Commentary
Volume 10:S2, 2021

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Advanced Homomorphic Encryption Schemes

Anitha Kumari Kumarasamy* and M. Ananyaa

Department of Information Technology, PSG College of Technology, Coimbatore, India

Abstract

In recent days most of the industrial firms have been searching for ways to keep their data as secured and protected as possible. They have indulged in research works to find a mechanism that can be simple, convenient and guarantees high level security to large amount of data that is being manipulated every now and then. Among such mechanisms, one mechanism that satisfies all these requirements is Homomorphic Encryption (HE). Homomorphic Encryption schemes facilitate computation on the encrypted data, yielding different output every time is considered as an edge over traditional encryption algorithms. HE schemes ensures integrity and security of data, against threats and violations. Researchers expanded the dimensionality of the homomorphic encryption to another level through Carmichael's Theorem-Based Homomorphic Encryption (CTHE) scheme and Modified Enhanced Homomorphic Encryption (MEHE) scheme. CTHE and MEHE schemes are reviewed in this article to show its robustness against invasive attacks.

Keywords

Homomorphic encryption ● CTHE ● MEHE

Description

Data security and privacy acts as the fundamental components for any industry/organization in the current situation where dynamic data processing, monitoring and rapid result analysis is indispensable. Homomorphic encryption schemes are considered to be the most efficient, ideal and adaptative mechanism that satisfies all these core requirements where large amount of operations are performed upon encrypted data [1, 2]. Advanced research schemes like Carmichael's Theorem-Based Homomorphic Encryption (CTHE) and Modified Enhanced Homomorphic Encryption (MEHE) are proven to be unconditionally secure that makes it very difficult for the intruders to decrypt the encrypted data [3]. In addition, these schemes are preferred and suitable for wide range of real-time applications to be deployed in resource constrained environments like edge system due to its less computational complexity and storage overhead [4, 5].

CTHE and MEHE schemes

CTHE and MEHE schemes serves the purpose best and proves efficient and secure on the hardness of integer factorization, discrete logarithm, and quadratic residuosity problem that is considered as NP-hard [3]. Modulo switching technique is adopted and proved theoretically to reduce noise in the described schemes. Also, to ensure high randomness in the keys and to distribute the keys effectively between edge system and storage server, quantum random number generator and quantum key distributor serves the purpose. Thus, freshness of the key and forward secrecy is ensured and distribution of key occurs between edge system and storage server. The above-mentioned schemes are tested for a healthcare application to ensure integrity of computation (tamper resistant), data security and record maintenance. Comparative analysis of CTHE and MEHE schemes are performed with the existing schemes such as Dijk-Gentry-Halevi-Vaikutanathan (DGHV) scheme, Paillier scheme and ElGamal scheme and proved its effectiveness in terms of computation, key size, noise reduction, key freshness and suitability for real-world applications [6-8]. Highest potential of the schemes are explored against attack vector space [9].

***Address for Correspondence:** Anitha Kumari Kumarasamy, Department of Information Technology, PSG College of Technology, Coimbatore, India; E-mail: anitha.psgsoft@gmail.com*

Received: September 03, 2021; **Accepted:** September 17, 2021; **Published:** September 24, 2021

Conclusion

Technological advancements and Innovations are progressing exponentially in the present era, emphasizing the importance of data security and integrity. CTHE and MEHE schemes well satisfy the core requirements of homomorphic encryption that facilitate computation on the encrypted data with minimal noise. Additional features such as querying and searching upon encrypted data can be incorporated with CTHE and MEHE schemes to showcase the maximum potential.

References

1. Potzelberger, Gerhard. "KV Web Security: Applications of Homomorphic Encryption." *Johannes Kepler University* 1 (2013): 1-10.
2. Fontaine, Caroline and Galand Fabien. "A Survey of Homomorphic Encryption for Non-Specialists." *EURASIP J Inf Secur* 1 (2007): 1-10.
3. Kumari, K Anitha, Avinash Sharma, Chinmay Chakraborty and M. Ananyaa. "Preserving Health Care Data Security and Privacy Using Carmichael's Theorem-Based Homomorphic Encryption and Modified Enhanced Homomorphic Encryption Schemes in Edge Computing Systems." *Big Data* 1 (2021): 1-12.
4. Mubarakali, Azath, Anand Deva Durai, Mohmmed Alshehri and Osama AlFarraj, et al. "Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications." *Big Data* 1 (2020): 1-16.
5. Zhang, Jiale, Bing Chen, Yanchao Zhao and Xiang Cheng, et al. "Data Security and Privacy: Preserving in Edge Computing Paradigm: Survey and Open Issues." *Mob Edge Comput* 6 (2018): 18209-18237.
6. Hariss, Khalil, Maroun Chamoun and Abed Ellatif Samhat. "On DGHV and BGV Fully Homomorphic Encryption Schemes." Cyber Secur Netw Conf 1 (2017): 1-9.
7. Paillier, Pascal. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes." *Lect Notes Comput Sci* 5 (1999): 223-238.
8. ElGamal, Taher. "A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms." *IEEE Trans Inf Theory* 31 (1986): 469-472.
9. Emekci, Fatih, Divyakant Agrawal, Amr El Abbadi and Aziz Gulbeden. "Privacy Preserving Query Processing Using Third Parties." *IEEE Comput Society* 1 (2006): 215-220.

How to cite this article: Kumarasamy, Anitha Kumari and M. Ananyaa."Advanced Homomorphic Encryption Schemes." *J Sens Netw Data Commun* 10 (2021): 003.