ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Survey on Secured Data Transferring in Cloud Computing

Nivedita B. Patil, Prof. Abhay Pawar, Rohit P. Vibhandik

P.G. Student, Department of Computer Science, Astral Institute of Technology & Research, Indore, India

Assistant Professor, Department of Computer Science, Astral Institute of Technology & Research, Indore, India

P.G. Student, Department of Computer Science, B. M. College of Technology, Indore, India

ABSTRACT: Cloud computing has gained a lot of hype in the current era and it is said to be the next big thing in the computer world after the internet. Cloud computing is using Internet for the tasks performed on the computer and it is visualized as the next- generation architecture of IT Enterprise. Cloud computing is attached to several technologies and the union of various technologies has emerged to be called cloud computing. Cloud Computing transfers the application software and databases to the enormous data centers, where the administration of the data and services may not be fully honest. This irreplaceable attribute poses many new security challenges which have not been well understood. In this paper, we discuss the mechanism that not only protect sensitive data by enabling computations with encrypted data, but also protect customers from malicious behaviors by enabling the validation of the computation result.

KEYWORDS: Cloud Computing, Homomorphic, IaaS, LP Problem, PaaS

I. INTRODUCTION

Cloud computing is the use of computational resources such as hardware and software that are delivered as a service over aninternet. The name cloud computing comes from the use of a cloud-shaped symbol to show the complex infrastructure it contains in system diagrams. Cloud computing trusts remote services with an user's data, software and computation. Cloud computing is a common term for anything that involves delivering hosted services over an Internet. A cloud service has three distinct characteristics that differentiate it from traditional hosting. It provides on demand access, typically by the minute or the hour; it is expandable - a user can have as much or as little of a service as he wants; and the service is fully managed by the service provider. A cloud may be private or public. A public cloud allows services to everyone on the Internet. AtPresent, Amazon Web Services is the largest public cloud service provider [6].

Quality of service is an important part from the point of data security. In cloud computing there are challenging security threats for various reasons. Firstly, we can't apply old cryptographic technique for data security protection because the user may lose control of data under cloud computing [2].

Each customer stores various kind of data in the cloud and customer wants longtime assurance of data security but the problem of verifying correctness of data stored in the cloud is morechallenging. Another security threat is the customer frequently changed data which is stored in the cloud like inserting, deleting, modifying, appending, re-ordering, etc [1]. Lastly, the deployment of Cloud Computing is powered by data centers running in a synchronized, cooperated and distributed approach. Each user's data is redundantly stored in numerous physical locations to reduce the data integrity intimidation. Therefore, distributed protocols for the purpose of storage, correctness and assurance will be most important in achieving a robust and secure cloud data storage system in the existent world. However, such important region remains to be fully opened up in this literature. The cloud computing possess various service models which are given below.

In this paper, we only focus on the Software as a service. In this model, cloud service providers install and operate application software in the cloud and cloud users uses the software from cloud clients. The cloud users need not manage the cloud infrastructure and platform on which the application is running. This thing eliminates the need to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

install and run the applications on the cloud user's computers, simplifying maintenance and support. Elasticity is the main feature which makes cloud computing different from other applications which can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand of the fastest growing IT world. Load balancers are those whodistribute the work over the set of virtual machines. This process is not noticeable to the cloud user who sees only a solitary access point. To hold a large number of cloud users, cloud applications can be multitenant-any machine serves many cloud user organization. Common namingconventions to refer to special types of cloud based application software are: communication as a service, business process as a service, test environment as a service, desktop as a service.

Numerous trends are opening up in the era of Cloud Computing is an Internet dependent development and use of computer technology. The low cost and more dominant processors in combination with the software as a service (SaaS) computing architecture, are transforming data centers in the pools of computing service on a large degree [4]. The growing bandwidth of network and reliable, flexible network connections make it possible that users can now subscribe high quality services from data and software that resides solely on remote data centers.

The remarkable benefits, outsourcing computation to the commercial public cloud is also grudging customer's direct control over the systems that consume and produce their data during the computation, which unavoidably brings in new security issues and challenges towards this promising computing model. On the one hand, the outsourced computation on the cloud server often contain sensitive information and data, such as the business related financial records, computational models, proprietary research data, property related useful information or personally identifiable health related information etc[1].

To take action against unauthorized information outflow, this sensitive data must be encrypted before outsourcing. So to provide end-to-end data confidentiality assurance on the cloud and beyond. However, usual data encryption techniques prevent cloud from performing any significant operation of the fundamental plaintext data information, making the computations over encrypted data information is a very hard problem [1]. On the other hand, the operational details inside the cloud are not transparent to customers. As a result, there exists various motivations for cloud server to behave deceitfully and to return inaccurate results, i.e., they may behave away from the classical semi honest model. For example, to carry out the computations that require a large amount of computing assets, there are huge financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output [1]. In addition, possible software bugs, hardware failures or even attacks from outsiders might also create an effect the quality of the computed results. Thus, we can say that, according to the customer's point of view the cloud is not secure.

The remaining paper is organized as follows. Section II contains the Literature Survey. Then we have discussed the problem in Section III. Section IV provides the Proposed Work and V demonstrates the result of the system. Finally, concluding remark of the whole paper.

II. RELATED WORK

According to "Non-interactive verifiable computing: Outsourcing computation to entrusted workers" the author R. Gennaro [4] said that, the work is based on the criticaland a bit surprisinginspection that Yao's Garbled Circuit Construction, in addition to providing safe two-party computation, also provides a "one-time" verifiable computation. In other words, we can get used to Yao's construction to allow a client to outsource the computation of a task on a single input. Specifically, in the preprocessing stage the client garbles the circuit C according to Yao's construction. Then in the "input preparation" stage, the client reveals the random labels associated with the input bits of x in the garbling. This allows the worker to compute the random labels associated with the output bits, and with the output bits client will reconstruct F(x). If the output bit labels are sufficiently long and random, the worker would not be able to guess the labels for an incorrect output, and therefore the client is assured that F(x) is the correct output.

According to "Secure outsourcing of sequence comparisons", the author M. J. Atallah [9] said that, we more precisely stated the edit distance problem, in which the cost of an insertion or deletion or substitution is a symbol-dependent non-negative weight, and the edited distance then the least-cost set of insertions, deletions, and substitutions necessary to transform one string into the other. More officially, if we let λ be a string of length n, $\lambda = \lambda_1 \ldots \lambda_n$ and μ

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

be a string of length m, $\mu = \mu_1 \ldots \mu_m$, both over some alphabet $\sum$. There are three types of allowed edit operations to be done on λ: insertion of a symbol, deletion of a symbol, and substitution of one symbol by another [5]. Each operation has a cost linked with it, namely I(a) denotes the cost of inserting the symbol a, D(a) denotes the cost of deleting a, and S(a, b) denotes the cost of substituting a with b [7][8]. Each sequence of operations that transforms λ into μ has a cost associated with it and the least-cost of such sequence is the edit-distance. The edit path is the actual sequence of operations that corresponds to the edit distance. According to "Secure outsourcing of scientific computation", the authors M. J. Atallah et al. [9] said that they created the first analysis of safe outsourcing of numerical and scientific computation. A set of problem dependent disguising methods are proposed for different scientific applications like linear algebra, sorting, string pattern matching, etc. However, these disguise techniques explicitly allow information disclosure to certain degree. Atallah et al. discuss in [10] and [11], produced two protocol designs for both secured sequence comparison outsourcing and secured algebraic computation outsourcing. However, both protocols used heavy cryptographic primitive such as homomorphic encryptions and/or oblivious transfer and do not scale well for large problem set.

In addition, both designs are built upon the hypothesis of two non-colluding servers and thus vulnerable to colluding attacks. Based on the same guess, Hohenberger et al. [3] give protocols for safe outsourcing of modular exponentiation, which is considered as prohibitively expensive in most public-key cryptography operations. Very recently, Atallah et al. [5] given a provably safe protocol for safe outsourcing matrix multiplications based on secret allocation. While this work outperforms their previous work [11] in the sense of single server hypothesis and computation effectiveness, the main drawback is the large communication overhead. Namely, due to secret sharing method, all scalar operations in original matrix multiplication are expanded to polynomials, introducing important amount of overhead. Considering the case of the result authentication, the communication overhead must be further doubled, due to the introducing of additional pre-computed "random noise" matrices [12][13].

Another large existing list of work that relates to (but is also significantly different from) Secure Multi-party Computation (SMC), first introduced by Yao [11] and later extended by Goldreich et al. [1] and many others. SMC allows two or more parties to together compute some general function while hiding their inputs to each other. As general SMC can be very ineffective, Du and Atallah et al. [5] have proposed a series of customized solutions under the SMC context to a spectrum of special computation harms, such as privacy-preserving cooperative statistical analysis, scientific computation, geometric computations, sequence comparisons, etc. [14]. However, unswervingly applying these approaches to the cloud computing model for secure computation outsourcing would still be problematic. With the major reason is that they did not address the asymmetry among the computational powers possessed by cloud and the customers, i.e., all these schemes in the context of SMC impose each involved parties comparable computation burdens, which we exclusively avoid in the mechanism design by shifting as much as possible computation burden to cloud only.

Lately, Li and Atallah [16] had presented a study for secure and mutual computation of linear programming under the SMC framework. The solution of this problem is based on the additive split of the constraint matrix between two involved parties, followed by a series of interactive (and arguably heavy) cryptographic protocols collaboratively executed in each iteration step of the Simple Algorithm. This solution has the computation irregularityproblem mentioned previously. Besides, they only consider honest-but-curious representation and thus do not guarantee that the final solution is optimal.

Some recent general result can be found in Goldwasser et al. In distributed computing as well as targeting the specific computation assignment of one-way task inversion, Golle et al. [15] planned to insert some pre-computed results (images of "ringers") along with the computation workload to defeat entrusted (or lazy) workers. In Du. et al. [14] planned a system of cheating detection for general computation outsourcing in grid computing. The server is required to provide aassurance via a Merkle tree based on the results it computed. The customer can then use the dedication combined with a sampling approach to carry out the result verification (without re-doing much of the outsourced work.) However, all above schemes allocate server actually see the data and result it is computing with, which is strictly forbidden in the cloud computing model for data privacy. Thus, the problem of result authentication essentially becomes more complex, when both the input/output isolation is demanded. So the duality hypothesis of LP

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

problem and efficiently bundles the result authentication within the method designs, with little extra overhead on both customer and cloud server [17].

III. ADVANTAGES AND DISADVANTAGES

Advantages of using cloud services: Achieve economies of scale, cloud increases the volume of output or productivity with less number of people.

1. Cloud reduces spending on technology infrastructure. It maintains easy access to user information with minimal upfront spending. Paying for cloud is on as per the use.
2. Cloud globalizes your workforce on the cheap. People all over the world can access the cloud provided they have an Internet connection.
3. Cloud allows user to get more work done in less time with less people.
4. Cloud reduces capital costs. There's no need to spend a lot of money on hardware, software or and also on licensing fees.
5. Cloud improves accessibility. It gives access anytime, anywhere, making the life so easy.
6. Cloud monitors projects more effectively.
7. It takes less number of people to do more work on a cloud, with aminimal curve of learning on software and hardware problems.
8. Use of cloud minimizes licensing new software. Stretch and grows without the need to buy expensive software licenses or programs.
9. Cloud improves flexibility. One can change direction without serious "people" or "financial" issues at stake.

In spite of having such a big list of advantages cloud has some of disadvantages too. Following are some of the disadvantages of cloud:

1. If your internet service suffers from frequent outages or slow speeds cloud computing may not be suitable for your business. And even the most reliable cloud computing service providers suffer server outages now and again.
2. Security issues- Data security is a very big issue for cloud computing.
3. Inflexibilityis also one of the biggest issue with the cloud computing Be careful when you're choosing a cloud computing one should make sure that you can add and subtract cloud computing users as necessary as your business grows or contracts.
4. In spite of having these disadvantages cloud is being used because it has some outstanding properties as follows:
5. Cloud provides on-demand self-service: A consumer can individually providecomputing capabilities, as needed automatically without requiring human interaction with each service provider.
6. It givesbroad network access as the capabilities are available over the network and accessed through standard mechanisms e. g. mobile phones, tablets, laptops and workstations.
7. Cloud computing uses resource pooling to serve multiple customers using a multi-tenant model, with variousvirtual and physical resources vigorously assigned and reassigned according to customer's requirement.
8. Cloud computing gains rapid elasticity, the capabilities can be elastically provided and released, in some of cases they are automatically, to scale rapidly outward and inward commensurate with demand.
9. Cloud systems automatically controls and optimize resource use. Resource usage can be supervised, controlled and informed, providing transparency for the provider and consumer.

Applications of cloud computing-

1. Infrastructure as a service (IaaS) & platform as a service (PaaS) IaaS is using an current infrastructure on a pay-per-use scheme seems to be an obvious choice for companies saving on the cost of investing to acquire, manage and maintain an IT infrastructure. There are also instances where organizations turn to PaaS for the same reasons while also seeking to increase the speed of development on a ready-to-use platform to deploy application.
2. Private cloud and hybrid cloud-Among the many incentives for using cloud, there are two situations where organizations are trying to assess some of the applications they intend to deploy into their environment through the use of a cloud. In the case of test and development it may be narrow in time, adopting a hybrid cloud approach allows for testing application workloads, therefore providing the ease of an environment without the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

initial investment that might have been rendered useless should the workload testing fail.Next use of hybrid cloud is the ability to expand during periods of narrow peak usage, which is frequently preferable to hosting a big infrastructure that might rarely be of use. An organization would seek to have the additional capacity and obtainability of an environment when needed on a pay-as you-go basis.

3. Test and development-Probably the best situation for the use of a cloud is a development and test environment. This involves securing a financial plan, setting up environment through physical assets, significant manpower and time. Then comes the installation and configuration of your platform. All this can often extend the time it takes for a project to be completed and stretch your milestones.
4. Big data analytics- One aspect offered by cloud computing is its ability to tap large quantities of both structured and unstructured data to harness the benefit of extracting business value.
5. File storage- Cloud can offer the possibility of storing your files and accessing, storing and retrieving them from any web-enabled interface. The web services interfaces are usually simple. At any time and place you have high availability, speed, scalability and security for your environment. In this scenario, organizations are only paying for the amount of storage they are actually consuming, and do so without the worries of overseeing the daily maintenance of the storage infrastructure.
6. Disaster recovery-This is yet another benefit derived from using cloud based on the cost effectiveness of a disaster recovery (DR) solution that provides for a faster recovery from a mesh of different physical locations at a much lower cost that the traditional DR site with fixed assets, rigid procedures and a much higher cost.
7. Backup- Back up the user's data is always a complex and time-taking process. This includes maintaining a set of drives, manuallyassembling them and send out them to a backup facility with all the problems that might happen in between the originating and the backup site. This way to ensure a backup is performed is not safe to problems such as running out of backup media , and there is also time to load the backup devices for a restore operation, which takes too much time and is likely to happen faults and human inaccuracies.Cloud-based backup, is certainly a good solution than the one what it used to be. One can now automatically send data to any location crossways the wire with the guarantee that there are no security, availabilityand capacity issues.

IV. CONCLUSION

In this paper, we study different method for securing the data outsourcing in cloud computing. In secure outsourcing of scientific computation we study about secure outsourcing of numerical and scientific computation. In secure outsourcing of sequence comparison we study about two protocol designs for both secure sequence comparison outsourcing and secure algebraic computation outsourcing. In the securely multi-party computation we study the method of cheating detection for general computation outsourcing in grid computing. So all the method is not fully secure for data outsourcing in cloud computing. So our system enables the customers to secretly transform original problem into arbitrary one while protecting sensitive input/output data.

ACKNOWLEDGMENT

At the time of making a survey on this area many people were helped me. I specially thankful to Prof. AtulThakkar, Principal, Astral Institute of Technology & Research for valuable guidance on this area. Last but not the least we also thank to our Faculty members, staff and friends for being instrumental towards the completion of this paper.

REFERENCES

1. C. Wang, K. Renand J. Wang, 'Secure and practical outsourcing of linear programming in Cloud computing', IEEE Transition on cloud computing, pp.820-828, April 2011
2. C. Wang, Q. Wang, K. Ren and W. Lou, 'Ensuring data storage security in Cloud Computing', in Proc. Of IWQoS'09, July 2009
3. S. Hohenberger and A. Lysyanskaya, 'How to securely outsource cryptographic computations', in Proc. of TCC, pp 264-282, 2005
4. R. Gennaro, C. Gentry and B. Parno, 'Non-interactive verifiable computing: Outsourcing computation to entrusted worker', in Proc. of CRYTO'10, Aug 2010.
5. M. Atallah and K. Frikken, 'Securely outsourcing linear algebra computation', in Proc of ASIACCS, pp. 48-59, 2010.
6. N. Gohring, 'Amazon's S3 down for several hours', Online at http://www.pcworld.com/businesscenter/article/142549/amazons_s3_down_for_several_hours.html, 2008.
7. Amazon.com, 'Amazon Web Services (AWS)', Online at http://aws.amazon.com, 2008.
8. Sun Microsystems, Inc., 'Building customer trust in cloud computing with transparent security', online at https://www.sun.com/offers/details/sun_trans parency.xml, 2009

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

9. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, 'Secure outsourcing of scientific computations', Advances in Computers, vol. 54, pp. 216–272, 2001
10. M. J. Atallah and J. Li, 'Secure outsourcing of sequence comparisons',Int. J. Inf. Sec., vol. 4, no. 4, pp. 277–287, 2005.
11. D. Benjamin and M. J. Atallah, 'Private and cheating-free outsourcing of algebraic computations', in Proc. of 6th Conf. on Privacy, Security, and Trust (PST), pp. 240–245, 2008.
12. A. C.-C. Yao, 'Protocols for secure computations (extended abstract)', in Proc. of FOCS'82, pp. 160–164,1982.
13. O. Goldreich, S. Micali, and A. Wigderson,'How to play any mental game or a completeness theorem for protocols with honest majority', in Proc. of STOC'87, 1987, pp. 218–229.
14. W. Du and M. J. Atallah, 'Secure multi-party computation problems and their applications: a review and open problems', in Proc. of New Security Paradigms Workshop (NSPW, pp. 13–22), 2001.
15. P. Golle and I. Mironov, 'Uncheatable distibuted computations', in Proc. of CT-RSA, pp. 425-440, 2001.
16. J. Li and M. J. Atallah, 'Secure and private collaborative linear programming', in Proc. of CollaborateCom, Nov. 2006.
17. W. Du, J. Jia, M. Mangal and M. Murugesan, 'Uncheatable grid computing', in Proc. Of ICDCS, pp. 4-11, 2004.
18. Nivedita B. Patil, Rohit P. Vibhandik, Prof. Abhay Pawar, 'Secured Data Outsourcing in Cloud Computing', International Journal on Recent and Innovation Trends in Computing and Communication(IJRITCC), Volume: 3 Issue: 3, ISSN: 2321-8169 1577 – 1581, 2015.

BIOGRAPHY

Nivedita B. Patil is a P.G. Student, Department of Computer Science Department, Astral Institute of Technology & Research, Indore, India. She received BE degree in 2011 from NMU, Jalgaon, India. Her research interests are Computer Networks and Cloud Computing.

Prof. Abhay Pawar is an Assistant Professor, Department of Computer Science Department, Astral Institute of Technology & Research, Indore, India. His research interests are Computer Networks and Cloud Computing.

Rohit P. Vibhandik is a P.G. Student, Department of Computer Science Department, B. M. College of Technology, Indore, India. He received BE degree in 2010 from NMU, Jalgaon, India. His research interests are Computer Networks and Cloud Computing.