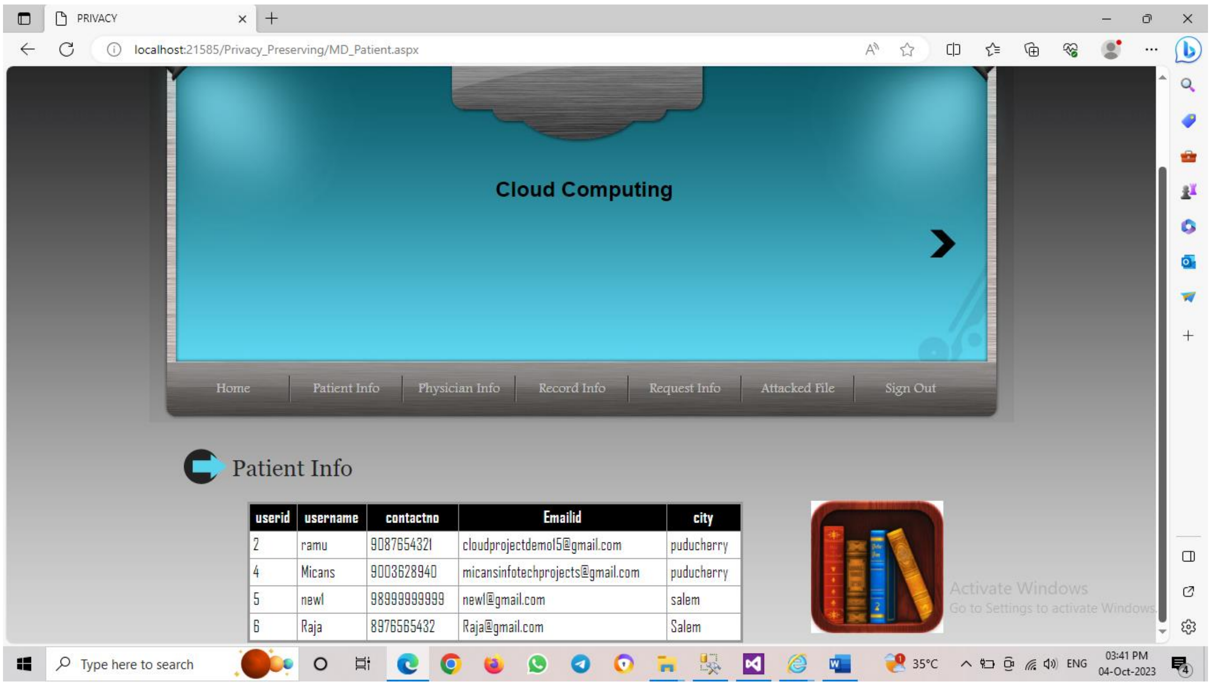
Keyword-1 leg2

Keyword-2 leg3

Select File Choose File 123.txt

FILE UPLOAD

Patient Info:



Patient Info

userid	username	contactno	Emailid	city
2	ramu	9087654321	cloudprojectdemo15@gmail.com	puducherry
4	Micans	9003628940	micansinfotechprojects@gmail.com	puducherry
5	new1	98999999999	new1@gmail.com	salem
6	Raja	8976565432	Raja@gmail.com	Salem

This paper designed an autonomous path broadcast proxy re-encryption as a new cryptographic primitive to support flexible data sharing in clouds. We formally define autonomous path identity-based broadcast proxy re-encryption and its security model, and demonstrate that our APIB-BPRE is CPA secure in the decision n-BDHE problem. More importantly, through performance analysis, our APIB-BPRE system is efficient and practical. In addition, our APIB-BPRE must be a multi-hop IB-BPRE, so that our APIB-BPRE system can provide much better fine-grained access control to delegation broadcast receiver sets than the traditional IB-BPRE employed in a cloud environment. It motivates researchers to design other APIB-BPRE schemes to support many interesting applications.

IV. CONCLUSION

This paper designed an autonomous path broadcast proxy re-encryption as a new cryptographic primitive to support flexible data sharing in clouds. We formally define autonomous path identity-based broadcast proxy re-encryption and its security model, and demonstrate that our APIB-BPRE is CPA secure in the decision n-BDHE problem. More importantly, through performance analysis, our APIB-BPRE system is efficient and practical. In addition, our APIB-BPRE must be a multi-hop IB-BPRE, so that our APIB-BPRE system can provide much better fine-grained access control to delegation broadcast receiver sets than the traditional IB-BPRE employed in a cloud environment. It motivates researchers to design other APIB-BPRE schemes to support many interesting applications.

V. REFERENCES

[1] I. Teranishi, J. Furukawa, and K. Sako, “k-times anonymous authentication (extended abstract),” in Advances in Cryptology ASIACRYPT 2004. Springer, 2004, pp. 308–322.

[2] D. Chaum, “Blind signature system,” in Advances in cryptology. Springer, 1984, pp. 153–153.

[3] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, “A practical and provably secure coalition-resistant group signature scheme,” in Annual International Cryptology Conference. Springer, 2000, pp. 255–270.

[4] M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2003, pp. 614–629.

[5] Y. Dodis and A. Yampolskiy, “A verifiable random function with short proofs and keys,” in International Workshop on Public Key Cryptography. Springer, 2005, pp. 416–431.

[6] A. de Solages and J. Traor´e, “An efficient fair off-line electronic cash system with extensions to checks and wallets with observers,” in International Conference on Financial Cryptography. Springer, 1998, pp. 275–295.

[7] O. Bic¸er and A. K¨upc¸ ¨ u, “Versatile abs: Usage limited, revocable, threshold traceable, authority hiding, decentralized attribute based signatures.” IACR Cryptology ePrint Archive, vol. 2019, p. 203, 2019.

[8] I. Teranishi and K. Sako, “k-times anonymous authentication with a constant proving cost,” in Public Key Cryptography - PKC 2006, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds. Springer, 2006, pp. 525–542.

[9] L. Nguyen and R. Safavi-Naini, “Dynamic k-times anonymous authentication,” in Applied Cryptography and Network Security. Springer, 2005, pp. 318–333.

[10] L. Nguyen, “Efficient dynamic k-times anonymous authentication,” in Progress in Cryptology - VIETCRYPT 2006. Springer, 2006,pp. 81–98