A Secure Client-Side Framework for Protecting the Privacy of Health Data Stored on the Cloud

ABSTRACT

- In the past decade, Cloud-Computing emerged as a new computing concept with a distributed nature using virtual network and systems. Many businesses rely on this technology to keep their systems running but concerns are rising about security breaches in cloud computing. Cloud providers (CPs) are taking significant measures to maintain the security and privacy of the data stored on their premises, in order to preserve the customers' trust. Nevertheless, in certain applications, such as medical health records for example, the medical facility is responsible for preserving the privacy of the patients' data.
- Although the facility can offload the overhead of storing large amounts of data by using cloud storage, relying solely on the security measures taken by the CP might not be sufficient. Any security breach at the CP's premises does not protect the medical facility from being held accountable. This work aims to solve this problem by presenting a secure approach for storing data on the cloud while keeping the customer in control of the security and privacy of their data.

EXISTING SYSTEM

- Cloud computing is gaining significant interest. The three cloud delivery models that are now well-known in the industry are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
- Particularly, IaaS can be used for storage purposes, i.e. the cloud provides storage infrastructure, and a client can offload the overhead of storing large amounts of data to the cloud provider (CP), in exchange of a fee, that is usually dependent on the storage space allocated to the client at the CP's premises.

PROPOSED SYSTEM

- In the past decade, Cloud-Computing emerged as a new computing concept with a distributed nature using virtual network and systems. Many businesses rely on this technology to keep their systems running but concerns are rising about security breaches in cloud computing. Cloud providers (CPs) are taking significant measures to maintain the security and privacy of the data stored on their premises, in order to preserve the customers' trust.
- Nevertheless, in certain applications, such as medical health records for example, the medical facility is responsible for preserving the privacy of the patients' data. Although the facility can offload the overhead of storing large amounts of data by using cloud storage, relying solely on the security measures taken by the CP might not be sufficient.

CONTINUE

- Any security breach at the CP’s premises does not protect the medical facility from being held accountable. This work aims to solve this problem by presenting a secure approach for storing data on the cloud while keeping the customer in control of the security and privacy of their data.

HARDWARE REQUIREMENTS

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

SOFTWARE REQUIREMENTS

Operating System	:	Windows 8
Front End	:	Java /DOTNET
Database	:	Mysql/HEIDISQL

CONCLUSION

- In this paper, we presented a simple and secure framework for protecting sensitive data stored on the cloud. It is based on splitting a given file into multiple parts, and storing each part, after encryption and permutation of the order of the parts, with a different cloud provider. The information to decrypt and reorder the file parts is stored in separate locations at the client premises.
- No extra cost is incurred since the total storage size is still the same, compared to the case of storing the file with a single cloud provider. The proposed approach allows the client to benefit from any security measures implemented by the cloud provider while still taking charge of the security and privacy of their data.

REFERENCE

[1] G. Ramachandra, M. Iftikhar, F. A. Khan, “A Comprehensive Survey on Security in Cloud Computing”, Procedia Computer Science, vol. 110, p.p. 465–472, 2017.

[2] M. A. Khan, “A Survey of Security Issues for Cloud Computing”, Journal of Network and Computer Applications, vol. 71, p.p. 11-29, Aug. 2016.

[3] Y. Liu, J. E. Fieldsend, and G. Min, “A Framework of Fog Computing: Architecture, Challenges and Optimization”, IEEE Access, DOI: 10.1109/ACCESS.2017.2766923, published online Oct. 2017.

CONTINUE

[4] G. Kurikala, K. G. Gupta, and A. Swapna, “Fog Computing : Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 4, p.p. 176-181, Aug. 2017.

[5] J. Dykstra, A. T. Sherman, “Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and EvaluatingTools, Trust, and Techniques”, Digital Investigation, vol. 9, p.p. 90-98, 2012.