

**Literature survey – Students should refer to 15-20 research papers from reputed journals and prepare a literature survey in the following format**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Title**  *(Name of the journal, author and publication details)* | **Methodology**  *(Provide a Summary of key studies and their findings)* | **Identification of gaps and limitations.**  *(Identify the limitations of the Research Paper)* |
| 1 | Odeh, A., Aboshgifa, A., Belhaj, N., 2023. Mitigating DDoS Attacks in Cloud Computing Environments: Challenges and Strategies. IEEE Access. | Discusses challenges in DDoS mitigation for cloud environments and proposes strategies like anomaly detection, ML models, and scalable architectures. | Limited testing on real-world, large-scale environments; lacks analysis of emerging attack vectors and their mitigation. |
| 2 | Wang, T., Lee, K., Zhou, X., 2022. Dynamic Defense Mechanisms Against DDoS in Cloud Computing. IEEE Trans. Cloud Comput. | Proposes real-time dynamic mechanisms for mitigating volumetric DDoS attacks in cloud systems by monitoring traffic patterns and applying adaptive scaling strategies. | Insufficient exploration of cost implications for dynamic scaling; limited adaptability for complex, multi-vector DDoS attacks. |
| 3 | Chen, R., 2022. AI-Based Detection for DDoS Attacks in Cloud Networks. IEEE Trans. Neural Netw. Learn. Syst. | Implements AI models to predict and mitigate DDoS attacks using historical data patterns and advanced neural networks in a cloud-based environment. | High computational overhead of AI models; reliance on historical data reduces real-time accuracy in detecting novel attacks. |
| 4 | Nguyen, T., Park, J., 2022. Advanced Architectures for Cloud-Based DDoS Mitigation. IEEE Trans. Emerg. Topics Comput. | Examines future-proof architectures incorporating SDN and distributed detection systems to efficiently mitigate evolving DDoS attack patterns. | Requires significant infrastructure changes to deploy SDN-based systems; limited scalability for small-scale or hybrid cloud setups. |
| 5 | lqahtani, H., Anwar, A., Ahmed, S., 2022. Comparative Study of Security Methods Against DDoS Attacks in Cloud Platforms. IEEE Access. | Provides a comparative analysis of DDoS mitigation techniques, emphasizing machine learning methods and their deployment in multi-cloud platforms. | Lack of testing under diverse attack scenarios; limited insights into long-term reliability and integration challenges. |
| 6 | Puri, M.E., 2023. Adaptive Filtering for DDoS Mitigation in Cloud Computing. IEEE Trans. Cloud Comput. | Introduces an adaptive filtering mechanism to detect and block anomalous traffic in real-time, ensuring minimal impact on cloud-hosted applications. | Does not address attack persistence or multi-vector strategies; potential false negatives in sophisticated attacks. |
| 7 | Chen, F., 2022. Machine Learning in DDoS Detection for Cloud Platforms. IEEE Access. | Explores supervised learning methods for anomaly detection and mitigation in cloud infrastructures facing volumetric attacks. | Limited scalability for large-scale deployments; over-reliance on labeled data for training ML models. |
| 8 | Wu, Y., 2022. Traffic Analysis in Cloud Networks for DDoS Detection. IEEE Trans. Dependable Secure Comput. | Focuses on using traffic analysis techniques to identify attack vectors, leveraging network-level metrics and cloud-native monitoring tools. | No integration with real-time defenses; lacks focus on novel attack methodologies like slow-rate or application-layer DDoS. |
| 9 | |  | | --- | |  |  |  | | --- | | Nguyen, H.M., 2022. Future Directions in Cloud DDoS Defense. IEEE Trans. Netw. Sci. Eng. | | Highlights advancements in DDoS protection tools and provides recommendations for hybrid cloud environments integrating SDN and AI-based systems. | Feasibility and cost concerns for deploying hybrid systems; lacks a unified framework for integrating diverse technologies. |
| 10 | |  | | --- | |  |  |  | | --- | | Xu, M., 2022. Performance Analysis of DDoS Mitigation Techniques in Cloud. IEEE Access. | | Evaluates the efficiency and scalability of various mitigation techniques, including anomaly-based filtering and resource scaling mechanisms in cloud setups. | No real-world validation under sustained attack conditions; neglects hybrid or multi-cloud operational complexities. |