INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Polandwith IC Value of 5.09 &number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2401 Cities in 155 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

Weinvite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Education, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: ____________

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE**: The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS**: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT**: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

   INTRODUCTION

   REVIEW OF LITERATURE

   NEED/IMPORTANCE OF THE STUDY

   STATEMENT OF THE PROBLEM

   OBJECTIVES

   HYPOTHESES

   RESEARCH METHODOLOGY

   RESULTS & DISCUSSION

   FINDINGS

   RECOMMENDATIONS/SUGGESTIONS

   CONCLUSIONS

   SCOPE FOR FURTHER RESEARCH

   ACKNOWLEDGMENTS

   REFERENCES

   APPENDIX/ANNEXURE

   It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

RELIABLE AND DISPERSED DATA SECURITY MECHANISM FOR CLOUD ENVIRONMENT

C.PRIYANGA
STUDENT
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SRINIVASAN ENGINEERING COLLEGE
PERAMBALUR

A.RAMACHANDRAN
ASST. PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
SRINIVASAN ENGINEERING COLLEGE
PERAMBALUR

ABSTRACT

Cloud computing has recently emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. On the one hand, remote data storage are subject to not only Byzantine failures, but also External and Internal attacks, as along the time the adversary may modify or pollute the stored data. To overcome these issues we propose a novel approach called RDSM (Reliable and Dispersed Data Security Mechanism). The proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. The batch auditing mechanism provides block level integrity checking in the cloud environment. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

KEYWORDS
cloud computing, storage security, ECC algorithm, byzantine faults.

1.INTRODUCTION

Cloud computing is an significant key idiom in rushing IT businesses. A feature of cloud computing is dispersed architecture based on variable nodes. Cloud computing lessens the total cost of a service by sharing all computational resources with other services. Platform-as-a-Service (PaaS) is the service model of cloud computing, and it offers a program executable environment for service providers. PaaS facilitates deployment of programs deprived of the cost and intricacy of buying and handling the fundamental hardware and software layers. However, some security risks have been tinted for cloud computing services. It is impossible for users to verify the honesty of all cloud computing environments, and the fear is that operations in cloud computing may be supported out without trusted environments. The dynamic and liquefied nature of the environments will make it difficult to maintain the consistency of security and ensure the ability to audit records. Thus, moving critical programs and delicate data to a public and shared cloud computing environment is a major concern for service providers. From the viewpoint of data security, which has always been a vital aspect of quality of service, Cloud Computing unavoidably poses new interesting security threats for number of reasons.

Firstly, outdated cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, confirmation of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Since various kinds of data for each user stored in the cloud and the demand of long term incessant pledge of their data safety, the problem of confirming accuracy of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important area remains to be fully explored in the literature.

Recently, the significance of ensuring the remote data integrity has been highlighted by the many research works. These techniques, while can be useful to ensure the storage precision without having users owning data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correct-ness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.In this paper, we propose a reliable and efficient dispersed storage verification scheme with obvious dynamic data support to ensure the accuracy and accessibility of users' data in the cloud. We rely on erasure-correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability against Byzantine servers, where a storage server may fail in arbitrary ways. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques.

By utilizing the Elliptic Curve Cryptography (ECC) token with distributed verification of erasure-coded data, RDSM achieves the storage correctness insurance as well as data error localization. In order to strike a good balance between error resilience and data dynamics, we further explore the algebraic property of our token computation and erasure-coded data, and demonstrate how to efficiently support dynamic operation on data blocks, while maintaining the same level of storage correctness assurance. In order to save the time, computation resources, and even the related online burden of users, we also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors (TPA) and be worry-free to use the cloud storage services. Our work is among the first few ones in this field to consider distributed data storage security in cloud computing.

2. REVIEW OF LITERATURE

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

In order to address the new problem in the third party auditing mechanism, user can able to audit the file one at a time. In the mechanism process time will be increased during the process. RSA algorithm was not suitable for small amount of file integrity process. The very first integrity tree was Merkles hash tree

(Merkle 1989). Originally it was proposed for public key authentication. Blum et al.(1994)it was applied as an integrity tree for protecting memory content. The method was referred to as tree authentication.

- It is possible for CSP to discard rarely accessed data without being detected in a timely fashion.
- Its lacking of offering strong assurance of data integrity and availability may impede its wide adoption by both enterprise and individual cloud users.
- The verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files.
- Disadvantage of Merkle trees is that data writes (or data changes) involved several sequential hashes which could not be parallelized for efficiency.
- They may be useful for QoS testing , but does not guarantee the data availability in case of server failures.

3.PROBLEM STATEMENT

Chapter 2 and the above sections in the current chapter have discussed some of the security auditing aspects of public clouds and the risks related to adoption of public cloud computing, as well as the public opinion stance towards adoption of public cloud computing. Two propositions have been formulated, regarding control over placement of the VM instance in batch auditing mechanism, with respect to the integrity guarantees of the cloud environment. That will help reduce the complexity of the addressed question and allow us to focus on the exact issue with a minimum number of complementary aspects.

3.1 SYSTEM MODEL

User: an entity, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers.

Cloud Server (CS): an entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter).

Third-Party Auditor: an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated, and distributed manner. Data redundancy can be employed with a technique of erasure-correcting code to further tolerate faults or server crash as user's data grow in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert, and append. Note that in this paper, we put more focus on the support of file oriented cloud applications other than non-file application data, such as social networking data. In other words, the cloud data we are considering is not expected to be rapidly changing in a relative short period.

3.2 DESIGN GOALS

To guarantee the security and reliability for cloud data storage, we aim to design efficient mechanisms for dynamic data verification and operation and achieve the following goals:

1.Storage correctness: to ensure users that their data are indeed stored appropriately and kept intact all the time in the cloud.

2.Fast localization of data error: to effectively locate the malfunctioning server when data corruption has been detected.

3.Dynamic data support: to maintain the same level of storage correctness assurance even if users modify, delete, or append their data files in the cloud.

4.Dependability: to enhance data availability against Byzantine failures, malicious data modification and server colluding attacks, i.e., minimizing the effect brought by data errors or server failures.

5.Lightweight: to enable users to perform storage correctness checks with minimum overhead.

4. OBJECTIVE

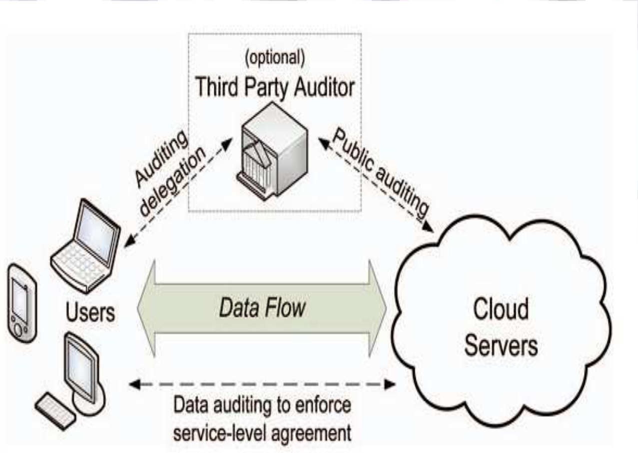
In the following chapters we examine a scalable solution for secure integrity checking done by elliptic curve cryptography algorithm in public clouds, to enable block level file integrity checking. The main objective of this paper should be able to check the integrity in cloud environment using batch auditing mechanism by the third party auditor.

5.ENSURING CLOUD DATA STORAGE

Since user requirements for cloud services are varied, service providers have to ensure that they can be flexible in their service delivery while keeping the users isolated from the underlying infrastructure. Recent advances in microprocessor technology and software have led to the increasing ability of commodity hardware to run applications within Virtual Machines (VMs) efficiently. VMs allow both the isolation of applications from the underlying hardware and other VMs, and the customization of the platform to suit the needs of the end-user. Providers can expose applications running within VMs, or provide access to VMs themselves as a service (e.g. Amazon Elastic Compute Cloud) thereby allowing consumers to install their own applications. While convenient, the use of VMs gives rise to further challenges such as the intelligent allocation of physical resources for managing competing resource demands of the users.

Cloud Computing is a large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet. Cloud is the network which is constructed through cloud computing model, and cloud service is the service provided in cloud. Now, Cloud Computing has become the hottest technology in IT, and is also the research focus in academic.

FIGURE1: SYSTEM ARCHITECTURE



6. IMPLEMENTATION

6.1 FILE DISTRIBUTION PREPARATION

It is well known that erasure-correcting code may be used to tolerate multiple failures in distributed storage systems. In cloud data storage, we rely on this technique to disperse the data file F redundantly across a set of n= m+k distributed servers. By placing each of the m+k vectors on a different server, the original data file can carry on the failure of any k of the m+k servers without any data loss, with a space overhead of k/m. For support of proficient sequential I/O to the original file, our file layout is systematic, i.e., the unmodified m data file vectors together with k parity vectors is distributed across m + k different servers. Suppose the user wants to challenge the cloud servers t times to ensure the correctness of data storage. Specifically, to generate the ith token for server j, the user acts as follows:

1. Derive a random challenge value and a permutation key.
2. Compute the set of r randomly-chosen indices.
3. Calculate the token.

After token generation, the user has the choice of either keeping the pre-computed tokens locally or storing them in encrypted form on the cloud servers. In our case here, the user stores them locally to obviate the need for encryption and lower the bandwidth overhead during dynamic data operation which will be discussed shortly. 3.2 Dispute Token Precomputation In order to achieve assurance of data storage correctness and data error localization simultaneously, our scheme entirely relies on the precomputed verification tokens.

The main idea is as follows: before file distribution the user precomputes a certain number of short verification tokens on individual vector, each token covering a random subset of data blocks. Later, when the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. Upon receiving challenge, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens precomputed by the user. Meanwhile, as all servers operate over the same subset of the indices, the requested response values for integrity check must also be a valid codeword determined by the secret matrix P.

6.2 FILE SPLITTING PROCESS

It includes file splitting process, which means storing of data into multiple servers. We propose the system with the data stored in the cloud may not only accessed but also be frequently updated by the users. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. The paper proposes services for data security and access control when users outsource sensitive data for sharing on cloud servers. The paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to assign most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents. In Order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed coded data. The splitting process is used to transfer the data to destination by using block by block method; proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve this goal by exploiting and uniquely combining techniques and algorithms *(Elliptic curve cryptography (ECC))*, Correctness Verification and Error Localization, traditional replication-based file distribution, adding random perturbations. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability and achieves fine - graininess, scalability and data confidentiality for data access control in cloud computing. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

6.3 FILE ENCRYPTION PROCESS

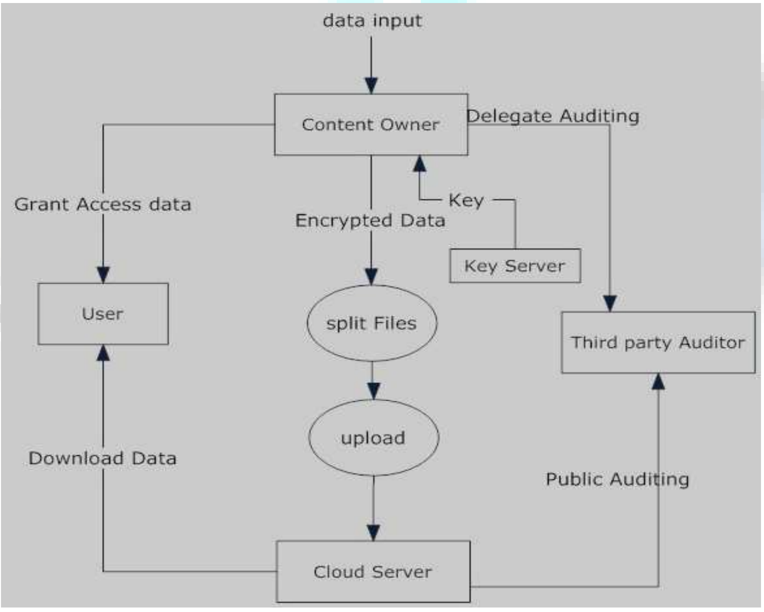
The user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one. However, by choosing system parameters appropriately and conducting enough times of verification, we can guarantee the successful file retrieval with high probability. On the other hand, whenever the data corruption is detected, the comparison of pre-computed tokens and received response values can guarantee the identification of misbehaving server(s) (again with high probability), which will be discussed shortly.

Therefore, the user can always ask servers to send back blocks of the r rows specified in the challenge and regenerate the correct blocks by erasure correction, as long as the number of identified misbehaving servers is less than k. (otherwise, there is no way to recover the corrupted blocks due to lack of redundancy, even if we know the position of misbehaving servers.) The newly recovered blocks can then be redistributed to the misbehaving servers to maintain the correctness of storage.

6.4 FILE RECOVERY PROCESS

Most websites and server-based applications run on particular computers or servers. What differentiates the cloud from the way those are set up is that the cloud utilizes the resources from the computers as a *collective virtual computer*, where the applications can run independently from particular computer or server configurations. They are basically floating around in a "cloud of resources" , making the hardware less important to how the applications work.

FIGURE 2: DATA FLOW DIAGRAM



With broadband internet, the need to have the software run on your computer or on a company's site is becoming less and less essential. A lot of the software that people use nowadays is completely web-based. The cloud takes advantage of that to bring it to the next level. To understand how does cloud computing work, imagine that the cloud consists of layers mostly the **back-end** layers and the **front-end** or user-end layers. The front-end layers are the ones you see and interact with. When you access your email on Gmail for example, you are using software running on the front-end of a cloud. The same is true when you access your Facebook account. The back-end consists of the hardware and the software architecture that fuels the interface you see on the front end.

Because the computers are set up to work together, the applications can take advantage of all that computing power as if they were running on one particular machine. Cloud computing also allows for a lot of flexibility. Depending on the demand, you can increase how much of the cloud resources you use without the need for assigning specific hardware for the job, or just reduce the amount of resources assigned to you when they are not necessary. The transition from being very 'personal hardware dependent' to a world where resources are shared among the masses is creeping up on us slowly and unobtrusively. Very many people have already transitioned to using a cloud environment for most of their time in front of the computer without even realizing it. Sure, most of us still use some version of Microsoft Office or Quickbooks that was installed on our computers, but even those kinds of software are now offering an online version that can be used instead.

The possibility of being able to access your data and software wherever you need it makes this transition very appealing to most people. Are there problems with this concept? Of course there are. If for some reason your internet goes down, your access to your data also disappears. There are security concerns with the data and the risk that companies will use proprietary formats for the files and that require that you pay for a certain service monthly or you may lose access to your own data permanently. So choose wisely when picking a service to use with your important data and make sure it can be downloaded if needed, but also enjoy the flexibility those services provide.

6.5 BATCH AUDITING

Data integrity is one of the most critical elements in any system. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity.

Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications. In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a failsafe manner. This can be done using a central global transaction manager. Each application in the distributed system should be able to participate in the global transaction via a resource manager.

7. CONCLUSION

In this paper, we examine the problem of user content security in cloud data storage, which is basically a dispersed storage system. To achieve the declarations of cloud data integrity and availability and enforce the quality of reliable cloud storage service for users, we propose an operative and elastic dispersed scheme with explicit dynamic data support, including block update, delete, and append. In this paper, we presented a possible solution for security issues in cloud computing environments. The batch auditing scheme provides block level security for user data and protects the whole data against malicious attacks. We quantitatively analyzed the security of our scheme. Our results show that our scheme achieves computational security against both internal and external attacks.

8. RELATED WORKS

In our vision, integrity of the cloud infrastructure is ensured through the use of Trusted Computing. In addition, we advocate the seamless extension of control from the enterprise into the cloud through the powerful combination of high-assurance remote server integrity, and cryptographic protocols supporting computation on cipher text. With our approach, content is protected in a manner consistent with policies, whether in the enterprise or the cloud. Yet, because the protection mechanisms support computation, it is possible for all cloud participants to mutually benefit from the cloud data *in a controlled manner*. Hence, there are business intelligence advantages derived from operating in the cloud that simply don't exist otherwise. We believe that the ability to get smarter through use of the cloud is the key differentiator that will sufficiently alleviate privacy fears to ensure widespread adoption.

Since user requirements for cloud services are varied, service providers have to ensure that they can be flexible in their service delivery while keeping the users isolated from the underlying infrastructure. Recent advances in microprocessor technology and software have led to the increasing ability of commodity hardware to run applications within *Virtual Machines* (VMs) efficiently.

VMs allow both the isolation of applications from the underlying hardware and other VMs, and the customization of the platform to suit the needs of the end-user. Providers can expose applications running within VMs, or provide access to VMs themselves as a service (e.g. Amazon Elastic Compute Cloud) thereby allowing consumers to install their own applications. While convenient, the use of VMs gives rise to further challenges such as the intelligent allocation of physical resources for managing competing resource demands of the users.

9. REFERENCES

3. A..Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Oct. 2007.
4. C. Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou," Toward Secure and Dependable Storage Services in Cloud Computing"june 2012.
5. C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage,", 2012,
6. C.Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," July/Aug. 2010.
7. C.Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," July 2009,
8. G.Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," 2007
9. H. Shacham and B. Waters, "Compact Proofs of Retrievability,", 2008.
10. J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure-Coded Data," 2007.
11. K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," , 2009
12. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," 2008.
13. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," 2009.
14. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"2011.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail i.e. **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals