ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 6, Issue 4, pp: (61-65), Month: October - December 2018, Available at: www.researchpublish.com

Investigation on the Data Protection in the Cloud using Predicate Based Encryption

[1]Dr.K.SAI MANOJ, [2]Ms. K. Mrudula, [3]Mrs G.Maanasa, [4]K.Phani Srinivas

[1]CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
[2]Director, Innogeecks technologies, Vijayawada, AP, India
[3]Research Scholar, Acharya Nagarjuna University, Guntur Dist, AP, India
[4]Editor and Reviewer, Head R&D, Associate Professor Amrita Sai Institute of Science and Technology, Vijayawada, AP, India

***Abstract*: This Research Paper investigates how Predicate Based Encryption (PBE) could be leveraged within the Cloud to protect data. PBE is a novel family of asymmetric encryption schemes in which decryption of a cipher-text is dependent upon a set of attributes satisfying a certain predicate, allowing for selective ne-grained access control to be specied over cipher-texts. It is argued that obfuscation of one's data is not enough when seeking to protect data. The control of how one's data is used and the trust a orded to service providers is equally as important. To this end, three archetypal scenarios are described that illustrate ways in which service users could specify precisely with whom they wish to share their data, for what purpose, and for how long. Furthermore, two additional scenarios are presented that would allow a service provider to facilitate keyword search over encrypted data using expressive queries supporting conjunction and disjunction of terms.**

***Keywords:* PBE, encryption, decryption, conjunction, disjunction.**

1. INTRODUCTION

Cloud Computing:

Cloud Computing is the name given to the recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. Functionality such as storage, processing and other functionality is now on demand, as a service and both freely and at cost. Data, that was once housed under a consumers own administrative and security domain, has now been extracted and placed under the domain of the Cloud Service Provider (CSP).The consumer has e ectively lost control over how their data is being stored, shared and used, and also over the security used to protect their data. Moreover, it can be the case that a surreptitious employee of the service provider will have access to your data for legitimate purposes but will abuse this power for their own means. Users are no longer in full control over the security of their data and the protection by the service provider is not absolute. There is a need for users to have more control over the protection of their data within the cloud: Users need to become empowered.

The investigation was divided broadly into three stages.

1) Data Security and the Cloud. The initial stage sought to provide a clear picture regarding Cloud Computing and the security issues therein, looking to identify precisely where and when threats can occur to data and how these threats ought to be mitigated.

2) Predicate Based Encryption. The next stage focused solely upon PBE schemes discussing how they work and what they allow for. This provided a foundation upon which their deployment as part of a crypto-system could be explored and to de ne the types of problem that PBE schemes can be used to solve.

3) Leveraging PBE. The final stage of the investigation built upon, and combined the results, of the previous stages. Here the investigation looked to determine the problems that PBE schemes can be used to solve within the Cloud, and the quality of solution provided.

Research Outcomes:

From the investigation, it was determined that PBE can be used to protect data within the cloud. The main results for each stage of the investigation are outlined below.

Data Security and the Cloud. From the initial stage two threat-models were produced: one user and the other CSP orientated. These models described the threats upon data in terms of the data lifecycle. Furthermore, it was determined that a privacy model centered around Kafka's. The Trial together with the idea that the CSP provider could be trusted facilitates a better understanding of the problems present within the Cloud and how such problems can be solved.

Predicate Based Encryption. Characteristics that can be used to categorise PBE schemes were identi ed. Of which predicate placement had the greatest a ect upon the access control a orded by the scheme. A generic model for deploying PBE schemes as part of a crypto-system was developed. From this model three modes of operation that characterises the deployment of a PBE scheme were identi ed.

Leveraging Predicate Based Encryption. Three scenarios are described that illustrate ways in which service users could specify precisely with whom they wish to share their data, for what purpose, and for how long. Furthermore, two additional scenarios are presented that would allow a service provider to facilitate keyword search over encrypted data using expressive queries supporting conjunction and disjunction of terms.

2. DATA SECURITY WITHIN THE CLOUD

Overview:

Cloud Computing is the name given to a recent trend in computing service provision. This trend has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely and en masse, by third-party service providers. This new means of service provision has evolved from and is the culmination of research stemming from (among others) distributed and networked systems, utility computing, the web and software services research .This paradigm shift has led to computing being seen as another household utility and has prompted many a business and individual to migrate parts of their IT infrastructure to the cloud and for this data to become managed and hosted by Cloud Service Providers (CSPs).

Computing as a Service:

One of the main tenets of Cloud Computing is the `as-a-Service' paradigm in which `some' service is o ered by a Service Provider (also known as a Cloud Service Provider) to a User (consumer) for use. This service can also be categorized according to the application domain of its deployment. Examples of application domains that services are: Financial e.g. Mint.com, Managerial e.g. Ever Note and Analytical e.g. Google Analytics. The agreed terms of use, indicating the actions that must be taken by both the provider and consumer, are described in a contract that is agreed upon before service provision. Failure to honor this agreement can lead to denial of service for the consumer or legal liability for the service provider. This contract is often described as a Terms of Service or Service Level Agreement. Moreover, as part of this agreement the service provider will provide a Privacy Policy which outlines how the user’s data will be stored, managed, used and protected.

Service Levels:

Software as a Service: Highest layer is known as: Software as a Service (SaaS). It represents the applications that are deployed/enabled over a cloud by CSPs. These are mature applications that often API to allow for greater application extensibility. For instance, Google Docs can be seen as the archetypal SaaS application, it has been deployed solely within the Cloud and several APIs to promote use of the application.

Platform as a Service: The next layer is known as: Platform as a Service (PaaS). This represents a development platform that developers can utilize to write, deploy and manage applications that run on the cloud. This can include aspects such as development, administration and management tools, run-time and data management engines, and security and user management services. For instance, Force.com and Amazon Web Services [AWS] a suite of services that allows developers to construct an application that is deployed using web-based tooling.

Infrastructure as a Service: Lowest layer is known as: Infrastructure as a Ser-vice (IaaS). CSP developers, a highly scaled and elastic computing infrastructure that are used to run applications. This infrastructure can be comprised of virtualized servers, storage, databases and other items. Two well known examples are the Amazon Elastic Compute Cloud, a commercial platform as part of Amazon.com's Web Service platform and Eucalyptus, an open source platform that the same functionality.

Entities Involved:

Cloud actors/entities can be divided into two main categories: A) CSP or Service Provider those who provide a service; and B) Cloud Service User (Users) those who use a service. Within Cloud Computing the between the role played by a service provider and a user can be blurred. The service provider could also be the user of another service e.g. when infrastructure is the service. The exact de nition whether an entity is a provider or user is dependent on the context of the interaction and the service being. Some service providers will do services at all three service levels, just one particular level of service and have their own internal IaaS infrastructure.

A possible could be that CSP providers are either: a) Infrastructure Service Providers those that IaaS and own and run the data centers that physically house the servers and software; or b) Service Providers those that PaaS or SaaS services. And that Cloud Service Users are either: A) Platform Users are users who buy into a service provider's platform e.g. face book; and B) Consumers are service users who use either SaaS or IaaS services.

Dening the Cloud:

The term `cloud' has been used traditionally as a metaphor for networks and helps abstract over their inherent complexity. This term, however, has evolved to encompass the transparency between the technological infrastructure of the CSP and the consumer's point of view. A cloud can be one of the following types:

Public Constituting publicly accessible services that are accessed over the Internet and are often described using the term \The Cloud".

Private These are private services deployed on private networks. Such clouds may also be managed by third parties.

Hybrid A combination of services both privately and publicly. For example core-services may be on a private cloud; other services originate from public clouds.

Benefits of Cloud Computing:

Many of the benefits to be had when using Cloud Computing are the lower costs associated. At the infrastructure level, virtual images can be scaled and contracted with complete disregard for any associated hardware costs such as equipment procurement, storage, maintenance and use. This is all taken care of by the service provider and will be factored into the payment for the service: capital expenditure has been converted into operational expenditure. Resources within the cloud can be treated as a commodity, an `unlimited' medium. At both the platform and software level similar benefits are seen. Aspects such as software installation, deployment and maintenance are virtually non-existent. This is taken care of by the provider within their own infrastructure. The service user only pays technical support.

Service providers at the SaaS level, often tout features that allow users to collaborate and interact with each other, in real-time, within the scope of the service being needed. For example, Google Docs allows users to edit documents simultaneously and for users to see each others edits in real time. Moreover, the provision of platform and software `as a service' allows cloud service users the ability to aggregate services together either for their own use or to promote as another service i.e. Mashups. The aggregation could imply the combination of functionality from several services, or the change/combination of output from the services involved.

Remark. Service aggregation is a good example outlining how a service user can become a service provider.

Cloud Security Issues:

Security issues come under many guises both technical and socio-technical in origin. To cover all the security issues possible within the cloud, and in-depth, would be herculean|a task not suited even for Heracles himself. The Cloud Security Alliance identify seven threats to cloud computing that can be interpreted as a classification of security issues found within the cloud. They are:

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities

5. Data Loss/Leakage
6. Account, Service
7. Unknown Risk Pro

3. CONCLUSION

Similarly, describing PBE's use as part of a crypto-system was also a necessary evil, it established not only how PBE schemes could be deployed (see Section 9.8) but also points of contention within such deployment. Of which the most notable issues were those surrounding key manage-ment such as constructing, issuing and revocation. Furthermore, the use of PBE identi ed three di erent modes of operation that describe the three di erent ways in which PBE schemes can be leveraged within an crpyto-system|see Section 9.8. When combined with the cloud setting, two di erent sets of scenarios emerged based upon whether the service user's or CSP's data was to be protected.

PBE schemes can be used to protect service user's data in three di erent scenarios: Scenario I saw the inclusion of PBE within a service; Scenario II saw the provision of PBE as-a-Service; and Scenario V saw PBE being deployed by the user themselves. In each of these three scenarios PBE can be used by service users to specify precisely with whom they wish to share their data, for what purpose, and for how long. Although Scenario V may be a privacy zealot's ideal choice| they are in full control|its practical feasibility has yet to be determined; the ability for service users' to act competently as a Key Authority is still unclear. The remaining two scenarios, on the other hand, do appear to be more promising. However, these scenarios in themselves do present a dilemma between usability and the guarantees made over end-to-end security|see Section 12.3.

When looking to protect CSP's data, PBE can facilitate keyword search with complex queries over encrypted data: Scenario III by the CSP; and in Scenario IV by a service user. This use of PBE is rather interesting in that the focus of these scenarios is on the CSP and not service user, and is most certainly worthy of further investigation.

The use of PBE within the cloud appears to be concentrated at both the PaaS and SaaS service layers. Though some may be surprised at PBE's lack of use at the IaaS layer, this was not totally unexpected. The primary interaction between a service user and CSP at this level is over managing virtual machines: Not much else happens.

Authors' contributions:

The other of the paper do all the work, the environment for research work are done by my best of my knowledge and supporting my family members.

ACKNOWLEDGEMENTS

This paper heartily dedicated to beloved Honble Secretary and Correspondent Sri. K.Ram Mohan Garu, & Smt.K.Bhavani Devi Garu Amrita Sai Institute of science and technology. Also to all the respected Amrita Sai Management members. Our special thanks to the Innogeecks technologies, Vijayawada for their technical support in all the aspects.

REFERENCES

[1] A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli, International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November- 2017, pg. 7-11

[2] Cloud Security Risk Factors and Security Issues in current trends research paper by Dr.K.Sai Manoj accepted and Presented in Scopus Based 2nd International Conference on Materials, Applied physics and Engineering (ICMAE 2018) at Indore. Proceedings of the 2018 First international conference on Materials, Applied physics and Engineering. After Clear scientific check this Paper was already Promoted to Science Publication Corporation.

[3] Literature survey on the destruction of attaches with MH HOP to HOP to HOP-AODV Routing Protocol in Vehicular Ad-hoc Network, Dr.K.Sai Manoj, Mrudula Kudaravalli , © December 2017 | IJIRT | Volume 4 Issue 7 | ISSN: 2349-6002

[4] Mmmmmm I. Hedenfalk, D. Duggan, Y. Chen, M. Radmacher, M. Bittner, R. Simon, P. Meltzer, B. Gusterson, M. Esteller, O. P. Kallioniemi, B. Wilfond, A. Borg, and J. Trent, “Gene Expression profiles in hereditary breast cancer,” N Engl J Med, vol. 344, no. 8, February 2001, pp. :539–548.

[5] M. M. Hossain, M. R. Hassan, and J. Bailey, "ROC-tree: A Novel Decision Tree Induction Algorithm Based on Receiver Operating Characteristics to Classify Gene Expression Data," Proc. SIAM International Conference on Data Mining, Atlanta, Georgia, USA, April 2008, pp. 455–465.

[6] S. Pandey, W. Voorsluys, M. Rahman, R. Buyya, J. Dobson, and K. Chiu, "A Grid Workflow Environment for Brain Imaging Analysis on Distributed Systems," Concurrency and Computation: Practice and Experience, Jul. 2009, doi:10.1002/cpe.1461.

[7] J. Yu and R. Buyya, "Gridbus workflow enactment engine," in Grid Computing: Infrastructure, Service, and Applications, L. Wang, W. Jie, and J. Chen Eds, CRC Press, Boca Raton, FL, USA, April 2009, pp. 119–146.

[8] F. Cappello and H. Bal, "Toward an international computer science Grid," Proc. 7th IEEE International Symposium on Cluster Computing and the Grid (CCGRID'07), pp 3–12, Rio, Brazil, 2007. IEEE.

[9] X. Chu, K. Nadiminti, C. Jin, S. Venugopal, R. Buyya, "Aneka: Next-Generation Enterprise Grid Platform for e-Science and eBusiness Applications," Proc. 3rd IEEE International Conference on e-Science and Grid Computing, Bangalore, India, December, 2007.