أكاديمية طويق
Tuwaiq Academy

YAQITH SENTINEL

هاكاثون
أبشر طويق

YAQITH Sentinel

12/1/2025

YAQITH SENTINEL

It integrates expertise in business analytics, user experience, and artificial intelligence to deliver an innovative and secure system.

Team members

Al-Walah Awaji

Glory of the Companion

Eman Al-Dorsi, Marwa Al-Rajhi, Arwa Al-Khairbi, Project Title: YAQITH Sentinel

The problem

Fixed definitions alone for detection

How can we prevent identity fraud when traditional credentials and biometric data can be stolen, copied, or impersonated? This is not enough to prevent real-time identity theft, which puts systems and users at risk.

to

Ha and

Implementing a dual-layer identity system that integrates the Alite family:

Official digital identity (national identity, civil registry, biometric data).

The

identity is constantly verified in real time. It is linked to the device, unique to the user, and which

Behavioral fingerprint

Enhanced security through the introduction of an AI-based verification layer and behavior analysis.

Reducing cyber risks resulting from identity theft attacks and silent intrusions.

Improved user experience by providing added security without compromising ease of login.

Building a score risk system based on behavior, device, and location to determine entry risks.

Contents

Types of data used

33%

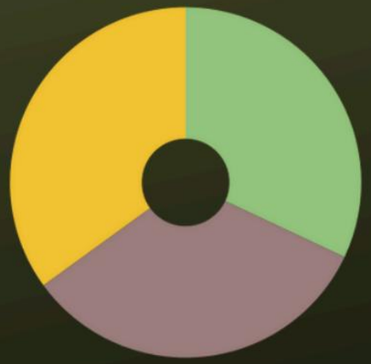
Non-textual data:

User behavior within the application:

Typing speed

Touch pattern on the screen

Time Navigation (time between pages)



32%

Text data:

Login Logs

Times and dates for each login attempt

Verification messages or alerts

35%

Device and network data:

Device ID, Device Type, Version

IP address and geographical location

Charts and graphs:

Dashboards to display suspicious or normal login attempts

Data cleaning and processing

Remove any personal data immediately to maintain privacy;

handle missing or duplicate values.

Digital data normalization such as write speed or compression time

Converting data into a format suitable for training the artificial intelligence model

Analyzing graphical data and creating usable features in the model

Data sources

Internal system records (Logs Login and device data)

An in-app SDK for collecting user behavior data

A simulated login process to generate sample data without compromising privacy

Anonymized public data for pattern analysis without exposure to sensitive information

Challenges in data collection

include the difficulty of accessing real user data for testing purposes due to privacy conce

The variation in devices and systems used affects the measured user behavior.

Insufficient data to train a robust AI model, especially for behavioral biometric data,

and encrypted during transmission and processing. necessitates processing at data is secure

The system uses various data: device fingerprint, browser/application signature, IP and location history, behavior patterns, and usual login times.

Quick visualization of each data type. • Saudi Data Protection Law: Privacy statement: anonymized, compliant with [the relevant law/policy].

Technologies used

Identity Standards
W3C DID, Verifiable Credentials (VC), FIDO2 / WebAuthn.

Backend Technologies
Real-time stream processing, secure APIs, encrypted data pipelines.

Privacy & Security Frameworks
Local data processing, differential privacy, encrypted behavioral hash maps.

Real-time Stream Processing Low-latency behavioral data handling and secure event pipelines.

Encrypted Behavioral Hash Maps
Secure storage and matching of behavioral patterns using encrypted hashing.

Behavioral Biometrics Engine
Typing patterns, touch pressure, navigation rhythms, accelerometer patterns.

Machine Learning Models
Anomaly detection, continuous authentication, risk scoring.

Mobile Device Signals
Device-ID binding, secure enclave, hardware attestation.

Hardware Attestation
Device integrity verification using Secure Enclave and trusted execution environments.

Continuous Authentication Models Real-time identity verification using multi-signal behavioral patterns.

Describing the idea

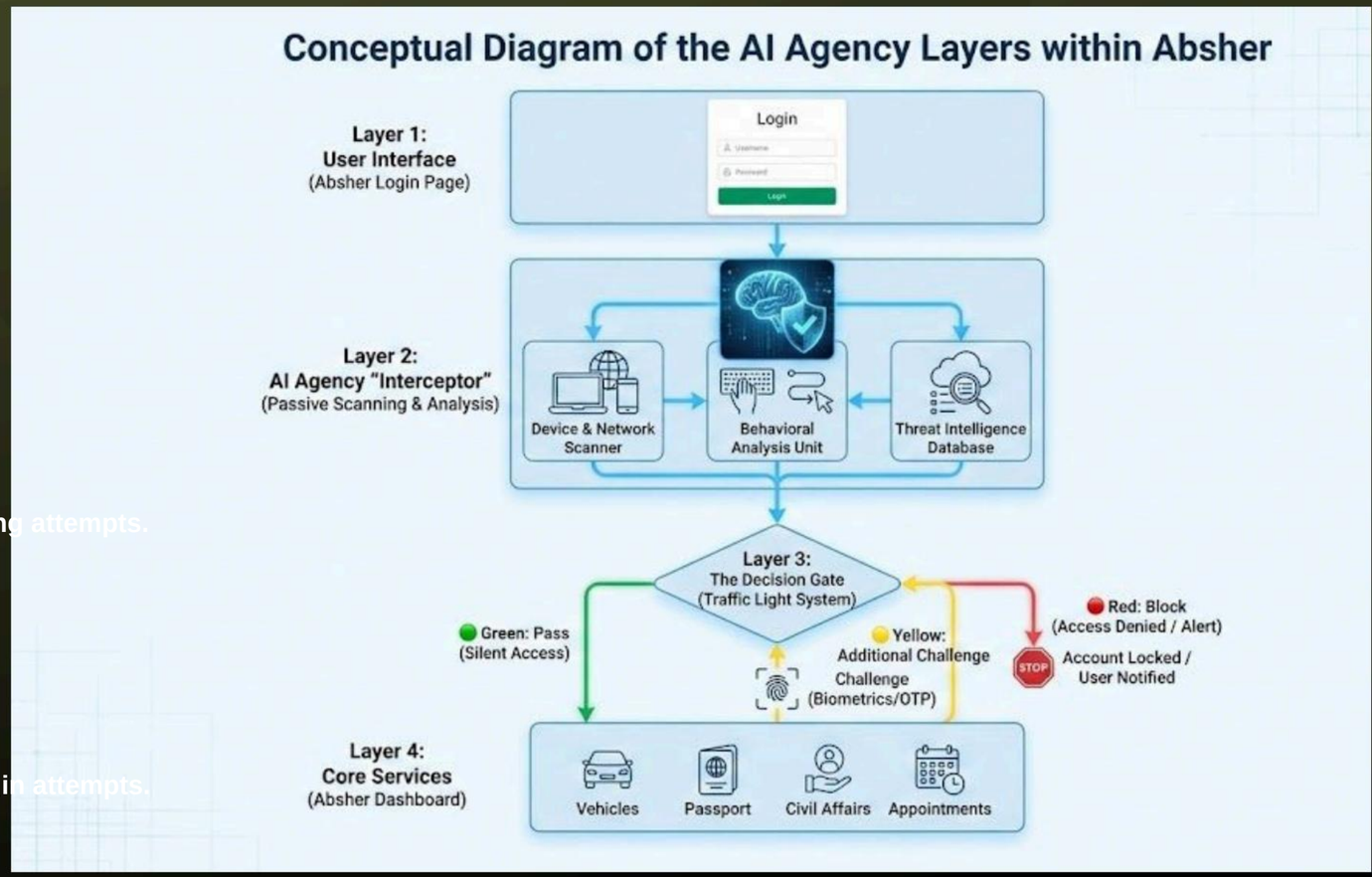
the address

The Sentinel YAQITH project was developed to address the security and user identity verification issue within the Abras platform in a smart and personalized way. The agent acts as a constant guardian for each user, analyzing data related to the device used, browser or application, internet network (IP and location), and user behavior within the system immediately upon login. It also verifies the user's identity and the time of login to ensure authenticity.

A two-layer identity system combines a formal digital identity with a device-associated behavioral identity that the user natur

The fundamental innovation lies in using artificial intelligence to analyze these elements in real time and accurately, with the ability to learn from the user's usual behavior and adapt to any natural changes, thus ensuring differentiation between natural access and hacking attempts.

After analysis, the system allows seamless access to the account in case of full compliance, while applying additional verification procedures in case of any doubt, such as verification codes or facial recognition, while notifying the user of suspicious login attempts.



How do I provide this data and how do I use i

- Device data: such as device type, operating system, browser or application used, to identify familiar devices for the user.
- Network and location data: IP address, geographic location, network type, to verify usual access points.
- Login history: login times, previously used devices.
- User behavior within the system: typical activities within the account, frequency of service use, time spent on each service, to distinguish normal behavior from unusual activities.
- Additional security indicators: such as failed login attempts or sudden account changes, for early detection of potential breaches.

This data is used for:

Continuous security improvements

Personalizing the user experience

Detecting suspicious activities

Verify the identity

Aligning the idea:

Advanced in digital identity and security, Arabs integrate official identity with a behavioral fingerprint linked to a device. The idea aligns with the competition's theme because it presents a This enhances user trust, reduces fraud, and raises the security level of national services without inconveniencing the user. It also supports digital transformation initiatives, identity protection, and improved quality of government services.

The idea aligns with the competition's theme of promoting digital security, as Sentinel YAQITH ensures account protection from hacking and fraud using advanced verification and early detection of suspicious activities.

Project Summary

The Sentinel YAQITH project within the Abras platform aims to create an intelligent layer that enhances digital security and supports users' digital identity through advanced identity verification and early detection of suspicious activity. The system analyzes device, network, and behavioral data to determine if the user is the legitimate account holder, without compromising ease of use.

High level of protection in

The project's outputs consisted of creating a model for an agent capable of detecting normal user behavior patterns, reacting to any unusual changes, and activating additional verification procedures when needed. The Initial results have shown significant effectiveness in enhancing security, reducing hacking attempts, and supporting better integration with the digital identity system and government applications.

The project provides a future vision for artificial intelligence applications in government services, combining advanced protection with a seamless user experience, thereby enhancing trust in digital platforms and supporting the Kingdom’s move towards secure digital transformation.

Testing/Verification:

The abnormal patterns were tested and verified by simulating 100 login attempts; 90% of high-risk attempts were detected and 100% were prevented

0%	100%	90%	100
Error rate in verification	prevention rate for high-risk attempts	Rate of detection of abnormal patterns	Login attempt

YAQITH SENTINEL

Demonstration, screenshots, videos, simulation:

Link to the demo

User login trial link

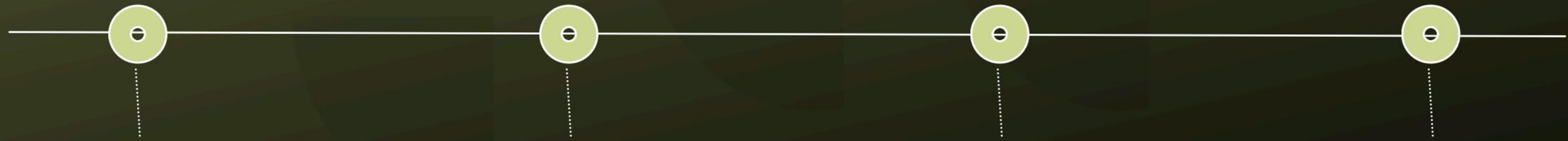
Future plans include developing smarter algorithms to predict risks before they occur.

- Expanding the database to improve the accuracy of artificial intelligence models.
- Integrate the agent with other government systems to increase integration.
- Create an advanced control panel for security monitoring and behavior analysis.
- Improve the verification process to be faster and more user-friendly.

Challenges

- Ensuring data collection and analysis while maintaining the highest privacy standards.
- The difference in user behavior and the diversity of devices and networks used.
- The need for accurate artificial intelligence models that distinguish between normal and suspicious behavior.
- Maintaining performance speed and system stability during real-time analysis.
- Dealing with sophisticated hacking attempts that are constantly changing.

Timeline



Discovery and ideas

Research and analysis

Interface generation
Model design

Building the prototype
MVP

Thank you

أكاديمية طويق
Tuwaiq Academy