IJAMSR

International Conference on Latest Trends in Engineering, Management, Humanities, Science & Technology (ICLTEMHST -2022)
27th November, 2022, Guwahati, Assam, India.

CERTIFICATE NO : ICLTEMHST /2022/C1122996

IMPACT OF SELF-ENCRYPTING DATA IN DECENTRALIZED NETWORKS

KP SAURABH

Research Scholar, Ph. D in Computer Science & Engineering,
Dr. A.P.J. Abdul Kalam University, Indore, M.P.

ABSTRACT

The integration of self-encrypting data within decentralized networks marks a significant stride towards fortifying their security and resilience. Self-encrypting data empowers individual nodes within the network to autonomously encrypt their stored information, ensuring that data remains protected from unauthorized access or tampering. This decentralized approach to encryption not only enhances data confidentiality but also mitigates the risk of single points of failure, as each node independently manages its encryption keys. Consequently, self-encrypting data contributes to the overall integrity of the network by minimizing vulnerabilities and reducing the potential impact of security breaches. Furthermore, self-encrypting data fosters a culture of trust and accountability within decentralized networks, as users can have confidence in the security measures implemented at the individual node level. Ultimately, the impact of self-encrypting data in decentralized networks extends beyond mere data protection, influencing the network's overall reliability, efficiency, and ability to withstand adversarial threats in an increasingly interconnected digital landscape.