ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

A Cloud Based Document Sharing Application Using Secret Key: A Survey

Snehal S. Deshmane[1], Anusaya S. Chougule[2], Esther S. Solomon[3]

U.G. Student, Dept. of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, Maharashtra, India[1,2,3]

ABSTRACT: Cloud computing technology is gaining an increased attention of the mobile device users nowadays. Cloud storage is becoming more popular due to its features like centralized infrastructure, monitored performance, device and location independence, reliability, scalability etc. Cloud helps its users to store and process their data in data centers located pervasively. Users can store as well as share the data anytime anywhere. The continuous integration of global information leads to more and higher value data. Challenges have increased in enterprise IT departments due to exponential growth of high value data. Cloud computing aims at providing an overview of privacy issues and legal frameworks for data protection in cloud environment. Security and authority always remains an issue when it comes to sharing data over cloud. The highlight over here is the use of mobile device for sharing the data.

KEYWORDS: Cloud computing, reliability, scalability, authority, mobile device.

I. INTRODUCTION

Cloud can be defined as a set of services dubbed at a remote location. Cloud is analogical to network. Cloud computing is a model for enabling ubiquitous, convenient, on demand access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third party data centres. The three types of services provided by cloud are: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). The three main types of clouds are Public clouds, Private clouds and Hybrid clouds. Mobile Cloud Computing (MCC) is a combination of cloud computing and mobile networks to bring benefits for mobile users, network operators and cloud providers. It refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud computing is an interaction between human and computer. Secure data protection is an important but comparatively accomplishable issue. Cloud computing offers can be various regarding the specification. Software as a Service (SaaS) describes the distribution of ready to use applications based on this technology model [4]. The basic aim of mobile computing is to send and receive data across cellular networks. However, the outsourced data typically contains sensitive privacy information, such as residential addresses, personal information, etc. which may lead to severe confidentiality violations, if efficient protection is not provided. It therefore becomes necessary to encrypt the sensitive data before outsourcing them to cloud [10]. Also privacy and integrity of the documents must be maintained in the cloud storage during the period of uploading and accessing [1].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

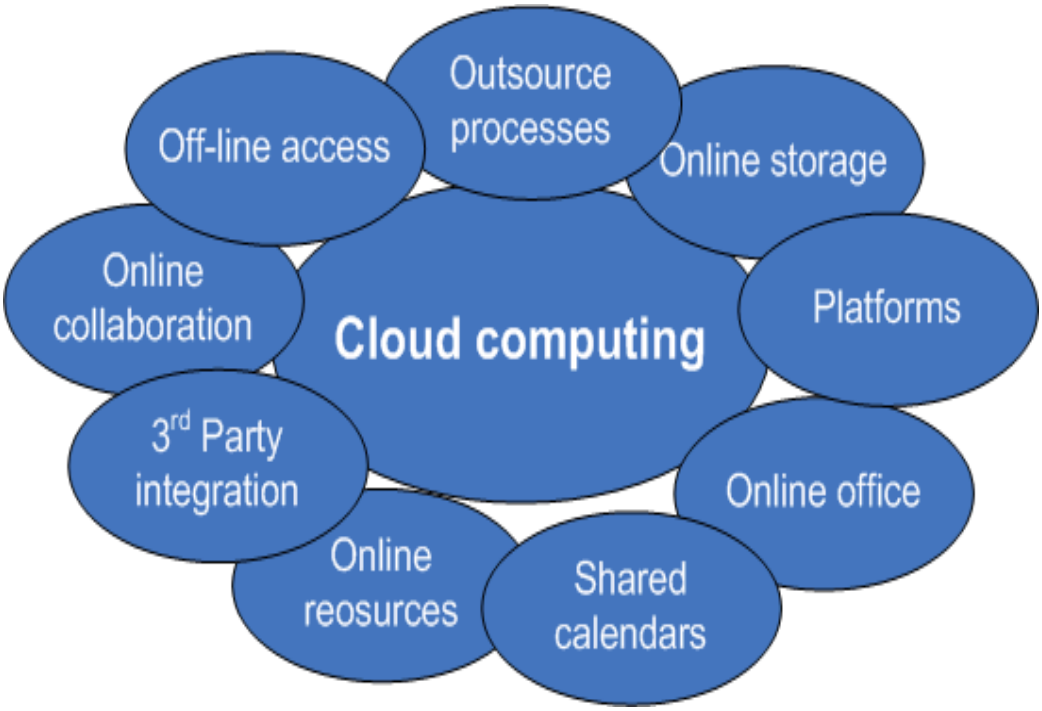

Fig 1: Cloud Computing

II. LITERATURE SURVEY

In this paper, the main focus is on the storage outsourcing in distributed cloud servers. Some solutions assume cloud servers to be trusted which may be a too strong assumption to constrain the applicability. Also, the mobility of mobile devices and cooperative accessibility of files on cloud servers are not yet carefully considered. Moreover, as mobile devices may be lost incidentally, the storage of mobile devices are vulnerable to exposure, which is ignored. To overcome all these problems, a family of schemes was designed to guarantee the privacy and integrity of outsourcing files or data. It firstly proposes an encryption based scheme (EnS), for a situation of single accessible Cloud Server. It then proposes a coding based scheme (CoS) for the situation that multiple cloud servers are available without relying on encryption. Then it proposes a sharing based scheme (ShS) to further decrease the computation overhead by only relying on exclusive – or operation. All these schemes are restricted to the storage compromise on mobile devices and all assume that the cloud servers are distrusted. Thus, they provide a stronger protection for more general and realistic application scenarios. The security requirement fulfilled in this paper is data confidentiality and data integrity users' files in mobile cloud computing [1]

To address the data privacy challenges on cloud, Cong Wang, proposed outsource image recovery service (OIRS). The design of the system is based on a compressed sensing framework which is a sampling and reconstruction framework enabling data acquisition. The design goals of OIRS system are security, effectiveness, efficiency and extensibility. The empirical evaluations are setting of experiment, evaluation of efficiency and evaluation of effectiveness. The system framework includes four probabilistic polynomial time algorithms as 'KeyGen' for key generation, 'ProbTran' for problem transformation, 'ProbSolv' for problem solving and 'DataRec' for data recovery. The major drawback of this system is that it lacks speedup in performance [2]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Based on the study of other data de-duplication technologies, especially the Similarity-Aware Partitioning (SAP) Algorithm, this paper proposes the Frequency and Similarity-Aware Partitioning (FSAP), algorithm on cloud storage. It also proposes the Space-Time Utility Maximization Model (STUMM), which is useful in balancing the relationship between space efficiency and access efficiency. It uses 100 web files downloaded from CNN for testing and the results show that relative to using the algorithm associated with the SAP algorithm, the FSAP algorithm based on STUMM reaches higher compression ratio and a more balanced distribution of the data block. De-duplication helps in achieving space efficiency, improving storage efficiency and reducing network traffic. Techniques like delta encoding, Bloom filter and sparse index were also used to enhance the performance of de-duplication First of all, data is partitioned based on similarity coefficient of files. Then redundancy is removed based on occurrence of frequency of blocks. Here, the problem of redundant data in cloud storage systems is discussed. The main goal of this paper is how to use less space to store more data files and not affect access efficiency [3]

Florian et al., did a literature survey on IT flexibility and its beneficial effects on costs, legal uncertainties regarding data processing on cloud computing storage especially between large economies. Due to complexity regarding international law, this study focused on data traffic between USA and EU. The main objective of this study is to review the literature on protection of data and privacy along with cloud technologies for establishment of existent law understanding. The basic problems surveyed were lack of regulations, legal uncertainty, missing control mechanism for users, and unauthorized access by third parties and cross border data flow. In this review, a detailed examination of legal literature is missing. Another limitation of this study is lack of investigation in relation to the imminent General Data Protection Regulation since the currently accessible information is rather vague [4].

Cloud based Personal Health Record System had been developed to handle large amount of medical data generated by the clinical institutions in an effective and efficient way. The system allows continuous capability of monitoring by supporting dynamic creation of clinical document architecture from a mobile device. One of the important concepts of this scheme is the cloud based file manager module which is similar to Dropbox. This Personal Health Record System (PHRS) helps in self monitoring and controlling health. The repository based on cloud can be shared with clinicians as and when required. The scheme provides the capability of constant monitoring by using easy uploading module and decision support system. The system does not talk about any security issues concerned with the data stored on cloud [5] The system shows current problems based on mobile cloud technology and focuses on its future potential. As the system tells, storing of data is not the only need of the user; the user also needs to share the contents. This need is satisfied by various social networks such as Facebook. This social interaction over such content cannot be globalized as it is limited for a group of particular closely related people. Hence device to device (D2D) strategy is used for content sharing. The key element of this system is Network coding. Network coding provides features like energy saving, bandwidth saving, delay reduction, privacy assurance and preventing false packet injection. Network coding implementation on mobiles is more feasible. Morten et al., mainly focused on the concept of mobile cloud and sharing data over it. The system has discussed the concept of content sharing only, but the sharing of other resources like spectrum onboard sensor information etc. is not concerned [6]

Event Based Mobile Social Networks (MSNs) allows any mobile users to create events to share group messaging, locations, photos and insights among participants. Event Based MSNs are a category of dynamic social networks having a shared feature that the events in the social network are immanently temporal. Here, event based MSNs with smart phone content technology elements such as context aware mobility and multimedia sharing are presented. MSNs combine techniques in social science and wireless communication for mobile networking. This paper explains possible researches on interoperability, middleware design, rich media, event detection and recommendation, security and privacy. However, event based mobile applications remain unsatisfactory for users, as there is no single application that provides an integrated feature to address all the issues of applications of event based social services [7].

Mobile Collaboration architecture (MoCA) is a middleware architecture for developing context processing services and context sensitive data. The new distributed computing environment poses new challenges such as host mobility, limited device resources and intermittent connectivity. This project aims to experiment with new forms of mobile collaboration and implement a flexible and extensible service based environment which can develop collaborative applications.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

MoCA was basically designed for infrastructure wireless networks. The MoCA infrastructure consists of client and server APIs and Proxy Framework. The server API offers interfaces that handle the servers configuration options. The client API offers interfaces to configure the client, find a proxy and send and receive data from the proxy. The proxy framework gives the application developer a simple mechanism for accessing context information related to client devices. The main goal is to design collaborative applications that use information about both user proximity and interest affinity to determine the participants of collaboration [8].

Carl et al., proposed an encryption scheme called Dynamic Searchable Symmetric Encryption which enables a client to store a dynamic set of documents in encrypted form with server. The system uses a concept of blind storage in which the clients store their files on remote server and the server does not know any parameter of the file, length of file and its place to be stored. Security guarantees are stronger and easier to understand. Blind storage construction is known as Scatter Store. A dynamic Searchable Symmetric Encryption scheme (SSE) has five probabilistic polynomial time procedures as SSE.keygen, SSE.indexgen, SSE.search, SSE.add and SSE.remove. The index generation process in this system is 20 times faster than the previous system. The major drawbacks of this scheme are insecurity against actively corrupt servers and insecured searches involving multiple keywords [9]

Hongwei et al., has developed an efficient multi keyword search scheme based n k-nearest neighbor techniques that returns ranked search accuracy based results. This system has been proposed to tackle the cloud storage issues like privacy and confidentiality. The system model consists of three entities as data owner, search user and cloud server. The data is stored by data owner on cloud by using encryption. This data can be accessed by a search user using a secret key receiver from the data owner. Due to the concept of encryption and secret key, the system becomes highly secured. The scheme uses the concept of blind storage in which the server does not know anything about the data stored on cloud. The proposed scheme can achieve confidentiality of documents in an efficient way as demonstrated by the security analysis. The system does not tell anything about the authorization and the access control issues [10]

III. CONCLUSION

The purpose of this paper is to get a better understanding of the existing systems with regard to currents measures for data protection in mobile clouds. Our content analysis revealed numerous challenges for future research in this area. The evaluation of previous papers motivates us to design a system which can provide more computational efficiency and a simpler infrastructure. Security analysis has demonstrated that a scheme can be proposed which can effectively achieve confidentiality of documents. For the future work we will investigate on security and integrity issues. Our study provides a valuable overview of currents key regulations to be taken into consideration by practitioners which are currents using mobile cloud computing or tend to apply this technology.

REFERENCES

1] Wei Ren, Linchen Yu, Ren Gao, Feng Xiong,"Lightweight and Compromise Resilient Storage Outsourcing with DistributedSecure Accessibility in Mobile Cloud Computing", TSINGHUA SCIENCE AND TECHNOLOGYISSN 1007 0214 06/09 pp520-528 Volume16, Number 5, October 2011.

2] Cong Wang (Member, IEEE), Bingsheng Zhang (Member, IEEE), Kui Ren (Senior Member, IEEE), AND JANET M. ROVEDA (Senior Member, IEEE), "Privacy-Assured Outsourcing of image Reconstruction Service in Cloud", IEEE Transactions on EMERGING TOPICS IN COMPUTING, Volume 1, No1, Date of Publication 17 July 2013.

3] Jianjiang Li, Jie Wu, Zhanning Ma,"Frequency and Similarity Aware Partitioning for Cloud Storage based on Space Time Utility Maximization Model",TSINGHUA SCIENCE AND TECHNOLOGYISSN 1007-0214 02/10 pp233-245, Volume 20, Number 3, June 2015.

4] Florian Pfarr, Thomas Buckel, Axel Winkelmann, "Cloud Computing Data Protection –A Literature review and Analysis", 2014 47th Hawaii International Conference on System Science, 978-1-4799-2504-9/14 IEEE, 2014.

5] Yeong-Tae Song, Sungchul Hong, Jinie Pak, "Empowering Patients Using Cloud Based Personal Health Record System", 978-1-4799-8676-7/15 2015 IEEE, June 1-3 2015.

6] Morten .V. Pederson, Member IEEE and Frank. P.H. Fitzek,, Senior member IEEE "Mobile Clouds: The New Content Distribution Platform", Proceedings of the IEEE, Volume 100, May 13th, 2012.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

7] AHMEDIN MOHAMMED AHMED, (Student Member, IEEE), TIE QIU, (Member, IEEE),FENG XIA, (Senior Member, IEEE), BEHROUZ JEDARIAND SAEID ABOLFAZLI (Student Member, IEEE), "Event-Based Mobile Social Networks: Services, Technologies and Applications", IEEE Access, Volume 2, 2014.

8]]Vagner Sacramento, Markus Endler, Hana K. Rubinsztejn, Luciana S. Lima, Klehr ,Gonçalves, Fernando N. Nascimento, Giulliano A. Bueno, "MoCA: The Middleware for Developing Collaborative Applications For Mobile Users", Volume 5, Number 10, October 2004

9] Muhammad Naveed, Manoj Prabhakaran, Carl .A.Gunter, "Dynamic Searchable Encryption via Blind Storage" 2014 IEEE Symposium on Security and Privacy, 2014.

10] Hongwei L1, Dongxiao Liu, Yuanshun Dai, Tom H. Luan, Xuemin Shen, "Enabling Efficient Multi- Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", IEEE Transaction On Emerging Topics in computing, Volume 3,No. 1, March 2015.

11] Park K W, Kim C, Park K H. Blast: Applying streaming ciphers into outsourced cloud storage. In: 2010 IEEE 16th International Conference on Parallel and Distributed Systems (ICPADS10). Shanghai, China, 2010: 431-437.

12] Liu Q, Wang G, Wu J. Efficient sharing of secure cloud storage services. In: 2010 IEEE 10th International ConferenceonComputer andInformation Technology (CIT10).Bradford, West Yorkshire,UK, 2010: 922-929.

13] Wei L, Zhu H, Cao Z, et al. Seccloud: Bridging secure storage and computation in cloud. In: 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops (ICDCSW10). Genoa, Italy, 2010: 52-61.

14] O. Goldreich, S. Micali, and A. Wigderson, ``How to play any mental game or a completeness theorem for protocols with honest majority," in *Proc.STOC*, 1987, pp. 218_229.

15] S. Goldwasser, Y. T. Kalai, and G. Rothblum, ``Delegating computation: Interactive proofs for muggles," in *Proc. STOC*, 2008, pp. 113_122.

16] S. Hohenberger and A. Lysyanskaya, ``How to securely outsource cryptographic computations," in *Proc. TCC*, 2005, pp. 264_282.

17] C. Jansson, ``An np-hardness result for nonlinear systems," Reliable Computing", vol. 4, no. 4, pp. 345_350, 1998.