Enhancing Security Levels at ISP Server Using Multiple Security Techniques with Proposed Crypo Application

Suraj U. Rasal[1,*], Varsha S. Rasal[2], Shraddha T. Shelar[3]

[1] Department of Computer Engineering, Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India

[2] Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India

[3]Department of Information technology, D Y Patil College of Engineering Akurdi, Pune, India

Received 18 April 2017; received in revised form 27 July 2017; accepted 08 January 2018

Abstract

The internet is widely used in computing. Security is an important aspect when the quality of service is evaluated and current security possesses high level encryption techniques. However, due to high data saturation and complexity, it is not enough for, only to rely on the common security techniques. In this paper, proposed application named Crypo is installed at both ends, including user and Internet Service Provider (ISP). User can connect to the public internet through providing credentials. Both ends work with same cryptographic techniques and logics. Crypo includes the existing security techniques with proposed logics. Attribute Based Encryption (ABE) is applied to user credentials. Cipher policy applies to data exchange between user and Internet Service Provider (ISP) to form a combined cipher data. Proposed logic is further applied to the binary formatted cipher data. According to proposed logic, the final encrypted binary formatted data are further applied with Advanced Encryption Standard (AES) to deliver it to the ISP. Decryption is done by the same logic applied to the sender side or vice versa. When data is retrieved by ISP from its end user, it is decrypted by the ISP after which is delivered to the public network in normal format. Four level security keeps the data and user credentials confidential. Intruders or hackers can't reach to the end user without decrypting the secured data at ISP. While delivering encrypted data, applied logic name is also delivered so that end users can decrypt data using the same logic. By using proposed application Crypo, a secure connection is established between the end user and the ISP. An outsider cannot cause threat to the ISP's users. Proposed multilevel cryptographic approach enhances the security.

Keywords: attribute based encryption (ABE), advanced encryption standard (AES), american standard code for information interchange (ASCII), cipher policy, crypo - proposed application name, internet service provider (ISP).

References

[1] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded cipher text policy attribute based encryption," Automata, Languages and Programming, pp. 579-591, 2008.

[2] A. A. Bruen and M. A. Forcinito, Cryptography, information theory, and error-correction: a handbook for the 21st Century, 1st ed. New Jersey: John Wiley & Sons, 2011.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of The 13th ACM Conference on Computer and Communications Security, Oct. 2006, pp. 89-98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption in security and privacy," IEEE Symposium, May 2007, pp. 321-334.

* Corresponding author. E-mail address surasal@bvucoep.edu.in

Tel.: +918793000079

[5] M. S. Rahman, A. Basu, and S. Kiyomoto, "Decentralized ciphertext-policy attribute-based encryption from learning with errors over rings," Trustcom/BigDataSE/I SPA IEEE, Aug. 2016, pp. 1759-1764.
[6] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," Proceedings of The 6th ACM Symposium on Information, Computer and Communications Security, March 2011, pp. 386-390.
[7] Y. S. Rao and R. Dutta, "Decentralized ciphertext-policy attribute-based encryption scheme with fast decryption," IFIP International Conference on Communications and Multimedia Security, Springer Berlin Heidelberg, Sept. 2013, pp. 66-81.
[8] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of applied cryptography, 1st ed. New York: CRC Press, 1996.
[9] C. P. Pfleeger and S. L. Pfleeger, Security in computing, 1st ed. New Jersey: Prentice Hall Professional, 2003.
[10] C. P. Pfleeger, Security in computing, 5th ed. New Delhi: Pearson Education, 2006.
[11] B. Waters, "iphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," International Workshop on Public Key Cryptography, Springer Berlin Heidelberg, March 2011, pp. 53-70.
[12] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, " Multi-authority ciphertext-policy attribute-based encryption with accountability, " Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 386-390.
[13] A. Lewko and B. Waters, "Decentralizing attribute-based encryption, " Annual International Conference on The Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, 2011, pp. 568-588.
[14] V. T. Mulik, K. Saritha, and S. U. Rasal, "Privacy preserving through mediator in decentralized ciphertext policy attribute based encryption, " IJRET: International Journal of Research in Engineering and Technology, vol. 5, pp. 535-540, June 2016.
[15] S. U. Rasal, S. T. Shelar, and V. S. Rasal, "Securing internet banking using multiple attributes scheme and OTP," The IIOAB Journal, vol. 7, pp. 26-30, Oct. 2016.
[16] S. U. Rasal, R. Agarwal, V. S Rasal, and S. T. Shelar, "IOT appliance access structure using ABE based OTP technique," The IIOAB Journal, vol. 7, pp. 180-186, Sept. 2016.
[17] S. Prettyman, PHP arrays, 1st ed. New York: Apress, 2017.
[18] S. Holzner, PHP: the complete reference. New York: McGraw-Hill Education, 2007.