Achieving Scalable Access Control Over Encrypted Data for Edge Computing Networks

ABSTRACT

- The concept of Internet of things has raised in the cloud computing paradigm as it adds latency when migrating all pieces of data from the network edge to the data center for them to be approached.
- Edge computing has been introduced to extend the cloud computing architecture to the edge of the network, which analyses most of the IoT data near the devices that produce and act on that data.
- Though edge computing solves the latency problem of data processing, it also brings issues to the data security and privacy preservation.

CONTINUE

- One technique which is potential to provide scalable access control to support data security and privacy in edge computing is attribute-based encryption.
- We, in this paper, propose a notion named proxy-aided ciphertext-policy attribute-based encryption, which outsources the majority of the decryption computations to edge devices.
- Compared to the existing ABE with outsourced decryption schemes, PA-CPABE has an advantage in that the key distribution does not require any secure channels.
- We present a generic construction of PA-CPABE, and then foramlly prove its security.
- In addition, we implement an instantiation of the proposed PA-CPABE framework to evaluate its performance.

EXISTING SYSTEM

- The idea of Internet of Things has become increasingly popular, which enables various objects including physical devices, vehicles, buildings and other items embedded with computing and communication capabilities to exchange data.
- However, because of limitations in the computation capability, battery, storage and bandwidth, smart devices sometimes may decrease the quality of services and weaken the user experience.
- Cloud computing supplies resources to end users in terms of software, infrastructure and platform, and delivers services to applications at a comparatively small cost, which has been considered as a promising solution to mitigate the limitation of devices with constrained resources.

PROPOSED SYSTEM

- We put forth a primitive called proxy-aided ciphertextpolicy attribute -based encryption to outsource the decryption workloads of ABE ciphertexts to an untrusted proxy but without requiring any secure channels for the key distribution, which can be seamlessly integrated into the edge computing network to accomplish the scalable access control.
- We give a generic construction for PA-CPABE via which a PA-CPABE scheme could be converted from a CPABE scheme, and then apply a concrete CP-ABE scheme which satisfies certain properties into the generic construction of PA-CPABE to obtain a concrete PA-CPABE scheme.

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

- Though edge computing facilitates cloud computing in addressing the latency problem of data processing, it also brings more security and privacy issues to the existing cloud computing network.
- Due to the fact that attribute-based encryption supports fine-grained access control for data items in encrypted forms, ABE has been widely believed to be an ideal solution to protect data security and privacy for scenarios of cloud computing.
- To achieve fine-grained access control for the edge computing environment.

REFERENCE

[1] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things,", *August 17, 2012*. ACM, 2012, pp. 13–16.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2005, 24th Annual, May 22-26, 2005, Proceedings*, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[4] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in *20th USENIX Security Symposium, San Francisco, CA, USA, August 8-12, 2011, Proceedings*. USENIX Association, 2011.

CONTINUE

[4] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[5] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2201–2210, 2014.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA*. IEEE Computer Society, 2007, pp. 321–334