



Survey of Different Methods of Privacy Preserving and Techniques

Sharmishtha D. Ronge

Department of Computer Network Engineering
Sinhgad College of Engineering
Pune, India

Mrs. C. A. Laulkar

Department of Computer Network Engineering
Sinhgad College of Engineering
Pune, India

Abstract-online services, such as Google, Yahoo and Amazon, a growing number of their storage users are starting to charge customers often e-mail, family photos and videos., such as valuable backup disk to store data and use these services today, a customer hosted data integrity perfectly intact and continue to return it to rely on such external services have unfortunately, Is a surefire service. storage service to create accountable for data loss From time to time to support a service and retain customer data to verify data stored by returning third party auditor and present this paper protocols that allow content that they never data. auditor open most importantly, these protocols are privacy protection, our solution removes the burden of verifying customer Both client and storage services data leak fear alleviates, and data retention contracts independent mediation provides a method for preserving privacy and techniques this paper reviews the various methods of shows.

Keywords—Cloud Computing, Utility Computing, Internet Data centres, Distributed System Economics, storage systems, storage security;

I. INTRODUCTION

National Institute of standards and technology (NIST) its statutory responsibilities under the Federal information security management Act (FISMA) of 2002, public law 107-347 developed this document to maintain. NIST standards and guidelines, all Agency operations and resources to provide minimum requirements for information security is responsible for the development, including; But national security systems shall not apply such standards and guidelines the guidelines in Office management and budget (OMB) Circular A-130, Section 8b is trusted with the requirements of (3), "to achieve agency information A-130, Appendix IV analysis systems,": analysis of key sections; A-130, Appendix III supplementary information. This guideline was prepared for use by Federal agencies. It might be used by nongovernmental organizations on voluntary basis and is not subject to copyright, though attribution have desired. [1] Verifying authenticity of data has emerged as a critical issue in storing data on un-trusted servers This peer-to-peer storage systems, network file systems, long term archives, Web-service object stores and database systems arise. Such systems storage server when accessing the data by examining the authenticity of the data is by modifying stop. [3]. Online services, like Amazon, Yahoo, Google, Snapfish.com, and Mozy.com, store, and maintain valuable user data to aim a lot of profit by the example of a growing number of uses online backup storage, email, photo sharing, These include services and video hosting several "teaser" (puzzle) storage for a small amount of free offers, and large, advanced versions of service [4] for some more trends are opening up cloud computing period. cloud computing Internet-based development and use of computer technology is coupled with ever cheaper and more powerful processors, "" software services (SaaS) architecture In data centers, computing are changing the rhythm of a large scale service computing, meanwhile, Increasing network bandwidth and reliable yet flexible network connection its customers now have high quality services data and software that resides on remote data centers [5] that can make possible to subscribe. Several trends are opening up computing systems to new forms of outsourcing, i.e., delegation of computing services to outside entities. Because of Improving network bandwidth and network reliability user become less dependent on local resources. Energy and labour costs as well as computing-system complexity are militating toward the centralized administration of hardware. Increasingly, a user employs software and data that resides thousands of miles away on machines those themselves do not own. Grid computing, the harnessing of disparate machines into a unified computing platform, has played a role in scientific computing for some years. Similarly, *software as a service (SaaS)* — loosely a throwback to terminal/mainframe computing architectures—is now a pillar in the internet-technology strategies of major companies [6]. This project give proof-of-irretrievability schemes with full proofs of security against arbitrary adversaries in the Juels-Kaminski model. This scheme has the shortest query and response of any proof-of-irretrievability with public variability and is secure in the random oracle model. This second scheme has the shortest response of any proof-of-irretrievability scheme with private variability (but a longer query), and is secure in the standard model [7]. Alice and Bob a family photo album, his daughter's marriage to Curly, and her baby pictures you want to include those in 2002 took these photos with a digital camera, and lens elephant photo sharing service uploaded their photos, they have for 25 years. to store a small fee is paid, but the lens elephant today They see nothing but an error they see Curly child full files-

after clicking on the thumbnails of the photos, the message "sorry, those files is corrupted." This is not just a dark fictional scenario. many online services customers, both end users and businesses as long as they want, and some services for the data store to the most popular sites allow can yet; even news report [1, 5] shows that data lost, And customers who to evaluate the risk of data loss or storage services is a rational basis for choosing between. While this paper focuses on the examples in the online storage service, newborn. Online service-oriented economy the problem generalizes. (OSOE) in which businesses and end users services online service providers (OSPs) are purchased from a variety of the growing economy to establish methods for assessing the risk of becoming and OSPs [8] is a capable computing cloud computing paradigms which recently drew widespread attention from both academia and industry will need to gain the trust customers. Service-Oriented Architectures (SOA) research areas and virtualization with existing and By combining a set of new technologies, Cloud computing is considered such as computing infrastructure that services provided in computing resources criteria on the Internet as these new criteria, with different business models, with the vocabulary as a service (Axis) "X" can be described by the developed [1] where X can be software, Hardware, data storage, and Amazon EC2 and S3, etc is successful examples [2], Google App engine [3], Microsoft Azure [4] which use relatively low cost pay-as you fashion provides users with scalable resources. For example, Amazon's S3 data storage service just \$ 0.12 to \$ 0.15 per gigabyte per month charges. Compared to their own infrastructures built by migration the users can save your investment in business on cloud. cloud computing technologies is increasing with the development of, It would in the near future more and more businesses being transferred to the cloud [9] is not difficult to imagine a human environment where small digital signatures manually key signature is said to need. For example, the product registration systems often users a CD label provided is for a signature key and more generally In short, sign-natures need bandwidth communication environment [10]. the project as in the era of pervasive computing, where computers are the surroundings, As part of the integrated everywhere there is equipment with each other Exchange of messages to a host for example, sensor networks, communication vehicle-2-move the vehicle [14]. In order to work properly, these systems should carry some form of message authentication, but especially on the certification system requirements [11] are demanding in recent years Third-party data warehousing and, more generally, the concept of outsourcing has become a popular data. essentially the outsourcing of data moves the data to the owner (client) its data through a third-party provider (server) which-possibly for a fee – to store data from the truth and it owns on demand (and maybe others) to make available to supposedly means to reduce cost savings from outsourcing attractive features. Storage Maintenance as well as keep up the increased availability and transparent-data [12] is involved in.

II. REVIEW OF ANALYSIS METHODS

A. On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

B. Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

C. Resource pooling

Provider of computing resources dynamically assigned multiple consumers and consumer demand according to reassign physical and virtual resources using a multi-tenant model, with service to deposit in the spirit of independence that are location customers usually don't control or knowledge over the exact location of the resources provided but abstraction (for example, Country, State, or enter data) is at a higher level may be able to specify the location. Storage, processing, memory, and network bandwidth are examples of resources.

D. rapid elasticity

Capabilities are elastically and provision, in some cases automatically, scale rapidly outward and inward to conform to the demands of released available for consumer, provisioning capabilities. Often appear to be unlimited and at any time in any quantity can be appropriated.

E. Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability¹ at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [1].

F. Threat model

The server S must answer challenges from the client C; failure to do so represents a data loss. However, the server is not trusted: even if the file is missing completely or partially, explain to the client that the server this file may try to server can be badly handled for inspiration and that is not or rarely (monetary reasons) data accessed discarding, Or no data loss incident hidden storage reclaiming (due to management errors, hardware failure, or understanding by indoors attacks etc). Receive a certificate of data capture potential PDP plan aims to detect badly handled when the server file server [3] is removed to a fraction of it.

At least with a) Audit: long-term State Auditor efficiently and check the contents stored on behalf of the client, you can service these audits must prove that material are completely unchanged.

B) Extraction: If the integrity of customer data retrieval, customer customers who suspected routes for auditor through data extraction protocol can use extraction, the Auditor can determine which party is at fault: If the service lost or which party is cheating by not assuming the protocol type, The Auditor can mediate a data retention contract. This data for all protocols Auditor do not disclose our content auditing Protocol zero-knowledge, Auditor to provide additional information to our extraction protocols to fix the data content from an auditor adversarial. Yet, they are still checking the integrity of recovered data lekhaprikshak and forward it so that a client can retrieve content efficiently to allow for.

A client to maintain any State does not require long-term. For example, the "fingerprints" or hashes stored data auditing, or secret key retrieval [4] to decrypt the data stored on the need to keep it.

With dynamic data integrity assurance c) operation: the project shows how this plan clearly and efficiently complete dynamic data including data revision (M) operations can handle data to delete data insertion (I) and (D) data storage [13] [17] cloud. Note that in the following details of the dynamic operation protocol for the design off file and sign the project value Φ has already been generated and properly stored on the server.

a) *Data Modification:* This project start from data modification, which is one of the most frequently, used operations in cloud data storage. A basic data modification operation refers to the replacement of specified blocks with new ones [5].

b) *Error correction:* This project carves this file F into k -block "chunks." To each chunk this project applies an (n, k, d) -error correcting code C over GF [2]. This operation expands each chunk into n blocks and therefore yields a file $F_0 = F_0 [1], F_0 [b_0]$, with $b_0 = bn/k$ blocks.

C) Encryption: the project file F_0 , a symmetric key is working to produce $F_0 E$ apply our Protocol for isolation, ability to decrypt data blocks are required whenever deletes or corrupts the collection blocks f the purpose of this project to recover. this type of project required that operates on plaintext blocks independently working E . to use an l -bit blocks are working An option for this case, We need the ability to distinguish a chosen-plaintext attack; It is for example, if an effect f in case of data content in practice were able to distinguish 2 blocks, a tweak to make a suitable choice of cipher strength e block will be like working a stream undesirable XEX working e . to work on a second option is to block the decryption key is missing some parts of the same section just be.

D) Sentinel creation: let $f: \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$ be a suitable one way function calculates the project s w sentinels $\{o\}$ as a set of o $f(_, w) = 1$. The project to produce these sentinels F_0 F_0 , attached to. (Thus, the project up to $b.s/qc$ challenges, each with q can accommodate queries.)

E) Permutation: let $g: \{0, 1\}^j \times \{1, b_0 + s\} \rightarrow \{1, b_0 + s\}$ is a pseudorandom permutation (PRP) is. $-j$ permute F_0 , output file apply to produce blocks of f student in particular, $SN F [i]$ let $= F_0 [-j(_, I)]$ [6].

F) Appraisal: formal security model. Such evidence-collection system should be evaluated by both "systems" and "crypto" criteria. includes: (1) system criteria e client both computational complexity and the complexity of the storage Protocol is evidence of communication as possible, as it should be, and storage overhead on the server should be as small as possible (2) rather than imposing a priori unbounded number of audit protocol that is bound to interactions² the system in use Should be allowed; (3) changes should be stateless And maintain and is difficult to maintain such a State if the State audits do not need to update changes the machine crashes or if changes have delegated to third parties or multiple machine role 3 is distributed between Statelessness and massive use of evidence with the public for variability of storage systems, Can a role in evidence-collection protocols varies, not only users who le [7] originally stored.

III. REVIEW OF PARALLEL PROCESSING METHODS

A. Internal audits are hard

Violating the integrity of the data to assess the risks, threats and existing best practices an auditor to prevent data loss should understand. Unfortunately, this information is for storage services are difficult to achieve: the only description of the failures and their causes in mass storage systems several studies [10, 12] deployed. Baker et al. [2] data protection is Such as natural disasters and attacks known as insiders to provide a list of hazards. Individual organizations have resulted in data loss to recognize some bad practices can learn, however. Determine best practices compare and experiments are needed. This in turn failure to share information across various environments and vendors need to share this data storage services. Reluctant to both clients and providers current position is counter-productive. Assessing the quality of the customer service cannot, and storage services internal data can improve once proper incentives with a System are established, Storage service will allow internal audits. Trusted third-party auditors then piece together this information gradually and it audit process will be in a position to integrate. [8] [17].

B. System Models

This project assumes that the system is made up of the following Parties: data owners, many data consumers, many cloud servers and a third-party auditor if necessary. The owner of the data, data consumers of data files or for brevity to reach shared by users, data files, and downloaded from the server to cloud their interest then decrypt. Not be always online user's data owner or they come just on the basis of required online Are for the sake of simplicity, the project assumes that users read-only access privilege data file. data to support the proposed scheme file write of data as the author makes each update [12] to sign up new data file is now despised by asking at the, The project also will call data files for brevity. Cloud Server always online and cloud service providers (CSP) are powered by the abundant storage capacity and computation they power are assumed. Third-party auditor is also an online party what each file is used for auditing access

event. In addition the project acknowledges that the owner of the data can not only data files but also to manage their cloud data files to run your code on the server. The assumption is most recent cloud computing which integrated ontology in Yourself et al. [9] the proposed matches.

Ring and ring the one ring signature scheme the signer to sign themselves in such a way that a verifier that the signer is one of the ring members, but he may not be able to tell which Member includes a set of users to sign up on a message from a signatory allows plans is the actual signer identity-based ring signature a Eigen., Sign and verify that, respectively, a user to generate a public and private key, Signing a message from the ring and ring a sign verified according to algorithms is a triple a ring in a user identity-based signature is an arbitrary string, for example your email address, you can choose as his public key corresponds to the private key private key. generator (PKG) is a trusted party called a master key with the user's identity, represents such a string binding Is created by any such plan consists of four algorithms: Setup, Eigen, Sign and verify that during Setup, set system parameter Pub PKG and selects a master secret key mask. Based on its identification string PKG Eigen, during a secret key allows the user. Except that only Pub and ring Member identity need are public keys instead of signing and verification algorithms again as before powered. [11] [16].

C. Security Analysis

Random oracle model security update algorithm follows directly from the evidence of the case stable. By the way the only difference is the sixth count project: XOR hashing instead link blocks each block hashes and anti-asked during the resulting outputs Simulator to remove the ability to single-block will not change. Indeed As, the project is a unique index "each individual section at random challenge to query an opposing forces by Oracle indicated that" Hash (1 r) are included in the. In addition, XOR-Ed hashes collision-resistance property analysis comes directly [12].

IV. CONCLUSION AND FUTURE WORK

This paper surveys privacy protection methods for auditing and digital content describes the extraction of two main contributions (1) motivation, beliefs, and third-party privacy auditing and extraction, and (2) different privacy protection audit and extraction of data stored with a service provider Protocol are set for protection. the auditing data stored remotely are intact verifies that a third-party auditor is included for extraction, The data is intact and to ensure that the original data to verify the client, returns the lekhaprikshak type, these schemes, auditor data retention contracts storage provider and the customer can mediate plans two pieces, an encryption key and encrypted data is data partitions. Protocol both those pieces without either a built-in audit and disclose the content to remove those pieces auditor At least allow with long-term State, using these protocols. All properties (19 secret keys or hashes) any longer to maintain the State can be achieved without the requirement of the client. Encrypt data protocols to cryptographic hashes and rely on symmetric key encryption. This project is key to the current encryption protocols that have different beliefs, but all agree that hard computing discrete logs. Project believes that such protocol if outsourcing truly Hold-in digital content protection will be required on.

ACKNOWLEDGMENT

We would like to thank Prof. Mr. P. R. Butane, H.O.D, Computer Engineering Department, for his support in helping us complete this paper in due time. We would like to thank the entire support staff of the Computer Engineering department in making sure that all our needs were met and all other issues were dealt with in a smooth and positive manner.

REFERENCES

- [1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at <http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>, 2009.
- [2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
- [3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 598–609.
- [4] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
- [5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *Proc. of ESORICS'09, volume 5789 of LNCS*. Springer-Verlag, Sep. 2009, pp. 355–370.
- [6] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of CCS'07*, Alexandria, VA, October 2007, pp. 584–597.
- [7] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. of Asiacrypt 2008*, vol. 5350, Dec 2008, pp. 90–107.
- [8] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in *Proc. Of HotOS'07*. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.
- [9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in *Proc. of IEEE INFOCOM'10*, San Diego, CA, USA, March 2010.

- [10] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
- [11] A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in *Proceedings of CT-RSA, volume 5473 of LNCS*. Springer-Verlag, 2009, pp. 309–324.
- [12] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proc. Of SecureComm '08*, 2008, pp. 1–10.
- [13] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.
- [14] "PORs: Proofs of Retrievability for Large Files," *Proc. ACM Conf. Computer and Comm. Security (CCS '07)*, pp. 584-597, Oct. 2007.
- [15] Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," *IEEE Trans. Service Computing*, vol. 5, no. 2, 220-232, Apr.-June 2012.
- [16] Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE *TRANSACTIONS ON COMPUTERS*, VOL. 62, NO. 2, FEBRUARY 2013.
- [17] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.