IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Enlargement of a Cloud Based Seclusion Monitoring Framework for the Health Division

A.Kaleemullah[1], R.Deepa Priyadarshni[2], P.Rizwan Ahmed[3]

[1]Assistant Professor & Head of Computer Science (Shift – II),
Mazharul Uloom College, Ambur (India)
[2]Research Scholar, Mazharul Uloom College, Ambur (India)
[3]Assistant Professor & Head of Computer Application & Information Technology,
Mazharul Uloom College, Ambur (India)

ABSTRACT

Cloud computing is growing in popularity due to its ability to offer dynamically scalable resources provisioned as services regardless of user or location device. However, moving data to the cloud means that the control of the data is more in the hands of the cloud provider rather than the data owner. This is a great challenge that continues to hinder cloud computing from successfully achieving its potential. This is due to the fact that with cloud computing, the storage and processing of private information is done on remote machines that are not owned or even managed by the cloud consumers. This brings about significant security and data privacy concerns that impede the broader adoption of cloud computing, which compromises the vision of cloud computing as a new IT procurement model.

Keywords: Service Models, Deployment Models, Third Party Audit (TPA), Trusted Platform Module (TPM)

I.INTRODUCTION

Cloud computing has become the most intriguing enticing technology of today due to its ability to offer dynamically scalable resources provisioned as services over the internet. Cloud Computing offers services that are cost effective, flexible and easy to use. However, despite these advantages and the strong interest in cloud computing, data privacy is a key concern that hinders the adoption of the cloud (Doelitzscher, Reich, & Sulistio, 2010a; Henze, Grossfengels, Koprowski, & Wehrle, 2013; Huang & Du, 2013a; Kun, Abraham, & Yuliang, 2013). As a result, there is a need for mechanisms to allay users' privacy concerns, so that cloud computing can fully reach its potential (Pearson, Shen, & Mowbray, 2009).

In an organisational context, privacy entails the application of laws, policies, standards and principles such as fair information practices which represent widely-accepted concepts concerning fair information practice. In a nutshell, privacy is about the accountability of organisations to data subjects, as well as the transparency of an organisation's practice around personal information. In an electronic world, these principles provide guidelines for the collection and use of collected data so as to protect consumer data. An emphasis is also put on openness and transparency that must be in operation during the process of collection and processing of Personally

Identifiable Information (PII) (Langheinrich, 2001).

II. PRELIMINARY BACKGROUND

Business frameworks and procedures have become more perplexing and sophisticated; organizations are gathering an expanding measure of data, especially PII. Subsequently, organizations are attempting to keep pace with their requirements for capacity in a way that minimizes costs. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable resources e.g. (Network, servers, storage, application and services) that can be quickly provisioned and discharged with negligible administration exertion of cloud provider interaction (Jansen & Grance, 2011).

While providing adaptable solution for complex information technology needs, cloud computing poses additional privacy challenges to those using it. Cloud provider may end up processing data without complying with requirements of privacy laws and regulations such as the privacy and data protection bill of South Africa. This requires that when the cloud consumer has personal information stored and processed in the cloud, the customer must be satisfied that the cloud service provider has implemented the proper technical security controls and organizational measures to secure customer’s personal information against unauthorized access to personal information which may result in violation of user privacy (South African Law Reform Commission, 2005; Parliamentary Monitoring Group, 2006).

III.STATEMENT OF THE PROBLEM

The shared nature of the cloud storage infrastructure and the fact that when the data is stored in the cloud, the control of the data is more on the hands of the cloud provider rather than the data owner is a challenge that continues to hinder cloud computing from successfully reaching its capability. If not monitored closely, public cloud services can place sensitive data at risk, jeopardizing enterprise data privacy just as much as they do end users’ privacy. From this stems the need for the means to allow the data owner to monitor what is happening to her/his data. Current solutions such as the best effort approach (Glott et al., 2011), Third-Party Audit (Glott et al., 2011), cloud provider self-service web portals and publications (Nemati & Van Dyke, 2009), Privacy-aware Role Based Access Control (Ni et al., 2007) and Service Level Agreements (SLAs) lack the capability to enable cloud customers to retrace in detail what happens to their data, where it is stored, who accessed it and what levels of security and privacy are applied to it.

IV. STATE-OF-THE-ART ANALYSIS

This chapter reviews the state-of-the-art in privacy monitoring mechanisms and further assesses the impact the current privacy compliance and regulation have on implementation of the cloud technologies. A lot of attention has been channelled to coming up with mechanism to mitigate security and privacy threats that continue to hinder cloud computing technology from reaching its success capability. Partial solutions have been proposed which range from superficial to academic. However privacy remains a challenge (Lemoudden, Bouazza, Ouahidi, & Bourget, 2013).

Approaches that were analysed and reviewed in this research are being discussed in the following sections.

Section 3.2 discusses third party based privacy monitoring approaches, in section 3.3 network based solutions are critically analysed. Section 3.4 discusses privacy by encryption solutions. Section 3.5 discusses privacy by computation solution and section 3.6, privacy by design is discussed respectively. Lastly anonymization techniques are discussed in section 3.7. From these discussions, the strength and weaknesses of these approaches are established. The categorization of different type of privacy enhancing technologies was carried out, in order to assess the solutions, compliance to privacy regulation and to assess if they instil trust back into cloud consumers. In addition to ascertain that cryptography satisfies the cloud security requirements in providing data confidentiality and integrity and the impact they have toward the implementation of cloud computing various encryption techniques have been evaluated and reviewed.

It is from this gained knowledge that a solution approach was systematically formulated that advocates the use of informative events and access logs to enable the cloud customers to retrace in details who accesses to their personal private information, operations performed on the information, by whom and the security safeguards applied to it.

V. PRIVACY MONITORING TECHNIQUES

The most commonly used approaches to provide privacy and data security are, Best Effort Approach, Third Party Audit, Privacy as a Service, Trusted Third Party Audit and Privacy Manager.

VI. THE BEST EFFORT APPROACH

Security and privacy are attributed to the lack of proper security control policies and weaknesses in security safeguards in cloud deployments (Prasad et al., 2011b). To tackle the privacy challenge, the best effort is proposed by Glott et al. (2011). This is done through the conduct of self-assessments to determine if the systems are compliant with privacy regulations and standards. These assessments are based on arbitrary frameworks which generally focus on the documentation of security policies.

However, this approach gives no guarantees of securing the data that is in cloud service provider’s custody. It only promises to set proper security safeguard to preserve data privacy without giving any guarantees, and should something goes wrong it could not be held liable since it would claim it did all that it could to protect the data. The Santos, Gummadi, & Rodrigues, (2009) and Pearson, (2013) contends that service providers should be able to provide attestation on why they claim their services are private and secure in the most transparent manner. These authors’ highlights that the promises of security are usually not enough, customers need to be shown convincing evidence that security measures are in place to ensure security.

VII. DESIGN AND DEVELOPMENT OF A PRIVACY MONITORING FRAMEWORK

The lack of transparency in cloud security controls and privacy measures is widely seen as an obstacle that is hindering the broad adoption of the cloud computing technology (Pearson, 2009). Researchers are advocating for a mechanism that would enable cloud consumers’ to have an insight into how their data is stored and processed by the cloud service provider and who else have access to it.

This research work, proposes a solution that builds on top of the strengths of the previous works to address the privacy issues in the cloud. To achieve this end in view privacy manager approach was adopted and to compensate for its drawbacks the informative event and access log analyser was developed. It enables cloud customers to retrace in details what happened to their data, where they are stored, who accesses them and the security safeguards applied to it. The conceptual solution put forward by this research work will attempt to solve the privacy issues that continue to hinder broader cloud computing adoption.

VIII. PRIVACY MONITORING FRAMEWORK

The framework presented below addresses the limitation identified in the knowledge base as discussed in the preceding chapter. The proposed framework illustrated in Figure 4.1 intends to realize this by using an information events and access logs analyser component which would enable cloud customers to retrace in detail what happened to their data, where they are stored and who accesses them and the security safeguards applied to it while it is in custody of the cloud service provider.

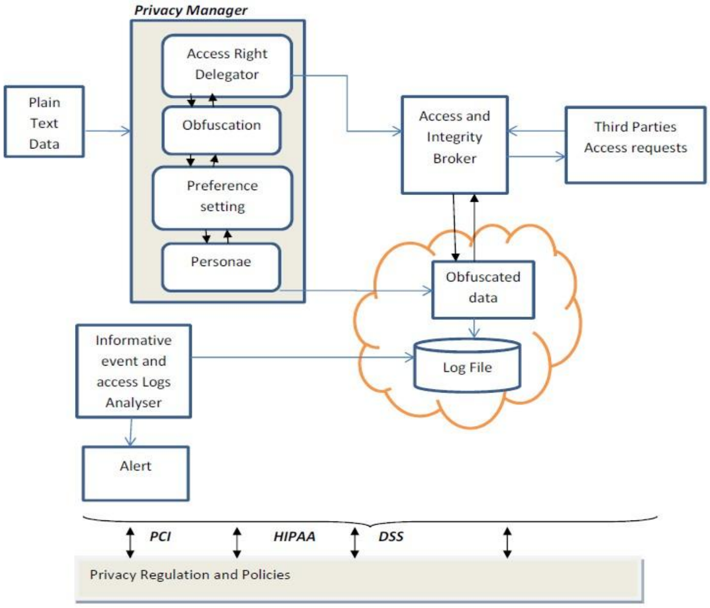
Privacy Manager
Access Right Delegator
Obfuscation
Preference setting
Personae
Plain Text Data
Access and Integrity Broker
Third Parties Access requests
Obfuscated data
Log File
Informative event and access Logs Analyser
Alert
PCI
HIPAA
DSS
Privacy Regulation and Policies

Figure 0.1 Privacy Monitoring Framework

Monitoring the privacy of the outsourced data plays a critical role in determining whether the privacy of user data stored in the cloud has been violated or not. Since the data owner by law remains responsible for the compliance with all the principles of data privacy regarding the outsourced data (Glott et al., 2011; South African Law Reform Commission, 2005; Reed, Rezek, Simmonds, 2011). The data subject must therefore be able to control and comprehend what happens to the data in the cloud. Monitoring gives answers to both parties with regards to data handling issues with regards to determining which party is responsible in the event of data loss.

IX. CONCLUSION

The lack of proper privacy and security mechanisms to monitor the sensitive information entrusted to cloud service providers by its consumers has been the barrier to broader adoption of cloud computing technology, as reported by a number of surveys conducted in this area of study. Despite many cloud computing services properties, such as low entry cost, elasticity is perfectly suited to support a variety of business operations and lower the operating costs, However, privacy has remained the most difficult proposition when a business is considering to adopt cloud computing. This owes to the fact that with cloud computing, the storage and processing of private information are done on remote machines that are not owned or overseen by the clients. All that the client can see is a virtual infrastructure built on top of possibly non-trusted physical hardware or operating environments.

The purpose of this research work was to develop a privacy monitoring framework for cloud computing environment, to allay users' privacy concerns and to allow for broader adoption in order for cloud computing to fully achieving its potential. The developed privacy monitoring framework has the potential to help cloud customers to comprehend what happens to their data while stored in the cloud, by employing an informative event which would enable users to trace in details what happens to the data, where they are stored and who accesses it. The framework realized this by using an informative event and an access logs analyzer, which enabled cloud customer to monitor the privacy of their data while it is kept in the custody of the cloud service provider.

REFERENCES

[1] Abadi, M. (2004). Trusted Computing, Trusted Third Parties, and Verified Communications. In In SEC2004: 19th IFIP International Information Security Conference.

[2] Adil Alsaid , David Martin , Saudi Arabian, M. A. (2003). Privacy Enhancing Technologies. (R. Dingledine & P. Syverson, Eds.) (Vol. 2482). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/3-540-36467-6

[3] Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017–1042. Retrieved from http://dl.acm.org/citation.cfm?id=2208940.2208951

[4] Bellare, M., Boldyreva, A., & O'Neill, A. (2007). Deterministic and Efficiently Searchable Encryption. In Proceedings of the International Cryptology Conference on Advances in Cryptology (CRYPTO) (pp. 535–552). doi:10.1007/978-3-540-74143-5_30

[5] Bertino, E., Martino, L. D., Paci, F., & Squicciarini, A. C. (2010). Security for web services and service-oriented architectures. Security for Web Services and Service-Oriented Architectures (pp. 1–226). doi:10.1007/978-3-540-87742-4

[6] Davies, N., & Langheinrich, M. (2013). Privacy By Design [From the Editor in Chief]. IEEE Pervasive Computing, 12(2), 2–4. doi:10.1109/MPRV.2013.34

[7] Brooke, J. (1996). SUS-A quick and dirty usability scale. Usability Evaluation in Industry, 189, 194. doi:10.1002/hbm.20701

[8] Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. Computer Law & Security Review, 29(5), 522–530. doi:10.1016/j.clsr.2013.07.005