Short Communication
Volume 10:S3, 2021

International Journal of Sensor Networks and Data Communications

ISSN: 2090-4886 **Open Access**

Applicability of Lattice Based Homomorphic Encryption

Anitha Kumari Kumarasamy* **and Prakaashini S**

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

Abstract

Protecting and processing data securely is considered as the highest challenge of most of the organizations. Manifold researches are ongoing to devise such a mechanism that can withstand against all possible invasive attacks including quantum attacks. Lattice based homomorphic encryption received recent attention nowadays among researchers' community to process and perform operation upon encrypted data by assuring high level of security. In this article lattice based homomorphic encryption and its applications are elaborated in detail.

Keywords

Robustness ● Errors ● Hackers

Description

Eventually in the recent times when the amount of data grew the importance and the necessity of a more secure system also demands high. Manifold secure homomorphic encryption schemes are designed efficiently and prove its applicability to real-time applications [1-3]. This article outlines lattice based homomorphic encryption and its various applications with evidence to prove its robustness against attacks and adaptive nature. Recent applications started using lattice based homomorphic encryption techniques as it provides a very accurate point-based encryption that makes it very difficult for the intruders to decrypt the encrypted data. The lattice based homomorphic encryption further divides into many more secured schemes such as Nth Degree Truncated Polynomial (NTRU), Learning with Errors (LWE), Ring Learning with Errors (RLWE) and many more. These various distributions pave the way to the success of lattice based homomorphic encryption [4, 5]. They use large prime numbers as inputs and provide a very highly protected encrypted data. This functionality is the main advantage of why companies and technology firms are adopting the lattice based homomorphic encryption. It also very transparent compared to the other encryption schemes. The work done behind the encryption is abstracted to the third parties; however, at the same time the sender and receiver possess the keys for encryption and decryption. Based on the fact, that various sectors are growing vastly nowadays, protecting and processing the sensitive data with utmost care is essential. Apart from the IT sectors, other sectors such as healthcare, government, education, etc., also started adapting lattice based homomorphic encryption for secure processing.

Evolution of lattice homomorphic encryption

In 1976, the first ever public key crypto system was invented by Diffie-Hellman. It was said to be one of the finest cryptosystems until 1978. Later RSA receives attention claims to be very secure asymmetric cryptography algorithm where the public key is shared and the private key is kept private. In 1985, ElGamal algorithm was designed by Taher ElGamal that is considered as partial homomorphic encryption technique. The algorithm seems to be highly secure and hard to break based on the hardness of discrete logarithms. It's a quite harder for the intruders to penetrate through and get access to the data. In the early 20s quantum computers started to boom that tends to break all classical cryptosystems. Quantum attacks are increasing to greater heights and it demands for a revolution in crypto world by designing a secure system that should be resistant to even all possible quantum attacks. In different dimension, researchers' community started exploring to provide a fool proof mechanism to protect the sensitive data.

Lattice based homomorphic encryption and its derivatives are considered as the wise choice to withstand all possible harmful attacks including quantum attacks. Lattice based homomorphic encryption technique is based on lattice points that makes every combination unique and different. Each time the scheme yields different key with unique pattern or sequence which is considered as the highest merit to prevent intruders from breaching the data. It marks its footprints in various domains such as healthcare, government, education, etc.

Applications of lattice homomorphic encryption

Nowadays, lattice based homomorphic encryption is widely adopted and applied in many applications and software's especially where highest level of protection is required [6, 7]. A few applications are Digital Signatures, Cloud Applications, and Real-time trackers.

Digital signatures are very important because it provides authorization and verifies the original owner of the asset. Initially when digital signature was found they were easily open to impersonation and prone to hacking. The later digital signatures started using lattice based homomorphic encryption in which it was very hard for the intruders or hackers to impersonate the signature or indulge in any fraud regarding the digital signature. This is one application which proves that lattice based homomorphic encryption provides a highest level of security. Albeit, RSA, ElGamal and ECC cryptosystems used to offer safe digital signature, comparatively, lattice based homomorphic encryption provides highest amount of security as it works based on lattices. Lattices are geometrical arrangement of point or numbers and are very unique when compared to other cryptosystems. Thus, it's very hard for the hackers to breakdown the security system.

Cloud applications also started to adapt the lattice based homomorphic encryption as the primary security mechanism to use any type of software, platform or infrastructure service in a pay-as-you-go model with highest level of security rest assuring. Applications that have adopted lattice based homomorphic encryption in the cloud prove that it provides a higher security mechanism compared to all the other security mechanisms.

Real time trackers refer to devices such as smart watches, fitness trackers, baby monitors and many more real time devices. People now-a-days started using these devices in order to capture different measures

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

Received date: September 30, 2021; **Accepted date:** October 14, 2021; **Published date:** October 21, 2021

such as temperature, blood pressure, humidity, number of steps taken, oxygen level and many more important sensitive private data. These data are very personal and important to every individual using it. Since it is very important to protect these data as the applications that accessing these data are constantly changing their security mechanisms and methods in order to protect these personal data. Few applications in this genre have already started using lattice based homographic encryption to store and process securely.

Conclusion

Lattice based homomorphic encryption are considered to be the wise choice for manifold applications that necessitates high level of security. Recent researches have shown that many IT firms working on large amount of data have started adapting to lattice based homomorphic encryption. This technique can be broadly used/applied in any domain/sector to protect massive data from breaching. Irrespective of the volume of data and the technology, homomorphic encryption based on lattices protects the data from hazardous attacks. Few applications such as digital signature, cloud applications and real-time tracker are analysed with use cases in this article to prove the merits of lattice based homomorphic encryption. Apart from these applications, its suitable to apply in various fields such as healthcare, military, government, e-commerce, finance, banking, education, etc. As lattice based homomorphic encryption is found to be very secure even various governments also started using this technique to safeguard highly confidential data.

References

1. 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.
2. 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.
3. Kumari, K Anitha, M Indusha and D Dharani. "Enhanced Human Activity Recognition based on Activity Tracker Data Using Secure Homomorphic Encryption Techniques." *Int Conf Emerging Technol* 1 (2021): 1-7.
4. Dai, Wei, Yarkin Doroz and Berk Sunar. "Accelerating NTRU Based Homomorphic Encryption Using GPUs." *IEEE High Perform Extreme Comput Conf* 1 (2014): 1-6.
5. Kadykov, Victor, Alla Levina and Alexander Voznesensky. "Homomorphic Encryption within Lattice-Based Encryption System." *Procedia Comput Sci* 186 (2021): 309-315.
6. Abdallah, Asmaa and Xuemin Sherman Shen. "A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid." *IEEE Trans Smart Grid* 9 (2016): 396-405.
7. Kumari, K Anitha and Santhiya, B. "Analysis on DGHV and NTRU Fully Homomorphic Encryption Schemes" Proc Int Conf Artif Intell Smart Grid Smart City Appl 1 (2020): 669-678.

How to cite this article: Kumarasamy, Anitha Kumari and Prakaashini S."Applicability of Lattice Based Homomorphic Encryption." *J Sens Netw Data Commun* S3 (2021): 008.