IJCTA, 10(02), 2017, pp. 27-31

Multidimensional Security Analytics Method for Storing A Information Over Multicloud Computing

T. Sumathy* and S. Saravana Kumar**

Abstract: Cloud computing is computing paradigm in which task are assigned to a combination of connections software, hardware, services over the internet. Several trends are opening up the era of cloud computing which is use for computer technology. Conceptually, users get computing platform from computing clouds and then inside run their applications. Always cheaper and more powerful processors together with the software-as-a-service computing architecture. These are transforming data centers into of computing service on huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality service from data and software that reside solely on remote data centers. Cloud offers great convenience to users „when transforming data into cloud since cloud client don"t have to care about the complexities of direct hardware management.

Keywords: Service, encrypted, attacks, planning, computing.

1. INTRODUCTION

Cloud computing technology is an open standard, service-based, The Cloud has become a new traveler for delivering resources such as computing and storage to customers on demand. Rather than being a new technology in itself, the cloud is a new business model wrapped around new technologies such as server virtualization that take advantage of economies of scale and multi-tenancy to reduce the cost of using information technology resources. Here we discusses the business drivers in the Cloud delivery mechanism and business model, what the requirements are in this space, and how standard interfaces, coordinated between different organizations can meet the emerging needs for interoperability and portability of data between clouds.storage and infrastructure. Cloud computing providers deliver the applications via internet, which are accessed from web browsers, desktop and mobile apps. Cloud Computing Technologies are grouped into 4 sections: they are, SaaS, DSaaS, IaaS and PaaS. **SaaS (Software as a Service)** is an on-demand application service. Itdelivers software as a service over the Internet.

PaaS isdelivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustainingcloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. It improves the flexibility in having multiple platforms in business environment. **DSaaS (Data Storage as Services)** is an on- demand storage service.Cloud computing provides internet- based on demand back up storage services to a customer. In this service, customers can keep their data backup remotely over internet servers. These backup data maintenance is taken care by DsaaS service Provider. Cloud DsaaS service providers are responsible for keeping the customer data confidential. Here customers need not worry on setting up the large discs array to keep their huge amount of data. **IaaS (Infrastructure as a Service)**

* Research scholars, Dept of Computer Science Engineering, Bharath University,Chennai

** Professor, Department of CSE, Karpagam College of Engineering, Coimbatore *sumathy_k2005@yahoo.com, saravanakumars81@gmail.com*

is an on- demand infrastructure service. It delivers the computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients can buy those resources as a fully outsourced service.

Security Threats and Mitigation : In today's competitive market, being able to explore data to understand customer behaviour, segment customer base, offer customized services, and gain insights from data provided by multiple sources is key to competitive advantage. Although decision makers would like to base their decisions and actions on insights gained from this data [4], making sense of data, extracting non obvious patterns, and using these patterns to predict future behaviour are not new topics. Knowledge Discovery in Data (KDD) [5] aims to extract non obvious information using careful and detailed analysis and interpretation. Data mining [13,8], more specifically, aims to discover previously unknown interrelations among apparently unrelated attributes of data sets by applying methods from several areas including machine learning, database systems, and statistics. Analytics comprises techniques of KDD, data mining, text mining, statistical and quantitative analysis, explanatory and predictive models, and advanced and interactive visualisation to drive decisions and actions [3,4,6].

The large volume and different types of the data can demand pre-processing tasks for integrating the data, cleaning it, and filtering it. The prepared data is used to train a model and to estimate its parameters. Once the model is estimated, it should be validated before its consumption. Normally this phase requires the use of the original input data and specific methods to validate the created model. Finally, the model is consumed and applied to data as it arrives. This phase, called model scoring, is used to generate predictions, prescriptions, and recommendations. The results are interpreted and evaluated, used to generate new models or calibrate existing ones, or are integrated to pre-processed data. Analytics solutions can be classified as descriptive, predictive, or prescriptive Descriptive analytics uses historical data to identify patterns and create management reports; it is concerned with modelling past behaviour. Predictive analytics attempts to predict the future by analysing current and historical data. Prescriptive solutions assist analysts in decisions by determining actions and assessing their impact regarding business objectives, requirements, and constraints.

Despite the hype about it, using analytics is still a labour intensive endeavour. This is because current solutions for analytics are often based on proprietary appliances or software systems built for general purposes. Thus, significant effort is needed to tailor such solutions to the specific needs of the organisation, which includes integrating different data sources and deploying the software on the company's hardware (or, in the case of appliances, integrating the appliance hardware with the rest of the company's systems)

[12]. Such solutions are usually developed and hosted on the customer's premises, are generally complex, and their operations can take hours to execute. Cloud computing provides an interesting model for analytics, where solutions can be hosted on the Cloud and consumed by customers in a pay-as-you-go fashion.

For this delivery model to become reality, however, several technical issues must be addressed, such as data management, tuning of models, privacy, data quality, and data currency.

2. RELATED WORK

Recently, much of growing interest has been pursued in the context of remotely stored data verification [2]–[10], [12]–[15]. Ateniese *et al.* [2] are the first to considerpublic auditability in their defined "provable data possession"

(PDP) model for ensuring possession of files on untrusted storages. In their scheme, they utilize RSAbased homomorphic tags for auditing outsourced data, thus public auditability is achieved. However, Ateniese *et al.* do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer design and security problems. In their subsequent work [12], Ateniese *et al*. propose a dynamic version of the prior PDP scheme. However, the system imposes a *priori* bound on the number of queries and does not support fully dynamic data operations, *i.e.*, it only allows very basic block operations with limited functionality, and block insertions cannot be supported. In [13], consider dynamic data storage in a distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors.Similar to [12], they only consider partial support for dynamic data operation. Juels *et al.* [3] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on archive service systems. Specifically, some special blocks called "sentinels" are randomly embedded into the data file F for detection purpose, and F is further encrypted to protect the positions of these special blocks. However, like [12], the number of queries a client can perform is also a fixed *priori*, and the introduction of pre-computed "sentinels" prevents the development of realizing dynamic data updates. In addition, public auditability is not supported in their scheme. [4] design an improved PoR scheme with full proofs of security in the security model defined in [3]. They use publicly verifiable homomorphic authenticators built from BLS signatures [16], based on which the proofs can be aggregated into a small authenticator value, and public retrievability is achieved.

Still, the authors only consider static data files [14] was the first to explore constructions for dynamic provable data possession. They extend the PDP model in [2] to support provable updates to stored data files using rank-based authenticated skip lists. This scheme is essentially a fully dynamic version of the PDP solution.

To support updates, especially for block insertion, they eliminate the index information in the "tag" computation in Ateniese's PDP model [2] and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure. However, the efficiency of their scheme remains unclear. Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing.

Password generation : In this level a team level password generation to authenticate the team for particular service. Example team needs to enter the team name, team id, team thumb image and sign. First all images get added and convert into number data. This data gets concatenate with textual inputs. The resultant output will be a TA (multidimensional team authentication) password.

3. SECURITY ANALYSIS

In this section, we evaluate the security of the proposed scheme under the security model . This level is a user level password generation. It authenticates the user privileges. User need to enter user name, age, phone number, id and DOB to generate his/her password. Algorithm will process these inputs and generate the PA(multidimensional privilege authentication) password. Organization password alone is not sufficient to access any cloud service. Organization password helps to move authentication into Intranet. Team password helps to move intra team and privilege password helps to access the cloud service for particular user.

Password Generation : Foresee the emergence of what they termed as Business Intelligence and Analytics (BI&A) 3.0, which will require underlying mobile analytics and location and context-aware techniques for collecting, processing, analysing, and visualising large scale mobile and sensor data. Many of these tools are still to be developed. Moreover, moving to BI&A 3.0 will demand efforts on integrating data from multiple sources to be processed by Cloud resources, and using the Cloud to assist decisions by mobile device users. More recently, terms such as Analytics as a Service (AaaS) and Big Data as a Service (BDaaS) are becoming popular. They comprise services for data analysis similarly as IaaS offers computing resources. However, these analytics services still lack well defined contracts since it may be difficult to measure quality and reliability of results and input data, provide promises on execution times, and guarantees on methods and experts responsible for analyzing the data. Therefore, there are fundamental gaps on tools to assist service providers and clients to perform these tasks and facilitate the definition of contracts for both parties.

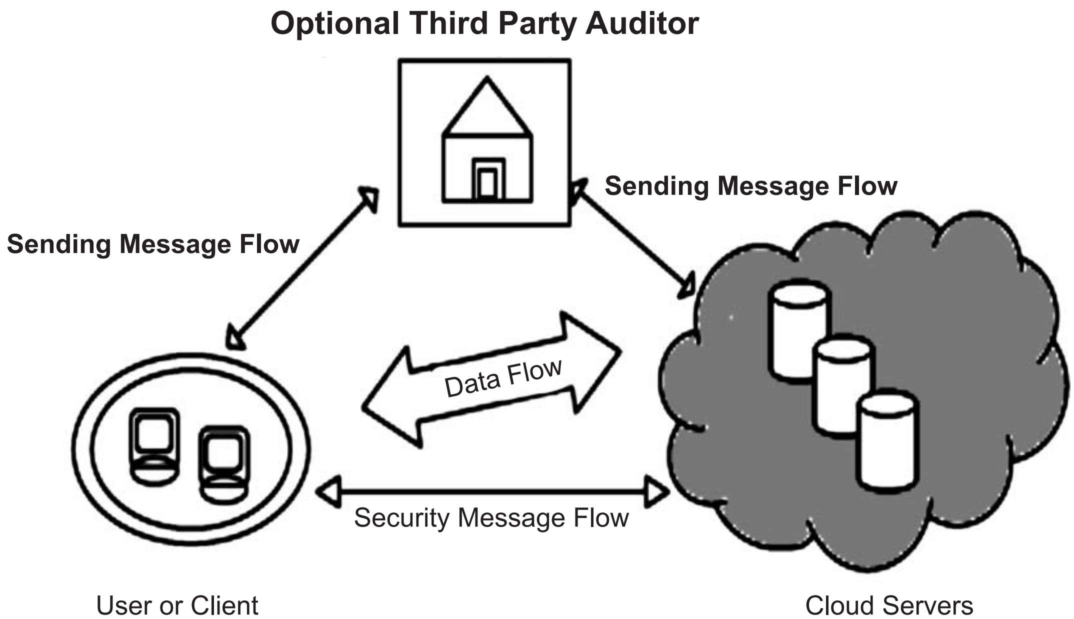

Figure 1

4. CONCLUSIONS

Cloud computing helps in alleviating these problems by providing resources on-demand with costs proportional to the actual usage. Furthermore, it enables infrastructures to be scaled up and down rapidly, adapting the system to the actual demand.Although Cloud infrastructure offers such elastic capacity tosupply computational resources on demand, the area of Cloudsupported analytics is still in its early days. In this paper, we discussed the key stages of analytics workflows, and surveyed the state-of-the-art of each stage in the context of Cloud-supported analytics. Model Building and Visualisation and User Interactions. For each of these areas, ongoing work was analysed and key open challenges were discussed. This survey concluded with an analysis of models for Cloud-assisted data analytics and other non-technical challenges. In research this paper, we examine the problem of data security problem stored the in cloud data storage, which is mostly a distributed storage system, In this research our scheme achieves the integration of data error localization and storage correctness insurance. security analysis shows that our scheme is highly efficient.

5. REFERENCES

1. IEEE - The Application of Cloud Computing in Education Informatization, Modern Educational Tech... center Bo Wang, HongYu Xing.
2. NIST Definition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc
3. CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx
4. X. Suo, Y. Zhu, G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annual Computer Security Application.
5. S. Wiedenbeck, J. Waters, J.-C.Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc. Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.
6. Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication,"IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008
7. Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%2 computing%20 services.

8. A User Identity Management Protocol for Cloud Computing Paradigm SafiriyuEludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehindeapered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

9. NandiniMishara, KanchanKhushwha, RituChasta, Er. AbhishekChoudhary, "Technologies of Cloud Computing – Architecture Concepts based on Security and its Challenges, International Journa of Advanced Research in Computer Enginering and Technology (IJARCET), Volume 2, Issue 3, March 2013

10. Michael Miller, "Cloud Computing, Web-Based Applications That Change the Way You Work and Collaborate Online", Pearson, Eight Impression, 2013.

11. AtifAlamri, WasaiShadab Ansari, Mohammad Mehedi Hassan, M.ShamimHossain, AbdulhameedAlelaiwi, M.AnwarHossain, "A Survey on Sensor-Cloud: architecture, Applications, and Approaches, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 917923, 18 pages, 2013

12. AnuRathi, Yogech Kumar AnisshTalwar, "Aspects of Security in Cloud Computing", International Journal of Engineering and Computer Science ISSN: 2319-7242, Volume 2, Issue 4, April 2013, Page no. 1361-1363

13. T. Neetha, CH. Sushma, "Security for Effective Data Storage in Multi Clouds", International Journal of Computer Applications Technology and Research, Volume 2, Issue 1, 16-17, 2013

14. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. of CCS'09*. Chicago, IL, USA: ACM, 2009.

15. K. D. Bowers, A. Juels, and A. Oprea, "Hail: A high-availability and integrity layer for cloud storage," in *Proc. of CCS'09*. Chicago, IL, USA: ACM, 2009, pp. 187–198.

16. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proc. of ASIACRYPT'01*. London, UK: Springer- Verlag, 2001, pp. 514–532.

17. R. C. Merkle, "Protocols for public key cryptosystems," *Proc. Of IEEE Symposium on Security and Privacy'80*, pp. 122–133, 1980.

18. S. Lin and D. J. Costello, *Error Control Coding, Second Edition*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004.

19. M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. of CCS'93*,1993, pp. 62–73.

20. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Of Eurocrypt'03*. Warsaw, Poland: Springer-Verlag, 2003.

21. Birst Inc., http://www.birst.com.

22. R. Bonney, J.L. Shirk, T.B. Phillips, A. Wiggins, H.L. Ballard, A.J. Miller-Rushing,J.K. Parrish, Next steps for citizen science, Science 343 (2014) 1436–1437.

23. D. Borthakur, J. Gray, J.S. Sarma, K. Muthukkaruppan, N. Spiegelberg, H. Kuang, K. Ranganathan, D. Molkov, A. Menon, S. Rash, R. Schmidt, A. Aiyer, Apache Hadoop Goes Realtime at Facebook, in: Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD 2011), ACM, New York, USA, 2011, pp. 1071–1080.

24. C. Bunch, N. Chohan, C. Krintz, J. Chohan, J. Kupferman, P. Lakhina, Y. Li, Y. Nomura, An Evaluation of Distributed Datastores Using the AppScale Cloud Platform, in: Proceedings of the 3rd IEEE International Conference on Cloud Computing (Cloud 2010), IEEE Computer Society, Washington, USA, 2010, pp. 305–312.

25. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Gener. Comput. Syst. 25 (6) (2009) 599–616.

26. B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu,S. Srivastav, J. Wu, H. Simitci, J. Haridas, Windows Azure Storage: A Highly Available Cloud Storage Service with Strong Consistency, in: Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP 2011), ACM, New York, NY, USA, 2011, pp. 143–157.

27. R.N. Calheiros, C. Vecchiola, D. Karunamoorthy, R. Buyya, The Aneka platformand QoS-driven resource provisioning for elastic applications on hybrid Clouds, Future Gener. Comput. Syst. 28 (6) (2012) 861–870.