The paper provides a structured survey of anomaly detection research categorizing techniques based on underlying approaches. It introduces anomaly detection as finding patterns not conforming to normal behavior, discussing its importance across domains like intrusion detection and challenges like defining normalcy. Distinguishing point, contextual and collective anomalies, it identifies factors impacting problem formulation. Applications discussed include intrusion detection, fraud detection, and fault detection specifying anomaly notions, data characteristics, challenges, and techniques. Classification techniques build models distinguishing normal and anomalous classes using methods like SVM, Bayesian, and neural networks, while nearest-neighbor techniques measure the distance to neighbors using KNN, the local outlier factor. Clustering techniques identify outliers not in large dense clusters applying partitioning, hierarchical and density-based clustering, and statistical techniques assume normal data distributions fitting distributions and detecting outliers. Information theory and spectral techniques are also explained. Addressing dynamic anomalies remains difficult as most techniques detect simple, not complex anomalies, though contextual techniques account for data neighborhood. The paper aims to systematically overview research across multiple areas and applications to facilitate understanding diverse techniques and cross-domain applications through its structured categorization analyzing assumptions.

"Anomaly Detection: A Survey":

The paper begins by introducing the concept of anomaly detection, which involves identifying patterns in data that deviate from expected behavior. These anomalous patterns are also referred to as outliers, discordant observations, exceptions, or contaminants. Anomaly detection is a widely researched problem that spans various research areas and application domains.

The authors highlight that different anomaly detection techniques have been developed, some specifically tailored for certain domains and others with more generic applicability. The aim of the survey is to provide a structured and comprehensive overview of the research conducted on anomaly detection. To achieve this, the authors categorize existing techniques based on their underlying approaches.

The paper emphasizes the importance of understanding the assumptions made by each technique to differentiate between normal and anomalous behavior. These assumptions serve as guidelines when applying a particular technique to a specific domain, enabling the assessment of its effectiveness. For each category of techniques, the authors present a basic anomaly detection technique and then demonstrate how other existing techniques in that category are variants of the basic approach. This template facilitates a clearer and more concise understanding of the techniques within each category.

Additionally, the authors discuss the advantages and disadvantages of the techniques in each category. This helps researchers and practitioners make informed choices regarding the selection of an appropriate technique based on the specific requirements and constraints of their application domain. The paper also addresses the computational complexity of the techniques, recognizing its significance in real-world application domains.

The survey aims to shed light on the diverse directions in which research has been conducted in the field of anomaly detection. It highlights how techniques developed in one area can be applied to domains for which they were not originally intended. This cross-pollination of ideas and methodologies can lead to valuable insights and innovative solutions in different domains.

The paper provides a glimpse into the categories and subject descriptors relevant to anomaly detection, such as database management and data mining. It also mentions the general terms associated with the field, namely algorithms. Furthermore, the authors include additional keywords and phrases related to anomaly detection and outlier detection, which further characterize the scope of the survey.

The paper concludes by citing the ACM reference format and providing the necessary information for citation. It acknowledges the support received for the research and emphasizes that permission is granted to make digital or hard copies of the work for personal or classroom use, as long as it is not distributed for profit or commercial advantage and appropriate credit is given.