The session is designed for students and practitioners interested in cyber / application security and backend engineering. I've included timing, format options, prerequisites and post-session deliverables so your committee can assess alignment with the society's goals.

Quick notes: I can deliver a 45–60 minute talk + 10–15 minute Q&A, or a more hands-on 90–120 minute workshop if you prefer.

Title: Securing APIs — Practical Patterns & Pitfalls (with FinTech examples)

Format options (pick one):

- **Talk:** 60 minutes total — 45 min presentation + 15 min Q&A.
- **Short talk:** 45 min total — 35 min presentation + 10 min Q&A.
- **Workshop:** 90–120 minutes — interactive exercises (token handling, safe rate-limiting config, token revocation demo).

Target audience: Undergraduate/postgraduate students, society members interested in cyber and backend engineering, junior devs wanting secure-by-design patterns. No advanced crypto knowledge required.

Prerequisites for attendees: Basic HTTP/API knowledge, familiarity with authentication concepts (helpful but not required).

Learning outcomes (what attendees will gain):

1. Practical threat model for modern APIs (esp. FinTech context).
2. Concrete authentication & authorization best practices and common failures.
3. Defensive controls to reduce attack surface: transport, headers, input validation, rate-limiting.
4. CI/CD, secrets management, and logging guidance for safe deployment.
5. Actionable checklist and resources to apply immediately.

Session timing & contents (60-minute talk example):

- **0–5 min — Welcome & speaker intro**
  Quick background, relevance to cyber society and FinTech context.

- **5–12 min — Threat model & real-world attacks**
  API misuse, broken auth cases, token theft, replay, abuse (FinTech examples).

- **12–25 min — Authentication & Authorization (core)**

  - OAuth2 & OpenID Connect basics (roles, flows)

  - JWT: pros/cons, signature vs encryption, expiry, revocation strategies

  - Token storage & rotation (refresh tokens, rotating refresh tokens)

  - Scopes, least privilege and claims hygiene

- **25–33 min — Transport & network controls**

  - TLS 1.2/1.3, enforce HSTS, certificate management, optional mTLS for service-to-service

  - API gateway placement, WAF basics

- **33–41 min — Request-level protections**

  - Input validation (allowlist), parameterized queries, content-type validation

  - Rate limiting & throttling (client-side vs server-side, IP vs token), IP reputation & bot detection

- **41–48 min — Deployment, secrets & CI/CD**

  - Secret managers, ephemeral credentials, least privilege for service accounts

  - Dependency & supply-chain scanning (SCA), SAST/DAST in pipeline

- **48–54 min — Observability & incident preparation**

  - Structured logs, PII redaction, tracing, alerting, playbooks for breached tokens

- **54–60 min — Quick checklist & wrap-up**
  Actionable checklist for devs and ops to apply in the next sprint.

- **+15 min Q&A (if 75–90 total)**

Optional hands-on workshop exercises (if workshop chosen):

1. Hardening an example API endpoint: add CORS, CSP, secure headers.
2. Implement token rotation and a safe refresh flow.
3. Configure rate-limiting rules in an API gateway (exercise + answers).
4. Simple incident playbook: revoke tokens, rotate keys, notify stakeholders.

Deliverables I'll provide after confirmation:

- Slide deck (PDF)
- One-page secure-API checklist / cheat-sheet (printable)
- Links to sample code & automated tests (GitHub gist)
- Optional pre-read (the Medium article)

Speaker bio (short, for committee):
Kamran Khalid — Senior Backend Developer with 12+ years building secure, scalable systems across FinTech, AI, and other domains. Mentor at DeveloperWeek USA 2025. (LinkedIn: https://www.linkedin.com/in/kamran-khalid-4310973a/)