International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

CAMP: Cloud Assisted Mobile Health Care System with Privacy

R.Abirami M.C.A[1], Dr. S.T. Deepa MCA., M.Phil., SET Ph.D[2]

[1]MPhil Scholar, Dept.of.Computer Science, Mother Teresa Women's University, Kodaikanal, India

[2]Assistant Professor, Dept. of Computer science, Shri Shankarlal Sundarbai Shasun Jain College for Women, Chennai, India

Abstract: ***A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. In cloud, it is hard to maintain patient healthcare information. To solve this problem, we proposed a monitoring and advising patient's health care via mobile health care system in the medical field. The main objective of the proposed system is preserving the privacy of the medical history of the patients and the service providers. Anywhere-Anytime accessible e-health care systems plays an important role in our daily life. Services supported by mobile devices such as home care, reduction of the cost and time of travel for patients and remote monitoring which reduces in-hospital treatment cause patients with minimal interruptions to their daily activities. We incorporate the recent technique called Advanced Encryption Standard (AES) which overcomes all the security issues in sharing the personal health data with privacy and auditability. By using this technique the user receives an alert message in mobile if any one hackers the health data. Finally, the formal security proof and simulation results illustrate our scheme can resist various kinds of attacks and far outperforms the previous ones in terms of computational, communication and storage overhead.***

Keywords: e-Health, Remote Monitoring, Advanced Encryption Standard, Privacy, Simulation results.

1. Introduction

Mobile devices are increasingly becoming an essential part of our everyday life due to the rapid reduction in cost of land wave, improved portability and increasing computational capability. Mobile Cloud Computing (MCC) is the combination of cloud computing, mobile computing and wireless networks. The purpose of applying mobile cloud computing in medical applications is to minimize the limitations of traditional medical treatment, such as physical storage, maintenance, security and privacy. Health care provides mobile users with convenience to store, access and maintaining patient's medical data including medical records, disease history, lab results, and prescription and billing information easily, quickly and safely. It also offers hospitals and healthcare organization a variety of on-demand services on clouds rather than owning standalone application on local server. There are many security and privacy risks in public health care services. Online collection of information, processing and transferring of personal data gave a server threat to privacy and security. We propose a feasible and promising approach of Advanced Encryption Standard (AES) to protect personal health data stored on semi trusting servers. To integrate AES into large scale PHR system, important issues such as key management scalability, dynamic policy updates and efficient on demand revocation are nontrivial to solve and remains largely up-to date.

2. Literature Review

G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis [4] proposed a medical information privacy assurance cryptographic and system aspects. It may be argued that medical information systems are subject to the same type of threats and compromises that plague general information systems and that does not require special attention from a search view point. Thresh and experience of expert information security and assurance that studied or worked with health applications has been of a die rent sort: While general principles of security still apply in the medical information held, a number of unique characteristics of the health care business environment suggest a more tailored approach. In this paper we describe some recent result so fan ongoing research on medical information privacy carried out at the Johns Hopkins University under the support of the National Science Foundation (NSF)[4].

In a flexible role-based secure messaging service by M. C. Mont, P. Bramhall, and K. Harrison (exploiting IBE technology for privacy in health care) suggested about the management of private and confidential information's major problem for dynamic organizations. Secure solutions are needed to exchange confidential documents, protect them against unauthorized accesses and cope with changes of people's roles and permissions. Traditional cryptographic systems and PKI show their limitations, in terms of flexibility and manageability. It describes an innovative technical solution in the area of secure messaging that exploits identifier-based encryption (IBE) technology. It illustrates the advantages against a similar approach based on traditional cryptography and PKI. It discusses a few open issues. Main contribution of this paper is a practical solutions based on IBE technology. A secure messaging system based on IBE has been fully implemented and it is currently used in a trial with a UK health service organization [3].

A. Cavoukian et al. [6] deals many remote home health care systems which allows individuals to personalize and convert devices, with the goal of enabling greater patients freedom, reducing cost and improving the ability for patients to be able to follow the wellness and treatment plan created for them by their medical practitioners. This remote home health care systems provide long term care to patients, to keep their physical fitness, nutrition, social activity, so they

may function independently in their own homes for as long as possible, can help to deal with the social and financial burden of an aging population.

Lee and Lee proposed a cryptographic key managementsolution for privacy and security regulations regarding patients'PHI. Patients have control over their PHI and are able to restrictaccess to it. When the physician needs to review the PHI fortreatment, he has to obtain agreement or consent from patientswho will use the proper keys stored on a smart card to decrypt thePHI ciphertexts. The authors then proposed a consent exceptionsolution for emergencies, where a trusted server possesses allsecret keys of the patient and hence can retrieve the PHI plaintextsupon emergency. Although technically correct, the proposedscheme is unreasonable since the trusted server is able to accessthe patients' PHI at any time. As a result, PHI privacy is notfully guaranteed which is unacceptable for extremely sensitiveinformation like PHI. Furthermore, the authors did not addressthe issues related to storing and retrieving PHI, which can beintricate given the privacy requirements.

3. Need of Cloud Computing In HealthCare Systems

The health care industry faces increased pressure to do more with less whether it's with patients, providers or regulators. Other industries facing similar pressures are increasingly running their business on the "cloud," giving them on-demand access to shared computing resources. Companies running on the cloud see lower costs, increased agility and improved ability to meet their business objectives.

a. The need to slash budgets

We must re-think health care IT purchasing habits. As the traditional black hole of cost, re-thinking how hospitals and care facilities document patient care can slash budgets dramatically. Cloud computing empowers providers to only pay for what they need. For example, there's no reason why every hospital room needs its own COW (computer on wheels) in addition to desktops at nurse stations and doctors' offices. By deploying iPads to document patient information at the point of care, hardware can be cut in half at a minimum.

b. Theneed to access increasing amounts of information

The importance of providing patient care with the correct records and information is widely understood. Moreover, information needs to be accessible at any time by anyone providing care. Cloud computing provides the flexibility of accessible data from a number of secure endpoints. From operating rooms, to examining rooms, to rehab facilities, information continuity is most effective when it's accessible to the right people.

c. The need to share and access information anywhere

Health care collaboration used to be synonymous with sending an email alert notifying a new patient has been added into the system. Today, it takes on a new meaning to focus on shared experience that increase information accuracy and overall patient care. Cloud-based platforms allow collaboration in real-time from any device with an Internet connection. Multiple care providers can update an EHR (electronic health records) synonymously, and those updates can be traced back to their original creators for as long as the EHR is around making information readily available and more thorough.

d. The need for secure adoption by health care Professionals

Patients don't need to worry that an executive or doctor is secretly accessing the network using his/her iPad or iPhone when there is no need for them to. Cloud-based applications have security at the application level not the device level. In other words, there is no risk of patient information being accessed directly from the device. This level of security opens up health care IT departments to make better use of consumer based hardware that they are already familiar with, such as an iPhone.

4. Proposed System

The proposed models will be a User module, a Trusted Authority module and a Service Provider module. User module consists of an android app which will allow users to use the application in mobile environment. It will present before the user a login and through which access to app showing their requests, also user will be able to query the app for their schedule of medication. Trusted Authority module will act as an interface between user and service provider. It will hold the information provided by the users and provide the users with keys. The information is held by the trusted authority is in encrypted format so no way of information leak. The System stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model.

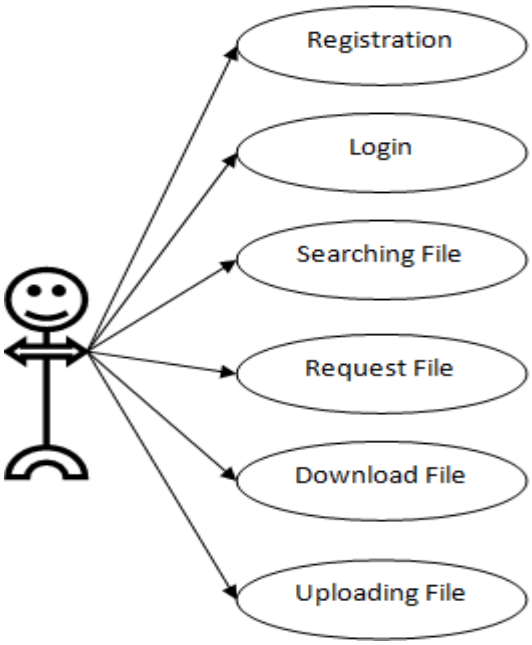

Figure 1: Use Case Diagram of Health care System

5. Technique Used

a. Advanced Encryption Standard (AES)

AES is an Advanced Encryption Standard used for secure transmission of data that is personal health record in encrypted format. In our system AES is used for sending user authentication data in encrypted format. AES allows three diverse key lengths: 128, 192, or 256 bits. For encryption, each round consist of the following four steps:

- Substitute Bytes
- Shift Rows
- Mix Columns
- Add Round Key

The last step consists of XORing the output of the previous three steps. For decryption, every round includes the following four steps:

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key
4. Inverse mix columns.

The third step consists of XORing the output of the previous two steps.

Step1: Substitute Bytes

- This step consists of using a 16 × 16 research table to find out a replacement byte for a given byte within the input state array
- The entries in the table are created by using the philosophy of summative inverses in GF (28) as well as scrambled bit to destroy the bit-level correlations inside every byte

Step2: Shift Rows

- The primary row of state is not altered
- The second row is shifted 1 byte to the left in a circular manner
- The third row is shifted 2 bytes to the left in a circular manner
- The fourth row is shifted 3 bytes to the left in a circular manner

Step3: Mix Columns

- Mix Columns for integration up of the bytes in every column individually during the process
- This step replaces each byte of a column by a function of all the bytes in the same column

Step4: Add Round Key

- Add Round Key to add the round key to the output of the cumulative step during the forward process
- In this stage, the 128 bits are bitwise XORed along with the 128 bits of the round key.
- The operation is viewed as column wise operation between is 4 bytes of status column along with one word of the round key

6. Performance Evaluation

a. Storage and Communication Efficiency

We analyze the storage and communication efficiency by looking at the storage and communication overheads during data outsourcing and retrieval. The overhead is defined to be any information that serves the purposes of management, security, bookkeeping, etc., but the essential healthcare data or its encryption. The storage overhead is mainly due to the use of Secure Index, which employs linked lists, the lookup table, and array.

We also investigate the communication overhead during an EMT's data request with a successful retrieval. For clarity, we decompose the communication into two parts, i.e., communication between data requesters, such as EMT, and the private cloud and that between the private cloud and the public cloud.

It is worth mentioning that although, the pattern hiding requires retrieving redundantfiles during data retrieval, which seems to significantly contribute to the overhead, it takes place only between the private and public cloud where the wired inter cloud connection is stable and fast, making the increased data transferring time negligible. On the other hand, the private cloud sends only the requested file to EMT (possibly through wireless channels, which are relativelyless predictable and of lower capacity). Therefore, it does not affect the overall performance very much. From the analysis above, we know that the storage overhead is linear with the number of outsourced healthcare data files, while the communication overhead can be considered as constant per data request. The result indicates that the proposed scheme is efficient as well as scalable.

b. Computation Efficiency

In this section, we analyze the computational efficiency of the proposed schemes. Specifically, we are interested in whether our schemes are efficient when mobile devices are involved, i.e., patients preparing the privacy-preserving storage and EMTs accessing the medical data in emergencies. We implemented our schemes using Samsung Nexus S smartphones (1-GHz Cortex- A8, 512-MB RAM) and measured the runtime. For implementations of AES, we used the Java Paring-Based Cryptography Library and used a pairing-friendly type-A 160-bitelliptic curve group. In privacy-preserving storage leveraging patient mobile devices, efficient secret key operations are mainly involved which we will not focus on in the evaluation. In emergency medical data access leveraging EMT mobile devices, the most costly real-time computation includes IBE decryption and ABE decryption, generating a regular signature on attributes and a partial threshold signature on the access request, and verifying the partial threshold signature from the private cloud. However, IBE decryption, ABE decryption, and regular signature can be performed once and for all access for the same patient, which isbeneficial if the EMT will issue multiple access requests. We still take this cost into account since an EMT is likely to access a patient's medical data only once in many cases.

7. Experimental Results

Many software applications, services, and dataonce in the domain of a local computer or local server safelysecure in your building are now in the domain of the publicInternet. Private health information once confined to theselocal networks is migrating, wholesale, onto the internet.Patients

voluntarily grant access to their healthrecords every time they sign a contract to the health insurerthat then decides on the payment disposition to the doctor,pharmacy, or hospital. For the most part, the collection andorganization of this data is completely legal.It then follows that companies want to automateand accelerate access to these records in order to offer "inthe cloud" products and services to patients, doctors, andinstitutions.

Registration is a mandatory process to get into a hospitalmanagement system for any doctor and Patient.

Figure 2: User Registration

A doctor and Patient have to provide their personal information to the patient healthcare monitoring to createtheir account.

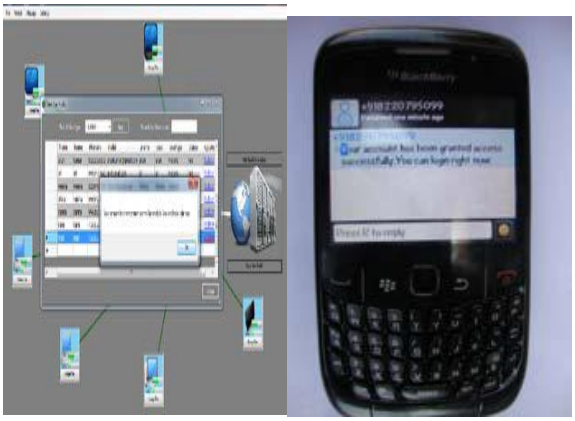

Figure 3: Admin updating

Admin will assess the given detail of a user and activatestheir account to view the patient healthcare monitoring. Afteractivation the user get message from admin by their mobile.An existing user can directly login to the system with theirvalid user name and password. Activated User can enter intopatient healthcare monitoring with their valid username andpassword.

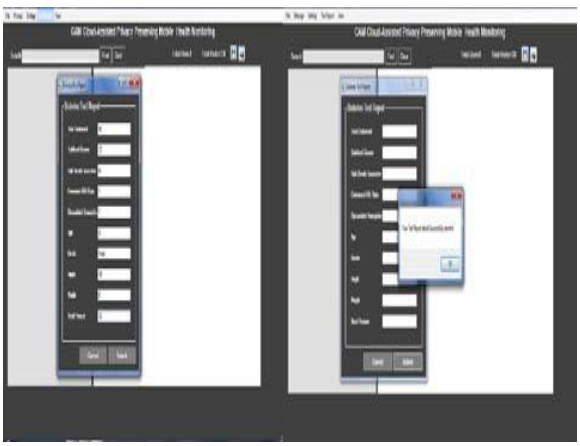

Figure 4: Patient upload test report

User should have all their test reports whatever related totheir disease which was advised by the doctor earlier. Cloudarea serves as a storage medium where all user records arebeing stored. When doctor login to the patient healthcaremonitoring by providing their valid user name and password,they can view the history of a patient.

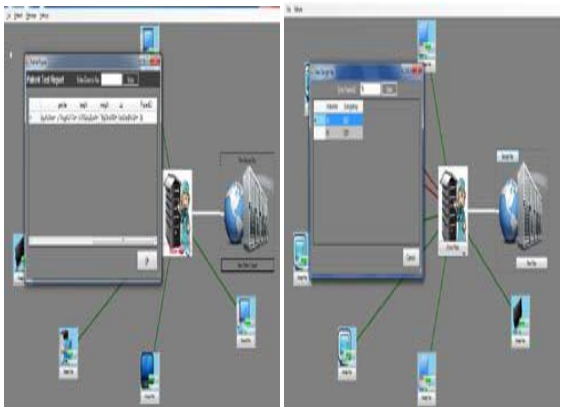

Figure 5: Doctor receives the ID & Private Master Key

When doctor wants to view the files of any patient, he will befinding all their reports in encryption format. To decrypt thistest report doctor have to get the patient ID from theappropriate column.

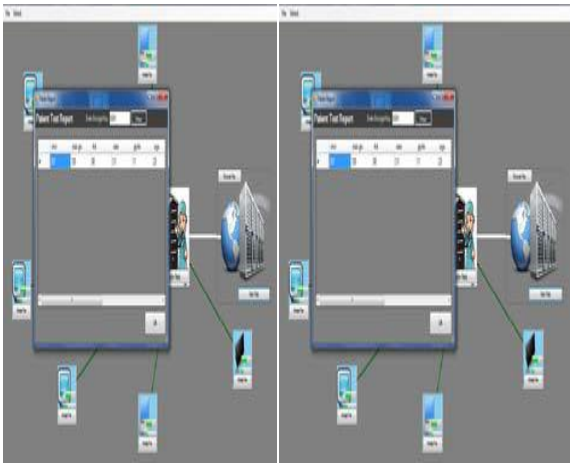

Figure 6: Doctor View the test report & gives prescription

This ID, which is used as Doctor's key. This helps him toview the patient test report in decrypted format. Then doctorwill decide the medicine to be prescribed, which will beentered by the doctor manually. This prescription to the userwill be saved in cloud server in encrypted format. If thepatient wants to view the doctor's prescription, user has tologin into the patient healthcare monitoring.

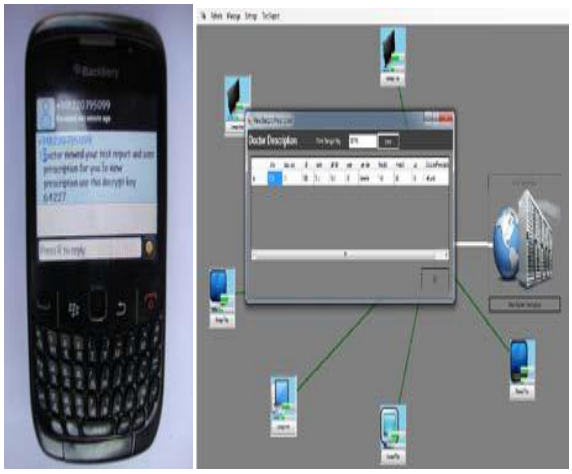

Figure 7: Patient get decrypt key & view prescription

Now the prescription will be in encrypted format. To decryptthey need a patient key. That will be sent to the given mobilenumber of the patient. Using patient key user can view thedoctor's prescription.

8. Benefits of Healthcare Systems

There are immense benefits and advantages upon implementation of cloud computing in healthcare industry some of which may include:

a. Mobility of records
In some cases a person's health information can be required by two or more health institutions in that case by implementation of cloud technologies a person's health information can be easily synchronized and shared at the same time. Hence this improves physician's ability to provide a better health care to the patients. Thus by implementation of cloud technologies a patients information is readily available.

b. Speed
By using cloud based technologies and services always enable faster and accurate access to all the important information for the healthcare services providers and the history of their patients.

c. Security and Privacy
By using cloud computing is mainly used for storage of medical records online. With the recent HIPAA update, cloud healthcare service providers are now accountable for HIPAA compliance as healthcare entities they serve. Thus this includes encryption of data and secure backup of this data which contains the health information of a person, then verifying if the data can be easily regained, and finally security can be improved by using permission based and secured data bases.

d. Reduction of costs
By adopting these cloud techniques in healthcare patients, physicians, other medical organizations experience cost savings to a great extent. Since there is no need for these healthcare institutions and doctors to invest huge amounts in hardware infrastructure and their maintenance as these problems are already handled and taken care by the cloud computing providers.

9. Applications of Mobile Health Care

There are a few schemes of Mobile Cloud Computing applications in healthcare. It presents five main mobile healthcare applications in the pervasive environment.

- **Comprehensive health monitoring services** enable patients to be monitored at anytime and anywhere through broadband wireless communications.
- **Intelligent emergency management system** can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.
- **Health-aware mobile devices** detect pulse-rate, blood pressure, and level of alcohol to alert healthcare emergency system.
- **Pervasive access to healthcare information** allows patients or healthcare providers to access the current and past medical information.
- **Pervasive lifestyle incentive management** can be used to pay healthcare expenses and manage other related charges automatically.

10. Conclusion

We proposed to build an application of mobile healthcare System using cloud. Use of Integrity is a vital aspect in health-care systems. This system provides data integrity by applying new modification to existing system for better accuracy measured in all phases of system. We use simple graphical user interface for health related applications which is easily learnable for rural area peoples, who are uneducated. This system is very useful in rural/remote areas where hospitals and health related facility is available far away from their home. Salient features of our health care system are to provide medical camp with their location, disease oriented information, primary solution to particular disease, and provide hospital locations. In case of emergency time, this application is most useful and offers easy access to medical care information at anytime and anywhere with privacy and confidentiality.

References

[1] U.S.Department of Health & Human Service, "Breaches Affecting 500 or More Individuals," (2001). [Online]. Available:
[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
[3] P. Ray and J.Wimalasiri, "The need for technical solutions for maintaining the privacy of EHR," in Proc. IEEE 28th Annu. Int. Conf., New York City, NY, USA, Sep. 2006, pp. 4686–4689.
[4] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care,"presented at the 14th Int. Workshop Database Expert Syst. Appl., Prague,Czech Republic, 2003.
[5] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd

Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.
[6] D. Boneh and M. Franklin, "Identity-based encryption from the Weilpairing. Extended abstract in CRYPTO 2001," SIAM J. Comput., vol. 32,no. 3, pp. 586–615, 2003.
[7] A. Cavoukian, A. Fisher, S. Killen, and D. Hoffman, "Remote home health care technologies: how to ensure privacy? build it in: Privacy by design," Identity in the Information Society , vol. 3, no. 2, pp. 363 – 378,2010.
[8] J. Sun, X. Zhu, C. Zhang, and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEEInt. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.
[9] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," in Proc.IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.
[10] E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003,p. 216, 2003.
[11] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric
[12] encryption: Improved definitions and efficient constructions," presented at the ACM Conf. Comput. Commun. Security, Alexandria, VA,USA, 2006.
[13] Y. Earn, R. Alsaqour, M. Abdelhaq, and T. Abdullah, "Searchable symmetric encryption: Review and evaluation," J. Theoret. Appl. Inf. Technol., vol. 30, no. 1, pp. 48–54, 2011.
[14] T. Xu and Y. Cai, "Location cloaking for safety protection of ad hoc networks," in Proc. IEEE Conf. Comput. Commun., 2009, pp. 1944–1952.
[15] A. Pingley,W. Yu, N. Zhang, X. Fu, andW. Zhao, "CAP: A context-aware privacy protection system for location-based services," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., 2009, pp. 49–57.
[16] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE—Simple privacy-preserving identity-management for cloud environment," in Proc. 10th Int. Conf. Appl. Cryptography Net. Security, 2012, pp. 526–543.
[17] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic secure cloud storage with provenance," in Cryptography and Security, Berlin, Germany, Springer-Verlag, 2012, pp. 442–464