HACKSECURE 2025

NULL VIT BHOPAL STUDENT CHAPTER

- **Problem Statement**

AI-Powered Data Leak Prevention Tool

- Increasing risk of sensitive API keys and secrets leaking in code repositories, chats, and cloud storage
- Manual scanning for secrets is time-consuming and error-prone
- Need for automated, real-time detection and alerting system to prevent data breaches

- **Team Name - Rooted**
- **Batch – 23**

Team Member Details

S.No	NAME	Reg. No	Mail Id	Mobile No
1.	Mayank Agarwal	23BCY10074	mayank.23bcy10074@vitbhopal.ac.in	9696201019
2.	Himanshu Kesarwani	23BCY10044	himanshu.23bcy10044@vitbhopal.ac.in	7905793455
3.	Bindupautra Jyotibrat	23BAI10963	bindupautra.23bai10963@vitbhopal.ac.in	8822693201
4.	Kunal Kumar	23BCG10101	kunal.23bcg10101@vitbhopal.ac.in	8931848984
5.	Sanjith moos	23BCE11149	sanjith.23bce11149@vitbhopal.ac.in	8929211185

Proposed Solution

- Develop an automated scanning workflow using AI-powered Gemini model to detect exposed API keys and secrets.
- Integrate with Multiple platforms Discord, Slack, GitHub and Drive.
- Generate real-time alerts via email for any detected secrets.
- Secure, scalable, and easy-to-integrate solution for any team environment.

Innovation and Uniqueness

- Uses Google’s Gemini 2.5 Flash LLM for precise secrets detection
- Supports multiple channels: Discord, Slack, GitHub, Drive
- No false positives due to AI-powered contextual understanding
- Customizable alerts to fit organizational needs
- Can be deployed without disrupting existing workflows

Technical Approach

Technologies Used:

1. Workflow Automation: n8n
2. AI & Machine Learning: Google Gemini 2.5 Flash
3. Programming Languages: JavaScript (for n8n custom nodes and logic)
4. Integrations:

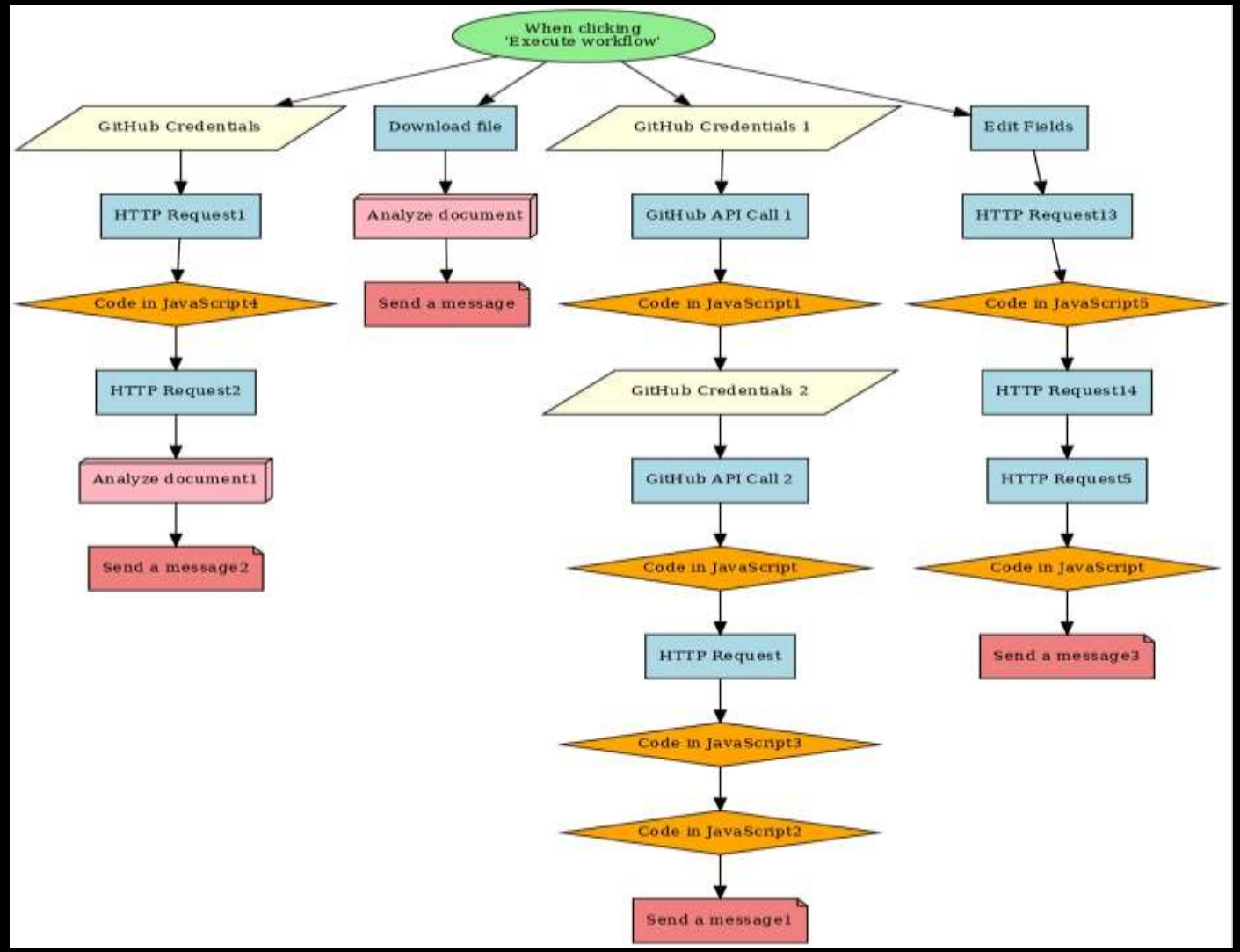
- GitHub API (for repository scanning)
- Google Drive API (for document monitoring)
- Slack/Discord API (for File Scanning)

    - Workflow orchestrated via n8n automation platform
    - Steps include: fetch recent messages/files → decode content → analyze text with Gemini → parse AI output → send alerts using mail
    - Use of HTTP API calls, Function nodes for data manipulation
    - Security via tokens and scoped bot permissions
    - Handles binary files by text extraction or skipping non-text

Methodology and process for implementation

- Define trigger events (e.g., new upload in chat or repo commit)
- Pull messages/repos for recent files with attachments
- Extract file text from different formats
- Send text content to Gemini API for secrets analysis
- Parse JSON response, filter for findings
- Send alert emails summarizing detected secrets
- Continuous monitoring with scheduled triggers

Architecture Diagram



Feasibility And Viability

- Feasible with existing APIs and n8n platform without heavy infrastructure
- Scalable to multiple communication and code channels
- Minimal user intervention once deployed
- Cost-effective leveraging Google AI Studio’s Gemini API
- Challenges: Handling large files, managing API rate limits
- Risks: False negatives—mitigated with prompt tuning and threshold adjustments

Challenges and Risks

- Token management and rate limiting from multiple APIs
- File format variations requiring adaptable decoding
- Potential delays in email delivery or alerting
- Ensuring bot permissions and security compliance
- Maintaining prompt efficacy as secrets' formats evolve

Strategies to Overcome Challenges

- Implement chunking and prompt restrictions for large files
- Use fallback mechanisms for unsupported file types
- Monitor API usage and refresh tokens automatically
- Regularly update AI model prompt with latest secret patterns
- Employ encrypted storage and secure access control

Impact and Benefits

- Proactive prevention of data breaches from leaked secrets
- Helps development teams maintain secure code repositories
- Enhances organizational security posture with minimal overhead
- Automates tedious manual secret scanning processes
- Enables compliance with data protection standards

Research and References

- Google AI Studio Gemini API documentation
- Slack and Discord API integration guides
- n8n workflow automation platform
- Industry best practices in secrets management
- Relevant open source tools and libraries

Thanks

Click Here to View Project
Click Here to View Video
https://drive.google.com/file/d/1YjfiFLFr1tFInaMWxBv-5StABhsMw9K-/view?usp=drivesdk