International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 26723-26735

http://www.ripublication.com

Health Care System Towards Elastic Multicloud With Load Balance And Group

R.Aruna Devi
Research Scholar, Manonmaniam Sundaranar University,
Tirunelveli, Tamilnadu, India.
Email: arunaa_2008@yahoo.com
Dr.K.Nirmala
Associate Professor, Department of Computer Science,
Quaid-e-Millath Government College for Women,
Chennai,Tamilnadu, India.
Email: nimimca@yahoo.com

Abstract

In the field of healthcare systems the medical data needs storage for large data sets using big data. The extensive applications over the challenge of mining the medical data records arrange the software in compatible format in such a way that have relevant data for retrieving at right time. In emerging cloud technology the essential cost reduction, high performance and potential quality will be increased in health care sectors. The integrated security proposed by cloud based healthcare system that makes the complete healthcare provided worldwide and globalize their availability of services like claiming insurance, patient details, doctor diagnosis and research centre details for particular epidemic disease. The group sharing policy in big data achieves the synchronization and will be highly secured using different types of effective cryptography for each group of data sets. The different set of people like patients, doctors, researchers and the insurance provider will have anonymity over others data and given assorted encryption for each of them. The enormous number of data split up in elastic data will be reduced by this upgraded technique and maintains their data integrity using timestamp. The deadlock situations will be waived off with synchronization technique and the anonymity will be validated for avoiding duplication. Here we enforce de-duplication or garbage collection that releases unused memory storage in the common sharing space.

Keywords: Cloud Health Care Storage, group sharing, assorted encryption, data integrity, anonymity, de-duplication.

Introduction

In a health care oriented web services the medical records will be the most unmanageable data sets with enormous amount of information processing in it. The government has intervention towards prioritizing the critical information regarding the healthcare organizations. The research oriented applications for storing data of diagnosed details of disease that affects the patients for future researches based on those diseases [1]. The patients receiving remote health care for their problem and getting diagnosed by the specialized physicians of their choice which might have problems in interoperability of the system without any appropriate consultation.

Data sharing and elastic data processing that shares collaboration information by improvising the performance and security with cloud based peer network structure [2]. The network applications for cloud storage needs better data sharing services that performs system overloads along with scalable peer node structure. In peer-to-peer database servers the elastic data infrastructure that stores data with Map Reduce method and the data retrieved using Join method in which the data fragmented in different racks will be combined together to form complete data set [3].

In the Hadoop system for high performance and utilizing low storage space the big data will be deployed in the management systems. The dynamic storage needs to eliminate redundancy of data in common cloud storage thus variety of applications with reliable applications provide execution of data over its performance and capacity orientations. The purpose of reliable storage system is to hold worldwide global access towards the medical record system of patient, doctor and disease oriented research results [4]. Data transferred here will be in the multimedia format so large file format needs to have storage space in Bigdata.

The insurance company will be linked with the hospitals worldwide so that regardless of the patient locations they can claim their hospital bills instantly. In our proposed paper we implement data sharing between distinct group of people integrated and interoperated within each other. Every group of people will have their own set of process execution depending upon their granted privileges. They share details in common cloud storage area which helps in group sharing along with big data. This common storage helps in achieving data integrity synchronizes data process and handles situations like deadlock efficiently [5]. Such data storage must concentrate on their security and data anonymity for storing secured data.

Further we are going to discuss the data will be stored using elastic data techniques using fragmentation and defragmentation method. Thus the data part ensures proper data transaction using timestamps. The final section defines how the garbage collection for common storage will be executed efficiently by de-duplication methods.

Related Work

In the existing Best Peer++ system the unstructured data querying process shares cloud services using elastic data management with conventional DB Engine [6]. They have access towards invalid data with software dedicated to Best Peer structure for submitting instant queries. The back-up process will be interrupted by different dimensions for processing the independent storage service. The reliable and flexible

data service applications are capable of changing virtual storage service. The cluster oriented storage service updates the partial level optimization of transitions.

In cloud computing the outsourcing can be done with administrators which does not involved in process can be compromised with data attacks that can be given required security and protection within the cloud. For achieving optimal performance over cloud security it implies data replication and division. In this method it fragments the files into data chunks and replicates its copy over the cloud nodes where it can ensure the prohibition of attack [7]. All the probable compromises were done over the locations of stored fragments for high security and performance. But still number of split ups for such fragments is comparatively higher which obviously occupies much storage space.

Moreover it does not have any data integrity and surety for data delivery. Thus there may be a chance of data loss in case if the sender sent the data and deletes it from its memory space. In such cases it leads to many complications even it leads to deadlock condition [8]. Patient care system mostly concentrates on efficient and safety patient care and face problems regarding leak of critical information system. There are research centers that guide people to produce knowledge over the upcoming disease and their symptoms related to patients. But while considering personal detail confidentiality for patients it is not possible to access the entire details but still improvisation and security is required.

The most of the service paradigm in cloud computing focus mainly on denial of service attacks. The service quality for cost maintenance leads to more resource consumption. Harmful attacks minimize the worst case of target system increases intensity for mechanism related to their services [9] [10]. The specified denials of service detection mechanism protect the attacker's rate of attacking latency. De-duplication of data is even more space providing and duplication reducing garbage collection methodology in cloud service. Authorized data de-duplication will eliminate duplicate copies during compression of data that proposes the scheme minimizing operation overheads caused by them during data storage. This is one of the efficient garbage collection prototype used in normal operations of data compression uses encryption for confidentiality of data.

Privileges For Group Shared Data

Data mining to describe the sharing of data the scenario for group of doctors, patients, insurance company and research centers will be considered for their interoperability. As they are different groups they need their own privacy for data as well as sharing of specified data towards specified group of people [11]. In such case of data sharing every time data will be copied and made duplicates and sent as much copies is needed. In case of cloud sharing global service for example when a patient update his personal disease history in common cloud storage then it could be easily shared and viewed among group of research people. They can know about the details like their age, disease and kind of medications they undergo.

In such case patients will be grant privileges for updating, editing and deleting his personal details online. Patients can also select the specialist doctors from whom they

like to get reports for which they could pay online by claiming their eligible insurance amount [12]. Here the insurance company is linked with this cloud global storage for which it has privileges to view the patient disease history and their accurate bill amount. Then it will crosscheck the medical bills with the hospital records or with doctor whom they want to get their results and settle them instantly.

Patient's entire details from the moment they entered the hospital will be recorded in the cloud storage which can be accessed globally. Then all their examination details will be shared globally as e-ECG, e-Scan, digital X-Ray with respect to the patients. They are in the format of images and video for which the reports sent by the doctors will be in audio format. Only to the selected doctors to whom the patient paid their consultation fees can access the details and can able to provide reports online. The patients can get reports from two or more doctors by making appropriate payment for them. The doctors rather than sending printed reports they record the reports by voice and share it for patient and their investigating doctor review.

Group of doctors linked with the common storage will also have restriction to certain access and grant privileges for viewing complete patient details and provide reports according to their examination results [13]. Even those doctors can refer or get reports from other senior doctors or their colleagues for providing better results in case of complication. When the doctor is in dilemma the patients will be redirected to other specialist who could handle it will. Large number of group participants involved in such data sharing analyze accurately on authenticity and anonymity of data storage purpose [14]. As multimedia format of data is stored and transferred even the single chunk lost makes the total file format obsolete. Efficient data integrity and data privacy of the group which shared among the cloud will be maintained.

In Big data form of cloud storage they contain different types of database that is collected from different datasets in different forms of data thus to achieve Velocity, Volume and Variety of data. As data sharing is involved different types of data that is variety will be achieved primarily [15]. By using assorted cryptography high security is given so the velocity is guaranteed for speed transactions of data. At last while we share datasets globally in cloud large amount of data shared and processed thus it also satisfies the volume criteria of Big data. Thus we endorse all the criteria of Bigdata like Volume, Variety and Velocity of data in an efficient way.

As it involves more images, audio and video format of data bulk of data needed to be transferred as block so it needs large database to send and receive blocks of data. We use Binary Large Object (BLOB) which is fault tolerant that manages the whole binary data as single data entity and stores all kinds of multimedia objects under universal storage database as binary executable codes. This helps in transferring large amount of data from one database to other without any loss in data format.

A patient identification login or just using his fingerprints, iris and in the least case if nothing is available then the DNA test result can easily fetch the entire medical history of the patient [16]. Whatever may be the patient condition the doctors could get their details and carry out further medical formalities indeed they could get their payment through the patient's insurance organization. This advanced facility helps the nation's health care system widely used and shared among the personal health care of each individual.

Data sharing will be mainly focused here with detailed analysis of provided personal details of a person his related medical history according to the consultants recommended reports. This also involved with research center which collects only data regarding particular disease, the recommended medicine and its further investigation procedures for their future study for disease or medicine oriented information [17]. The data shared by research center will be more than other group of data shared. Here it only collects data from other groups and saves only research related information rather than patients or medicines intricate details. This kind of anonymity requires efficient operation and privacy policy for acquired authentication.

Providing Assorted Cryptography

In large scale sharing system there is a need to provide security for various set of group of data shared. Here we classify the groups as patients, doctors, insurance company and research center. Each group will be associated with different type of cryptography for securing the data they share with strong protecting technique [18] [19]. Only the authenticated data to be shared by the particular group will be shared among the global cloud storage but it should reach only the authorized viewers but not to the other outsiders.

For every group sharing we provide assorted cryptography techniques so that everyone will be protected in their own way and while shared among common cloud only the authenticated data will be shared. Here we achieve authenticity and security for data shared globally. The assorted cryptography assigned with data groups as follows.

1. **Data group of Patients** implements RSA (Rivest-Shamir-Adleman) algorithm for securing their personal details. RSA algorithm uses public key cryptography that uses public key and private key cryptography for securing public communications. This public key encryption provides both authenticity and confidentiality. They protect data transacted from eavesdroppers and it has guaranty for data from authorized sender. It has digital signature over every data sent and private key for every authorized receiver where the public key will be computationally complex to decipher. The public key use pair of integers for creating cipher text which can be consequently decrypt by the private key with each authenticated user [20]. Thus here patient sends their examination results encrypted using their private key and sent to doctors who could decrypt it using their private key. So no data is lost and only the specified doctors the patient selected can view results and provide reports accordingly. Only if that particular doctor or patient wants other doctor to view results for second opinion they can send them those results along with public key for decrypting it in that particular doctors login. As the results like X-Ray, ECG, etc will be in digital and image format it uses block cipher method for message encryption subsequently generates computational overheads. This is more standardized cryptographic technique helpful for sending video format data like patients results for scan.

2. **Data group of Doctors** implements AES (Advanced Encryption Standard) algorithm for protecting reports sent to patients. Here AES uses symmetric key cryptography that enables long key encryption standards for fast encryption and requires low latency using protocols. It use block cipher that encrypts and decrypts providing symmetric or secret key where the sender and receiver both have same secret key for getting final cipher text data. Doctors are optionally selected by patients where they need accessing rights for patient information. They can provide reports by examining the whole history of patients and the recent results sent by them. They provide audio format of results to the patients by sending the recorded voice reports. Doctors have access to entire details only till the access is given after which those details will be deleted for their further reference. If they want to get associated remarks then they need to search it only from the research center where they could fetch only common details about them without furnishing any personal details. Without intimating about the doctor or patients personal results research center can provide wide variety of symptoms and medications taken for particular type of disease. Thus here AES algorithm helps in providing security by creating same single secret key for entire data protection.
3. **Data group of Insurance Company** integrates Tiny Encryption algorithm (TEA) for proceeding their verification and insurance amount settlement process. This kind of cryptography used because it is one of the fastest block cipher encryption algorithm that use unsigned bit of integers that use key as data block that is implemented as cycles. The schedule of those key will use constants that can prevent from simple symmetry based attacks. The effectiveness of their keys can be used for cryptographic hash function that can easily detects any kind of hacking attacks within less time taken. They use plain text related key pairs for eliminating time complexity over the cipher text key design [21]. Thus the insurance company can get the medical details of patients from their database and can easily estimate real amount for those tests and treatments taken. The insurance company will pay the doctor fees and medical treatment fees directly without more procedures done by patients all they need is only the authentication by the patient or caretakers. Insurance will be claimed on behalf of patient undertaking treatment and the appropriate amount will be settled for the hospital.

Data group of Research center implements ECC (Elliptic Curve Cryptography) model for securing their data regarding disease and its medications regardless of patient or medicines intricate details. Elliptic Curve Cryptography is the method of ellipse or oval pattern of 32 oval layers that has cloud of points in each field for transforming the integer curve equation that determines the coefficients for representing those points. ECC generates key pairs for getting the private key as random integer this accompanies public key with scalar point multiplication with number of curve points involved. In ECC the discrete logarithm is used as multiplications of non-zero numbers that has finite point fields corresponding to the problem [22]. It uses public key for encryption and private key for decryption. It

computes discrete algorithm that is equivalent with the key lengths for integrating encryption standards.

System Architecture

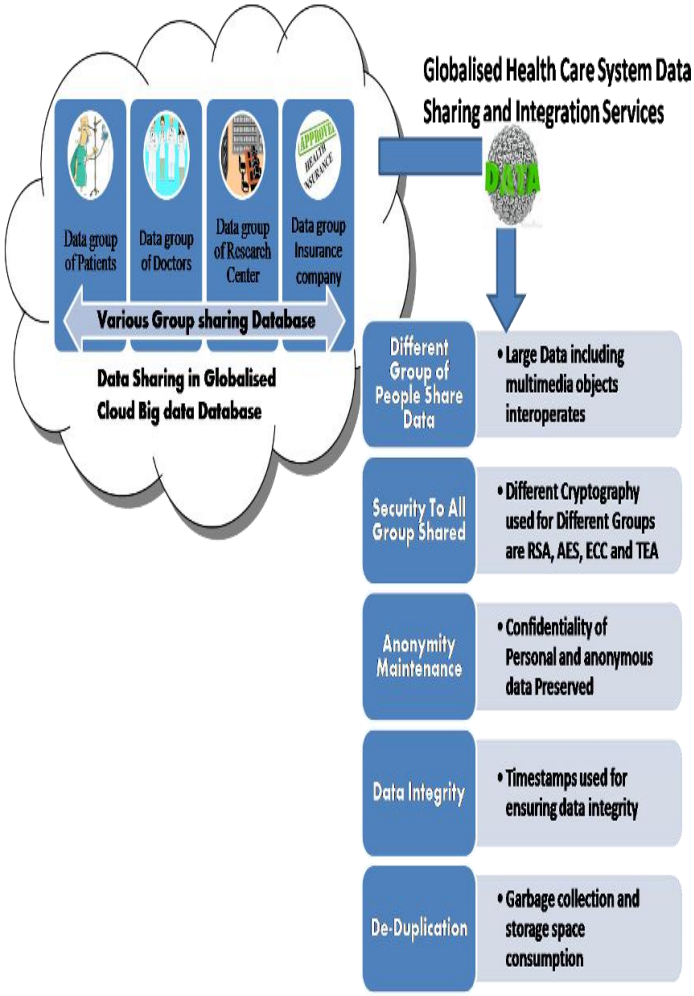

Figure 1: Sharing Services with Group for Health Care System

In research group they collect details of patient's age and gender criteria. Then disease details with their entire process of examination history along with reports given by doctors regardless of doctor's personal history. It stores medicines where only its compositions percentage will be noted and not their brand or company names. The strong security protects personal details of any of the other group traced from this research center might be misused by the malicious attackers. Even the recorded voice reports of the doctors will be transcript and transformed into the printed readable format and stored in research centers for future use.

Time Stamp For Ensuring Data Integity

While sending and receiving data in the group sharing methodology we need to ensure integration of entire data sent. They accelerates inputs with hash functions have unique data for validating same values that implements many password checking systems and it is explained in Fig.1. Fingerprints and randomization functions with cipher text can strongly intend to probability distribution for optimization codes. It is not only used for login purpose but the digital X-ray, ECG, EEG and further clinical examination procedures results will be automatically transferred as multimedia format files. Some video format files also stored and transacts like for example instead of sending scan results as images it could be sent as color video for better review for patient medical treatment.

To ensure data integrity the from multiple fragments of storage racks to one join fragment each data to be shared will sent only copy along with timestamp [23]. When the data reaches the receiving end it will be checked for the data integrity and when it confirms entire data received then only the original copy will be deleted from its origin. In fragments of data while sending the threshold value towards the destination they will send timestamp details like where it is sent from and how much data is transferred. When it reaches the destination it checks for how much time it takes to reach the destination with this it also checks for any attacks in between. As the last step it checks the number of bytes sent along with number of bytes received by the receiver. It uses hash function to perform this step which maps inputs with distinct values along with hash code thus the hash table helps for additional searching along with its originated hash table.

The threshold values used as integration for hash table values will confirm with the entire data collaboration to the receivers end [24]. When any data sent without having copy might have chance for loss of data they may not be intimated to both the senders and receivers end. In such case the loss of data may not have any threshold so there is a large gap in that place of data which leads to many misconceptions.

In group sharing they involve numerous data shared among the datasets such as the patients need to get their personal and medical related details which should be shared with doctor for getting reports. The doctors in turn send the reports which shout reach the patients without any data loss. If any data lost or wrong data reached the receivers end it leads to big trouble for both patient and to doctor. So they should ensure data integrity here.

In case of insurance group sharing they also need full details about the patient bill amount and their treatments or clinical examination undertaken. All the details should be sent without any loss as they impart main role in claiming insured amount facility. In such a situation for missing any details to be sent then it could claim lesser amount than fees or it might get delay to pay the appropriate amount. This is a serious problem which leads to delayed attention to patient care which might seriously affects their health conditions.

Research center while getting the data related to particular patients or disease they have to be very careful about data orientation. As these data stored will have only anonymous information all the data shared should be authenticated and authorized without any data loss. So that in future when any people wanted the disease or

medicine oriented details they could get the whole details like the symptoms, number of days symptoms persists, clinical examinations, treatments and medicines undertaken for number of days. If in case of loss of data or any malicious data intruded then the whole details will be spoilt for taking as research into consideration. Thus in this place data integration is mandatory for transaction of data.

Anonymity Maintenance

Maintaining large set of database in Bigdata is not an easy task as it involves much security to be given for data. The database stored in DB Engine should maintain its own secured protection and anonymity towards the outside access. In each group of shared data they maintain certain details as too confidential and never let it accessed by any people of other group or any other related access will be permitted. The research institutes produce knowledge about health care system that relies on potential care given for patients having profits over verdict outcomes.

This kind of anonymous data protection helps in avoiding many problems regarding leakage of any personal details. For example if any patient detail is leaked then when the people know about that particular person may treat them as diseased as they know whole details of him. It spoils the total reputation of that specified person. This type of hypothetical situations can be avoided by maintaining anonymity towards the data. This is least case problem only but it also leads to major crisis like any medicine details is incorporated in disease history. Anonymity maintenance could be bit difficult in terms of multimedia format files where name of the patients and their age details should be included for getting appropriate results of specified person. But here we can make it as coded documents so that when talking about a patient he will be mentioned with his code number throughout the process thus it maintains anonymity successfully.

In deliberate case if any medicine didn't cure that particular patient body condition then it might be considered as failure product so to avoid such misconceptions that brand or product name will be kept anonymous. But to intimate the treatment or drugs taken only the composition standards and the constituted proportions of chemicals used will be inculcated in the report history. It helps in getting knowledge about the drugs used in spite of its brand name.

The anonymity maintenance also involves synchronization process which detects deadlock situations and release those unhandled problems. When inculcating the group shared data there are many problems involved in data transactions. When many data transaction employed there might be the chance for locked process that may lead to cease further process. Regardless of this situation we need some synchronization techniques for handling such deadlock situations.

Anonymity endorsed with data that contains message authentication use static information assures efficient protection over adverse situations. This kind of application provides protection over reluctance for data sharing system. Computational and communication cost will be largely reduced by efficient sharing of anonymous and synchronized data. To eliminate the redundancy of data this anonymous data will be improvised with intervention for evaluation outcomes.

Anonymity is must in all group involved in data sharing for efficient patient, doctor, insurance and research center collaboration.

De-Duplication For Acquiring Storage Space

Garbage collection is the mandatory process to be involved in large data base storage collection. In wide spread database of health care system containing huge data sets mostly will have number of copies of data that are transacted between different groups of shared data. For accommodating newly updated or created data for group the unwanted or unused data storage should be cleared. Thus it elongates the storage space by reducing the bulk of unwanted or data not to be used any more.

De-Duplication is the method implies data compression technique that eliminates and reduces the redundant copies of repeated data in cloud storage. For securing confidential data only the copies will be sent for reference to other group but the original data will be stored constantly in its original data space. Authorized data de-duplication methods used for checking duplications and redundant data in global cloud storage that proposes prototypes for minimizing the operational overheads.

Once when it completes the entire process then the data copy regarding details should be automatically disabled for that particular group and can be further referenced only in its main database. This is one kind of overhead to be handled with group shared data. So each group user will have certain duplicate copies of data thus everything will be collected and deleted for further data space usage. For example in case of patient details accessed by doctors after getting the reports those copy of data is negligible to the doctor so that could be deleted from doctors database. After settlement process the medical history of patient is unwanted for insurance database so that can be released.

The memory space shared by the cloud computes resources at low cost and specifies the privileges for stored data having access rights towards the storage services. It comprises of critical resource computation and managing increase in volume or amount of data. We specify the management over variety of data shared thus it have large volume of data that automatically increases the speed of data to be transferred. It can be defined as one of the main challenges the cloud shared group of data to be faced.

It becomes more complicate when inculcating audio, image and video format of files. As the digital X-ray is in image format while scan will be recorded as video and the doctors will record their voice reports instead of typing their investigation to reduce time consumption. All these data formats will acquire lot of space in database. While transferring the data numerous copies of such data formats have to be taken and sent across the cloud storage. Only by clearing audio, video and image format redundancies itself we could provide more storage space for future storage.

Redundant data will be eliminated by file level and block level de-duplication method by deleting duplicate files and leaving unique data copies. The attacks can also be avoided by sensitive data de-duplication. Garbage collection is the main task for protecting the confidentiality over sensitive and compatible data. The large database like Bigdata for storing data in fragments using Map Reduce methods and

retrieve data with join method can efficiently manage the compatible information stored. The duplicate blocks of data will be eliminated and includes encryption technique for making scalable data management in common cloud storage.

Feasibility For Cloud Shared Storage

In group shared cloud storage the common database used for storing and retrieving large sets of data which can be accessed by variety of user groups is an efficient Bigdata perception. While integrating such a huge group of data together without the knowledge of such common cloud data storage is a tedious task. But here we make it possible and feasible for handling huge database together and makes its process in convenient way with easy collaboration of variety of groups together. It uses assorted type of encryption which implements different types of cryptography for different group of people shared among the cloud. This helps in providing the group only its appropriate kind of security needed rather than making use of common encryption that makes clumsy when either group transmitting data with each other. By maintaining datasets in global common cloud storage space the Health Care systems personally don't need any server or database for storage. So maintenance cost for database is eliminated thus it is cost effective.

Multimedia objects to be considered as a large set of data when stored in each health care system individually makes the whole database system a cumbersome process. But by using this common cloud storage we can transfer this large set of data as BLOB that is binary large object which considers the whole multimedia file as single binary entity and can easily share among group of data need this kind of file. It not only reduces the space consumption but also minimizes the time taken for transferring each file for every different group of data. Thus this sharing of health care system in common cloud storage globally as groups is certainly feasible for users.

Conclusion

In our proposed paper we implement common cloud shared database inculcates variety of group sharing their common information and collaborating data within each other. Here we handle Health Care Management System for such kind of large database in Bigdata that communicates huge data sets in convenient way without any mesh. The detailed database will be stored as fragments for each group and will be commonly shared among other group of people and after getting their appropriate assessment and evaluation over the data the redundant copies will be deleted and the main details will be shared and stored under common storage space. This is globalised by sharing under cloud storage environment so anybody can access this information regardless of their locations just by providing their login identification. This makes the system more efficient by enabling data access globally. Moreover it provides assorted cryptography for furnishing strong and appropriate security for variety of user groups. The main advantage in this proposed work is data integrity maintained for entire process. De-duplication of data or garbage collection is well equipped by

eliminating redundancy and reducing the space occupied by large set of multimedia files.

References

[1] M. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson, "Security and privacy governance in cloud computing via SLAS and a policy orchestration service," in Proc. 2nd Int. Conf. Cloud Comput. Serv. Sci., 2012, pp. 670–674.

[2] F. Cheng and C. Meinel, "Intrusion Detection in the Cloud," in Proc. IEEE Int. Conf. Dependable, Autonom. Secure Comput., Dec. 2009, pp. 729–734.

[3] C. Metz. (2009, Oct.). DDoS attack rains down on Amazon Cloud [Online]. Available: http://www.theregister.co.uk/2009/10/05/ amazon_ bitbucket_outage/S

[4] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," J. Cryptol., vol. 22, no. 1, pp. 1–61, 2009.

[5] M. Bellare and A. Palacio, "Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, pp. 162–177.

[6] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, "Twin clouds: An architecture for secure cloud computing," in Proc. Workshop Cryptography Security Clouds, 2011, pp. 32–44.

[7] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," in Proc. Int. Conf. Distrib. Comput. Syst., 2002, pp. 617–624.

[8] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.

[9] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc.Annu.Int. Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.

[10] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.

[11] J. Camenisch, "Efficient and generalized group signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233, pp. 465–479.

[12] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sublinear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434.

[13] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: Avision for socially motivated resource sharing," IEEE Trans.Serv.Comput.,vol.5,no.4,pp.551–563,FourthQuarter2012.

[14] D. Chaum and E. van Heyst, "Group signatures," in Proc. Workshop Theory Appl. Cryptographic Techn., 1991, vol. 547, pp. 257–265.
[15] L. Chen, C. Kudla, and K. G. Paterson, "Concurrent signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 287–305.
[16] H.-Y. Chien, "Highly efficient ID-based ring signature from pairings," in Proc. IEEE Asia-Pacific Serv. Comput. Conf., 2008, pp. 829–834.
[17] S. S. Chow, R. W. Lui, L. C. Hui, and S. Yiu, "Identity based ring signature: Why, how and what next," in Proc. 2nd Eur. Public Key Infrastructure Workshop, 2005, vol. 3545, pp. 144–161.
[18] S. S. M. Chow, V.K.-W. Wei, J. K. Liu, and T. H. Yuen, "Ring signatures without random oracles," in Proc. ACM Symp. Inform., Comput., Commun. Security, 2006, pp. 297–302.
[19] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, vol. 3531, pp. 499–512.
[20] R. Cramer, I. Damgard, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in Proc. 14th Annu. Int. Cryptol. Conf. Adv. Cryptol., 1994, vol. 839, pp. 174–187.
[21] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," in Proc. ACM Conf. Comput. Commun. Security, 1999, pp. 46–51.
[22] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in Ad Hoc groups," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 609–626.
[23] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen. (2009). Practical short signature batch verification," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., vol. 5473, pp. 309–324 [Online]. Available: http://eprint.iacr.org/2008/015