KAUST ACADEMY

2024 SPECIALIZATIONS



KAUST Academy

academy.kaust.edu.sa

KAUST ACADEMY SPECIALIZATIONS 2024

VISIT OUR WEBSITE

academy.kaust.edu.sa



TABLE OF CONTENT

CYBERSECURITY

01
Enhancing Privacy in Critical Agencies IDS
Decentralized AI with Federated Learning

02
PentPeek
An Integrated Dynamic Application Security Testing (DAST) Tool

03
Lumin
Blockchain-Based Solar Energy Management System.

04
InternalEYE
Insider Threat Detection Using Machine Learning

05
Decentralization of Financial Transactions
Using Blockchain Technology (DFTBT)

06
Phish Me If You Can
Detecting Phishing Websites Using Machine Learning

07
Malware
Analysis Using AI

08
Drone
Security Testing Framework

09
SafePost
AI-Powered Post PII Detection

10
Compliance Compass
Automated Cybersecurity Adherence

11
CookieGuard:
Cookies & the Dark Web

BIOINFORMATICS

12
From CNA Profiles to Prognostic Predictions:
Utilizing Hilbert Curve Images for Cancer Subtype Classification and Survival Analysis

13
Development Of Deep Learning Solutions
For 4D Image Segmentation Of Spatial Omics Data

14
YOLO-AR
A CT Process Analytics Framework

15
GWAS Of Cystic Fibrosis Lung Disease
Using A Variable Number Of Tandem Repeats Called From Long-Read Sequencing

16
Data Science To Optimize Cardiovascular Disease Prevention

17
The Impact Of Co-Occurring
Chronic Pain And Depression/Anxiety In The Us

18
The Search For Novel DNA Viruses In Alzheimer's Disease Brains

19
Quantifying the Effect of Joint Calling

20
All Of Us Ancestry Concordance Across Tools

21
Investigating the Role of the X-Chromosome in Autoimmune Diseases:
A Bioinformatics Approach Leveraging Single-Cell Genomics

22
Enhancing Harmful Covariate Shift Detection in Medical Imaging with LoRA

23
Exploring the Impact of Environmental and Climate Exposures and Social Determinants of Health (SDoH) on Multiple Sclerosis (MS)

24
MISTRAL
Dynamic Data Analysis of Security Threats within Biomedical Research Environments

25
Evaluating Long-Read Breakend Calls

26
Monitoring Spartina Alterniflora Using Self-Supervised Learning

27
GANLA
GPU Accelerated Network Layout Algorithm

28
Evaluation of Transcript -Guided Cell Segmentation
on GBM-Derived Single Molecule Spatial Transcriptomics Data

29
Enhancing Named Entity Normalization in Biofactoid Using NLP Techniques

30
Understanding Mistakes in Variant Calling

31
Distributed Dataloader for Spatial Transcriptomics

32
AI for Examining Commercial Determinants of Health in Online Gaming and Gambling

33
Making Climate Hazard Risk Data Useful for North Carolina Communities

34
Further Developing Duke's Wearable Infection Detection Platform

35
Multi-Omics Data Analysis and Visualization
to Investigate the Molecular Profile of Breast Cancer Cells in anOrgan-on-a-Chip Model

36
ThunderPack for EHR Ingestion

37
A Textual Analysis of Agricultural Research

38
Exploring Novel Machine Learning Techniques
for Brain Computer Interface (BCI) Applications

39
Refining and Evaluating the Usability of a Maternal Health Equity Dashboard

ARTFICIAL INTELLIGENCE

40
3D Printing Failure Detection and Analysis

41
Arabic NLP
Generating Multiple Choice Questions of Saudi Schoolbooks

42
Deep Learning-Based Fault Detection System
for Structural Defects in Nano-Quadcopters

43
ChartWise
Case-Specific Multimodal Tool for Enhanced Data-Driven Analytics

44
A Cost-Efficient, LLM Routing System

45
Customized Hybrid Deep Learning Approach
for Symptom-Driven Pneumonia Diagnosis
(Pneumonia Diagnosis Assistant)

46
Recognition of Recyclable Materials using Real-time Object Detection

47
Autonomous UAV Swarms for Wildfire Combat Utilizing Swarm Intelligence

48
Zero-shot Multimodal Video Querying with Adaptive Candidates Ranking

49
Leveraging Language Models for Islamic Question and Answering Systems

50
MedTwin
Biomedical Knowledge Graphs for Early Prognosis of Diabetes Using Digital Twin Technology

51
Real-Time Intelligent Control System to Address Faults for DC Motors

52

Hurricane Trajectory Prediction

53

Automated Classification of Parkinson's Gait Severity
Through Activity Recognition

54

AI-Driven Text Simplification
Unraveling Complex Sentences

55

FARAH-Chatbot
Fine-Tuned Arabic Response for Assessment of Mental Well-being in Pediatrics

56

BreachSeek

57

Enhancing Video Frame Interpolation
A Depth-Aware UNet with Residual and Attention Mechanisms

58

Augmenting Phi-3 for Arabic
Granting LLMs Multilingual Capability with Minimal Training Time

59

Detection of Brain Diseases Using Advanced Deep Learning Techniques

60

The Meeting Wizard
Unlock the Power of In-person Meeting Using LLM + LAM Capabilities

61

Fault Detection for Industrial Robotic Arm

62

Lightweight Model for Saliency Prediction

63

Beneath the Waves
Leveraging SAM for Coral Reef Dataset Generation and Advanced Vision Models

64

Insight
Analysis Using AI

65

AF-100 Tactical Target Differentiation

66

SunAgent

67

Accelerated Post-Disaster Recovery
An AI-Powered System for Damage Assessment and Reconstruction Prioritization

أكاديمية كاوست
KAUST ACADEMY

جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

KAUST ACADEMY SPECIALIZATIONS PROGRAM SPONSORED BY

CYBER SECURITY

الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

SITE
الشركة السعودية لتقنية المعلومات
Saudi Information Technology Company

ARTIFICIAL INTELLIGENCE & BIOINFORMATICS SPONSORS

NEOM نيوم

SAUDI BUSINESSMEN

AbdulRehman Alagil Sons (Jairi Investment)

Ahmed Alagil

Tarek Othman Alkasabi

Eng.Abdullah Bugshan

SUCCESS PARTNERS































KAUST
Academy

SECTION 1

CYBER SECURITY.



academy.kaust.edu.sa

01

ENHANCING PRIVACY IN CRITICAL AGENCIES IDS: DECENTRALIZED AI WITH FEDERATED LEARNING


ZEYAD ALAMOUDI


ABDULAZIZ ALSHARIF

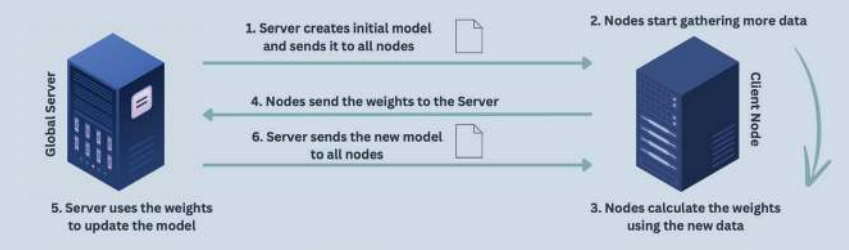

ANAS ALZAHRANI

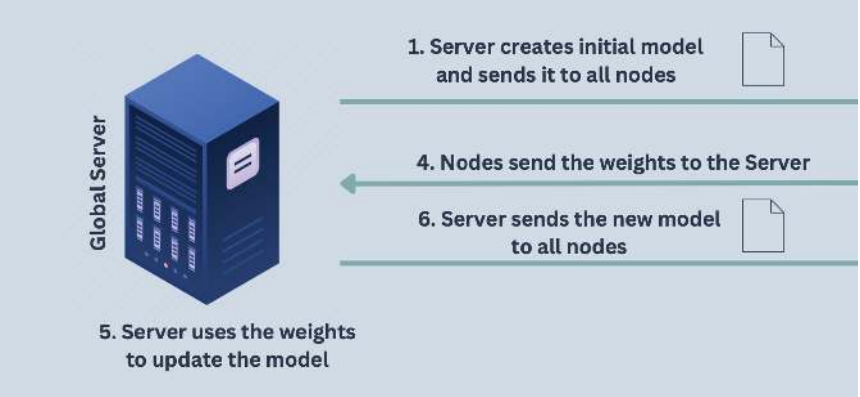

AMMAR ALSHEHRI

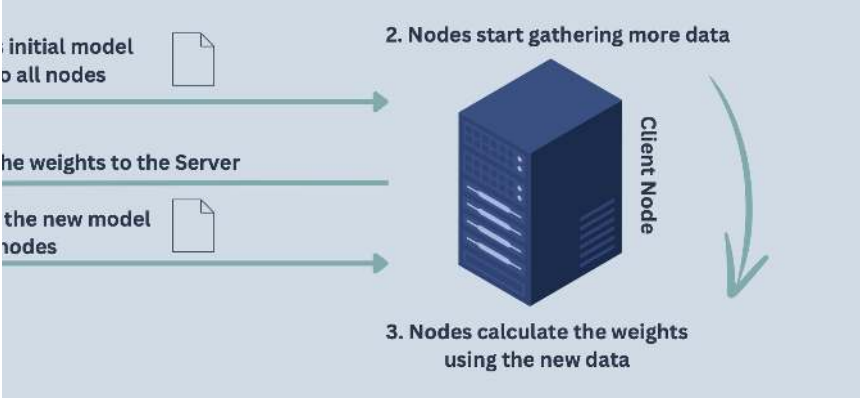

FAISAL BALAMASH

The project enhances privacy in government and critical agencies by using a decentralized approach to train AI models for detecting security threats. Instead of sharing sensitive data, agencies only share the insights gained from their data, ensuring privacy.

This method allows agencies to work together securely, improving their ability to detect and prevent cyberattacks while keeping their data safe and meeting privacy regulations.


1. Server creates initial model and sends it to all nodes
2. Nodes start gathering more data
Global Server
Client Node
4. Nodes send the weights to the Server
6. Server sends the new model to all nodes
5. Server uses the weights to update the model
3. Nodes calculate the weights using the new data


1. Server creates initial model and sends it to all nodes
Global Server
4. Nodes send the weights to the Server
6. Server sends the new model to all nodes
5. Server uses the weights to update the model


initial model
all nodes
2. Nodes start gathering more data
he weights to the Server
the new model
nodes
Client Node
3. Nodes calculate the weights using the new data

02

PENTPEEK - AN INTEGRATED DYNAMIC APPLICATION SECURITY TESTING (DAST) TOOL


YARA ALMANEE


NORAH ALMACKENZY


WASAN THABIT

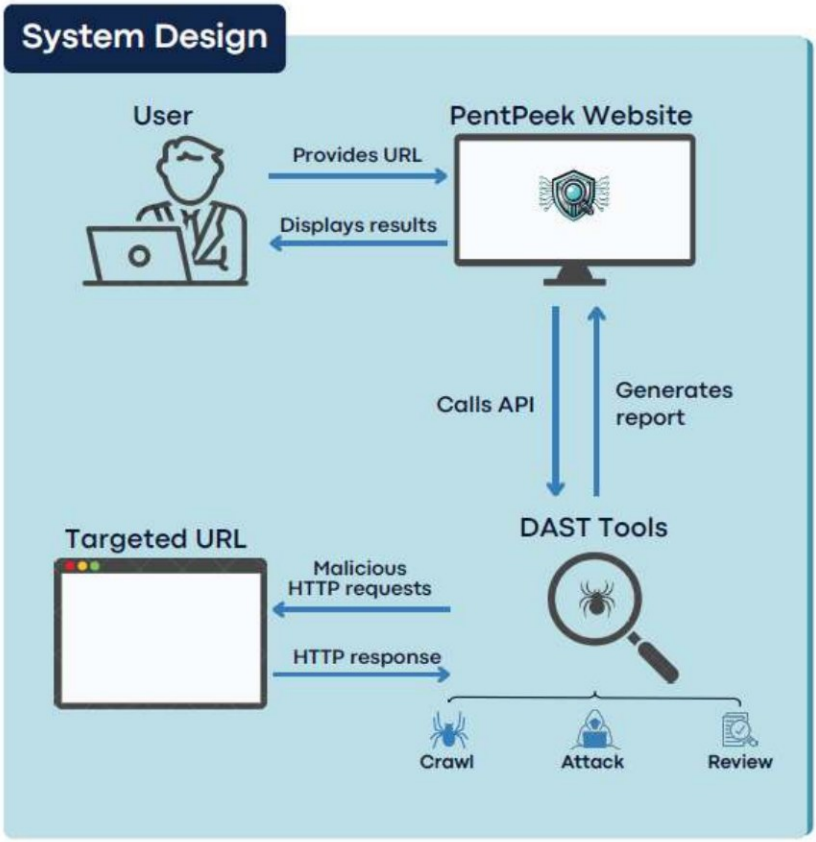

ATHEER ALEYADHY


JUMANAH ALHARBI

Our project, PentPeek, is built on Dynamic Application Security Testing (DAST), which is a method that identifies security vulnerabilities in web applications by simulating real-world attacks.

With PentPeek, users can select specific vulnerabilities they want to test for, and the tool will automatically run tests using a selection of trusted penetration testing tools.

The results are then compiled into a clear, comprehensive report. This user-friendly tool combines in-depth analysis with an intuitive interface, making it easier to secure web applications.


System Design
User
PentPeek Website
Provides URL
Displays results
Calls API
Generates report
DAST Tools
Targeted URL
Malicious HTTP requests
HTTP response
Crawl
Attack
Review

03

LUMIN:
BLOCKCHAIN-BASED SOLAR ENERGY MANAGEMENT SYSTEM


SAHAR FAISAL JAMANI


RAMA AHMED ALSAFRY


RAWAN IBRAHIM ALSHAYIB


SARA MOHAMMED ALTURK

Lumin is a blockchain-based decentralized energy management system designed to address the limitations of centralized control within Saudi Arabia's rapidly growing renewable energy sector. Targeting high-profile initiatives such as NEOM, KAUST, and Red Sea Global, Lumin aims to enhance the security, transparency, and efficiency of solar energy management.

Leveraging blockchain technology, Lumin facilitates peer-to-peer energy trading, allowing users to buy and sell solar energy with ease and efficiency. This approach ensures transaction security and data integrity, while also optimizing the management of energy surpluses and shortages.

The system features an advanced user interface for monitoring energy usage and trading, and a comprehensive management interface for detailed performance monitoring of each solar panel. By integrating these capabilities, Lumin promotes the adoption of solar energy and supports a cultural shift towards renewable energy solutions.

Aligned with Saudi Arabia's Vision 2030, Lumin supports sustainable energy strategies and strengthens the country's significant investments in renewable energy infrastructure.

Lumin: Blockchain-Based Solar Energy Management System

Rawan AlShayib, Rama AlSafry, Sahar Jamani, Sara AlTurk

INTRODUCTION

The energy sector in Saudi Arabia, including projects like **NEOM, KAUST** and **Red Sea Global** faces growing cyberattack risks, leading to financial losses. Our **blockchain-based decentralized solar energy management** project offers a secure, efficient solution by enabling **transparent, tamper-resistant transactions,** reducing reliance on centralized systems, and supporting Vision 2030's renewable energy goals.

$266 B Investments in Renewable Energy by 2030

$10 B Global Annual Cyberattack Losses in the Energy Sector

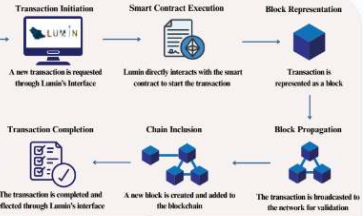
PROBLEM STATEMENT



METHODOLOGY



Figure 1: Real-world Solar Panels Environment.



TOOLS



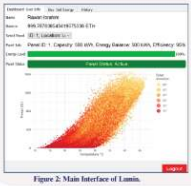


Figure 2: Main Interface of Lumin.

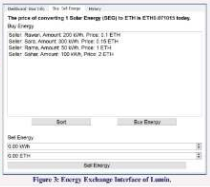


Figure 3: Energy Exchange Interface of Lumin.



Figure 4: Management Interface of Lumin.

OBJECTIVES



SECURITY FEATURES



CONCLUSION

- Enhanced Energy Management System.
- Successful application of blockchain technology.
- User Friendly System.

LEARN MORE

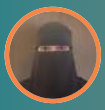
04

INTERNALEYE: INSIDER THREAT DETECTION USING MACHINE LEARNING


RAGHAD ABDULMONEM


LARA SAAD

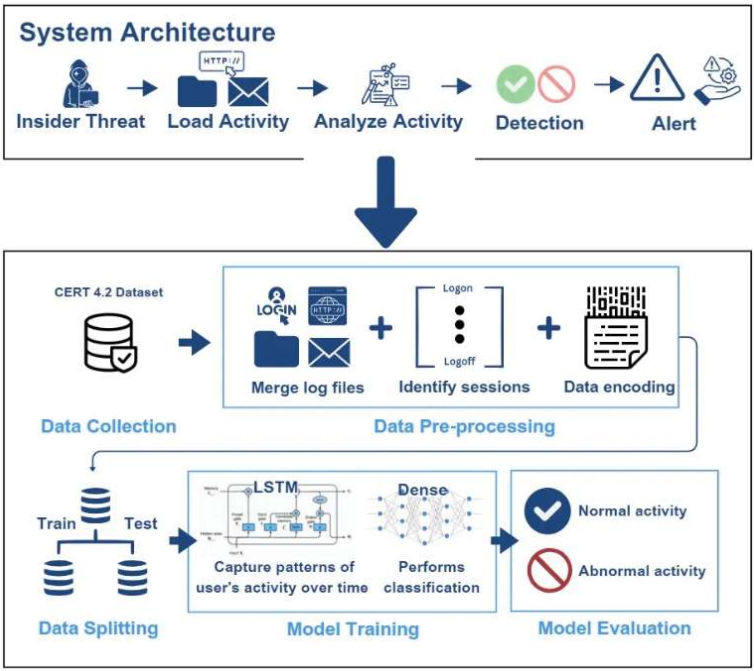

RAGHAD SALEH


BAYADIR SULTAN


REEMA MOHAMMAD


MONA MOHAMMEDSAEED

Insider threats are a critical challenge to organizational security, often evading traditional detection methods. This study proposes a machine learning approach using Long Short-Term Memory (LSTM) networks combined with dense layers to detect insider threats. By analyzing temporal patterns in user behavior, the LSTM model learns normal activity and identifies deviations as potential threats. The proposed method is evaluated on benchmark datasets, demonstrating improved detection accuracy and reduced false positives compared to traditional models. This approach offers a robust solution for enhancing the detection of insider threats in organizational environments.


System Architecture
Insider Threat
Load Activity
Analyze Activity
Detection
Alert
CERT 4.2 Dataset
Merge log files
Logon
Logoff
Identify sessions
Data encoding
Data Collection
Data Pre-processing
Train
Test
Data Splitting
LSTM
Dense
Capture patterns of user's activity over time
Performs classification
Model Training
Normal activity
Abnormal activity
Model Evaluation

05

DECENTRALIZATION OF FINANCIAL TRANSACTIONS USING BLOCKCHAIN TECHNOLOGY (DFTBT)


OMAR ALJANDAL


ABDULAZIZ ALSUDAIS


AHMAD AL ARFAJ

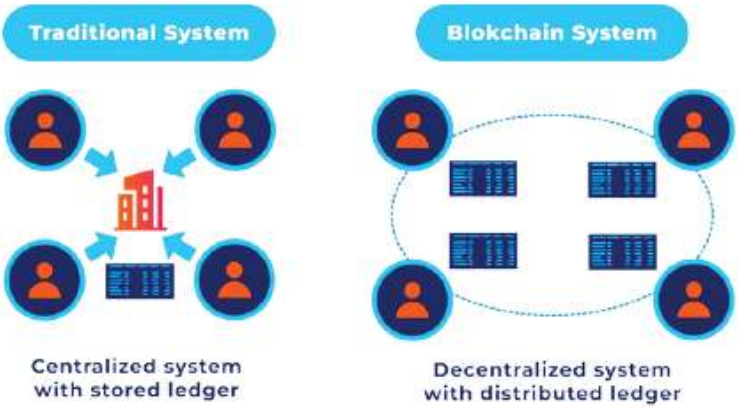

ALI BABTAIN

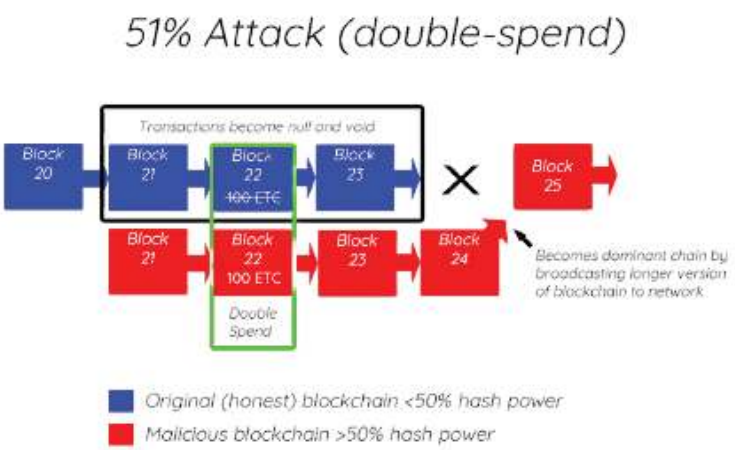

TARIQ ALABISI

Decentralization of Financial Transaction using Blockchain Technology (DFTBT) is a digital currency designed to facilitate secure, transparent, and decentralized financial transactions.

DFTBT operates on a peer-to-peer network without relying on traditional financial intermediaries. Its blockchain-based infrastructure ensures that all transactions are recorded on a public ledger, providing transparency and security.

DFTBT aims to enhance financial autonomy by allowing users to conduct transactions directly, promoting a decentralized approach to finance. The currency is designed with a focus on scalability and efficiency to support widespread adoption in the digital economy.


Traditional System
Blokchain System
Centralized system
with stored ledger
Decentralized system
with distributed ledger


51% Attack (double-spend)
Transactions become null and void
Block 20
Block 21
Block 22
100 ETC
Block 23
Block 25
Block 21
Block 22
100 ETC
Block 23
Block 24
Becomes dominant chain by broadcasting longer version of blockchain to network
Double Spend
Original (honest) blockchain <50% hash power
Malicious blockchain >50% hash power

06

PHISH ME IF YOU CAN - DETECTING PHISHING WEBSITES USING MACHINE LEARNING



MUATH KHALID



ABDULLAH EMAD

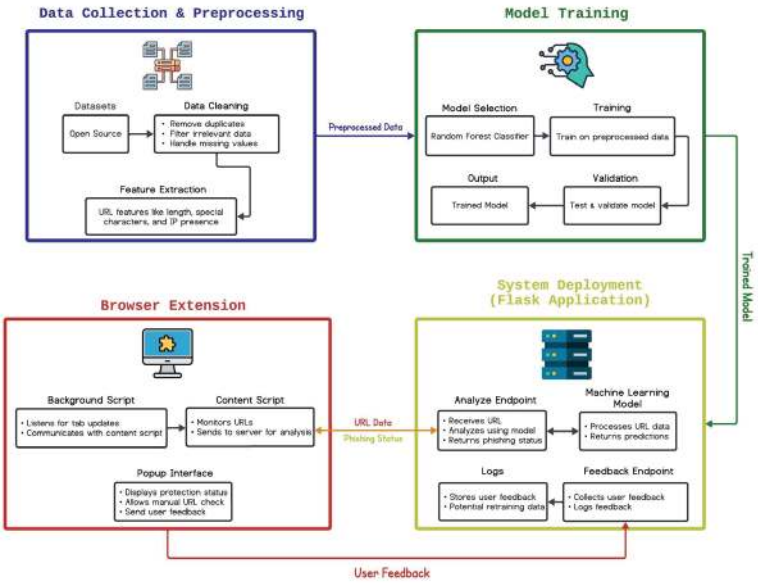


ABDULRAHMAN IBRAHIM

Phishing attacks pose a significant threat to online security. Our project, "Phish Me If You Can", addresses this issue by developing a machine learning-based browser extension that detects and blocks phishing websites in real-time.

Utilizing a Random Forest classifier, our solution analyzes URL characteristics to accurately identify phishing attempts. The browser extension not only provides real-time alerts but also integrates with Security Operations Centers (SOC) for enhanced monitoring.

Additional features include a URL Check function and a user feedback loop to continuously refine the detection model, ensuring robust and adaptive protection against evolving phishing threats.


Data Collection & Preprocessing
Datasets
Open Source
Data Cleaning
• Remove duplicates
• Filter irrelevant data
• Handle missing values
Feature Extraction
URL features like length, special characters, and IP presence
Preprocessed Data
Model Training
Model Selection
Random Forest Classifier
Training
Train on preprocessed data
Output
Trained Model
Validation
Test & validate model
Trained Model
System Deployment (Flask Application)
Browser Extension
Background Script
• Listens for tab updates
• Communicates with content script
Content Script
• Monitors URLs
• Sends to server for analysis
Popup Interface
• Displays protection status
• Allows manual URL check
• Send user feedback
URL Data
Phishing Status
Analyze Endpoint
• Receives URL
• Analyzes using model
• Returns phishing status
Machine Learning Model
• Processes URL data
• Returns predictions
Logs
• Stores user feedback
• Potential retraining data
Feedback Endpoint
• Collects user feedback
• Logs feedback
User Feedback

07

ENHANCING MALWARE **ANALYSIS** USING AI


MOHAMMED ALQURASHI


HUSAM HADDAD


ABDULRAHMAN AL MUTAIRI


HUSSAIN BABONGI

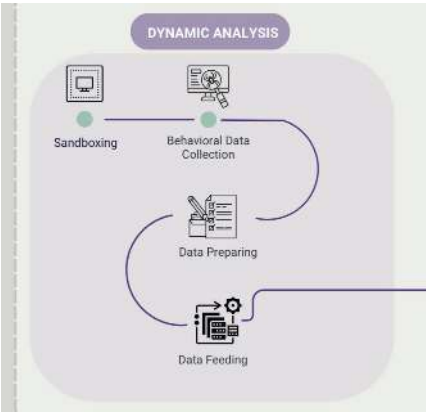

ABDULLAH ALGHAMDI

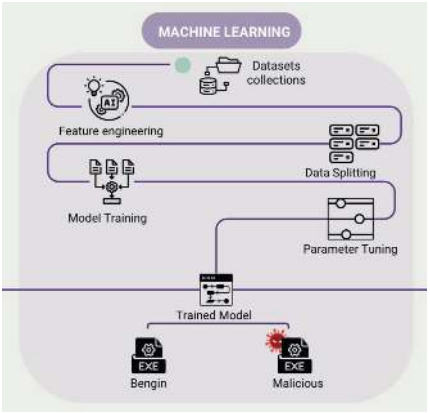

MOHAMMED ALMALKI

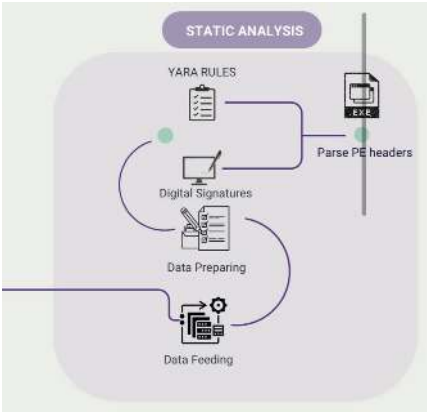
This system uses AI to provide a comprehensive solution for malware analysis, integrating both dynamic and static techniques. Users submit malware samples, which are analyzed in a controlled Windows 7 64-bit sandbox environment.

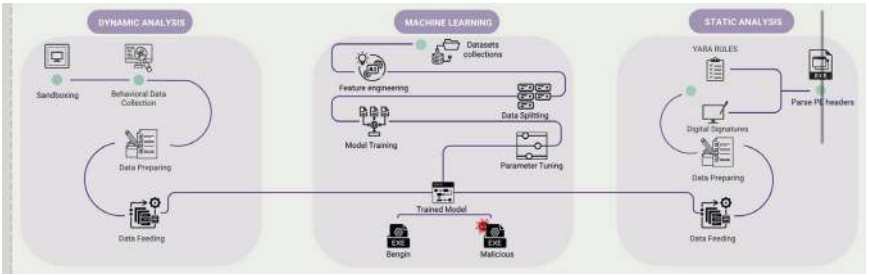
Dynamic analysis observes and records key interactions like API calls, while static analysis examines the file's structure using PE header parsing, Yara rules, and digital signature verification. Machine learning models are employed in both analysis stages for accurate malware classification.

The system then delivers clear results, including classification, behavioral reports, and structural insights, aiding cybersecurity professionals in threat mitigation.


DYNAMIC ANALYSIS
Sandboxing
Behavioral Data Collection
Data Preparing
Data Feeding


MACHINE LEARNING
Datasets collections
Feature engineering
Data Splitting
Model Training
Parameter Tuning
Trained Model
EXE
Bengin
EXE
Malicious


STATIC ANALYSIS
YARA RULES
EXE
Parse PE headers
Digital Signatures
Data Preparing
Data Feeding


DYNAMIC ANALYSIS
Sandboxing
Behavioral Data Collection
Data Preparing
Data Feeding
MACHINE LEARNING
Datasets collections
Feature engineering
Data Splitting
Model Training
Parameter Tuning
Trained Model
EXE
Bengin
EXE
Malicious
STATIC ANALYSIS
YARA RULES
EXE
Parse PE headers
Digital Signatures
Data Preparing
Data Feeding

08

DRONE SECURITY TESTING FRAMEWORK



MOHAMMAD MAZEN ALMAHALLAWI



ASIM ABDULRAHMAN BARNAWI



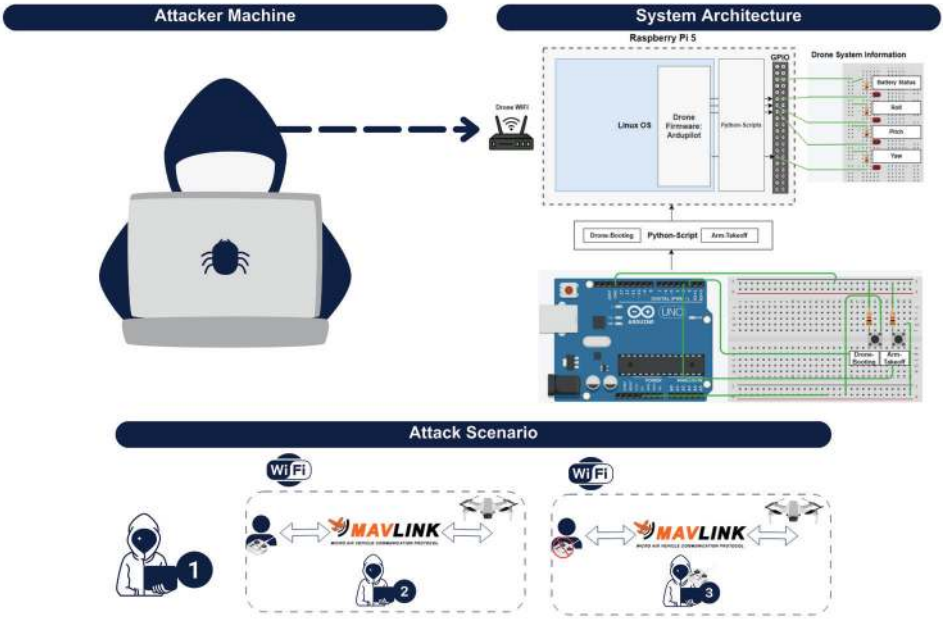
ANAS RAJAB ABDULLAH



ANAS MOHAMMED ALAMRI

The "Drone Security Testing Framework" is designed to assess and enhance the security of unmanned aerial vehicles (UAVs) by simulating real-world attack scenarios. This framework deploys the ArduPilot firmware in a system-in-the-loop (SITL) environment on a Raspberry Pi, with a basic remote controller built using Arduino, featuring two buttons for drone boot/reboot and takeoff. To keep the testing process budget-friendly and risk-free, key drone information such as roll, pitch, yaw, and battery status are visually represented using LEDs connected to the Raspberry Pi's GPIO pins.

The framework includes a comprehensive suite of attack modules that focus on exploiting vulnerabilities in drones. These modules cover a range of attack types, including Wi-Fi Deauthentication, Attitude Spoofing, System Fault Injection, Camera Feed Eavesdropping, and more. The framework guides users through the attack lifecycle, starting with the identification of the drone's Wi-Fi network, capturing packets to crack encryption, and then executing targeted attacks on the drone's data-link connection. By providing a controlled environment for testing, this framework aims to strengthen drone security by identifying weaknesses before they can be exploited in the real world.


Attacker Machine
System Architecture
Raspberry Pi 5
GPIO
Drone System Information
Drone WiFi
Linux OS
Drone Firmware: Ardupilot
Python Scripts
Battery Status
Roll
Pitch
Yaw
Drone Booting
Python-Script
Arm-Takeoff
Attack Scenario
WiFi
MAVLINK
WiFi
MAVLINK
1
2
3

09

SAFEPOST:
AI-POWERED POST PII DETECTION



HAYAT HASHIM ALZAHRANI



RAHAF BANDAR ALGARNI



LAYAN FAISAL ALABOUDI

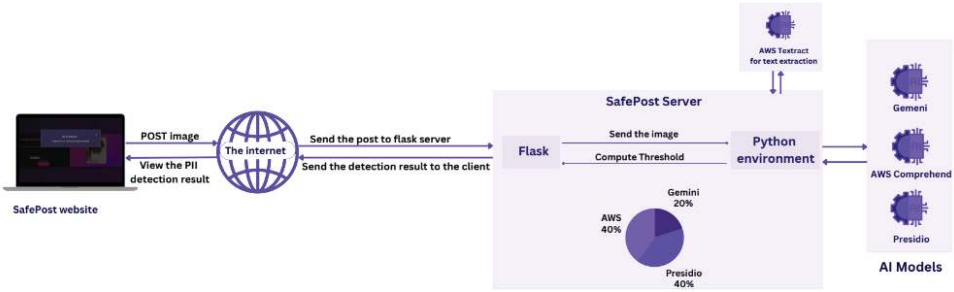


RETAJ KHALED ALGHAMDI

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity. With the rise of social media, people are increasingly sharing sensitive information and PII, often without realizing the potential risks.

This oversharing can lead to serious privacy breaches, including identity theft, harassment, and other malicious activities. Despite existing platform warnings, many users remain unaware of the dangers, making it crucial to develop tools that help safeguard their privacy. Our project utilizes AI to analyze posts shared by users on our dummy social media platform, detecting PII and alerting users to potential privacy risks before they publish their content.

The process starts by the user uploading an image to the SafePost website, which is then sent to the SafePost server. The server processes the image using the AWS Textract for text extraction, followed by analyzing the extracted text with three AI models—Gemini (0.2), AWS Comprehend (0.4), and Presidio (0.4)—to detect any PII. A weighted threshold is then applied, where the total weight is compared against a threshold of 0.7 to determine if PII is present before sending the detection result back to the user. SafePost aims to enhance user privacy by proactively detecting and alerting users about the sharing of sensitive information. This functionality can be integrated into today's social media platforms, offering proactive


SafePost website
POST image
View the PII detection result
The internet
Send the post to flask server
Send the detection result to the client
SafePost Server
Flask
Send the image
Compute Threshold
Python environment
AWS Textract for text extraction
Gemini
20%
AWS
40%
Presidio
40%
Gemeni
AWS Comprehend
Presidio
AI Models

10

COMPLIANCE COMPASS: AUTOMATED CYBERSECURITY ADHERENCE


AZZAM TURKISTANI


MOHAMMED ALSAYED


OMAR DAYILI


OSAMA ALDOSSARY

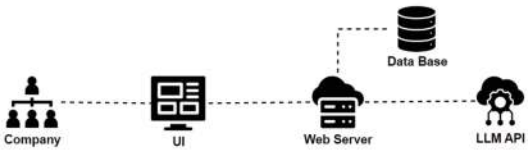

SALMAN ALDHALAAN

Cybersecurity compliance presents significant challenges for organizations worldwide. As companies allocate substantial portions of their cybersecurity budgets to compliance efforts, manual processes have shown limitations and are susceptible to errors.

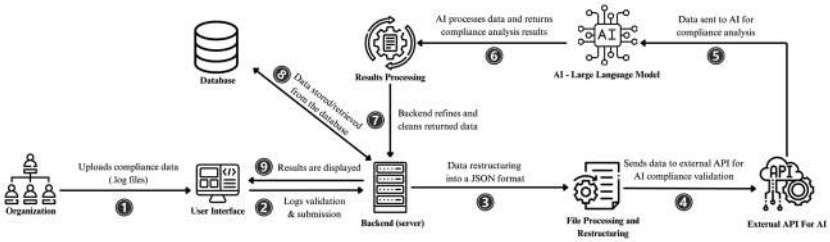
The "Compliance Compass" project offers an automated solution that utilizes Large Language Models (LLMs) to generate comprehensive compliance reports. This system reduces the time and costs associated with compliance management while enhancing accuracy by prioritizing higher-impact standards in the compliance scoring process. Through an intuitive interface, organizations can effectively evaluate their compliance status, identify gaps, and receive actionable recommendations for improvement.

The results demonstrate the system's ability to reduce manual effort and mitigate compliance risks, making it a valuable tool for strengthening an organization's cybersecurity posture.

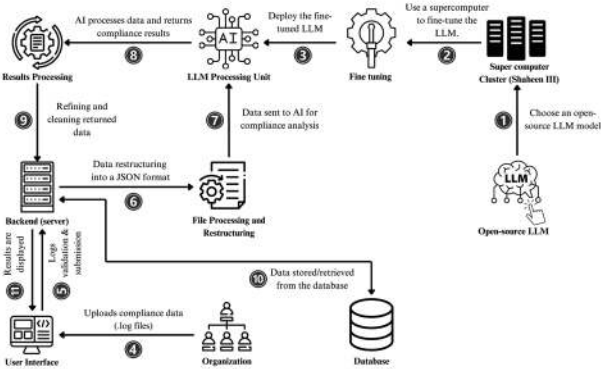
System Architecture



Data flow



In-progress Data flow



COOKIEGUARD: COOKIES & THE DARK WEB

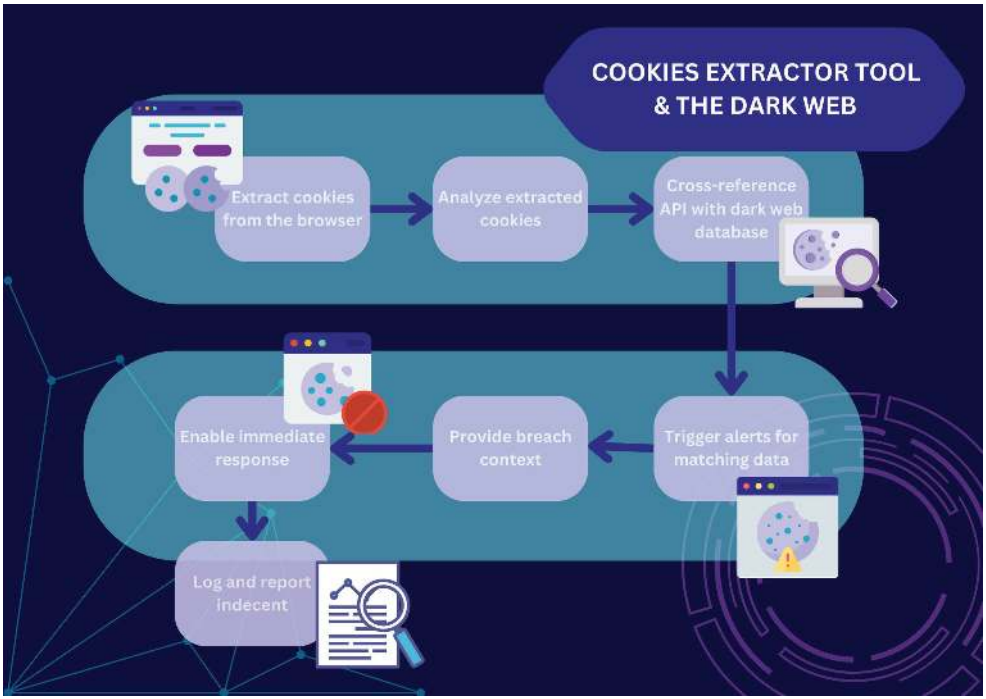

AMIRAH ALTURKI


LAMA ALHAZMI


DANAH ALREHAILI


FOTOON SAMMAN

In the hidden corners of the dark web, stolen cookies are traded like digital assets, granting unauthorized access to online services and violating user privacy, posing a growing threat to personal security. Current forensic tools lack in-depth cookie analysis and dark web integration, leading to incomplete investigations and prolonged exposure to security threats. This is where our project comes in, we built a forensic cookie extractor tool that not only extracts and analyzes cookies from various web browsers but also integrates with dark web monitoring services. This integration allows the tool to cross-reference extracted cookies with known dark web databases, providing real-time alerts if any cookies have been compromised and are being traded illicitly.


COOKIES EXTRACTOR TOOL
& THE DARK WEB
Extract cookies from the browser
Analyze extracted cookies
Cross-reference API with dark web database
Trigger alerts for matching data
Provide breach context
Enable immediate response
Log and report indecent