META JACKET

CAPSTONE PROJECT REVIEW-1

VIT UNIVERSITY
VELLORE INSTITUTE OF TECHNOLOGY

VIT®
BHOPAL

OUR TEAM

Priyam Jain	20BAI10087
Ishaan Shukla	20BAI10105
Anagh Garg	20BAI10127
Naman Purkar	20BAI10259
Varun Shukla	20BAI10292

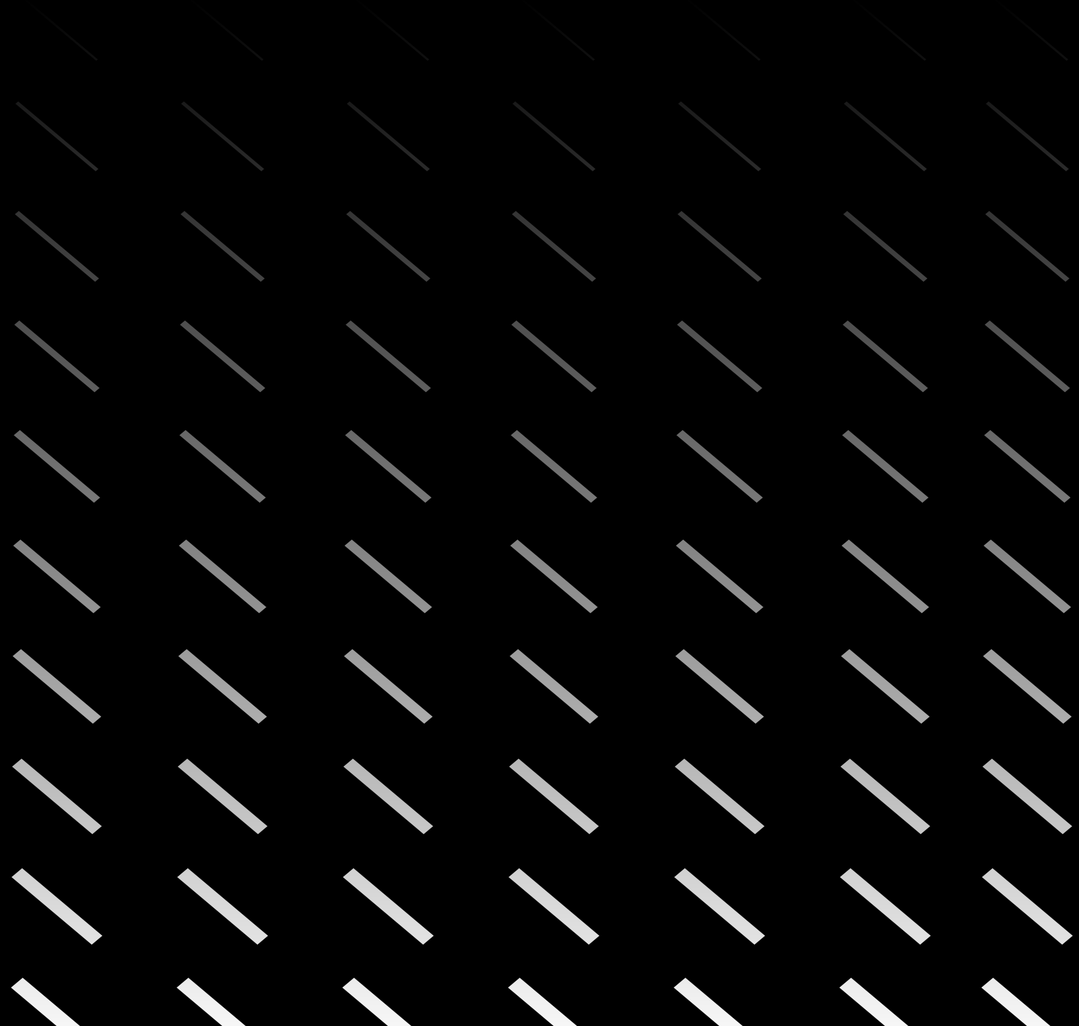
Our Mentor and Reviewers

Dr. Pranshu Pranjal

Dr.S.Periyanayagi

Dr. Venkata Prasad Padhy

Agenda



INTRODUCTION

Existing work with limitations

Methodology

Novelty of the project

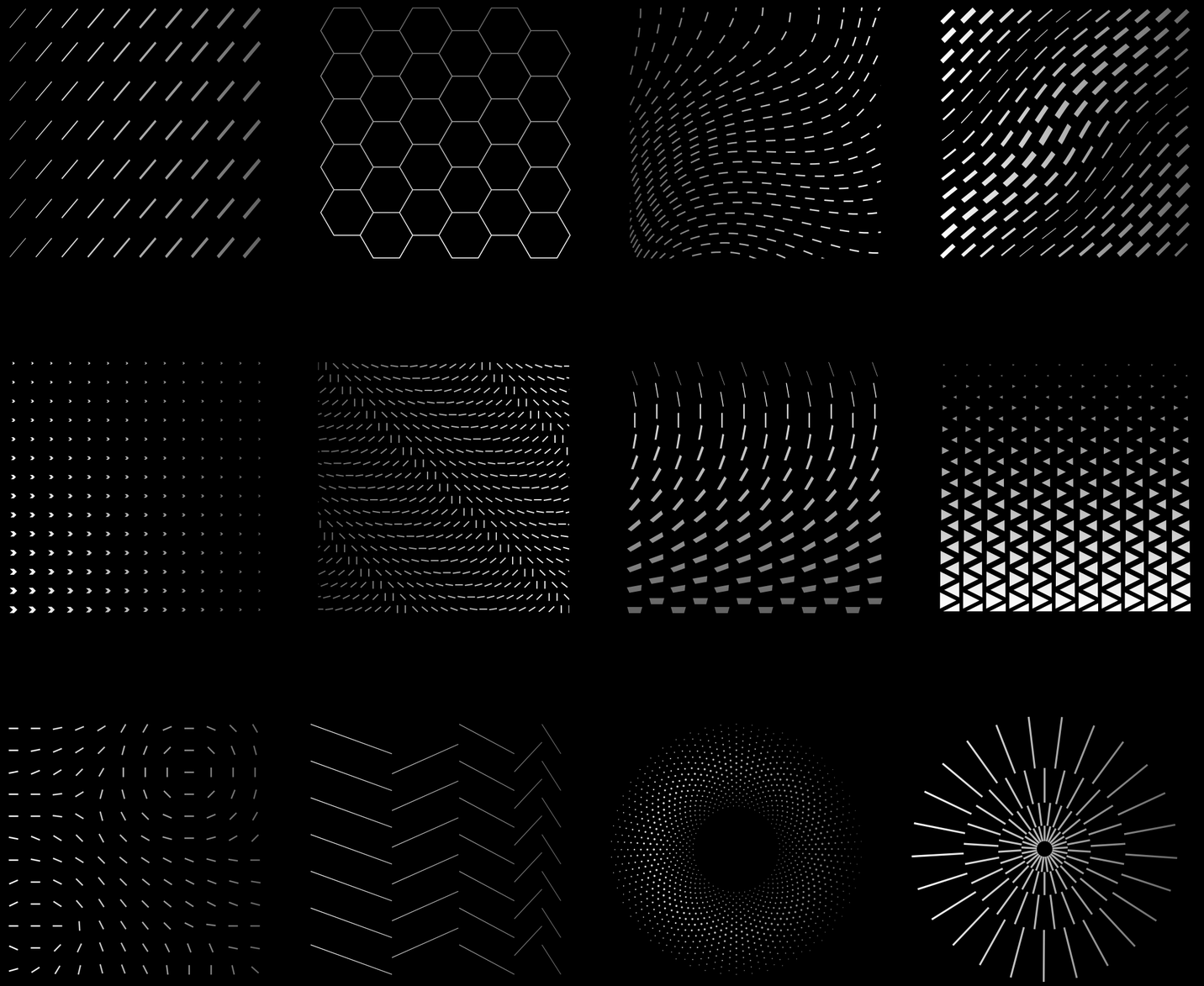
Real time usage

Hardware & software requirements

Overall system architecture diagram

Conclusion

Introduction



Challenges

- Traditional methods face limitations.
- Polymorphic threats evade detection.
- Swift spread necessitates innovation.

Solutions

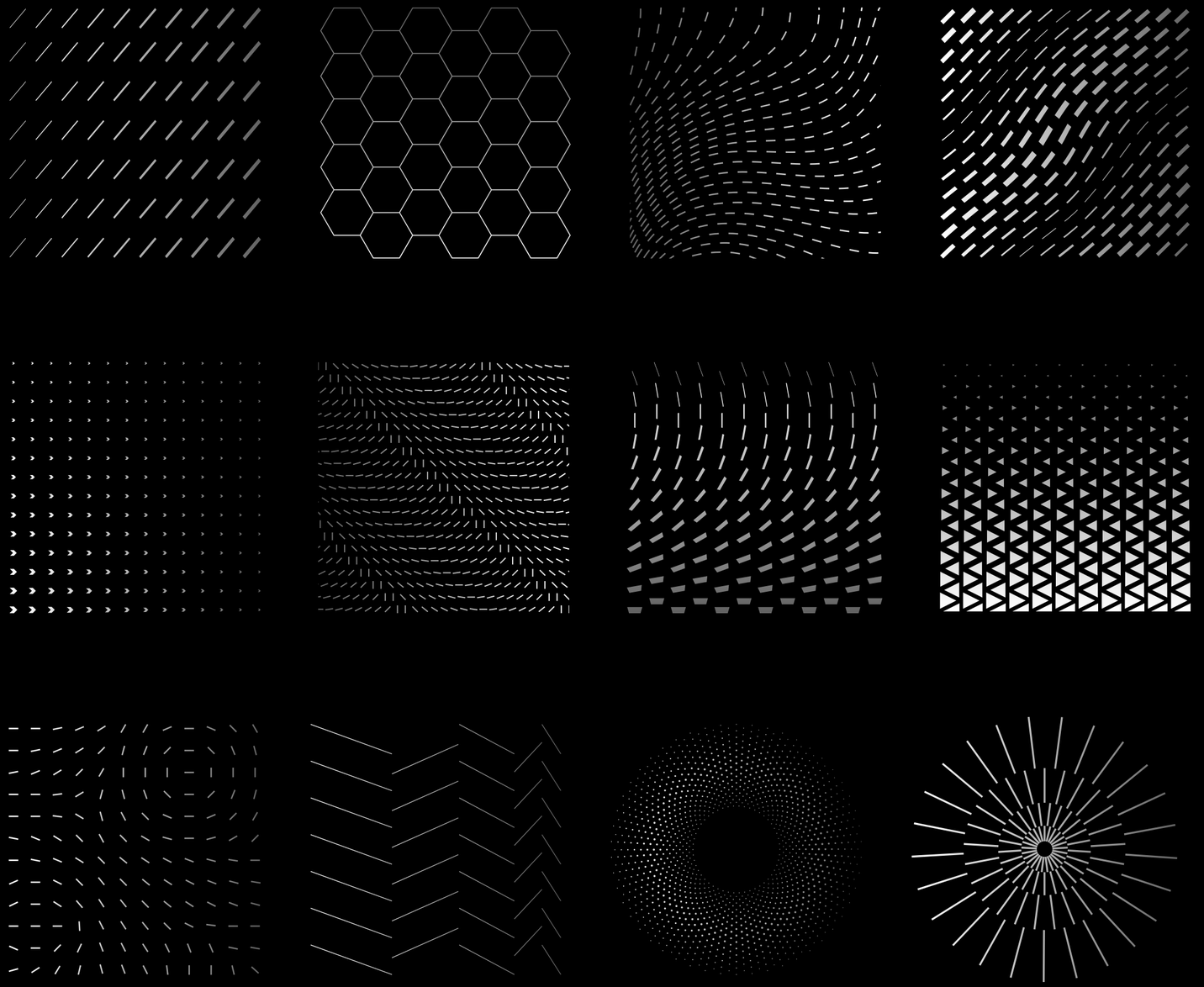
- **Behavioral Analysis:** Uncover patterns through behavior.
- **Machine Learning and AI:** Adaptive algorithms for threat recognition.
- **Cloud-Based Detection:** Real-time analysis and sharing.

Conclusion

- **Holistic Defense:** Combine methods for comprehensive protection.
- **Continuous Innovation:** Stay ahead of evolving threats.

INTRODUCTION

Existing work with limitations



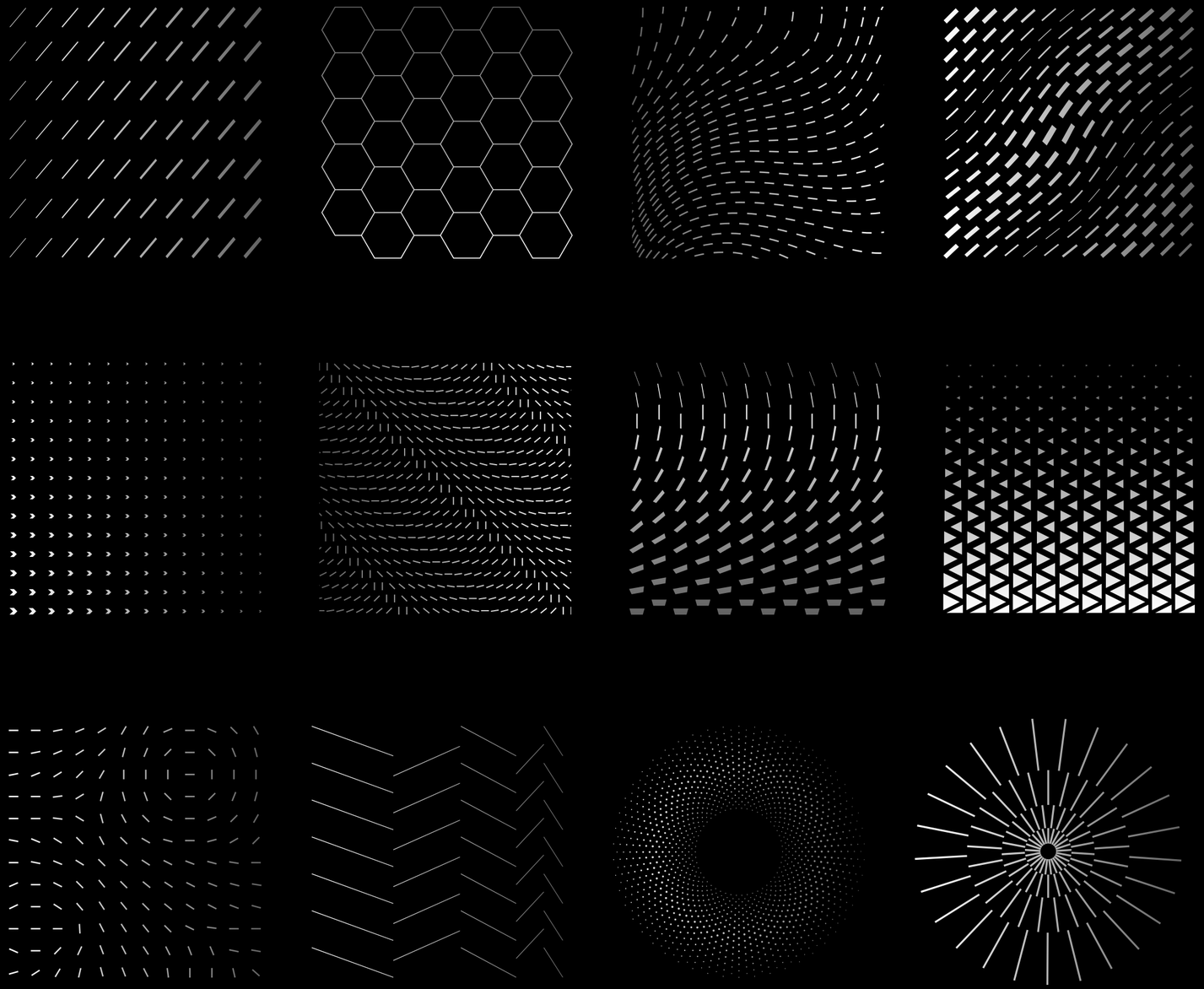
Existing work with limitations

Although not widely implemented, the concept of machine learning methods for malware detection is not new. Several types of studies were carried out in this field, aiming to figure the accuracy of different methods.

“Malware Detection Using Machine Learning” Dragos Gavrilut aimed for developing a detection system based on several modified perceptron algorithms.

“A Static Malware Detection System Using Data Mining Methods” proposed extraction methods based on PE headers, DLLs and API functions and methods based on Naive Bayes, J48 Decision Trees, and Support Vector Machines.

Methodology



Introduction

Malware detection methods categorized into:

- Signature-based
- Behavior-based

Analysis Approaches

- Static Analysis:
  - Code examination without execution.
- Dynamic Analysis:
  - Real-time observation of behavior.

Signature-Based

- Identifies using virus codes/hashes.
- Cloud-based database cross-check.

Methodology

Behavior-Based

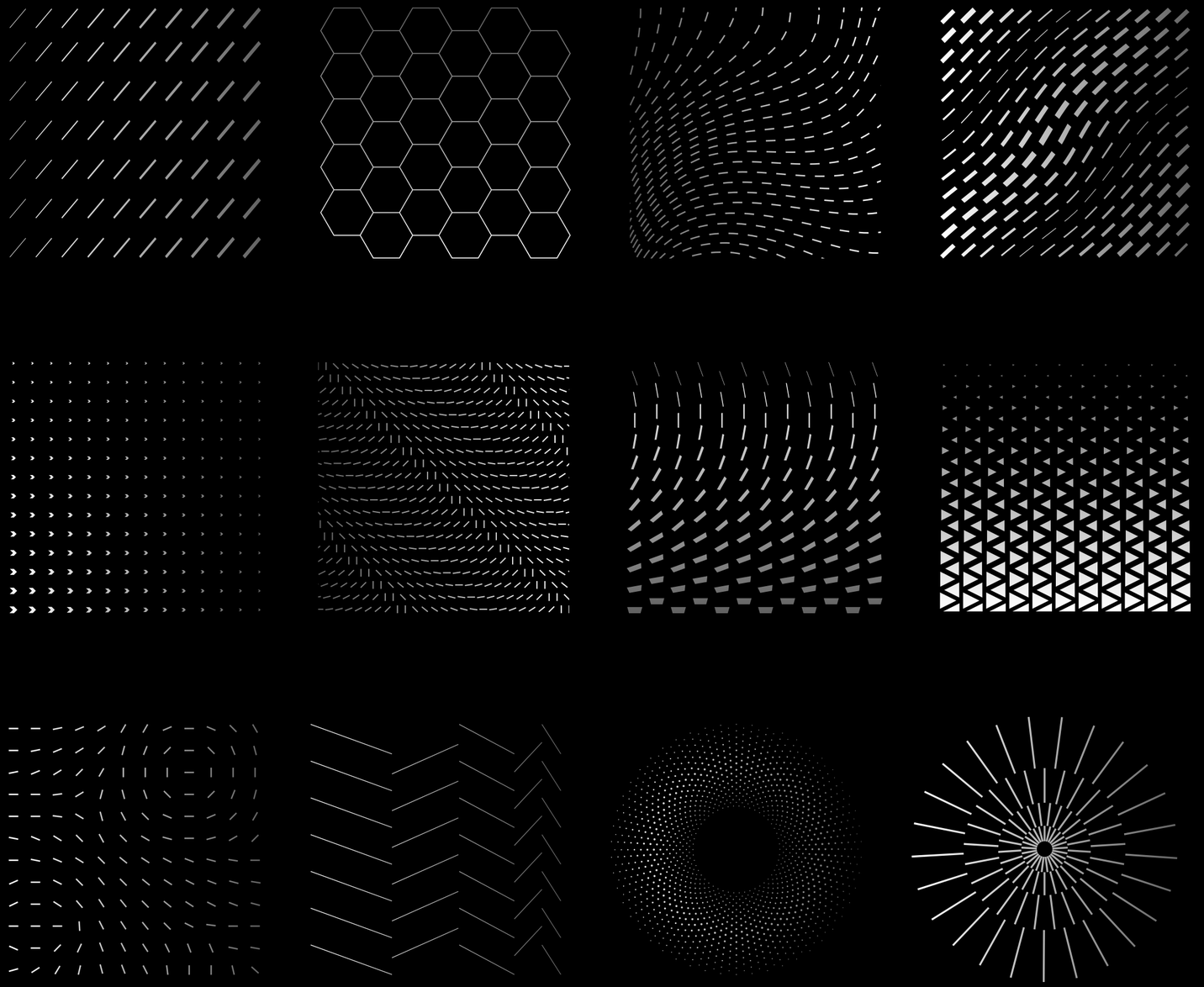
- Identifies through behavior observation.
- Malware behaves distinctly.

Key Takeaways

- Static and dynamic analysis essential.
- Signature-based relies on known codes.
- Behavior-based focuses on actions.
- Combined use enhances detection.

Methodology

NOVELTY



Real-time Protection

- Swift response to cyber threats.
- Constant monitoring for immediate defense.

AI-Based Counteraction

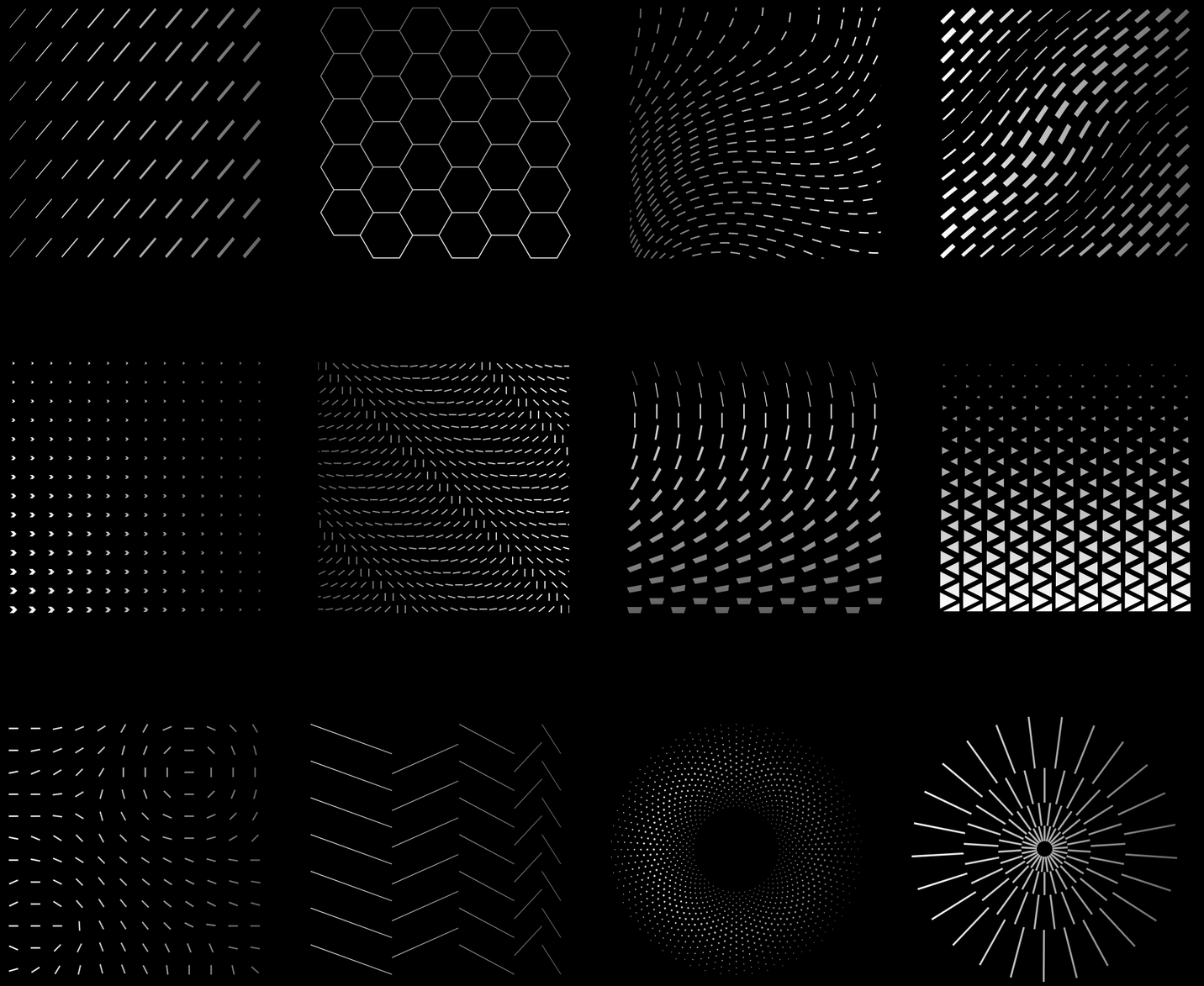
- Intelligent response to ongoing attacks.
- Adaptive measures guided by AI algorithms.

Evolutionary Defense

- AI-driven malware analysis.
- Defense evolves in tandem with emerging threats.

NOVELTY

Real Time Usage



Introduction

- **IoT Security Challenge:**
  - Growing threat landscape in smart homes.
- **Smart Homes Protection:**
  - Machine learning defends against IoT threats.

Unique Capabilities

- Adaptability to IoT Environment: Swift identification of unusual device communication.
- Continuous Learning: Machine learning models update and refine.

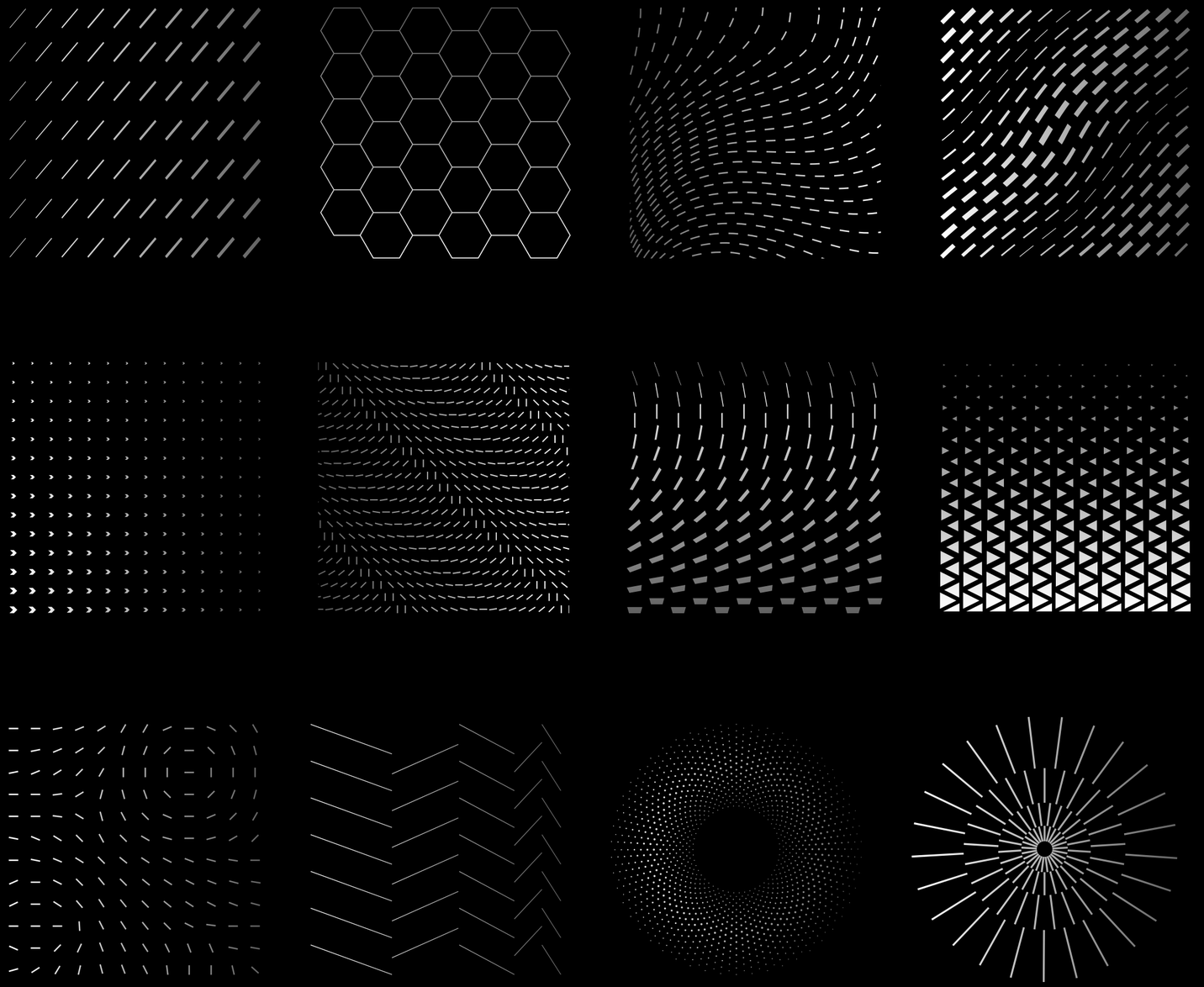
Benefits

Agile Defense:

- Proactively counters evolving threats

Real Time Usage

HARDWARE AND SOFTWARE REQUIREMENTS



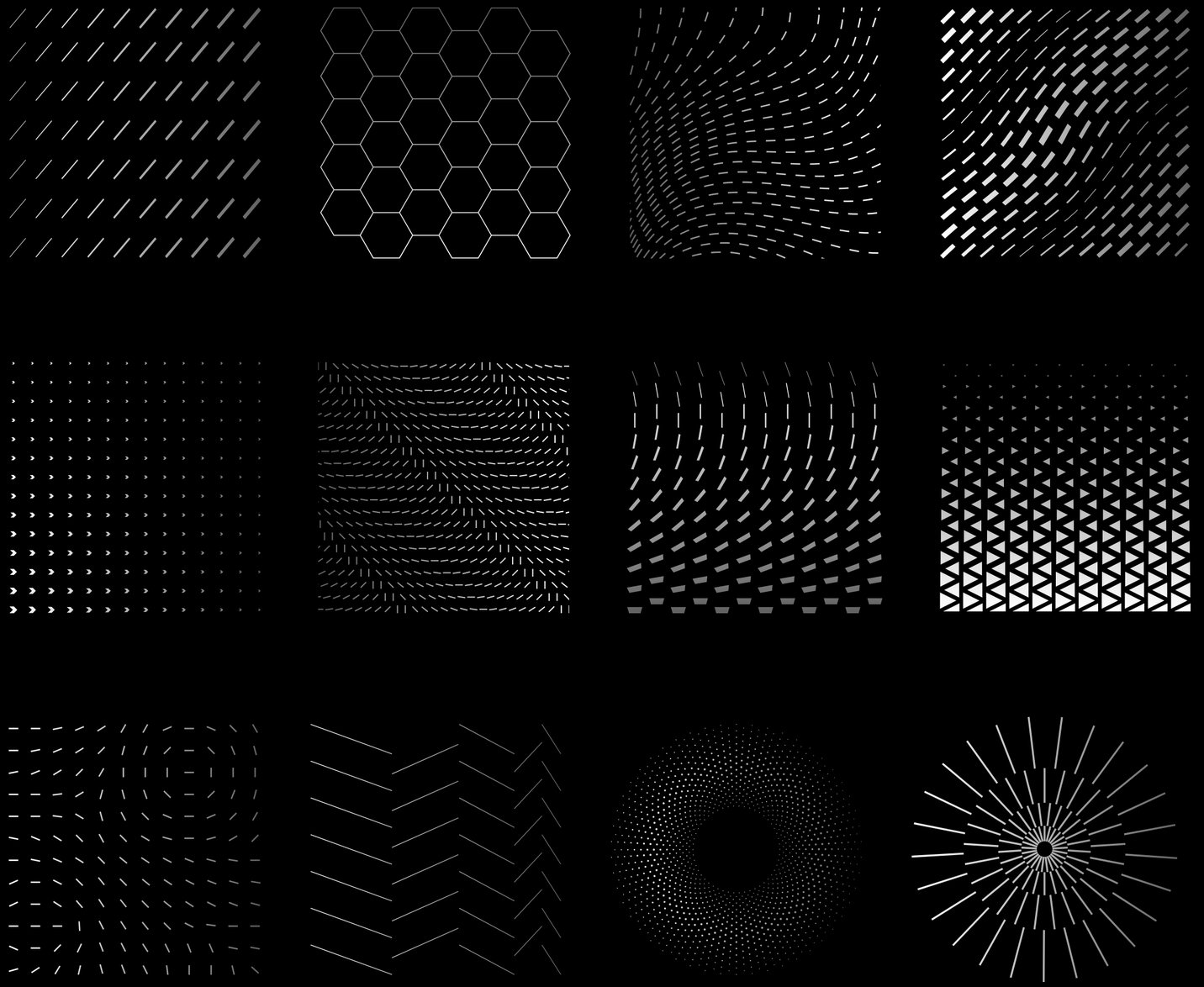
HARDWARE REQUIREMENTS

Anti Virus Malware	**Device** Laptop , desktop or pc.
RAM Recommended 8GB or above	**Ethernet or Wifi**

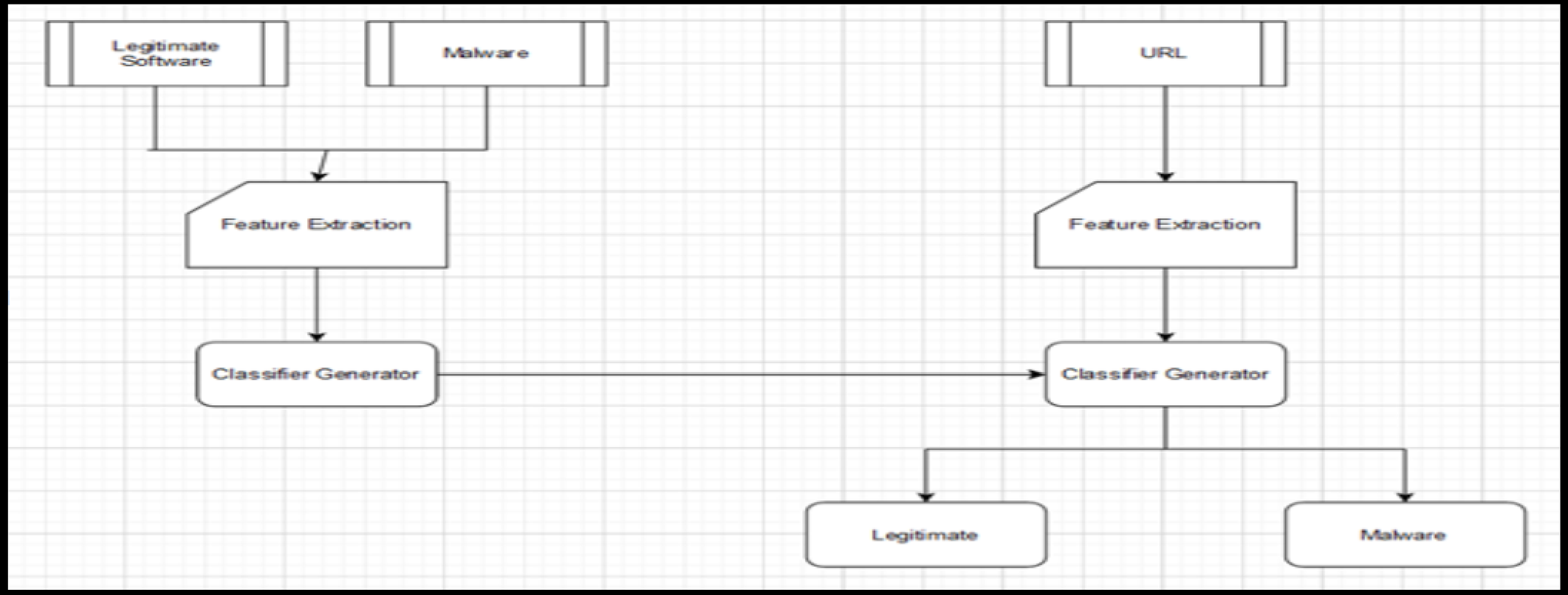
SOFTWARE REQUIREMENTS

Operating System Mac , Linux , Windows	**Latest PiP Version** Used to install libraries	**Python Libraries** Numpy , Pandas , Seabon , Matplotlib Scikit-learn
Compilers Jupyter Notebook , Vs Code , PyCharm , Google Colab	**Latest Kernel Version**	**Latest Kernel Version** To make the model accessible to all using website

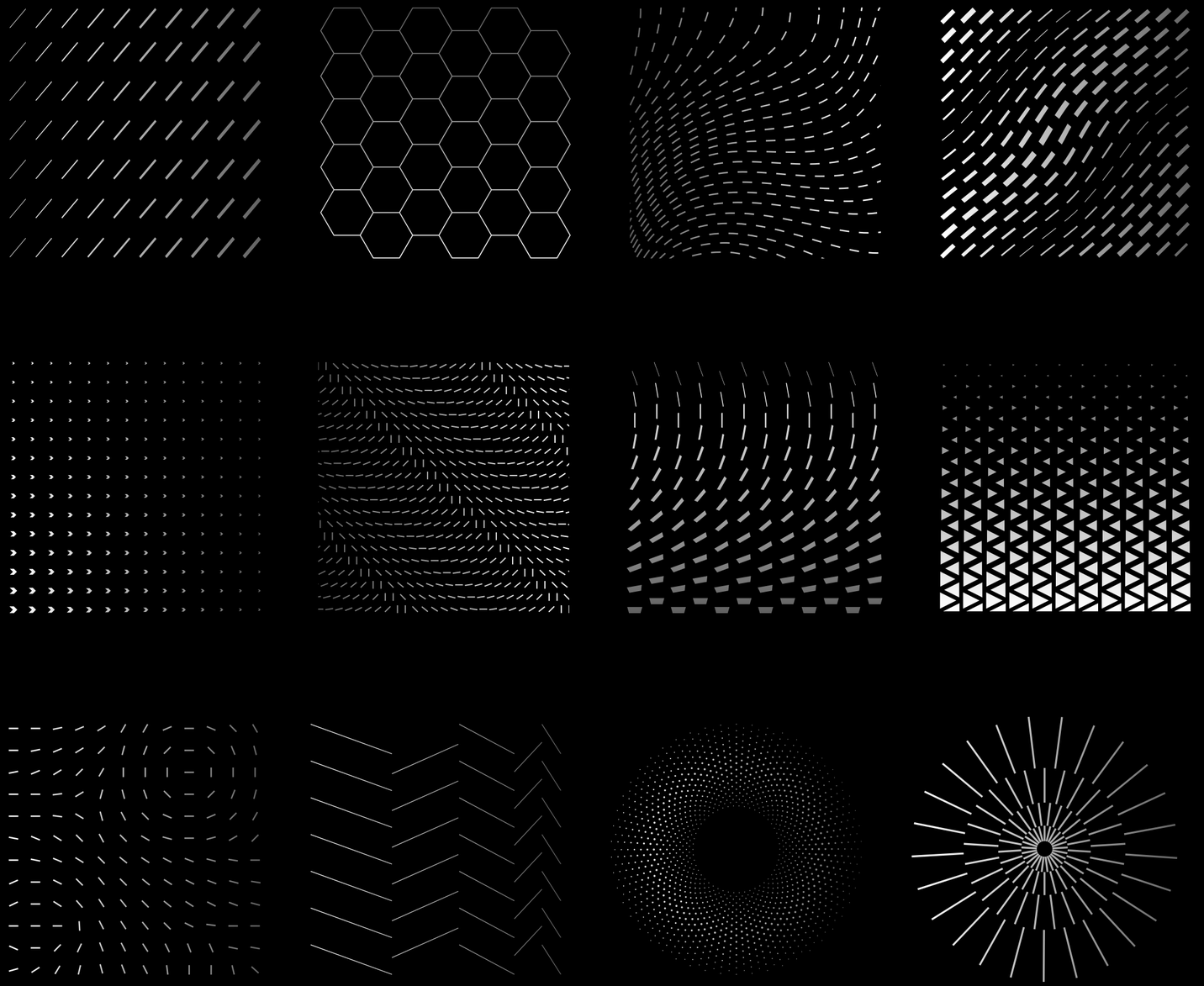
Overall system architecture diagram



Overall system architecture diagram



Conclusion



Conclusion

1) Malware

2) Advantages of Malware detection system

3) Existing algorithms used for malware detection

4) Explaining detecting malware

5) Using Data Science and Mining Techniques

Thank You