M.After a thorough analysis of the extracted data, the findings VOLUME 8, 2020 76563 reveal essential results.3) Only journal articles and conference proceedings were included, whereas some other studies that may help 76562 VOLUME 8, 2020 M. Yahuza et al.: Systematic Review on Security and Privacy Requirements in Edge Computing with additional information, such as patents, maga- zines, and symposium, were excluded.Thirdly, the findings classified the identified techniques under their cor- responding technological methods employed with the aim of identifying the trend.B. FINE-GRAIN SECURITY FEATURES To attain fine-grain security features, a dynamic auto-update function needs to be incorporated into the privacy-preserving mechanisms, as well as an efficient data-sharing mechanism, due to the huge amount of data produced at the edge of the network by end-devices.C. PRIOR INVESTIGATION OF ATTACKS In most of the reviewed studies, attacks were not fully inves- tigated and dealt with sufficiently prior to the design process of the techniques, especially the authentication and privacy- preserving schemes.F. PROPER UTILIZATION OF INTRUSION DETECTION MECHANISMS Intrusion Detection Systems (IDS) are employed for detect- ing and mitigating of the various attacks in a network.Fourthly, the review work has identified limitation of each of the techniques which lead to research opportunities for future researchers to concentrate on. More- over, the attacks affecting the edge computing network have been thoroughly explored.It can be observed that most of the techniques under Confidentiality and Authenticity are not lightweight, that was the reason why they did not evaluate the techniques using the lightweight evaluation metrics (i.e. computation and communication costs).Hence, future research on security and privacy in edge computing should focus on lightweight security, for example, Elliptic Curve Cryptography, Permutation Based Lightweight Cryptogra- phy, Block-Ciphers Lightweight Cryptography, etc.It aimed at providing a comprehensive and reflective understanding of the security and privacy requirements, the state of the art techniques for ensuring the requirements, as well as the technological methods employed by the techniques.Secondly, the study dis- covered that each requirement has its specific techniques designed mainly for it, except integrity, nonrepudiation, and reliability which were considered together with other requirements in four different identified schemes.The most commonly fine grain secu- rity evaluation metrics as depicted in Table 11 are Tracking Accuracy, and Privacy protection level, which were employed by only five techniques [55], [63], [64], [66], [68].Moreover, it was observed that each category of the techniques under a particular requirement has specific metrics used for evaluating its performance for ensuring certain aim.Below are some of the factors: 1) The data acquisition process is subjected to a biased opinion because only one author searched for the pri- mary study articles.The major open issues include: A. LIGHTWEIGHT SECURITY FEATURES Lightweight security is required in the edge comput- ing network because of the minimum resource and stor- age characterized by the edge devices.As such, lightweight cryptographic protocols with smaller encryption keys that require fewer memory and CPU resources are preferred in edge computing.For example, from the find- ings, the Availability requirement is having only 1 technique under it, whereas Reliability, Nonrepudiation, and Integrity requirements are not considered by any technique, except in combination with other requirements.Consequently, utilization of software-based secu- rity and privacy analysis will help in quick and efficient identification of such issues.The summary of evaluation metrics employed by the

.techniques