Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur

Final Year Project

Proxy & VPN Detector

Under the guidance of :

Ms. Sneha Sharma

Assistant Professor,

Department of Computer

Science and Engineering

Project Team Members :

Kartik Khorwal (22ESKCS112)

Hitesh Tank (22ESKCS105)

Khushang Ameta (22ESKCS115)

Jitendra Kumar (22ESKCS108)

Introduction: Project Overview

Project Vision

A web-based cybersecurity tool for law enforcement and security professionals to detect and analyze masked IP addresses, offering real-time threat assessment.

Primary Objective

Develop an automated system for identifying proxy/VPN-masked IP addresses, crucial for digital forensics and cybercrime investigation.

Relevance

Addressing the critical need for advanced IP intelligence in an era of rising cybercrime and evolving online anonymity tools.

The Core Problem: Evading Attribution

> Cyber offenders are increasingly using proxy servers and VPN services to mask their original IP addresses, making it extremely difficult for law enforcement and cybersecurity professionals to trace malicious activities back to their source.

1

IP Masking

Criminals use proxy servers and VPNs to hide their real location, making it nearly impossible to trace them back to their actual computer or identity.

2

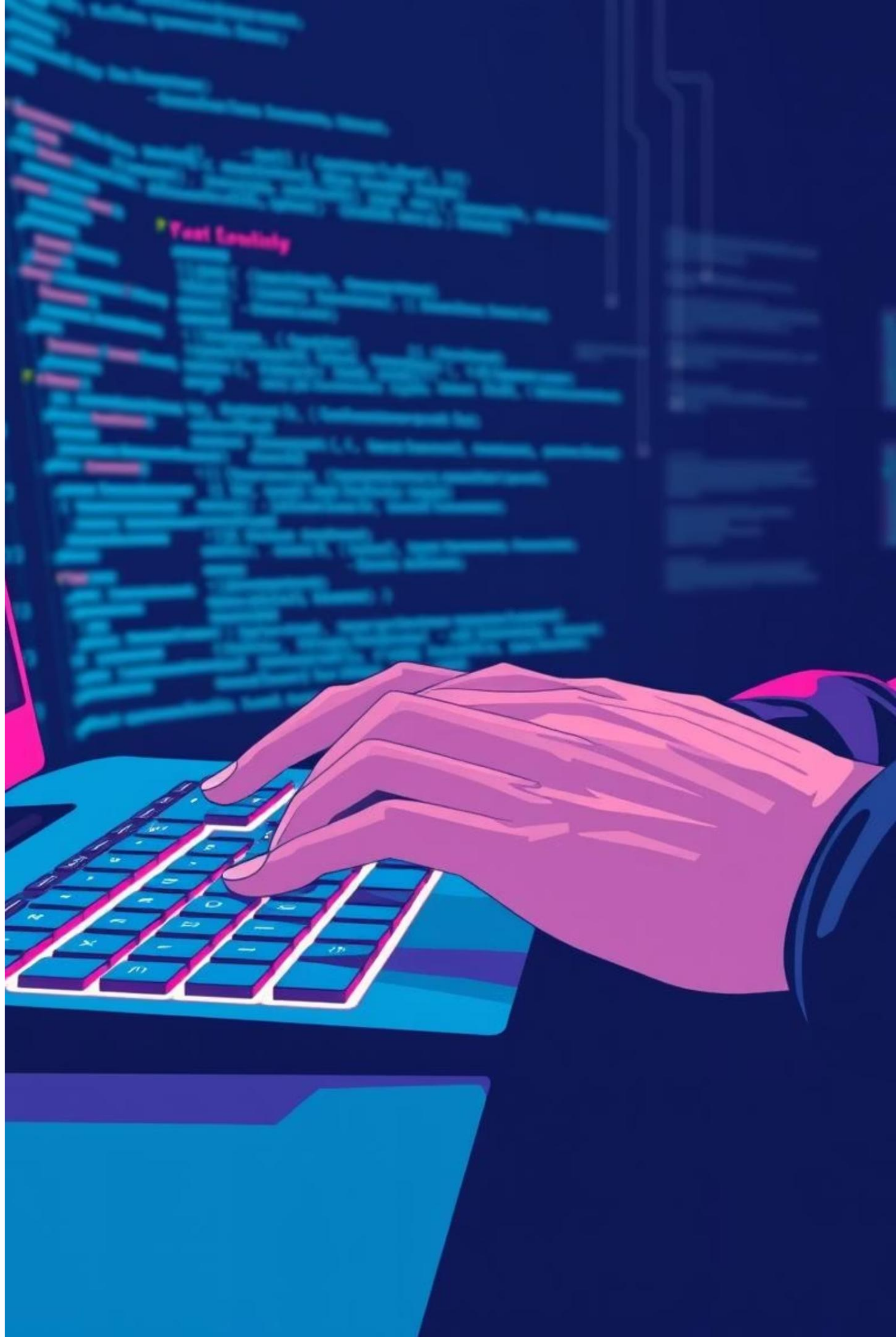
Manual Investigation

Police and security teams have to manually check each IP address one by one, which takes hours or days and requires special computer skills

3

Fragmented Data

IP data is spread across many websites and databases, so investigators have to visit multiple place to get complete information.



Why This Problem Matters:

- **Crime Investigation:** Delayed IP tracing leads to evidence loss and cold cases
- **Network Security:** Organizations need immediate threat detection to prevent breaches
- **Digital Forensics:** Law enforcement requires reliable IP intelligence tools for court proceedings
- **Fraud Prevention:** Financial institutions need instant risk assessment to protect customers

Current Solution Limitations:

- **Commercial Services:** Expensive and not designed specifically for law enforcement needs
- **Academic Research:** Fragmented approaches with no unified implementation
- **Existing Tools:** Limited integration, poor user interfaces, and lack comprehensive reporting

Reviewing Existing Solutions

Commercial Services

- **MaxMind GeoIP2:** Shows where an IP address is located geographically and which internet company owns it.
- **IPQualityScore:** Detects fake/suspicious IP addresses and helps prevent online fraud.
- **IPinfo:** Provides location details and information about the organization using the IP.
- **Limitation:** These services are very expensive and aren't designed specifically for police investigations.

Academic Research

- **IEEE 2023:** Machine learning for VPN detection.
- **ACM 2022:** Network fingerprinting for proxy ID.
- **Springer 2023:** Digital forensics in anonymous networks.
- **Gap:** Insufficient integration of diverse detection methods.

Identified Gaps

- **Integration:** No unified platform for proxy/VPN detection with WHOIS analysis.
- **User Interface:** Existing tools lack law enforcement-friendly interfaces.
- **Real-time:** Most solutions do not provide immediate threat assessment.
- **Reporting:** Limited comprehensive reporting for investigations.

Our Proposed Solution: Integrated IP Intelligence

> A comprehensive web-based platform combining multiple detection techniques with a user-friendly interface designed specifically for cybersecurity professionals and law enforcement.

Multi-layered Detection

API integration with services like IPQualityScore and custom algorithms for threat scoring and historical data analysis.

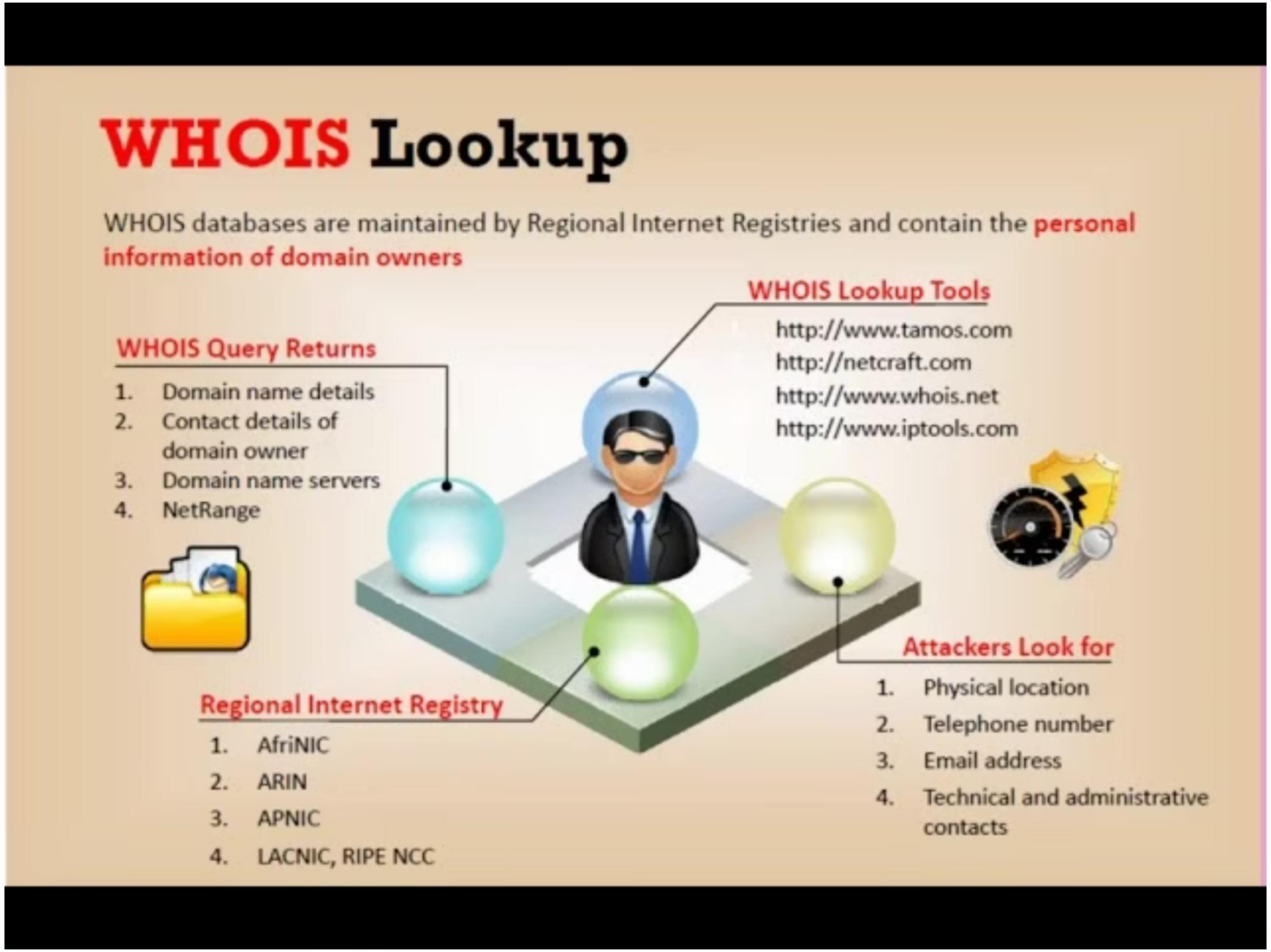
WHOIS Integration

Real-time and historical WHOIS lookup for IPs and domains, including contact information extraction.

Law Enforcement Focus

Investigation-friendly interface with audit trails for legal compliance and court-ready report generation.

WHOIS



WHOIS Lookup

WHOIS databases are maintained by Regional Internet Registries and contain the **personal information of domain owners**

WHOIS Lookup Tools

http://www.tamos.com
http://netcraft.com
http://www.whois.net
http://www.iptools.com

WHOIS Query Returns

1. Domain name details
2. Contact details of domain owner
3. Domain name servers
4. NetRange

Attackers Look for

1. Physical location
2. Telephone number
3. Email address
4. Technical and administrative contacts

Regional Internet Registry

1. AfriNIC
2. ARIN
3. APNIC
4. LACNIC, RIPE NCC

Technolgies Proposed

Web Application

Pros:

- **Cross-platform** - Works on any device with a browser
- **Easy deployment** - Host on cloud platforms
- **Real-time updates** - No installation required
- **Database integration** - Easy to store/retrieve data

Cons:

- Requires internet connection
- Depends on external APIs

Desktop Software (Standalone Application)

Pros:

- **Offline capability** - Can work without internet (limited)
- **Better performance** - Direct system access
- **Professional look** - Native OS integration
- **No browser dependency**

Cons:

- Platform-specific development
- Installation required
- Harder to update

Technical Architecture & Key Technologies

Frontend Stack

- **React.js 18 & TypeScript:** Creates interactive and user-friendly web pages with better code quality.
- **Material-UI:** Pre-built professional design elements for consistent look and feel.
- **Chart.js:** Creates graphs, charts, and visual reports from IP analysis data

Backend Stack

- **Node.js & Express.js:** Server technology that handles user requests and processes IP analysis logic.
- **MongoDB & Mongoose ODM:** Database that stores user data, analysis history, and threat intelligence.
- **JWT for authentication:** Secure login system that keeps user sessions safe.
- **Rate limiting and input validation:** Security features that prevent abuse and protect against attacks.

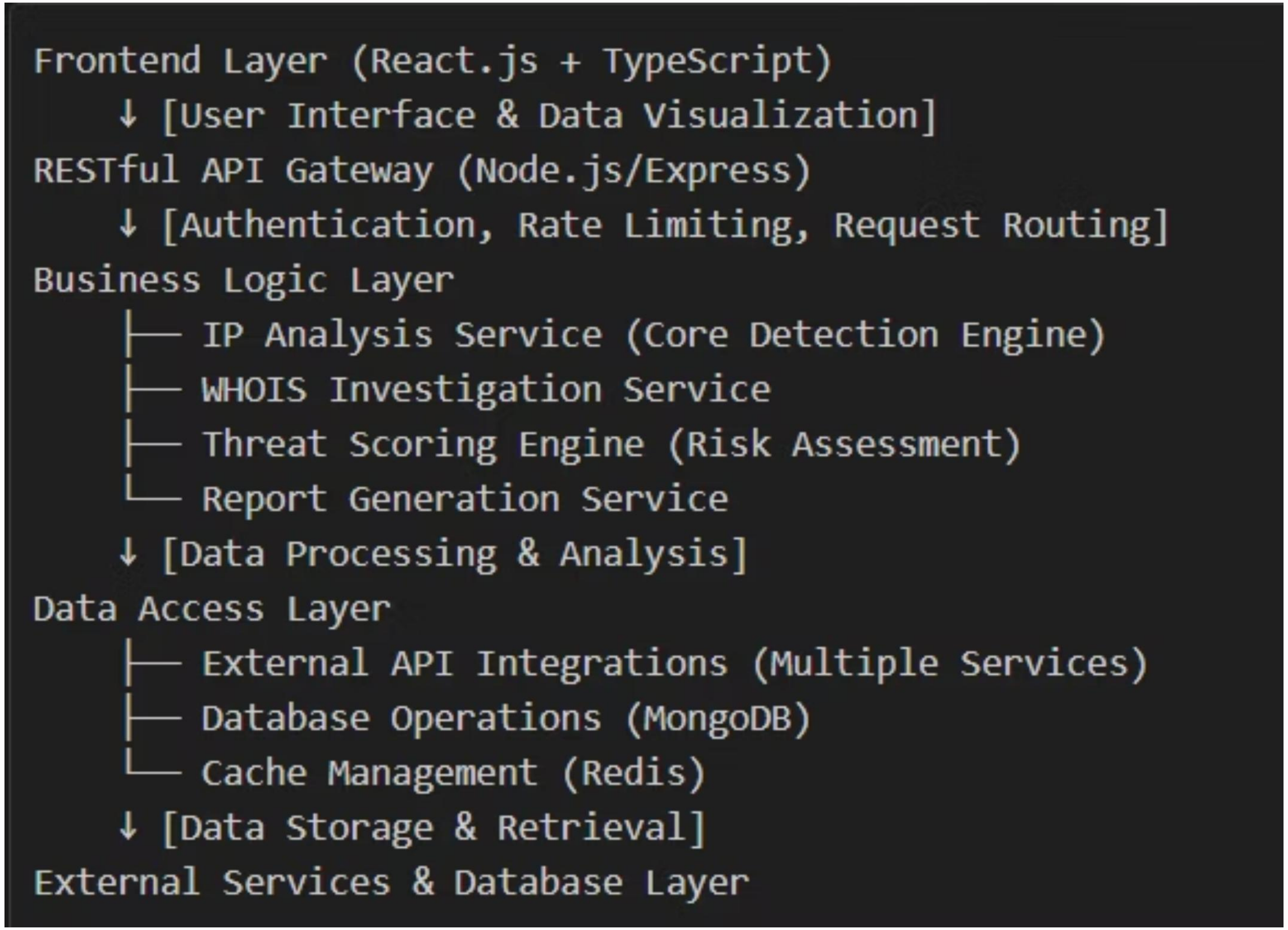
External API Integration

- **IPQualityScore API:** Main service that detects if an IP address is using a proxy or VPN.
- **IPinfo API:** Provides location information and details about the internet service provider.
- **WhoisXML API:** Gets detailed registration information about domains and IP addresses.
- **MaxMind GeoIP2:** Additional threat intelligence.

Security & DevOps

- **HTTPS/SSL & CORS:** Ensures all data transmission is encrypted and secure.
- **Git & GitHub:** Version control, tracks all code changes and enables team collaboration.
- **Jest & Supertest:** Automated testing tools that verify everything works correctly.

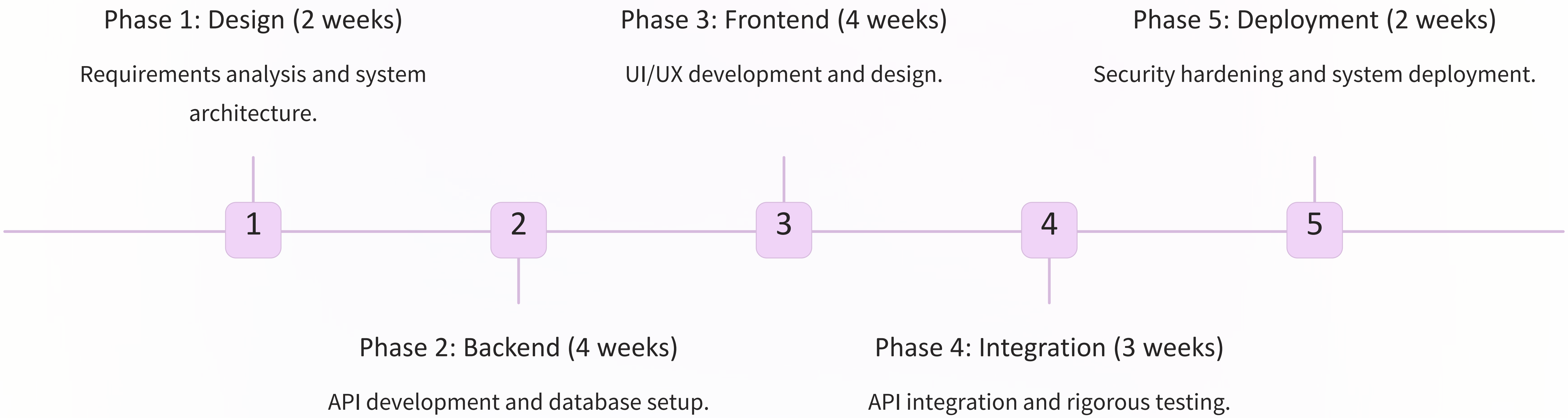
System Architecture



```
Frontend Layer (React.js + TypeScript)
    ↓ [User Interface & Data Visualization]
RESTful API Gateway (Node.js/Express)
    ↓ [Authentication, Rate Limiting, Request Routing]
Business Logic Layer
    ├── IP Analysis Service (Core Detection Engine)
    ├── WHOIS Investigation Service
    ├── Threat Scoring Engine (Risk Assessment)
    └── Report Generation Service
    ↓ [Data Processing & Analysis]
Data Access Layer
    ├── External API Integrations (Multiple Services)
    ├── Database Operations (MongoDB)
    └── Cache Management (Redis)
    ↓ [Data Storage & Retrieval]
External Services & Database Layer
```

Implementation Milestones & Challenges

The project was structured into distinct phases, ensuring a systematic and agile development approach.



1. **Phase 1: Design (2 weeks)**

   Requirements analysis and system architecture.

2. **Phase 2: Backend (4 weeks)**

   API development and database setup.

3. **Phase 3: Frontend (4 weeks)**

   UI/UX development and design.

4. **Phase 4: Integration (3 weeks)**

   API integration and rigorous testing.

5. **Phase 5: Deployment (2 weeks)**

   Security hardening and system deployment.

⚠ Challenges & Solutions:

API rate limiting was addressed with caching. IPv6 variations creates hinderance to standard format. Real-time performance was optimized via WebSockets. Security concerns were mitigated with encryption and GDPR compliance.

Implementation Challenges and Solutions

1. API Rate Limiting Challenge

Problem: External services only allow a limited number of requests per minute

Solution: Built a smart caching and memory system

2. Security and Privacy Compliance

Problem: Need to protect sensitive investigation data and follow privacy laws

- Compliance with international privacy regulations like GDPR
- Secure data transmission and storage requirements

Solution: Comprehensive security implementation

- Designed the system to automatically follow international privacy rules (GDPR)
- Implemented HTTPS/SSL for secure data transmission

Core Features & Functionality

IP Analysis Dashboard

- Single and bulk IP lookup (up to 100 IPs).
- Real-time threat scoring (1-100 scale).
- Geographic visualization on interactive maps.

WHOIS Investigation Tool

- Comprehensive domain/IP WHOIS lookup.
- Historical WHOIS data tracking.
- Contact information extraction and registrar analysis.

Proxy/VPN Detection Engine

- Uses multiple services (3 or more) to double-check if an IP is using proxy/VPN for better accuracy.
- Gives each IP a trust score from 1-100 to show how likely it is to be suspicious.
- Compares current IP behavior with past data to spot patterns that indicate criminal activity.

Advanced Analytics

- Pattern recognition in IP behavior.
- Suspicious activity alerts and trend analysis.
- Risk assessment algorithms for proactive defense.

Project Impact & Future Vision

The Proxy & VPN Detector sets a new standard for IP intelligence in cybersecurity and law enforcement.

Immediate Impact

- **Law Enforcement Efficiency:** 70% reduction in IP investigation time from hours to minutes
- **Case Resolution:** Faster evidence collection leads to quicker case closures

Medium-term Impact

- **Industry Adoption:** Potential use by cybersecurity firms, financial institutions, and government agencies

Long-term Vision

- **AI Enhancement:** Advanced machine learning for predictive threat analysis and behavioral pattern recognition

Societal Benefits

- **Public Safety:** Faster identification of cyber threats protects citizens from online crimes
- **Economic Protection:** Reduced financial fraud and cybercrime losses for businesses and individuals

✓ Future Enhancements:

Integration of AI for predictive threat analysis, native mobile applications, an API marketplace for broader integration, and advanced behavioral pattern recognition.

Thank You

We appreciate your time and attention. We are now open for questions and discussion.

Contact Information:

- Email: ***kartikkhorwal011@gmail.com***
- GitHub: [github.com/Kartik-Kh
- LinkedIn: www.linkedin.com/in/kartik-khorwal-2909441b3

> Special Thanks to our Project Mentor Sneha Sharma, College Faculty for their invaluable guidance and support.