

Editorial

In this edition, we focus on a critical area of the digital era: data security. As the sophistication of the internet and the volume of data transmission continue to grow, ensuring the security of files, databases, accounts, and networks has become paramount. Databases, often housing sensitive and private information, are prime targets for cyber attacks. This issue underscores the need for advanced solutions to mitigate threats and reduce risks associated with data processing and storage. The featured research paper introduces a cutting-edge approach to data security using homomorphic encryption for device authentication, emphasizing the

The paper addresses the pressing need to enhance data security in an environment increasingly susceptible to cyber threats. With the continuous evolution of encryption technologies and trends, staying updated is essential for protecting confidential information and sensitive data. The study underscores the significance of adopting robust encryption methods to bolster system security and protect against unauthorized access [1].

The featured paper in this edition presents a groundbreaking approach to data security, addressing a critical need in the digital age. By proposing a homomorphic encryption-based device authentication method, the research offers a robust solution to safeguarding template data and enhancing overall system security. The use of the CKKS technique further demonstrates the potential of advanced encryption methods in protecting sensitive information. We are pleased to share these innovative findings with our readers and look forward to further advancements in data security research.

References:

- [1] S. Yadav, G. Howells, "Device Authentication using Homomorphic Encryption," *Journal of Engineering Research and Sciences*, vol. 2, no. 10, pp. 1–8, 2023, doi:10.55708/js0210001.

Editor-in-chief

Prof. Paul Andrew