I.J. Wireless and Microwave Technologies, **2024, 2, 55-64**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2024.02.04

Cryptographic Resilience and Efficiency: A Comparative Study of NTRU and ECC Cryptographic Mechanisms for Internet of Medical Things

Alina Pervaiz
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: miraleena94@gmail.com
ORCID ID: https://orcid.org/0009-0009-2812-0745

Adil Bashir*
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: adilbashir.445@gmail.com
ORCID ID: https://orcid.org/0000-0003-0927-908X
*Corresponding author

Maheen Fayaz
Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, India
E-mail: maheenmalik.0901@gmail.com
ORCID ID: https://orcid.org/0009-0009-0455-0396

Numrena Farooq
National Institute of Technology Srinagar, India
ORCID ID: https://orcid.org/0000-0002-0461-1795

Ajaz Hussain Mir
National Institute of Technology Srinagar, India
ORCID ID: https://orcid.org/0000-0001-9777-0850

Received: 09 January, 2024; Revised: 11 February, 2024; Accepted: 13 March, 2024; Published: 08 April, 2024

Abstract: In the dynamic realm of Smart Healthcare Systems (SHS), the integration of IoT devices has revolutionized conventional practices, ushering in an era of real-time data collection and seamless communication across the healthcare ecosystem. Amidst this technological shift, the paramount concern remains the security of sensitive healthcare data within intricate networks. Several cryptographic algorithms have been proposed for smart healthcare systems for the protection of critical and sensitive data in SHS, however, the majority of newly proposed algorithms have shortcomings in terms of resource utilization and the level of security that they provide. Our research delves into the existing highly secure cryptographic algorithms and provides a comparative analysis of two popular and secure cryptographic algorithms viz N-th Degree Truncated Polynomial Ring (NTRU) and Elliptic Curve Cryptography (ECC) and verifies their applicability in SHS. Recognizing ECC's compact key sizes and its vulnerability to quantum computing threats, our study finds NTRU as a resilient and quantum-resistant alternative, providing a robust defense mechanism in the evolving landscape of healthcare cybersecurity. Key findings underscore the efficacy of NTRU in safeguarding healthcare data, emphasizing its superior performance compared to ECC, especially in the face of emerging quantum computing challenges. The comparative analysis depicts that ECC excels in key generation speed, delivering efficient and swift key creation. However, it requires larger keys to withstand potential quantum computing vulnerabilities. On the other hand, the key generation time in NTRU is slightly more than ECC but being quantum-resistant, it provides high security.

Index Terms: ECC, NTRU-Encrypt, Fog Computing, Internet of Things, Smart Healthcare System, Quantum Resistance.