UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

ADVANCED ATTRIBUTE BASED SEARCHABLE ENCRYPTION SCHEME FOR CLOUD INTRUSION DECTION SERVICE

Katuboina N V Bala Ganesh Pavan Kumar[1] Kola Sangeetha Supriya[2], Devarasetti Prasad[3], Anumula Sruthi[4]

[1]M.Tech Student,CSE Department, DVR and Dr.HS MIC College of Technology,Kanchikacherla,NTR District, Andhra Pradesh, India

[2]Assistant Professor,CSE Department ,DVR and Dr.HS MIC College of Technology,Kanchikacherla,NTR District, Andhra Pradesh, India

[3]Professor,CSE Department ,DVR and Dr.HS MIC College of Technology, Kanchikacherla,NTR District, Andhra Pradesh, India

[4]Assistant Professor, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur District, Andhra Pradesh,India

Abstract: The searchable encryption (SE) is used structured encryption, which has been analysis secure cloud storage system stored information and encryption keys are usually managed by the cloud provider. New method of the data access control for Industrial Internet of Things (IIoT) applications is integrated industrial system contains all kinds of data with rigorous access permissions. We propose a proxy re encryption technique which performs a two level encryption before storing the actual data into the cloud. We have used AES (Advanced Encryption standard) technique to encrypt data as well as decrypt data this paper also introduce the Cloud Intrusion Detection Service (CIDS) which detect the different attack and fire the alert to other cloud user. We have extracted different features like extra security forward secrecy, confidentiality, and secure data sharing. In this paper we used RS- IBE (Revocable Storage Identity- Based Encryption) algorithm for the security as well as recognized all members of system. To ensure the security of data we proposed a method by implementing RSA algorithm. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations

and to determine the cheating party in the system (CSP or Owner). Trusted authority send file to CSP module to store on cloud.

Index Terms: HealthCare, Fog computing, Cloud computing, Security, Sensitive data, Patient information, Attribute-based signatures, Attribute-based encryption, proxy server, encryption, privacy

1. INTRODUCTION

Advanced Industrial Internet of Things (IIoT) is new role increasingly significant connecting a larger number of physical objects in industrial systems, including sensors, intelligent method, RFID tags, and other intelligent terminal devices [1]. Sensitive data should be encrypted before uploading to cloud servers and a secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage [2]. . It provides the most modern security protocols. Conventionally, Cryptographic techniques provide protection for data and information transmitted over the network [3]. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity [4]. The large utilization of sensors, mobility, and geographic distribution lead to issues of data volume, velocity, and variation, along with requirements for accuracy, security, Quality of Service (QoS) user expectations, and operational costs [5]. In this paper proposes encryption technique to providing extra-large security in cloud computing. Key is used to encrypt any type of data. Key function provide random key to data provider and number of user [6]. Data Provider is nothing but the server and data provider is responsible for the upload the data or files to storage sever. Number of user access the uploaded data of files or download the files using the key as well as opt code [7]. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures [8]. Cloud computing is a hub of various server and many database to store data. The availability of these resources are very flexible in nature i.e. few are available to customers free of cost but some on a pay as use basis [9].

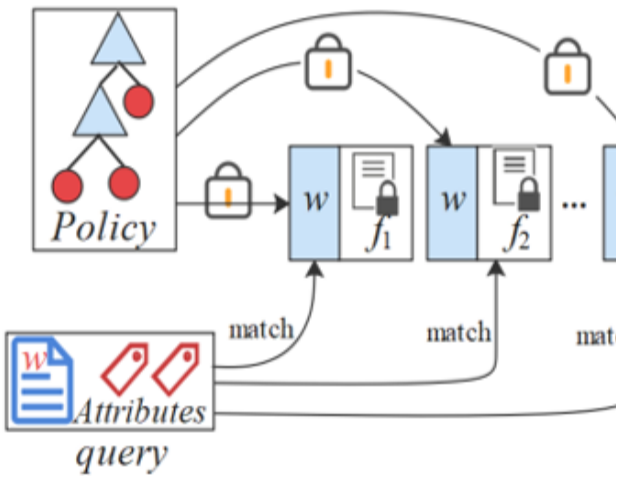

Figure 1: Naive application schemes.

2. RELATED WORK

Researches on data privacy in cloud computing are still in its early stages. Security and privacy is another concern for scientific cloud computing users. Data in cloud can be protected through giving valid access control to valid user [10]. The defense strategy should is flexible architecture to be applied to several cloud architecture and to Integrate both behavior and knowledge based techniques scheme propose the deployment of IDS on each layer of the Cloud to gather and correlate the alerts from different sensors [11]. Later proposed a authenticated key agreement scheme by applying chaotic map-based cryptography to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process allowing the patient to enjoy the secure and convenient healthcare through the TMIS [12]. The Health IoT enabled framework collects ECG data from smart phones and other sensors. Later send the collected to the cloud so that Doctors can access and assess the data seamlessly [13]. Cloud-based data analytics is used to detect the abnormality and error of the health data. Normally forward secrecy backward secrecy provided for security [14]. Forward secrecy is used for advanced security. Revoke user can't access the previous or subsequent data so that revocable identity based encryption technique is used. Data providers upload the files into storage server using the encryption technique [15].

Figure 2: Generalized Fog environment

3. SYSTEM DESIGN

User send request for accessing data permission to data provider via storage server. Then key authority generates the key as per user requested data. These generated key is send to user receiving key data provider key and user key will be match [16]. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety [17]. It is asserted that the plan can accomplish fine-grained access control and repudiated clients won't have the capacity to get to the sharing information again once they are revoked.

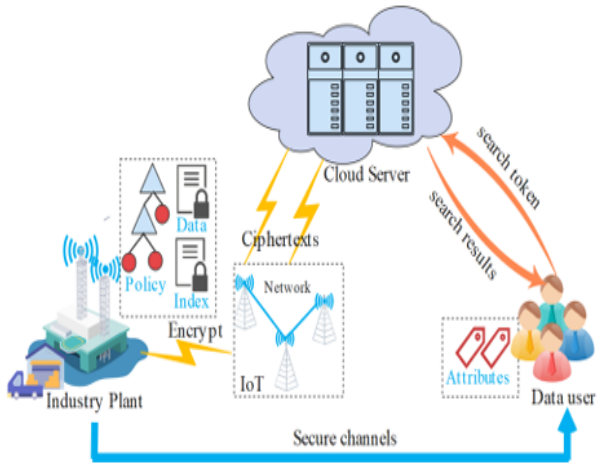

Figure-3: System Architecture

4. RESEARCH METHODS

We introduced novel concept “two level encryption” for that we uses DES algorithm and linear congruential generator. All stored patient information has search index and privacy table. Search index contains only the keywords that are searchable since encryption keys are common to all patients [18]. Network admin maintains the Privacy table which contains unique encryption key for all the patients. RSA is a block cipher in which every message is mapped to an integer

[19]. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data [20]. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the entrusted cloud [21].

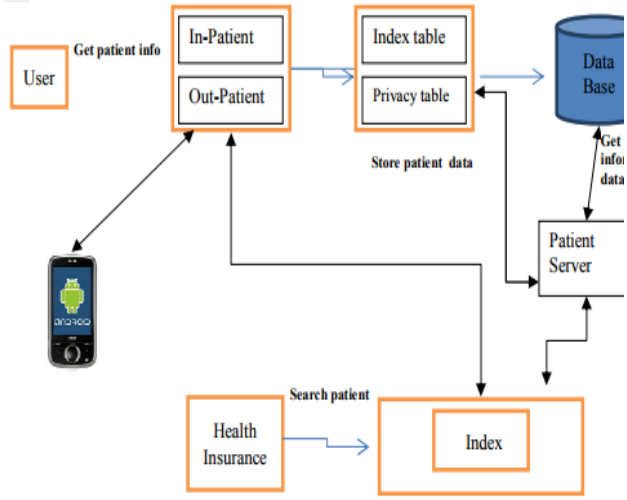

Fig. 4 Privacy preservation in Health care system

A. Homomorphism Scheme

Cryptographic techniques provide protection for data and information transmitted over the network. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity. Modern cryptography includes the disciplines of mathematics as well as computer sciences and engineering [22]. A cryptosystem performs a pair of transformations called encrypting and decrypting. Encryption means encoding the data so that it cannot be intercepted by anyone except the one who is intended receiver after transforming back to plaintext [23].

1. Key Generation (λ)
   - **Input:** Security parameter λ
   - **Output:** A tuple (Si , Pi) consisting of the secret key Si and public key Pi .
2. Encryption (Pi , Pt)
   - **Input:** A public key Pi and a plaintext Pt
   - **Output:** cipher text Ct
3. Decryption (Si , Ct)
   - **Input:** a secret key Si and a cipher text Ct
   - **Output**: the corresponding plaintext Pi
4. Evaluation (Pi , C, Ct)
   - **Input:** a public key Pi a circuit C with x inputs and a set Pt of x ciphertext,Pt1,Pt2,Pt3,..,.Pt x
   - **Output:** a cipher text Ct

5. HEALTHCARE SOLUTION STRUCTURE

We discuss a general structure of the Cloud-based IoT-Healthcare solutions. Later a Fog-based IoT-Healthcare solution structure in proposed which can be interoperable with the Cloud-based solutions Cloud-based IoT-Healthcare usually comprised of several entities IoT sensors wearable devices [24]. In Healthcare solution, hand held or body connected devices for example; pulse dosimeter ECG monitor smart watches perceive health context of the users. Resource manager is responsible for coordinating the Cloud resources while dealing with IoT enabled Healthcare data [25]. In Cloud-based Healthcare system, two types of Servers are used predominantly Application Server and Database Server. In Application Server the backend applications web-services are hosted whereas Database Server solely handles the data repository and associate operations [26].

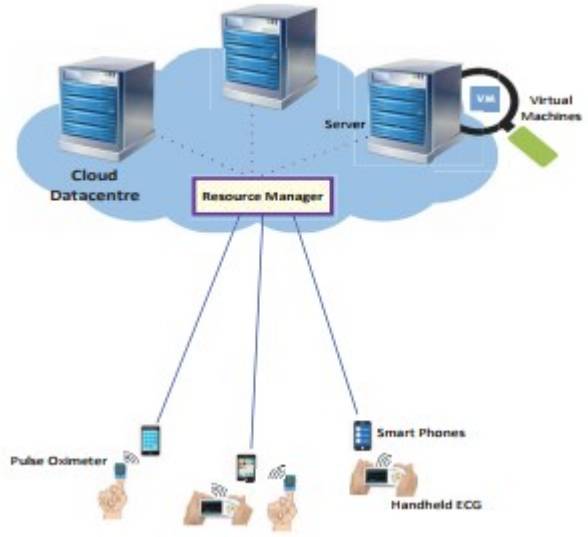

Figure 5: Cloud-based Healthcare System Architecture

A. RSA Algorithm:

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data [27]. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only [28].

The data is encrypted, Key generation should be done. This process is done

between the Cloud service provider and the user

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.

2. Compute n = a * b.

3. Compute Euler's toting function, Ø(n) = (a-1) * (b-1).

4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.

5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplication inverse of e mod Ø(n).

6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).

7. The Public-Key consists of modulus n and the public exponent e (e, n).

8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret (d, n).

User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

B. AES Algorithm

Algorithm finds the Proxy Re-Encryption: A PRE scheme is represented a topple of polynomial time algorithms (KG; RG; E; R; D). (KG; E; D) are the standard key generation, encryption, and decryption algorithms [29].

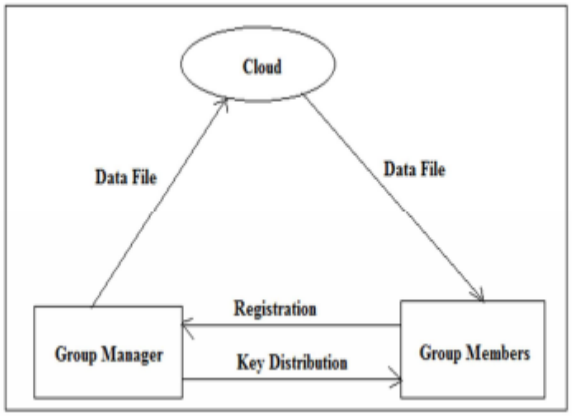

Fig. 6. System Architecture

Step 1: Choose two distinct prime numbers p and q.

Step 2: Find n such that n = pq. n will be used as the modulus for both the public and private keys.

Step 3: Find the toting of n, ϕ(n) ϕ(n)=(p-1)(q-1).

Step 4: Choose an e such that 1 < e

In other words pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or ϕ(n). This is often computed using the Extended Euclidean Algorithm, since e and ϕ(n) are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent Another research direction would be to give the data owner physical access control over the data [30]. Instead of accountability the data owner can create a set of access control rules on his data and send the data along with the access control policy.

6. PERFORMANCE ANALYSIS

Performance analysis on RSA, ElGamal, Paillier algorithms based on the following parameters on local system for different input size DES uses 56-bitkey (8 bit parity) and produce output of 64 bit block. In AES, key length varies from 128, 192, to 256 bits .In Triple Data Encryption algorithm, use 192 bits key size.

RSA uses 1024-bit keys but its not secure and it works only if it is correctly implemented and good key management is employed. So here in my system papillae with homomorphism property containing mathematical operation over encrypted data is utilized, encrypted with 308 bit of keys with advanced technology to protect the data. Hackers will find it difficult to decrypt such encrypted data. Hence papillae cryptosystem is proved to be a stronger mechanism.

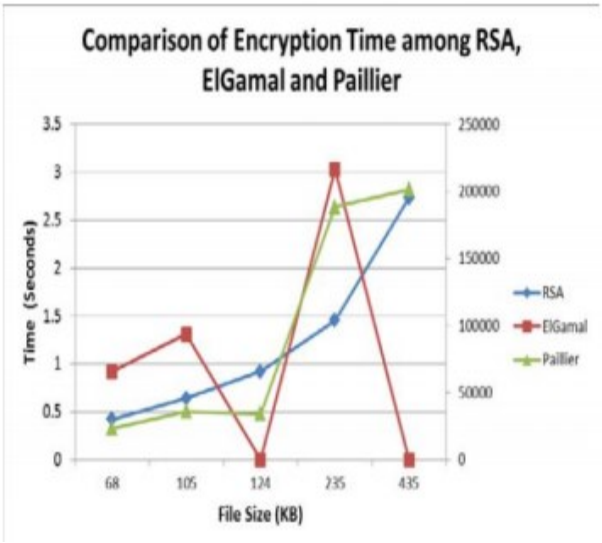

Figure 7: Comparing RSA, Elgamal and Paillier Encryption Time

7. CONCLUSIONS AND FUTURE WORK

Our construction achieves fine-grained keyword search privilege control and data searching over encrypted IIoT data. More importantly, our scheme is with the same search complexity as the traditional SE, which is only linearly dependent on the number of matching data files. This method can solve the issue of protecting

patient private information against unauthorized viewers and provide high level of protection. With the inclusion of modern techniques like the Internet of Things (IoT) these Cloud-based solutions become more dynamic and user oriented. However, Cloud itself has some limitation due to its geographically centralized architecture and multi-hop distance from the IoT data source. We have used RS-IBE and AES algorithm to revoke as well as encryption, re-encryption and decryption. We have given time period to users for downloading data. Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.

8. REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] Fang-Yie L., Jia-Chun L., Ming-Chang L., and Chao-Tung Y., —A Performance-Based Grid Intrusion Detection System,‖ in Proc. 29th Annual IEEE International Computer Software and Applications Conference (COMPSAC), pp.525-530, July, 2005

[3] Jansen W., Karygiannis, T. 1999, —Mobile agents and security‖. Special Publication 800-19, NIST

[4] C. Doukas and I. Maglogiannis. 2012. Bringing IoT and Cloud Computing towards Pervasive Healthcare. In In Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 922–926.

[5] Dubey, Harishchandra and Yang, Jing and Constant, Nick and Amiri, Amir Mohammad and Yang, Qing and Makodiya, Kunal. 2015. Fog Data: Enhancing Telehealth Big Data Through Fog Computing. In In Proceedings of the ASE BigData & SocialInformatics 2015 (ASE BD&SI '15). ACM, New York, NY, USA, Article 14, 6 pages

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[7] International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518

[8]. P.Kalpana, "Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3, ISSN 2249–071X, June 2012.

[9]. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[10] Jansen W., Karygiannis, T. 1999, ―Mobile agents and security‖. Special Publication 800-19, NIST.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[12] C. Doukas and I. Maglogiannis. 2012. Bringing IoT and Cloud Computing towards Pervasive Healthcare. In In Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 922–926.

[13] Dubey, Harishchandra and Yang, Jing and Constant, Nick and Amiri, Amir Mohammad and Yang, Qing and Makodiya, Kunal. 2015. Fog Data: ACM, New York, NY, USA, Article 14, 6 pages.

[14] G. Muhammad and S. M. M. Rahman and A. Alelaiwi and A. Alamri. 2017. Smart Health Solution Integrating IoT and Cloud: A Case Study of Voice Pathology Monitoring. IEEE Communications Magazine 55, 1 (January 2017), 69–73.

[15] Gupta, Harshit and Vahid Dastjerdi, Amir and Ghosh, Soumya K. and Buyya, Rajkumar. A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. Software: Practice and Experience, 2017 ([n. d.])

[16]. Zaigham Mahmood, "Data Location and Security Issues in Cloud Computing", Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[17] Vishwa gupta, Gajendra Singh, Ravindra Gupta, “Advance Cryptography algorithm for improving data security”, International Journal of Advanced Research in Computer

[18] Rongxing Lu, Xiaohui Liang, Xu Li, XiaodongLin andXuemin (Sherman) Shen, ” SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency” IEEE Transactions on Parallel and Distributed Systems ,Volume: 24, Issue: 3, March 2013 .

[19] Rongxing Lu, Xiaohui Liang, Xu Li, XiaodongLin andXuemin (Sherman) Shen, ”EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications”,IEEE Transactions on parallel and distributed systems Volume: 23, Issue: 9, Sept. 2012.

[20] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed paper on “Privacy Preserving Delegated Access Control in Public Clouds”.

[21] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong” proposed a paper on ”A DFABased Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”.

[22] Tzu-Wei Tseng, Cheng-Yi Yang, Chien-Tsai Liu, “Designing Privacy Information Protection of Electronic Medical Records”, IEEE2016 International Conference on Computational Science and Computational Intelligence, April 2016.

[23] Jisha S, Mintu Philip, “RFID based Security Platform for IOT in Health Care Environment”, IEEE Online International Conference on Green Engineering and Technologies ,(IC-GET) 978-1-5090-4556-3/16 , 2016 .

[24] M. Shamim Hossain and Ghulam Muhammad. 2016. Cloud-assisted Industrial Internet of Things (IIoT) âĂŞ Enabled framework for health monitoring. Computer Networks 101, Supplement C (2016), 192 – 202. Industrial Technologies and Applications for the Internet of Things.

[25] Jindal, Vasu. 2016. Integrating Mobile and Cloud for PPG Signal Selection to Monitor Heart Rate During Intensive Physical Exercise. In In Proceedings of International Conference on Mobile Software Engineering and Systems

(MOBILESoft ’16). ACM, New York, NY, USA, 36–37.

[26] M. Chen and Y. Qian and J. Chen and K. Hwang and S. Mao and L. Hu. 2017. Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing. IEEE Transactions on Cloud Computing PP, 99 (2017), 1–1

[27]. G. Jai Arul Jose, C.Sanjeev, Dr. C.Suyambulingom, “Implementation of Data Security in Cloud Computing”, International Journal of P2P Network Trends and Technology, Vol 1, Issue 1, 2011.

[28].William Stallings, “Network Security Essentials Applications and Standards”, Third Edition, Pearson Education, 2007.

[29]Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou” proposed a paper on ”Privacy Preserving Ranked MultiKeyword Search for Multiple Data Owners in Cloud Computing”.

[30]Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou” proposed a paper on ”CostEffective Authentic and Anonymous Data Sharing with Forward Security”.