# ABSTRACT

RansomGuard is a user-friendly cybersecurity tool meticulously designed to evaluate an organisation's readiness against the rising threat of ransomware attacks. Focused on bolstering prevention, detection, usability, and reporting, RansomGuard aims to enhance overall resilience, ensuring robust defence mechanisms are in place to thwart potential cyber threats. The core strategy involves integration of an Intrusion Detection and Prevention System (IDPS), antivirus software, and a firewall, forming a robust defence against ransomware. The IDPS functions as a vigilant sentry, monitoring network activities to identify anomalies indicative of potential ransomware threats. Utilizing signature-based and anomaly based detection, it ensures a robust defence against both known and emerging ransomware variants. Complementing the IDPS, antivirus software adds a proactive layer of defence. Using signature-based detection and heuristic analysis, it identifies known patterns and behavioural anomalies associated with ransomware, strengthening the organization's cybersecurity infrastructure. The firewall acts as a strongest barrier, monitoring network traffic to filter and block potential ransomware attacks. The integration of advanced mechanisms will assess prevention strategies, detection capabilities, usability of security protocols, and reporting mechanisms.