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 8, August 2015

TPA Authentication Based Security and Privacy Setting in Muticloud Environment

Dr.P.Sumitra[1], M.Kavinnela[2]

Assistant Professor, Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, Tamil Nadu, India.

M.Phil Full-time Research Scholar, Department of Computer Science and Applications, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, Tamil Nadu, India.

ABSTRACT Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [8]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Even more, if deploying data-processing applications to the cloud (via IaaS or PaaS), a cloud provider gains full control on these processes. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. Depending on the political context this trust may touch legal obligations. For instance, Italian legislation requires that government data of Italian citizens, if collected by official agencies, have to remain within Italy. Thus, using a cloud provider from outside of Italy for realizing an e-government service provided to Italian citizens would immediately violate this obligation. Hence, the cloud users must trust the cloud provider hosting their data within the borders of the country and never copying them to an off-country location (not even for backup or in case of local failure) nor providing access to the data to entities from abroad. An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data. Even though in the majority of cases it may be legitimate to assume a cloud provider to be honest and handling the customers' affairs in a respectful and responsible manner, there still remains a risk of malicious employees of the cloud provider, successful attacks and compromisation by third parties, or of actions ordered by a subpoena.

KEYWORDS: Cloud Computing, Multicloud, Privacy, Security, Partitioning, Implementation.

I.INTRODUCTION

Replication of applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result. Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic. Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

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 8, August 2015

II.LITERATURE SURVEY

A. TOWARDS ENSURING CLIENT-SIDE COMPUTATIONAL INTEGRITY (A POSITION PAPER)

In this paper [2], the authors GEORGE DANEZIS and BENJAMIN LIVSHITSstated that privacy is considered one of the key challenges when moving services to the Cloud. Solution like access control is brittle, while fully homomorphic encryption that is hailed as the silver bullet for this problem is far from practical.

There are two key problems with this approach: first, no practical fully homomorphic encryption schemes exists yet [10]; second, as we will argue, even if fully homomorphic encryption was available at the cost of other cryptographic operations today, it would still be inefficient for most computations and could be replaced with a simpler architecture that is already realisable at a low cost today.

They devoted the remaining of this paper in describing a cryptographic architecture that could be made available today to solve aspects of the problem of privacy in the cloud at a relatively similar cost as if homomorphic encryption was used. While the network overheads of the proposed approach will be higher, its advantage is that it can be deployed today.

B. TOWARDS USER CENTRIC DATA GOVERNANCE AND CONTROL IN THE CLOUD

In this paper [2], the authors STEPHAN GROß and ALEXANDER SCHILL stated that cloud computing, i. e. providing on-demand access to virtualised computing resources over the Internet, is one of the current mega-trends in IT. Today, there are already several providers offering cloud computing infrastructure (IaaS), platform (PaaS) and software (SaaS) services. Although the cloud computing paradigm promises both economical as well as technological advantages, many potential users still have reservations about using cloud services as this would mean to trust a cloud provider to correctly handle their data according to previously negotiated rules.

A sound and trustworthy monitoring system for cloud services that is able to gather all relevant information to detect or even predict SLA violations without manipulations by the cloud provider under control. To support the configuration of the monitoring system, there should be some mechanism that derives relevant monitoring objectives from negotiated SLAs. Thus, we need a formalised language for machine-readable SLA focussing on the technical details of a cloud computing environment.

The proposed cloud platform should be adaptive, i.e. it should provide mechanisms to react on SLA violations detected by the monitoring system in order to mitigate the resulting negative effects. These mechanisms should include migration tools to transparently transfer resources to another cloud provider as well as adaptation tools that leaves the resources at the chosen provider but transforms them to further meet the user's non-functional and security requirements.

C.SEPIA:PRIVACY-PRESERVING AGGREGATION OF MULTI-DOMAIN NETWORK EVENTS AND STATISTICS

In this paper [5] the authors MARTIN BURKHART, MARIO STRASSER, DILIP MANY and XENOFONTAS DIMITROPOULOS stated that secure multiparty computation (MPC) allows joint privacy-preserving computations on data of multiple parties. Although MPC has been studied substantially, building solutions that are practical in terms of computation and communication cost is still a major challenge. In this paper, they investigated the practical usefulness of MPC for multi-domain network security and monitoring. They first optimized MPC comparison operations for processing high volume data in near real-time. They then designed privacy-preserving protocols for event correlation and aggregation of network traffic statistics, such as addition of volume metrics, computation of feature entropy, and distinct item count.

Furthermore, the basic operations of the SEPIA library are significantly faster than those of existing MPC frameworks and can be used as building blocks for arbitrary protocols. They believed that their work provides useful insights into the practical utility of MPC and paves the way for new collaboration initiatives.

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 8, August 2015

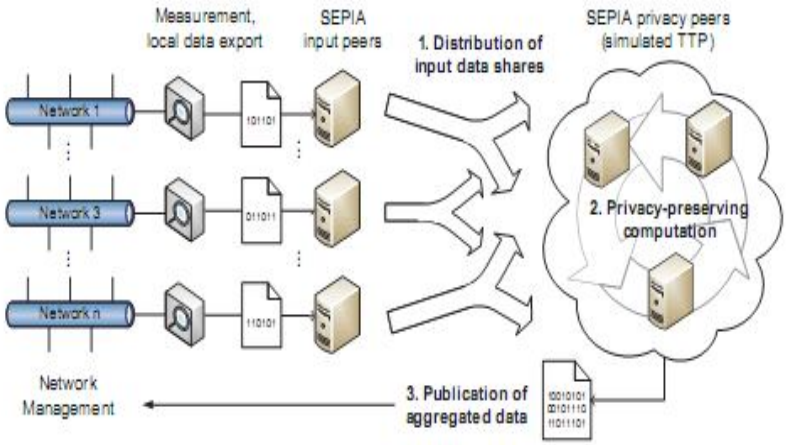

FIG 1. DEPLOYMENT SCENARIO FOR SEPIA

Their future work includes improving SEPIA's robustness against host failures, dealing with malicious adversaries, and further improving performance, using, for example, polynomial set representations. Furthermore, in collaboration with a major systems management vendor, they had started a project that aims at incorporating MPC primitives into a mainstream traffic profiling product.

D. TWIN CLOUDS: SECURE CLOUD COMPUTING WITH LOW LATENCY (FULL VERSION)?

In this paper [2] the authors SVEN BUGIEL, STEFAN NURNBERGER, AHMAD-REZA SADEGHI and THOMAS SCHNEIDER stated that Abstract. Cloud computing promises a cost effective enabling technology to outsource storage and massively parallel computations. However, existing approaches for provably secure outsourcing of data and arbitrary computations are either based on tamper-proof hardware or fully homomorphic encryption. The former approaches are not scaleable, while the latter ones are currently not efficient enough to be used in practice.

Their proposed solution has several advantages over previous proposals (cf. x2):
1. Communication Efficiency. They minimized the communication between the client and the Trusted Cloud as only a program, i.e., a very compact description of the function, is transferred and compiled on-the-fly into a circuit.
2. Transparency. The client communicates with the Trusted Cloud over a secure channel and clear interfaces that abstract from the underlying cryptography.
3. Scalability and Low Latency. Their approach is highly scalable as both clouds can be composed from multiple nodes. In the Query Phase, the Trusted Cloud performs only few computations (independent of the function's size).
4. Multiple Clients. Their protocols can be extended to multiple clients such that the Commodity Cloud securely and non-interactively computes on the clients' input data.

III.IMPLEMENTATION

1. IMPLEMENTATION PROCESS

When the initial design was done for the system, the client was consulted for the acceptance of the design so that further proceedings of the system development can be carried on. After the development of the system a demonstration was given to them about the working of the system. The aim of the system illustration was to identify any malfunction of the system.

After the management of the system was approved the system implemented in the concern, initially the system was run parallel with existing manual system. The system has been tested with live data and has proved to be error free and user friendly.

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 8, August 2015

Implementation is the process of converting a new or revised system design into an operational one when the initial design was done by the system; a demonstration was given to the end user about the working system. This process is uses to verify and identify any logical mess working of the system by feeding various combinations of test data. After the approval of the system by both end user and management the system was implemented.

IV.DISCUSSIONS

EXPERIMENTAL RESULTS

TABLE 1. REPLICATION REQUIREMENT AND COMPUTATION OVERHEAD

METHOD	REPLICATION	COMPUTATION OVERHEAD
Resource Replication	Required	In client only
PIR based segmentation	Not required	Low in client tier/ More in database tier (stored procedure) and negligible in web tier
Segmentation of application logic and data	Not required	In client only
Third party auditing	Not required	High In client, Low in third party system and negligible in cloud node

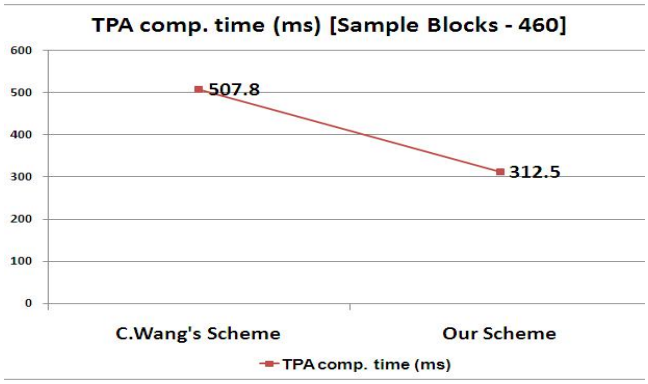

FIG 2.TPA COMPUTATION TIME CHART COMPARISON (C.WANG;S SCHEME VS OUR SCHEME) (CHART TYPE – LINE CHART).

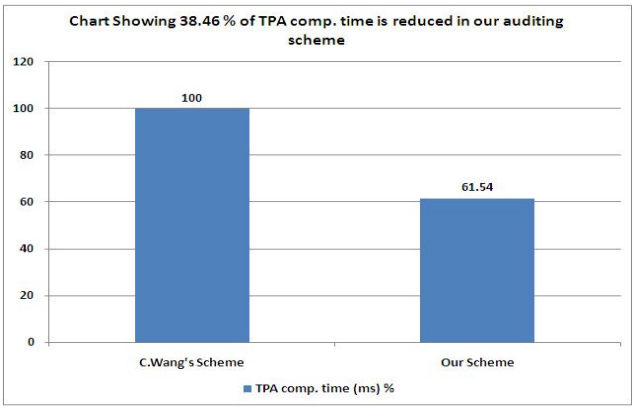

FIG 3. CHART COMPARISON FOR TPA COMPUTATION TIME IN %.

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 8, August 2015

V. FINDINGS

- The proposed system provides a safe cloud storage methodology which supports privacy-preserving third party auditing better than existing system.
- This thesis suggests that the security can be increased if the architecture is changed from single cloud to multi cloud environment.
- Security mechanisms involved during third party auditing of outsourced data is discussed.
- Hiding resource usage statistics of a single resource for a single cloud provider is achieved if first method is applied.
- The computation and data transfer size is very low if the second method is applied.
- The third method provides the security such that a single provider may not be aware of the execution flow of the single application as well as the cloud provider could not know or access all the data.
- The fourth method provides the benefit of auditing with very low credential data to verify the file content.
- It is proved that the third party auditing computation time is better than existing approach.
- The future study should focus on security proof and enhancements in data retrieval of the proposed framework.

VI.CONCLUSION AND FUTURE ENHANCEMENTS

A. CONCLUSION

Through this project, the problem of secure communication is eliminated. In addition, the application required less working experience in systems to run the software. The application is tested well so that the end users use this software for their whole operations.

It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the project is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The project effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

B. SCOPE FOR FUTURE DEVELOPMENT

The following enhancements are should be in future.

- ✓ The application if developed as web services, then many applications can make use of the records.
- ✓ The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- ✓ The web site and database can be hosted in real cloud place during the implementation

VII.REFERENCES

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 199-212, 2009.
[2] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM Conf. Computer and Comm. Security (CCS '12), pp. 305-316, 2012.
[3] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, "All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces," Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, 2011.
[4] S. Bugiel, S. Nu ¨ rnberger, T. Po ¨ppelmann, A.-R. Sadeghi, and T.Schneider, "AmazonIA: When Elasticity Snaps Back," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, 2011.
[5] G. Danezis and B. Livshits, "Towards Ensuring Client-Side Computational Integrity (Position Paper)," Proc. ACM Cloud Computing Security Workshop (CCSW '11), pp. 125-130, 2011.
[6] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: a virtual machine-based platform for trusted computing. In ACM Symposium on Operating Systems Principles, pages 193–206. ACM, 2003.

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 8, August 2015

[7] O. Acii¸cmez. Yet another microarchitectural attack: Exploiting I-cache. In ACM Workshop on Computer Security Architecture, pages 11–18, October 2007.
[8] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In 16th ACM Conference on Computer and Communications Security, pages 199–212, 2009.
[9] Gnu Privacy Guard. www.gnupg.org, 2012.
[10] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. Openpgp message format. Technical report, RFC 2440, November, 1998.
[11] McIntosh, M., and Austel, P. XML Signature Element Wrapping attacks and Countermeasures. In SWS '05: Proceedings of the 2005 workshop on Secure web services (New York, NY, USA, 2005), ACM Press, pp. 20-27.
[12] SIMPSON, C. R., JR., AND RILEY, G. F. Neti@home: A distributed approach to collecting end-to-end network performance measurements. In Passive and Active Measurement Conference (PAM) (2004).
[13] PORRAS, P., AND SHMATIKOV, V. Large-scale collection and sanitization of network security data: risks and challenges. In Workshop on New security paradigms (NSPW) (2006).
[14] OHM, P. Broken promises of privacy: Responding to the surprising failure of anonymization. 57 UCLA Law Review (2010).Available at http://ssrn.com/abstract=1450006.

TEXT BOOKS

1. Alistair Mc Monnies, "**Object-Oriented programming in Visual C#. NET**", Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.
2. Robert D.Schneider, Jetty R.Garbus, "**Optimizing SQL Server**", Second Edition, Pearson Education Asia, ISBN: 981-4035-20-3
3. Jittery R.Shapiro, "The Complete Reference Visual C# .NET" Edition 2002, Tata McGraw-Hill, Publishing Company Limited, New Delhi.
4. Hannes Hartenstein (Editor), Kenneth Laberteaux (Editor) "Vehicular Applications and Inter-Networking Technologies"