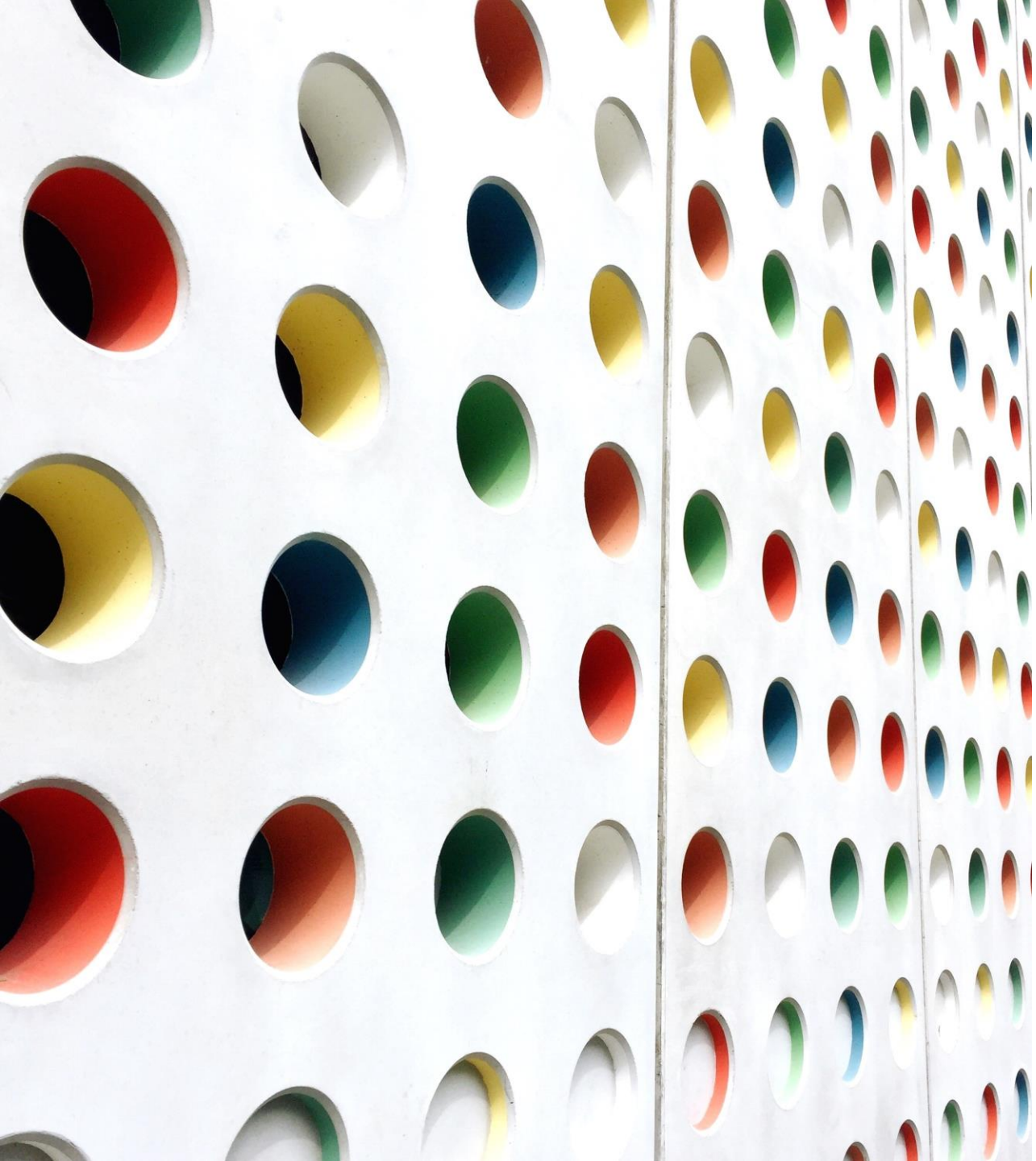

Ransomware

RESEARCH PAPER ANALYSIS

Assignment Summary

- Identify the purpose, problem, objective or research question of the paper, contrast with personal reflections on the same topic?
- Is the research methodology appropriate for the paper?
- Does the data collection and analysis support the paper?
- How effectively does the paper support conclusions?
- How could the paper be enhanced?

Literature Survey

- Detecting ransomware attacks using intelligent algorithms: recent development and next direction from deep learning and big data perspectives (Bello, et. Al, 2022)
- Stated purpose: Comprehensive review of using intelligent algorithms to detect ransomware
  - No alignment to malware protection implemented in real organizations but good primer for those seeking to understand current state
- Analyzed ten other surveys 2017-2020 and twenty-five papers discussing malware detection via machine learning
  - Limited description of how sources were selected but classified across a taxonomy – aligns with presenting data in a novel way
  - All sources less than five years old aligns with reviewing recent research
- Claims of increased ML adoption are suspect with ~ 35 papers, none of which represent active defenses currently implemented.
- Conclusion could have been made stronger by identifying one or two areas of research that show promising application of deep learning rather than discuss improvements for each ML classifier

Classifier Experiment

- Automatic Ransomware Detection and Analysis Based on Dynamic API Calls Flow Graph (Zhi-guo et. Al, 2017)
- Stated purpose: Assess the effectiveness of a dynamic analysis system through a controlled experiment
  - The experiment validates false positive and false negative rates, a practical interest for real organizations
- Controlling all variables but the classifier used in each experiment provides good basis for comparing detection rates
- The paper uses charts and recognized data processing methods such as normalization to provide meaningful comparison.
- The paper could have expanded on the criteria that lead to one feature being meaningful while others are not since gain ratio was one of the benefits claimed from this approach. Overall very little could improve this work as it is very thorough