International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 8; Issue 10 (D); October 2019; Page No.20283-20284
DOI: http://dx.doi.org/10.24327/ijcar.2019.20284.3957

Research Article

INVESTIGATION ON THE ON THE CLOUD COMPUTING SECURITY USING PET AND REMOTE ATTESTATION IN CLOUD ARCHITECTURES

Sai Manoj K and Mrudula K

CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
Director, Innogeecks Technologies, Vijayawada, AP, India

ARTICLE INFO

Article History:
Received 06th July, 2019
Received in revised form 14th August, 2019
Accepted 23rd September, 2019
Published online 28th October, 2019

Key words:

Trust, Privacy, PET, remote attestation

ABSTRACT

Cloud computing offers opportunities for organizations to reduce IT costs by using the computation and storage of a remote provider. Despite the benefits offered by cloud computing paradigm, organizations are still wary of delegating their computation and storage to a cloud service provider due to trust concerns. The trust issues with the cloud can be addressed by a combination of regulatory frameworks and supporting technologies. Privacy Enhancing Technologies (PET) and remote attestation provide the technologies for addressing the trust concerns.

INTRODUCTION

Privacy Enhancing Technologies

Privacy Enhancing Technologies (PET) enable clients to transact with providers securely even if the clients do not trust the providers. PET denotes the set of tools and mechanisms that allow users to protect their privacy online against adversaries.

Blarkom et al. [1] defines PET as a system of information and communication technology measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. Privacy preserving protocols [2], a class of PET, enable users to perform computation over cryptographically protected data.

Homomorphic encryption and searchable encryption schemes are notable privacy preserving protocols. Homomorphic encryption is an asymmetric encryption technique, where algebraic operations are performed directly on the cipher text which represents the encryption of plain text. This was first introduced by Goldwasser et al. [3], where the authors performed modular addition of two bits using multiplication of ciphertexts. Craig Gentry [4] designed an homomorphic encryption scheme that allows both addition and multiplication on plain text through their cipher texts.

Searchable encryption allows users to search for particular keywords on encrypted data. Public Key Encryption with Keyword Search (PEKS) [5] is one of the seminal works in the area of making encrypted data searchable.

The authors of PEKS propose to encrypt the message using the Public-Private key infrastructure. Along with this cipher text a Public-Key Encryption with Keyword Search (PEKS) of each keyword (the words that make up the message) is appended to the final message.

Although homomorphic encryption and searchable encryption are viable proven ways of preserving privacy of data in the cloud without compromising on the functionality, cryptography increases the computational and storage overhead on the server [6]. Computation over encrypted data even though theoretically possible is not yet practically feasible [7].

Need for trust: Remote Attestation

As the solutions proposed by PET are mostly in the theoretical realm, clients are forced to trust the cloud provider with the data and hope that the provider will not breach that trust. Trust is defined as "a particular level of subjective assessment of whether a trustee (cloud provider).

The client establishes trust on emotional and cognitive (evidence based) grounds. To enforce the strict security requirements on the server, the trust relationship between the client and server should be formed more based on cognitive, evidence based grounds. The evidence should be unforgeable and should assure that the server will not act against the client's interest. Remote attestation provides such evidence by allowing clients to accurately verify if the remote server's state

Corresponding author:* **Sai Manoj K
CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India Director, Innogeecks Technologies, Vijayawada, AP, India

is compromised. A server can be trusted if the client can accurately verify all the software binaries that the server has executed [8].

The veracity of software is established through its identity, which is expressed by means of the hash1 of the software binary. For verification of the server's state, the measured hash of all the software binaries (measurement list) is sent to the client. The client performs the comparison against known software hash values, whose security has been verified. This will enable clients to verify that the server is free of malware or any unauthorized software. Remote attestation [8] refers to the process of authenticating and verifying the state of the remote platform and its operating system outside of the platform.

The remote platform can either be hosted on a physical server or a Virtual Machine (VM) in the physical server or both. In the context of cloud computing, remote attestation of the cloud server is performed either by cloud clients or a trusted third party on behalf of the cloud clients. Based on remote attestation, trusted computing technology was developed by the Trusted Computing Group (TCG). It provides specifications for securely reporting and verifying a remote platform (i.e. server hardware and software).

Important concept in this research paper

Existing research work in remote attestation of the server includes: securely collecting and storing information about the software state (hash values) of the server [8], methods for using the information on the state locally in the server [9], for conveying the state information to an external client for remote attestation [10] and for managing the list of software that is allowed to be executed in the server.

CONCLUSION

This research paper focused on architectures [11] that enable secure transactions between cloud clients and untrusted provider. We studied the feasibility of these architecture in a real world system using a Privacy Enhancing Technology (PET). We further investigated the limitations of PET and how Trusted Computing architectures (remote attestation) can be used to address these limitations. We identified issues with state of the art in remote attestation architectures and proposed improvements to it. Finally we introduced the concept of subjective and dynamic trust in the cloud computing context

One of the applications of this research work in the Improvements of the traditional webmail

Using a webmail system requires disturbing levels of trust from the cloud service client on the cloud service provider.

Declarations

Availability of data and material:

Not applicable.

Competing interests

Not applicable.

Funding

No funding was applicable.

Authors' contributions

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

Acknowledgements

First of all, I am thankful to Honourable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

References

1. G W Van Blarkom, J J Borking, and JGE Olk. Handbook of privacy and privacy enhancing technologies. Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 2003.
2. Keith Frikken and Mikhail Atallah. Privacy-Preserving Cryptographic Protocols. In Digital Privacy, pages 47–69. Auerbach Publications, November 2009.
3. Shafi Goldwasser and Silvio Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In Proceedings of the fourteenth annual ACM symposium on Theory of computing, pages 365-377, New York, NY, USA, 1982. ACM.
4. Craig Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
5. Qin Liu, Guojun Wang, and Jie Wu. An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing. Computational Science and Engineering, 2009. CSE '09. International Conference on, 2:715-720, August 2009.
6. Karthick Ramachandran, Hanan Lutfiyya, and Mark Perry. Chaavi: A Privacy Preserving architecture for Webmail Systems. In Cloud Computing 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization, page 133 to 140
7. Daniele Micciancio. A first glimpse of cryptography's Holy Grail. Communications of the ACM, 53(3):96–96, March 2010
8. Morrie Gasser, Andy Goldstein, Charlie Kaufman, and Butler Lampson. The Digital distributed system security architecture. In Proceedings of the 1989 National Computer Security Conference, pages 305-319, 1989
9. S Bajikar. Trusted platform module (tpm) based security on notebook pcs-white paper. White Paper, Mobile Platforms Group-Intel Corporation, 20, 2002.
10. B Bertholon, S Varrette, and P Bouvry. Certicloud: A novel tpm-based approach to ensure cloud iaas security. Cloud Computing (CLOUD), 2011
11. Conceptual oriented study on the cloud computing architecture for the full security Dr.K.Sai Manoj *International journal of Engineering and Technology*, Volume 7, Issue 4, 2018, Scinence Publishing Corporation
12. Investigations on the Cloud Data Storage Security Based Using Diffie Hellman Algorithm Dr.K.Sai Manoj appreciated article in *International Journal of Computer Engineering and Applications*, Volume XIII, Issue VI, JUNE. 19, www.ijcea.com ISSN 23213469

****