🔐 CYBERSECURITY PROJECT REPORT

TITLE;

Security Analysis of Spotify

A Major Project Report
submitted in partial fulfillment of the requirements
for the award of the degree of

Bachelor of Technology
in
Computer Science / Cyber Security

Company Context: Spotify

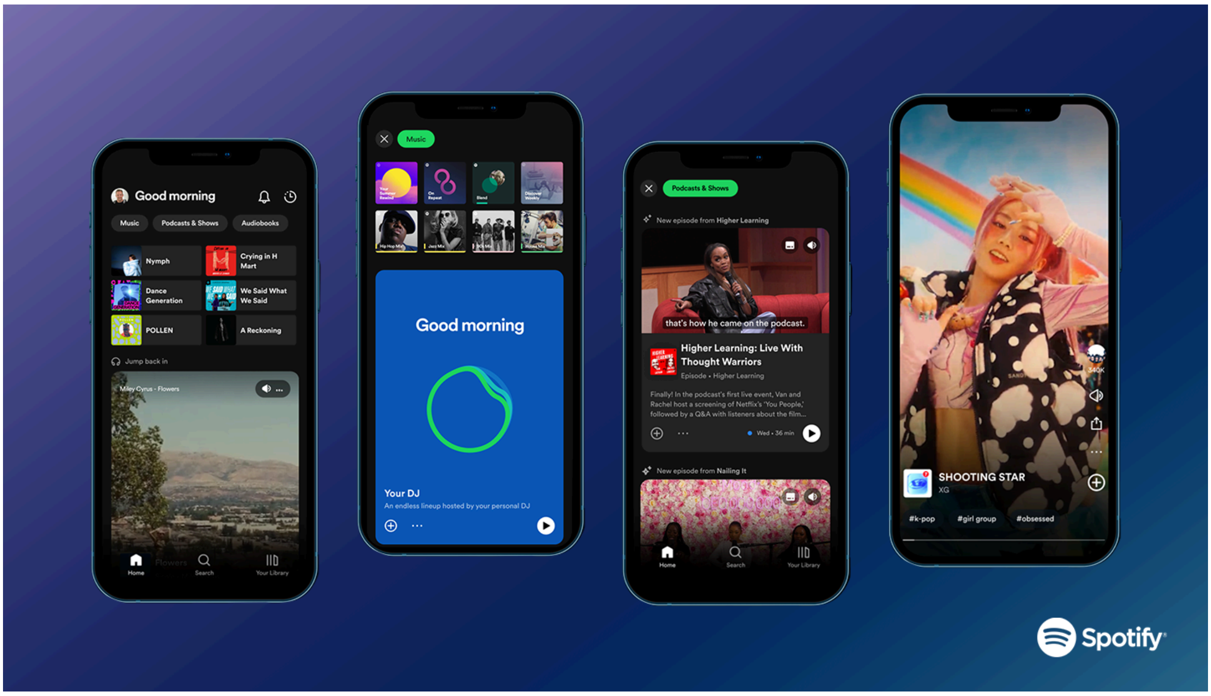
Submitted by:
Name: ADARSH KUMAR SINGH
Roll No: 301302224025 (erp - 6606714)

Under the guidance of:
Project Guide Name = PRASHANT SIR

College / University Name = RUNGTA COLLEGE OF ENGINEERING AND TECHNOLOGY
Year: 2025–2026

🔐 CYBERSECURITY PROJECT REPORT

Security Analysis of Spotify



Finally! In the podcast's first live event, Van and Rachel host a screening of Netflix's 'You People,' followed by a Q&A with listeners about the film...

1. ABSTRACT

Spotify is one of the world's largest music streaming platforms with millions of daily users. Due to its massive user base and cloud-based architecture, Spotify becomes a prime target for cyberattacks.
This project focuses on analyzing Spotify's cybersecurity infrastructure, identifying potential threats, vulnerabilities, and the security mechanisms used to protect user data, payment information, and streaming services.

---

2. INTRODUCTION

In today's digital era, online streaming platforms store huge volumes of sensitive data such as user credentials, payment details, listening history, and personal preferences. Spotify operates globally using cloud services and distributed networks, which makes cybersecurity a critical requirement.

This project studies:

- Spotify's system architecture
- Possible cyber threats
- Security measures used
- Preventive strategies and recommendations

---

3. COMPANY OVERVIEW – SPOTIFY

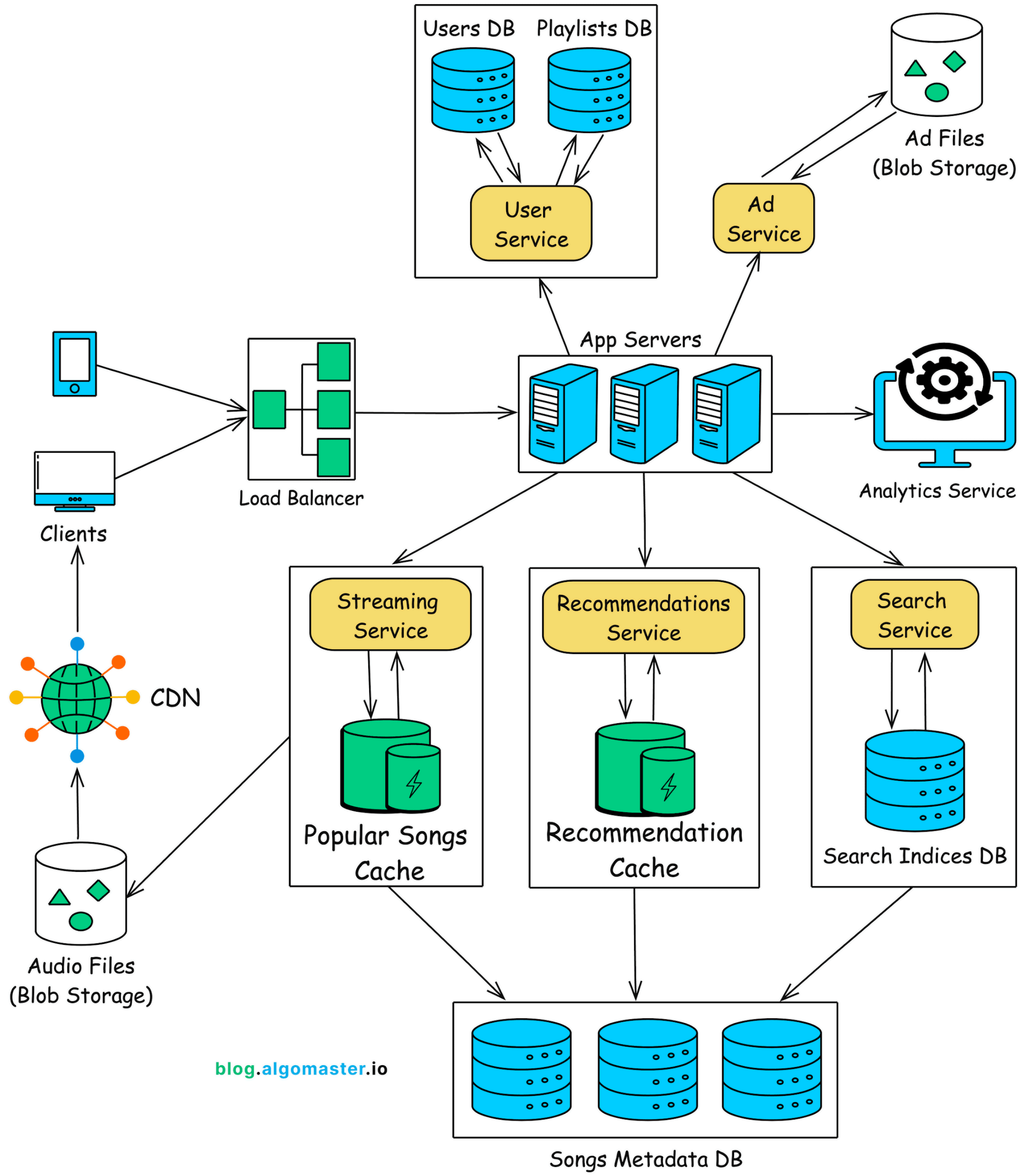
Spotify is a digital music, podcast, and video streaming service that provides access to millions of songs and podcasts worldwide.

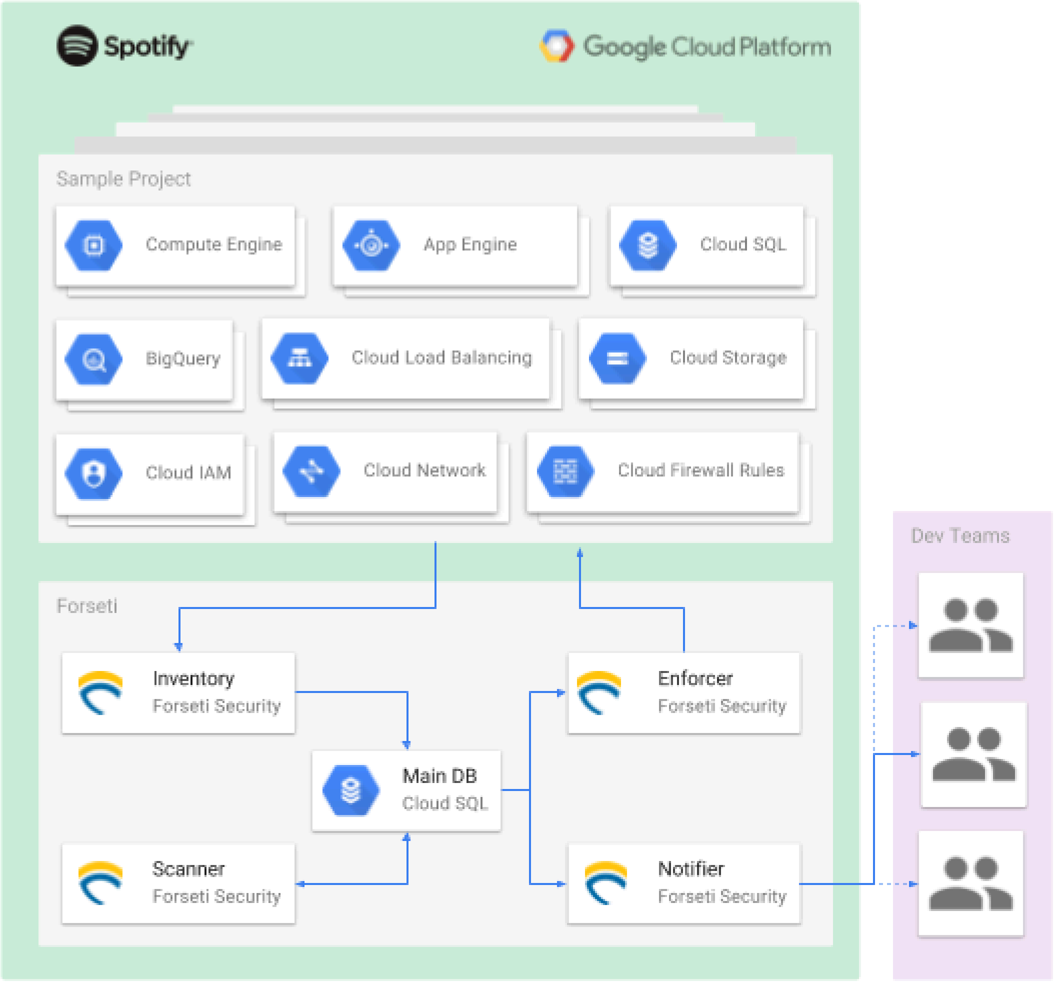
Key Details:

- Founded: 2006
- Headquarters: Stockholm, Sweden
- Users: 600+ million (Free + Premium)
- Platform: Mobile, Web, Desktop
- Technology: Cloud computing, microservices

---

4. SYSTEM ARCHITECTURE OF SPOTIFY


Users DB
Playlists DB
User Service
Ad Files (Blob Storage)
Ad Service
App Servers
Load Balancer
Clients
Analytics Service
CDN
Streaming Service
Popular Songs Cache
Recommendations Service
Recommendation Cache
Search Service
Search Indices DB
Audio Files (Blob Storage)
blog.algomaster.io
Songs Metadata DB



Spotify uses a **cloud-based microservices architecture**.

Components:

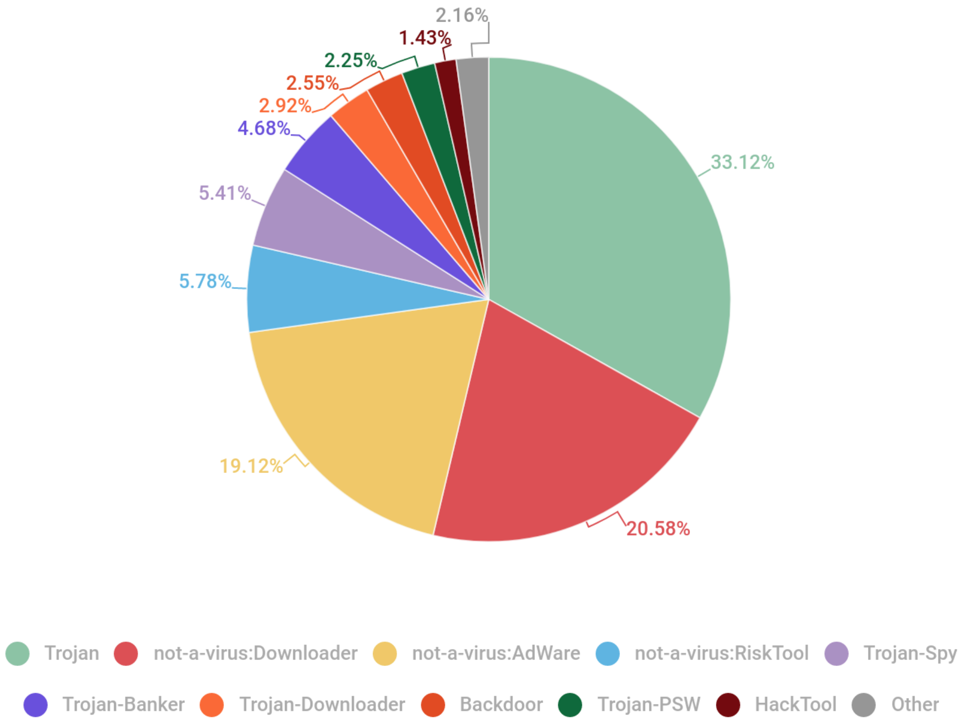
1. Client Applications (Android, iOS, Web, Desktop)
2. Authentication Servers
3. Content Delivery Network (CDN)
4. Cloud Storage
5. Payment Gateways
6. Recommendation Engine

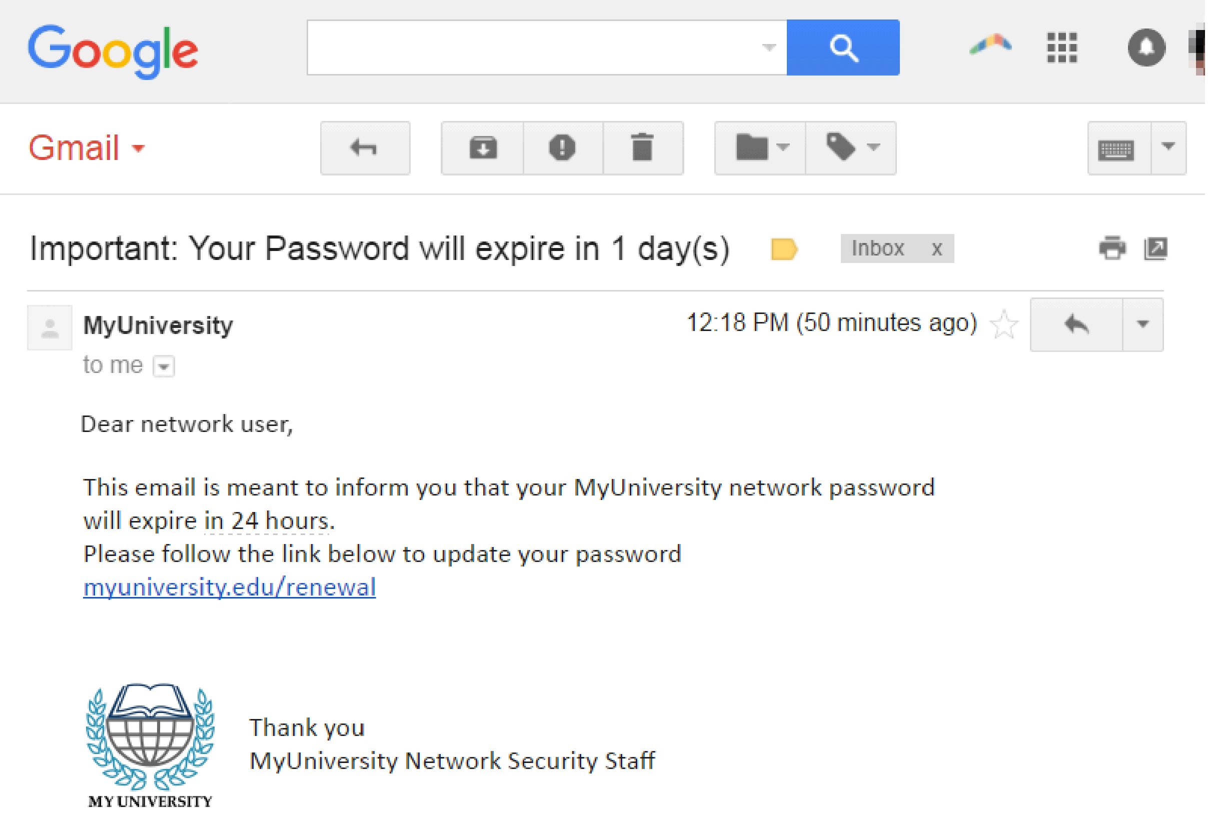
5. DATA TYPES USED BY SPOTIFY

- User login credentials
- Personal information (email, location)
- Payment details (for premium users)
- Listening history
- Playlist data

- Device information

6. CYBER THREATS TO SPOTIFY





Important: Your Password will expire in 1 day(s)

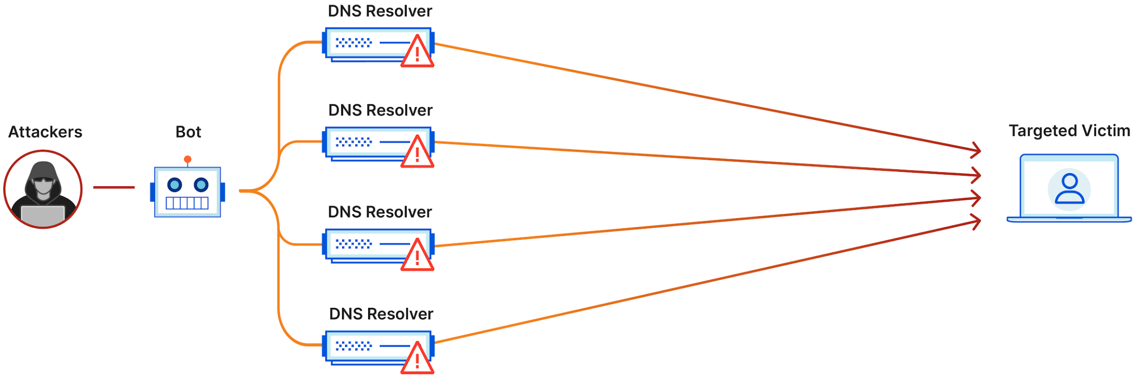
MyUniversity

12:18 PM (50 minutes ago)

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff



Major Threats:

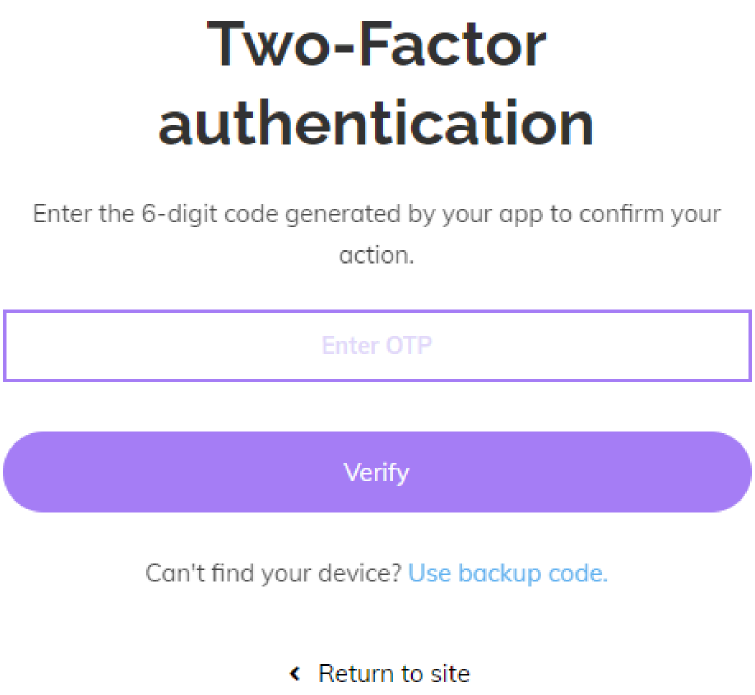
1. **Phishing Attacks** – Fake emails to steal credentials

2. **Account Takeover (ATO)** – Credential stuffing attacks
3. **DDoS Attacks** – Service disruption
4. **Malware Injection** – Through third-party apps
5. **Data Breaches** – Unauthorized access to databases
6. **API Abuse** – Exploiting public APIs

7. VULNERABILITIES ANALYSIS

- Weak passwords by users
- Reused credentials
- Third-party integrations
- Insecure public Wi-Fi usage
- Unpatched software vulnerabilities

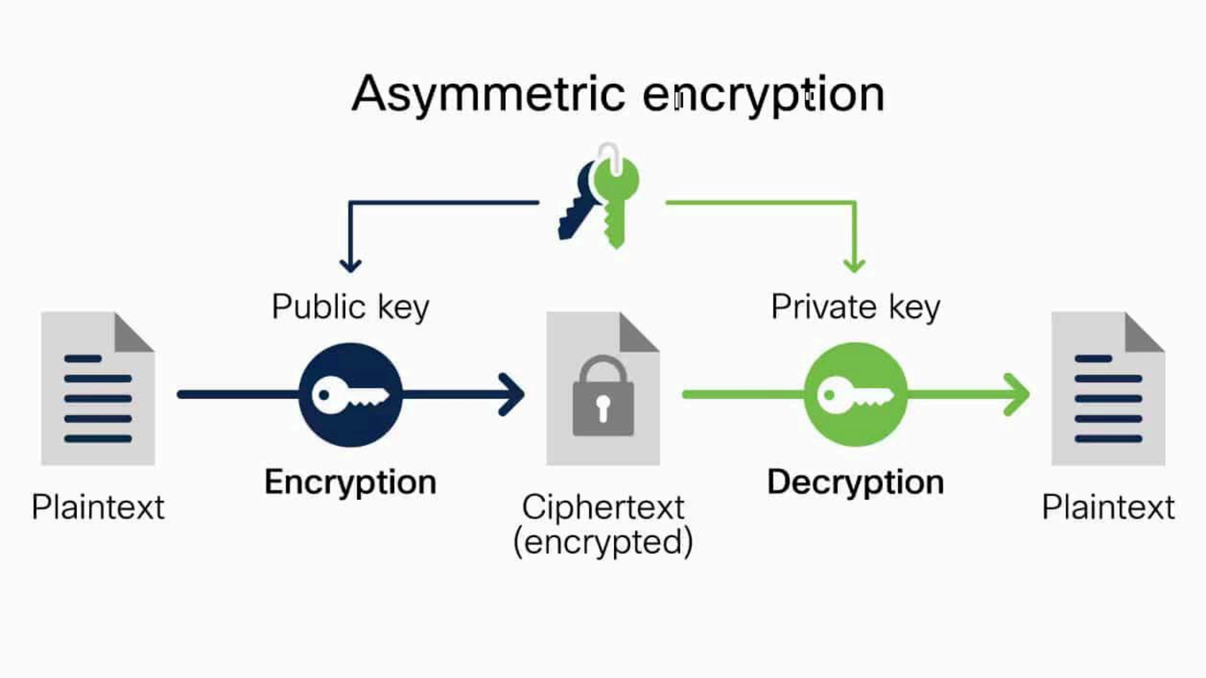
8. SECURITY MEASURES IMPLEMENTED BY SPOTIFY

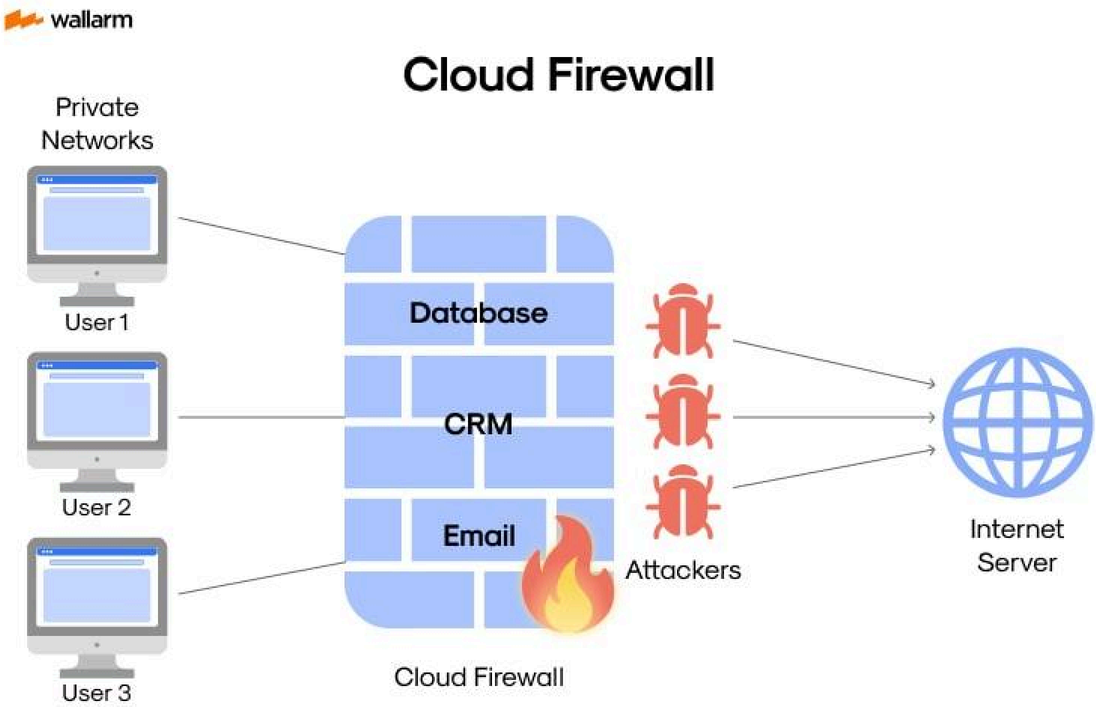


Two-Factor authentication

Enter the 6-digit code generated by your app to confirm your action.

Can't find your device? Use backup code.





Security Techniques:

1. **Encryption**
   - HTTPS / TLS encryption
   - Encrypted data storage
2. **Authentication**
   - OAuth-based login
   - Two-Factor Authentication (2FA)
3. **Network Security**

    - Firewalls
    - Intrusion Detection Systems (IDS)
4. **Cloud Security**
    - Secure cloud infrastructure
    - Regular audits
5. **Bug Bounty Program**
    - Ethical hackers report vulnerabilities

---

9. CASE STUDY: ACCOUNT TAKEOVER ATTACK

Problem:
Attackers use leaked credentials from other platforms to log into Spotify accounts.

Impact:

- Playlist manipulation
- Unauthorized premium usage
- Privacy breach

Solution:

- Password reset
- 2FA enforcement
- Monitoring unusual login behavior

---

10. TOOLS & TECHNOLOGIES USED (STUDY PURPOSE)

- Wireshark (Traffic Analysis)
- Burp Suite (Web Security Testing)
- OWASP Top 10
- Kali Linux
- Cloud Security Frameworks

---

11. FUTURE SECURITY ENHANCEMENTS

- Mandatory Two-Factor Authentication
- AI-based threat detection
- Zero Trust Architecture
- Advanced anomaly detection

- User cybersecurity awareness

12. ADVANTAGES OF STRONG CYBERSECURITY

- User trust enhancement
- Protection of personal data
- Business continuity
- Legal compliance
- Brand reputation protection

13. LIMITATIONS OF THE STUDY

- No real internal access to Spotify systems
- Analysis based on public information
- Ethical and legal boundaries followed

14. CONCLUSION

Spotify's cybersecurity infrastructure is robust and continuously evolving. However, increasing cyber threats demand advanced security strategies, constant monitoring, and user awareness. This project highlights the importance of cybersecurity in protecting large-scale digital platforms.

15. REFERENCES

1. Spotify Security Whitepapers
2. OWASP Official Documentation
3. Cloud Security Alliance
4. Cybersecurity Research Papers

THANK YOU !