Tracking of computer network system attacks is a proactive measure to protect against attacks on data, that are basically encrypted for confidential security reasons, while in transit on the computer information channel. Cyber security threat continues to increase in direct proportion to the rate at which internet based services are deployed. In this systematic review, 53 research papers from reputable publishers were downloaded out of which 41 papers that are closely related to tracking of malicious attackers on encrypted data online were review under the consideration of attacks on encrypted data, and tracking malicious attacks; with respect to proposed technique, problem addressed, comparison to existing methodology, parameters used, major findings and then limitations and future knowledge. The authors then deduce the classification of four varying types of attacks (Keyword Guessing Attack, Selective opening attacks, Leakage-Abuse Attacks, and Key Reinstallation Attacks) from the review, to narrow down research into the future countermeasures for these attacks. 11 research papers actual discuss countermeasures for these classification types, with Keyword Guessing Attack being the focus of 6 research work, Selective Opening Attacks have 3 papers trying to solve vulnerabilities permitting such attacks, 2 papers aimed research solutions at Leakage-Abuse Attacks, and Key Reinstallation Attacks, has mention but none of the papers reviewed proffer mitigation techniques. The remaining 30 papers concentrated discussions on general attacks on encrypted data. Inclining future research attention to the four kinds of attacks against encrypted data will improve attack detection contrary to the commonly post mortem approach.