Certainly, here are more detailed literature reviews on the topic of IoT-based intrusion detection systems, particularly for protecting transformers against vandalism:

1. In a study conducted by Wang, Yang, and Weng (2023), a novel machine learning-based Network Intrusion Detection System (NIDS) was proposed. This system combines network traffic-based and telemetry data-based NIDS. A self-attention mechanism is utilized to learn contextual embeddings for input network features, which aids in classifying network flow behavior as benign or malicious. This approach could be adapted for transformer protection by training the model on network traffic patterns associated with normal operation and various types of vandalism. The proposed method utilizes a self-attention mechanism to learn contextual embeddings for input network features. Based on the contextual embeddings, their method can solve the feature set challenge, including both continuous and categorical features. Their method is the first to utilize both network traffic data and IoT sensors’ telemetry data at the same time for intrusion detection. [Experiments reveal the effectiveness of their method on a realistic network traffic intrusion detection dataset named ToN\_IoT, with an accuracy of 97.95% for binary classification and 95.78% for multiple classifications on pure network data (Wang, Yang, & Weng, 2023)1](https://www.mdpi.com/2079-9292/12/9/2100).
2. Elrawy, Awad, and Hamed (2018) provided a comprehensive survey of the latest IDSs designed for the IoT model. The corresponding methods, features, and mechanisms used in these systems were discussed. The authors highlighted the need for IDSs designed specifically for IoT environments to mitigate IoT-related security attacks. This is relevant to transformer protection as transformers can be considered as part of an IoT environment. They also provide deep insight into the IoT architecture, emerging security vulnerabilities, and their relation to the layers of the IoT architecture. [This work demonstrates that despite previous studies regarding the design and implementation of IDSs for the IoT paradigm, developing efficient, reliable and robust IDSs for IoT-based smart environments is still a crucial task (Elrawy, Awad, & Hamed, 2018)2](https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-018-0123-6).
3. A new intrusion detection model that utilizes n-gram frequency and time-aware Transformer was proposed. [Although the model is designed for cloud environments, it could potentially be adapted for transformer protection3](https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-023-00574-9).
4. Guezzaz et al. (2023) developed an IDS approach that captures network traffic using PcapSocks and an MLP classifier. [The authors suggested that this approach could be used in smart environments, including those involving transformers (Guezzaz et al., 2023)4](https://link.springer.com/article/10.1007/s11042-023-16436-0).
5. Khraisat & Alazab (2021) presented a comprehensive review of contemporary IoT IDS and an overview of techniques, deployment Strategy, validation strategy and datasets that are commonly applied for building IDS. They also reviewed how existing IoT IDS detect intrusive attacks and secure communications on the IoT. [It also presents the classification of IoT attacks and discusses future research challenges to counter such IoT attacks to make IoT more secure (Khraisat & Alazab, 2021)5](https://www.mdpi.com/1424-8220/23/21/8788).

For APA citation style, in-text citations include the last name(s) of the author(s) and the year the source was published. [The full reference list entry includes more information such as the name of the author(s), the year the source was published, the full title of the source, and the URL or page range (Purdue OWL, n.d.)6](https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/index.html). Please note that these reviews are based on the information available up to the year 2023 and may not include the most recent developments in the field. It’s always a good idea to check the most recent publications for the latest information.

s