

Social Cybersecurity and Data Leak Detection

BITS F112 TRW Group - 1

Group Members

- | | |
|------------------------|---------------|
| • Anoushka Martin | 2022A9PS0129U |
| • Dev Dahiya | 2022A7PS0319U |
| • Dhanush Krishna | 2022A7PS0302U |
| • Drisya Mannikath | 2022A9PS0254U |
| • Karthik Narayanan | 2022A7PS0321U |
| • Mohammad Shamshuddin | 2022A7PS0333U |
| • Sivaa Balamurugan | 2022A7PS0323U |
| • Xec Abdul Kader | 2022A9PS0252U |



Agenda

01

Introduction

02

Discussion

03

Conclusion

04

Recommendations





01

Introduction

Introduction

01

Background of the Study

02

Objectives

03

Scope

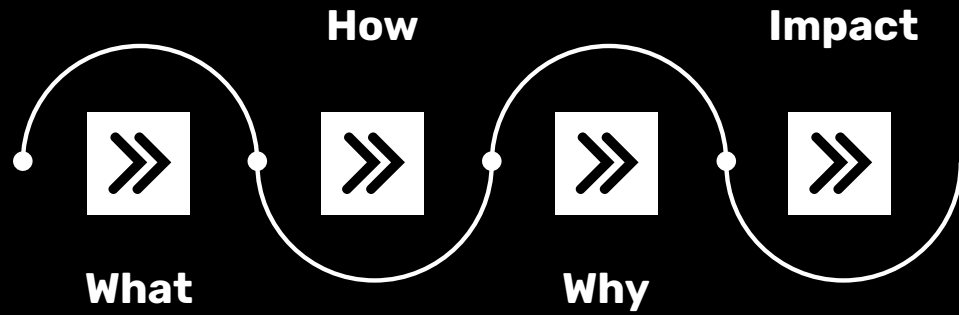
04

Limitations

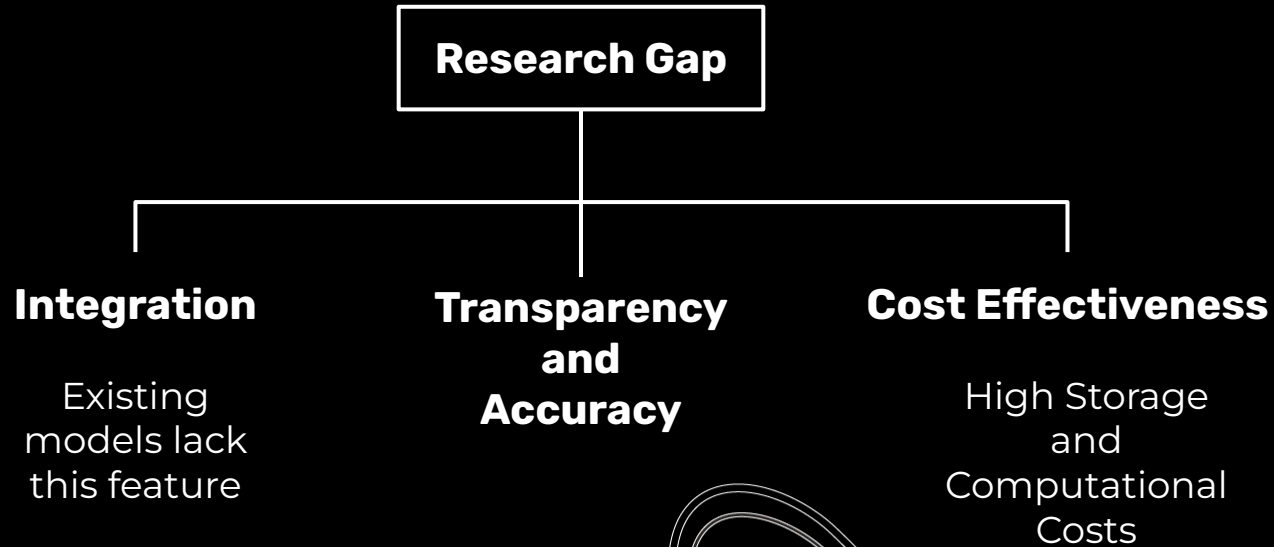
05

Methodology

Background of the Study



Background of the Study



Objectives



1

To explore the methods, mediums and causes of data leakage.

2

To study existing data leakage models and identify their limitations.

3

To propose an improved model that integrates multiple use cases.

4

To propose a model based on python daemon thread tech that is more efficient.

Scope



Analyze
various data
leakage
scenarios.



Investigate
the scope for
using
machine
learning
algorithms



Implement
risk
management
techniques to
mitigate
losses

Scope



Deploy

appropriate
models for
relevant
use cases.



Daemon Thread

algorithm to
identify data
leakage



Email Model

paired w/ a
companion
software for
ease of access

Limitations



Support for Large Scale

At the moment the model is targeted towards a smaller scale.



File Versioning

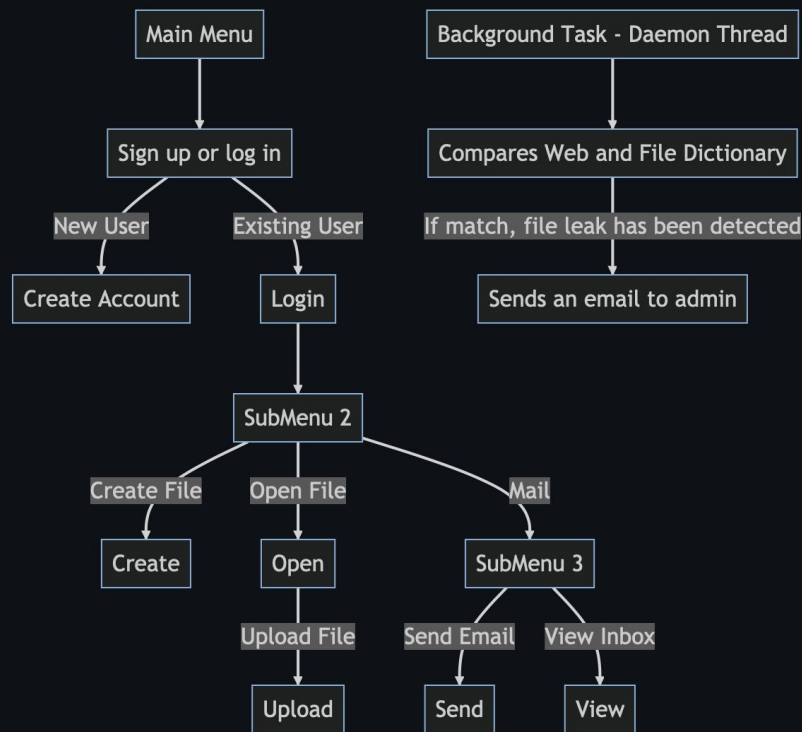
Doesn't allow rollback to previous version, will have to re-upload.



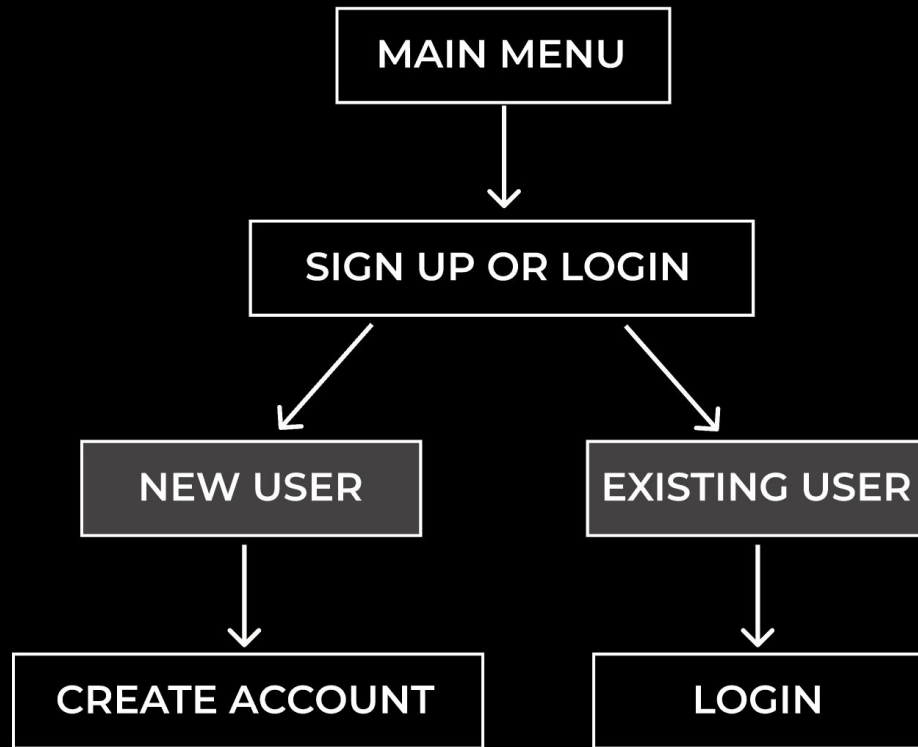
LAPTOP MOCKUP

This is what a user / admin
would see when they use
our model.

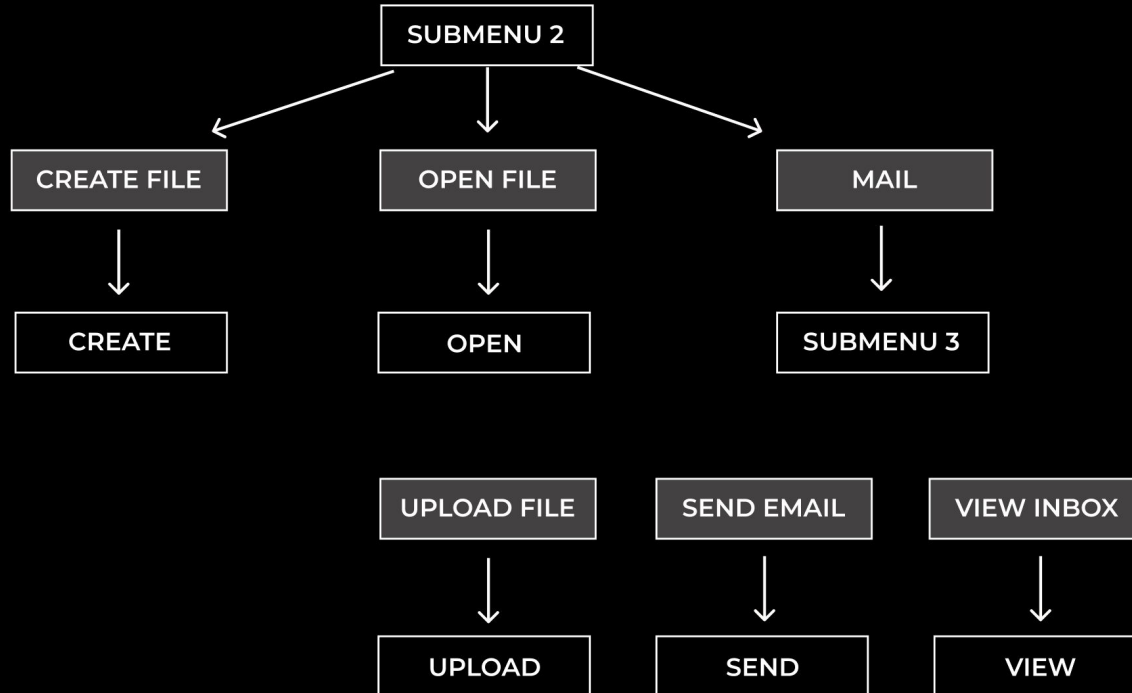
Methodology



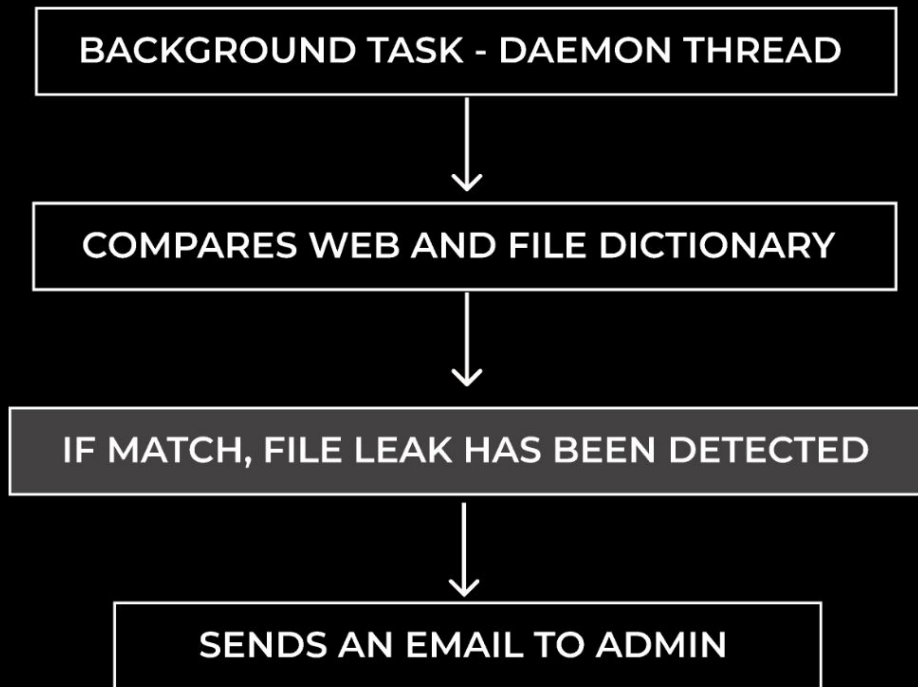
Methodology



Methodology



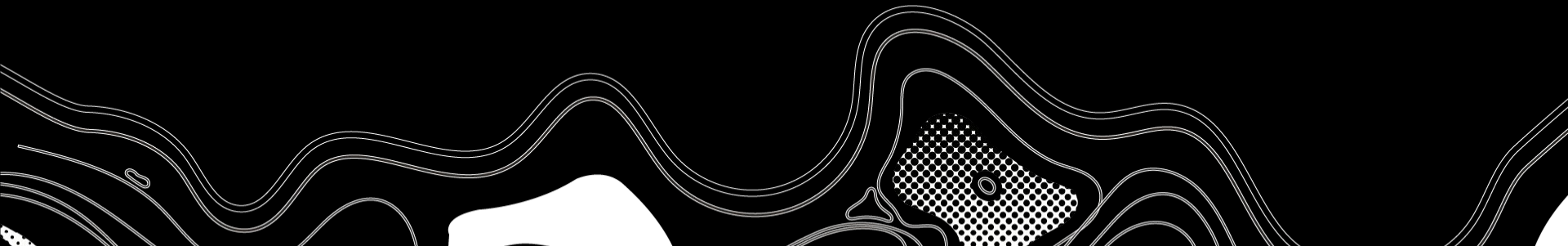
Methodology



Methodology

Python Daemon Threads:

- Background Thread
- Daemon vs Non-Daemon Threads
- Flow of Execution

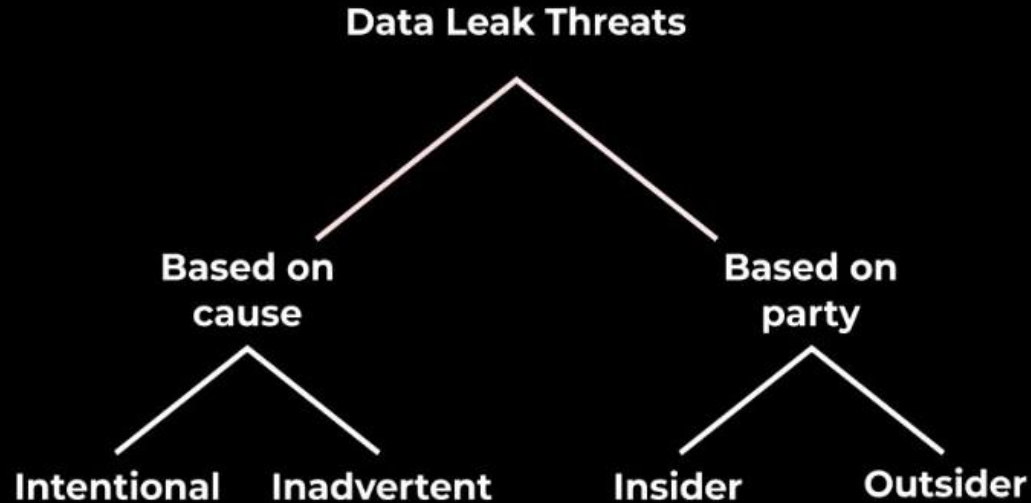


02

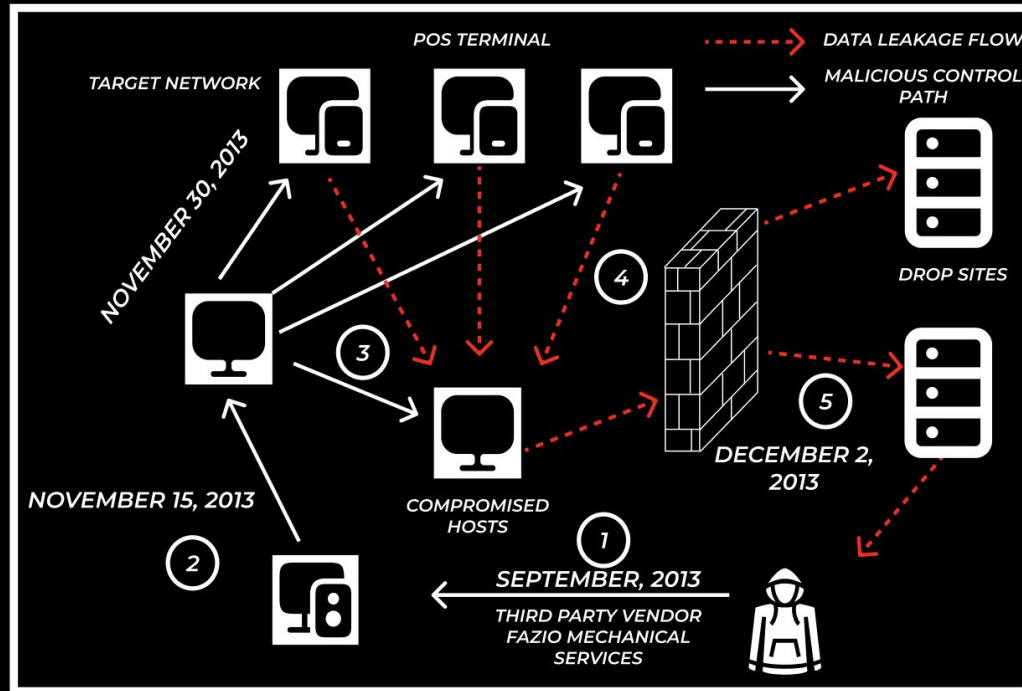
Discussion



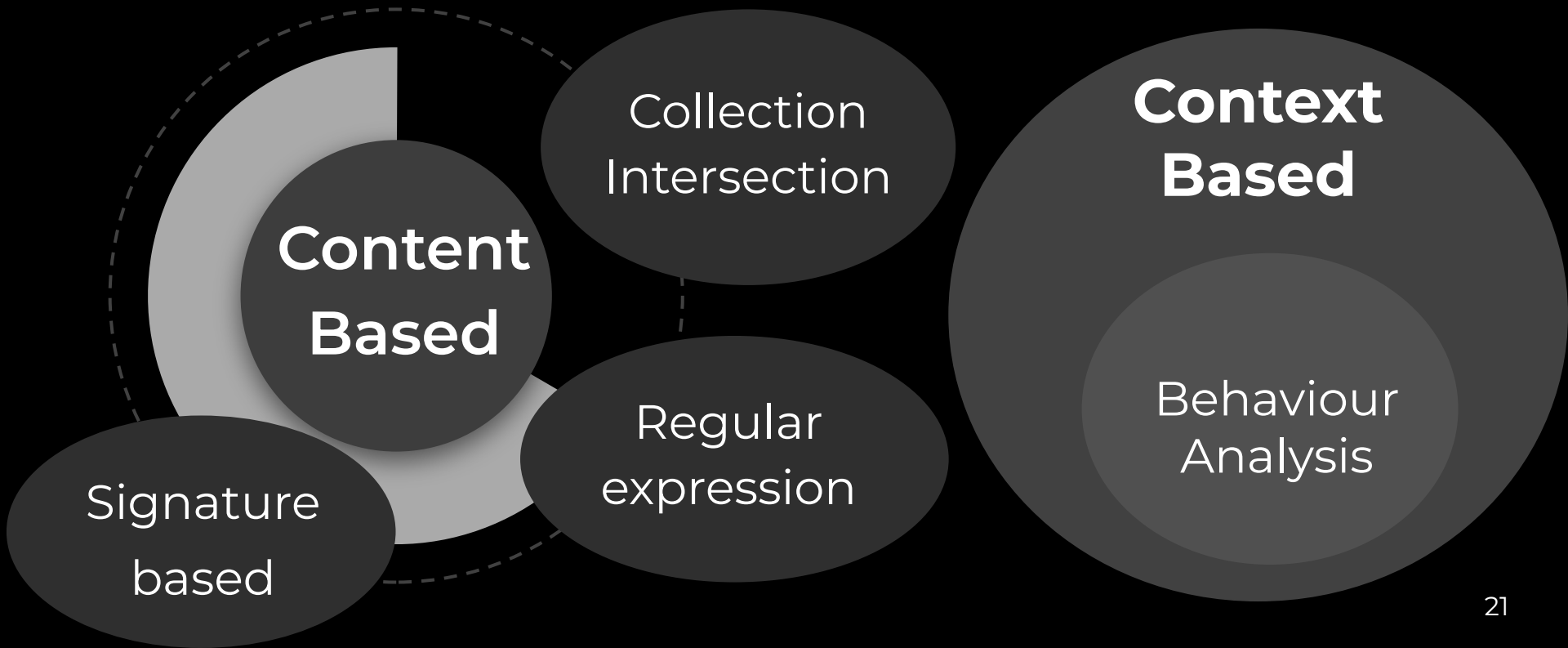
Data Leak Threats



Data Leak Incident



Data Leakage Prevention Techniques



Drawbacks of Existing Models

<u>TECHNIQUE</u>	<u>ANALYSIS</u>	<u>CONS</u>
COLLECTION INTERSECTION	CONTENT	HIGH COMPUTATION & STORAGE COSTS, INAPPLICABLE TO EVOLVED OR OBFUSCATED DATA
MACHINE LEARNING	CONTENT/CONTEXT	LARGE TRAINING DATA, COMPLICATED
BEHAVIOUR ANALYSIS	CONTEXT	LARGE TRAINING DATA, HIGH FALSE POSITIVES
WATERMARKING	CONTEXT	VULNERABLE TO MALICIOUS REMOVAL OR DISTORTION
HONEYPOTS	CONTEXT	LIMITED APPLICATIONS



03

Conclusion

Conclusion

- Data leakage is a major security concern
- Caused by malicious outsiders or insiders
- Leaked information includes financial data, intellectual property and medical information
- Organizations should implement appropriate security measures



Conclusion

- Measures include access control mechanisms and user security awareness
- DLPD tools like encryption, firewalls, and antiviruses can help
- Detecting and preventing data leaks is an ongoing challenge that requires research and innovation



04

Recommendation



How does our model address pre-existing limitations?

Collection Intersection

Incurs significant processing and storage costs



Watermarking

Prone to Malicious Removal or Tampering



Behavioral Analysis

Requires large amounts of training data.



Machine Learning

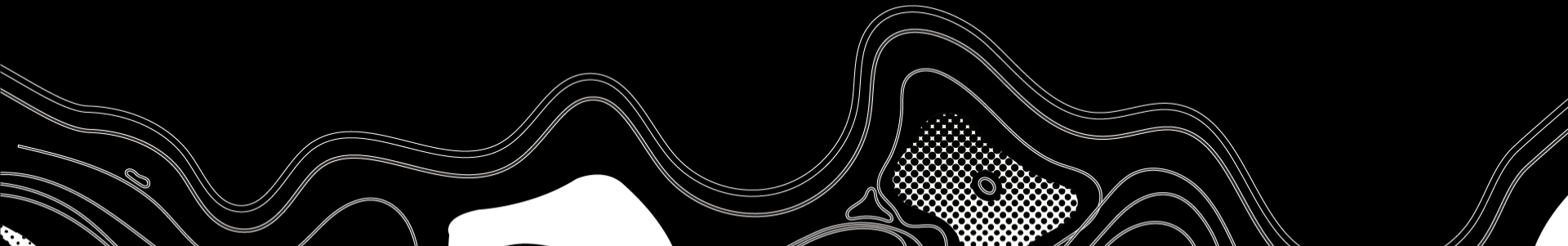
Lack of Transparency



Recommendation

The proposed model offers a comprehensive solution to the challenge of data leakage by incorporating user authentication, file management, periodic data leak checks as well as warning the admin via email when a leak has been detected.

We have gone one step ahead of our competition by integrating multiple functionalities within a single model, providing a more fuller and cost effective alternative, one stop solution to all your needs.



05

REFERENCES

REFERENCES

- L. Cheng, F. Liu, and D. Yao, “Enterprise data breach: causes, challenges, prevention, and future directions,” *Wiley Interdisciplinary Reviews-Data Mining and Knowledge Discovery*, vol. 7, no. 5, p. e1211, Sep. 2017, doi: 10.1002/widm.1211.
- V. Sundareswaran, “STUDY OF CYBERSECURITY IN DATA BREACHING,” ResearchGate, Mar. 2018, [Online]. Available: https://www.researchgate.net/publication/325300571_STUDY_OF_CYBERSECURITY_IN_DATA_BREACHING
- A. H. Juma’h and Y. Alnsour, “The effect of data breaches on company performance,” *International Journal of Accounting and Information Management*, vol. 28, no. 2, pp. 275–301, Mar. 2020, doi: 10.1108/ijaim-01-2019-0006.



THANK YOU!

We are open to any questions
now!