METHAQ · CYBERSECURITY & DIGITAL IDENTITY

UNIVERSITY OF HAFR AL-BATIN

Methaq

Intelligent Identity & Access Management with Active Defense

A FIVE-NODE CLOSED-LOOP CYBERSECURITY SYSTEM

College of Computer Science & Engineering
Advisor — Dr. Ibrahim Al-Zahrani

SECOND SEMESTER 2025-2026
MAY 2026

Eight engineers, one covenant.

A senior project built end to end by a team of eight, advised by Dr. Ibrahim Al-Zahrani.

PROJECT LEADER · SYSTEM ARCHITECT Abdulrahman Al-Anazi	APPLICATION & OIDC ENGINEER Mansour Al-Anazi	SECURITY & FRONTEND ENGINEER Abdulmohsen Al-Anazi	FRONTEND & WAF LEAD Abdullah Al-Harbi
INFRASTRUCTURE & IAM LEAD Hamed Salem Al-Anazi	MACHINE LEARNING ENGINEER Faisal Al-Harbi	APPLICATION TESTER · DATA ENGINEER Abdullah Al-Anazi	ACTIVE DEFENSE ENGINEER Yousef Al-Anazi

Identity has become the primary attack surface.

74%

of breaches involve the human element — stolen or weak credentials lead the way

— Verizon DBIR 2023

$4.45M

average cost of a single data breach

— IBM

220%

year-over-year increase in phishing attacks

292

days, on average, to identify and contain a credential breach

Traditional IAM was built for a static world.

01

Static authentication

Multi-factor applies the same challenge regardless of threat. A phished one-time password grants the same access as a legitimate user.

02

No adaptive learning

Firewalls enforce known signatures. They cannot learn from attack patterns they have never seen before.

03

Siloed intelligence

Honeypots capture attacks. Identity providers grant access. The two never share what they know.

A closed loop that couples honeypot-driven attack intelligence with machine-learning risk authentication — so the identity layer *learns from every attack it sees.*

CAPTURE → CLASSIFY → RETRAIN → ENFORCE ↺

Six measurable goals.

Analyze Identity-attack patterns & IAM deficiencies to derive requirements.	**Design** A five-node distributed architecture for the intelligence pipeline.	**Implement** The closed loop from capture through retraining to enforcement.
Test Security via OWASP ZAP, manual pen-testing & STRIDE modeling.	**Evaluate** Accuracy, response time & security-control effectiveness.	**Document** Architecture, implementation & results for reproducibility.

— 07 — SYSTEM ARCHITECTURE

Five nodes, one system.

Each node owns a distinct security responsibility. Together they form a self-improving defense.

01

The Fortress

Methaq IAM — risk-based identity provider

02

The Shield

WAF & public frontend — ModSecurity + CRS

03

The Brain

ML risk engine — FastAPI + ensemble

04

The Trap

Cowrie honeypot — active defense

05

The Demo

Next.js banking app — OIDC / PKCE

□ DEFENDER NODES ■ INTELLIGENCE CORE

• METHAQ

— 08 — THE CLOSED LOOP

How intelligence flows.

Attack data never sits idle. It becomes the next authentication decision.

01

Capture

Cowrie honeypot records live SSH & Telnet attacks.

~5 min

→

02

Classify

Ensemble model scores each pattern's risk.

~2 min

→

03

Retrain

Model refreshes on new attack features with SMOTE.

~12 min

→

04

Enforce

Updated thresholds deploy to Methaq IAM.

~45 sec

↺ FEEDBACK LOOP — AUTHENTICATION LOGS RETURN TO FEATURE EXTRACTION, CONTINUOUSLY

— NODE 01 — THE FORTRESS

Methaq IAM Identity Provider

01

A purpose-built identity provider extended with a custom `RiskScoreAuthenticator` SPI — turning a static gatekeeper into an adaptive enforcement point that queries the ML engine on every login.

PROTOCOL	OIDC · Authorization Code + PKCE
CUSTOM SPI	RiskScoreAuthenticator · EventListener
DATASTORE	PostgreSQL 16 · LUKS2 encrypted
TLS	Caddy 2.7 · TLS 1.3 · A+ SSL Labs
OWNER	Hamed Salem Al-Anazi

— NODE 02 — THE SHIELD

WAF & Public Frontend

02

The system's public face. Nginx reverse-proxies the application behind ModSecurity and the OWASP Core Rule Set — 917 virtual-patch rules inspecting every request in real time.

PROXY	Nginx 1.24 · Next.js 15
WAF	ModSecurity 3.0 · OWASP CRS 3.3.5
RULES	917 OWASP Top-10 signatures
DEFENSE	fail2ban 1.0 · Cloudflare proxy
OWNERS	Abdullah Al-Harbi · Abdulmohsen Al-Anazi

— NODE 03 — THE BRAIN

ML Risk Engine

03

A FastAPI service scoring authentication risk from 15 features. A three-model ensemble — Random Forest, XGBoost and LightGBM — returns a verdict in a median of 118 ms.

API	FastAPI 0.109 · /risk-score
ENSEMBLE	RF 0.3 + XGBoost 0.4 + LightGBM 0.3
RUNTIME	scikit-learn 1.4 · XGBoost · ONNX 1.17
ACCURACY	98.87% · 118 ms median latency
OWNER	Faisal Al-Harbi

— NODE 04 — THE TRAP

Active Defense & Honeypot

04

A Cowrie honeypot emulates a vulnerable server. Kernel-level `iptables` redirect makes the trap invisible — and the source of organization-specific intelligence no static feed can match.

ENGINE	Cowrie 2.6.1 · Docker 24.0
SURFACE	SSH (port 22 → 2222) · Telnet
CAPTURED	4,710+ events · 5,394 unique IPs
REACH	38 countries · first week
OWNER	Yousef Al-Anazi

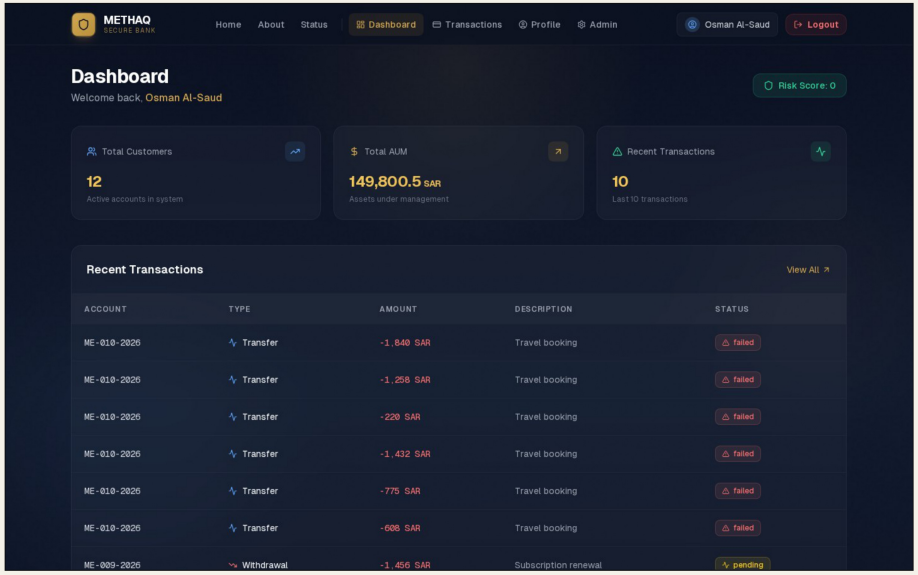
— NODE 05 — THE DEMO

Demo Banking Application

05

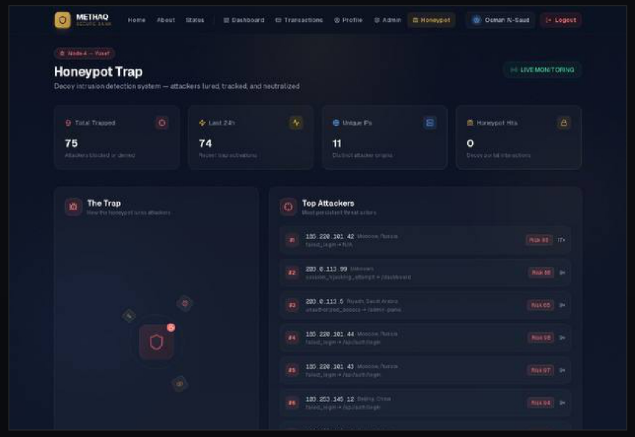
A realistic banking interface that exercises the full flow end-to-end — login through Methaq IAM, then the live verdict: access granted, TOTP challenge, or access denied.

STACK	Next.js 14 · oidc-client-ts 2.2 · SQLite 3.42
OWNERS	Mansour Al-Anazi · Abdullah Al-Anazi

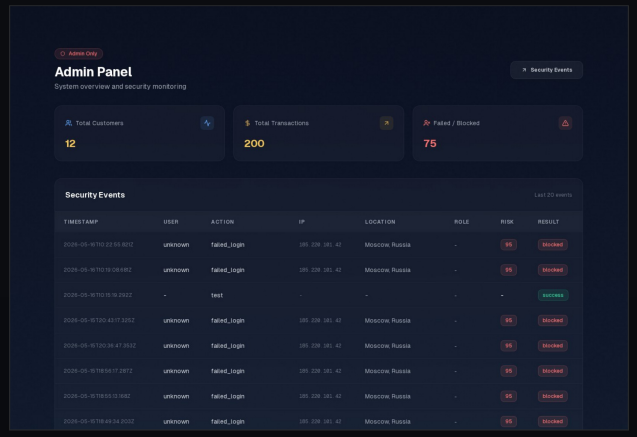


Deployed and live.

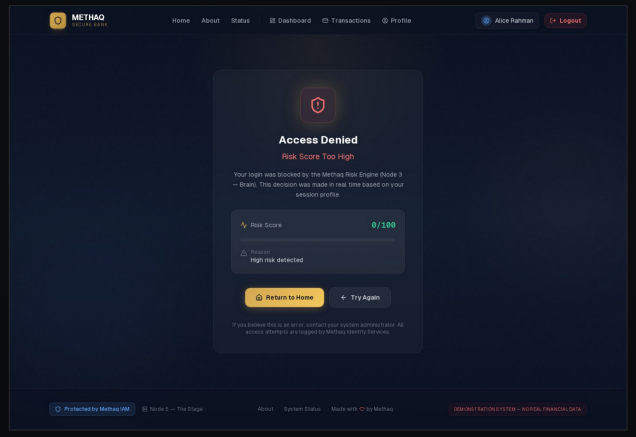
All five nodes are deployed and reachable on owned infrastructure.



N04 The Trap — live attacker capture



N01 Admin — security event audit log



N05 Demo — a risk-based block, in action

Every login is scored 0–100 before access is ever granted.

One score. Three decisions.

0 - 49

Allow

Low risk. Immediate access — the experience is invisible to legitimate users.

50 - 74

Challenge

Elevated risk. Step-up TOTP multi-factor before the session is allowed to continue.

75 - 100

Block

High risk. Session denied and the attempt is written to the audit log.

An ensemble, not a black box.

Random Forest NON-LINEAR FEATURE INTERACTIONS	0.3
XGBoost BEST SINGLE-MODEL PERFORMANCE	0.4
LightGBM FAST, EFFICIENT GRADIENT BOOSTING	0.3

Soft-voting ensemble trained on 45,000 labeled events, balanced with SMOTE to a 50/50 split and exported to ONNX for fast inference.

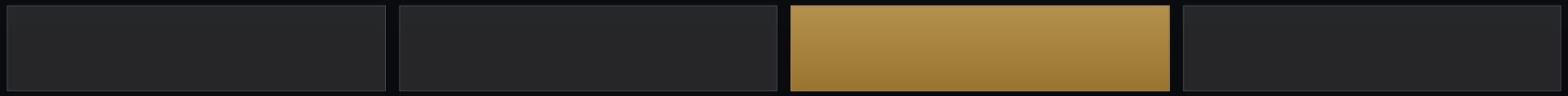
98.87% ACCURACY	99.38% RECALL · MALICIOUS
98.35% PRECISION	98.86% F1-SCORE · MALICIOUS

— 16 — THE 12-MINUTE CYCLE

From attack to adaptation.

12 *min*

VS. WEEKS OF MANUAL RESPONSE · >1,000× FASTER



Capture	Classify	Retrain	Enforce
Honeypot	Ensemble	SMOTE	Methaq IAM

MEASURED END-TO-END — HONEYPOT CAPTURE TO POLICY ENFORCEMENT — ACROSS 10 CONSECUTIVE INTEGRATION RUNS.

— 17 — DEFENSE IN DEPTH

Layered by design.

If any single control fails, another stands behind it.

EDGE	Cloudflare proxy & DDoS filtering
PERIMETER	ModSecurity + OWASP CRS · 917 rules
ACCESS	fail2ban progressive IP blocking · UFW default-deny
TRANSIT	TLS 1.3 · mutual TLS between nodes · A+ SSL Labs
AT REST	LUKS2 full-disk encryption on every node

Tested like a target.

AUTOMATED · OWASP ZAP

0/0

High and medium findings after remediation across all endpoints.

MANUAL PENETRATION

5/5

SQLi, XSS, credential stuffing, session fixation & privilege escalation — all blocked.

THREAT MODELING · STRIDE

6/6

Spoofing through elevation of privilege — each category mapped to a control.

98.87% CLASSIFICATION ACCURACY	118 ms MEDIAN RISK-API LATENCY	4,710+ ATTACK EVENTS CAPTURED
38 COUNTRIES OF ORIGIN	A+ SSL LABS RATING	99.97% 30-DAY UPTIME

Chosen, not defaulted.

IDENTITY

- Methaq IAM 1.0
- PostgreSQL 16
- Caddy 2.7

FRONTEND & WAF

- Next.js 15
- Nginx 1.24
- ModSecurity 3.0
- OWASP CRS

ML & RISK API

- FastAPI 0.109
- scikit-learn 1.4
- ONNX 1.17
- SMOTE

ACTIVE DEFENSE

- Cowrie 2.6.1
- Docker 24.0
- iptables

APPLICATION

- oidc-client-ts 2.2
- SQLite 3.42

INFRASTRUCTURE

- Ubuntu 22.04 LTS
- Hetzner Cloud
- Cloudflare
- LUKS2

Active defense, coupled to identity, works.

Methaq closes the gap between attack detection and identity enforcement — adapting to new threats within minutes, not weeks, with measurable gains in accuracy and resilience.

PHASE 2

- → Native iOS & Android SDKs
- → Multi-region deployment
- → LSTM temporal sequence model
- → System-wide MFA rollout
- → PostgreSQL migration · Node 5

— THANK YOU

Questions & discussion.

Presented by the Methaq team
Led by Abdulrahman Al-Anazi · Advised by Dr. Ibrahim Al-Zahrani

UNIVERSITY OF HAFR AL-BATIN
MAY 2026