SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

- **Problem Statement ID –SIH1744**
- **Problem Statement Title- Automated Digital Forensics Tool**
- **Theme- Cyber Security / Forensics**
- **PS Category- Software**
- **Team ID- MITADTSW049**
- **Team Name (Registered on portal): Secure mavericks**

Secure Mavericks

Automated Digital Forensics Tool

SMART INDIA HACKATHON 2024

Describe your Idea/ Solution/ Prototype:

Implementation of **a cyber triage tool** that could significantly enhance the efficiency and effectiveness of digital forensic investigations.

- Interactive and Accessible Interface
- Automated Data Collection
- Automated Analysis and Log reading
- AI and ML Integration
- User-Friendly learning Options

Problem Resolution :

- This tool automates data collection, scanning, and analysis, allowing analysts to focus on high-level analysis and decision-making by enhancing overall efficiency.
- The tool is optimized with techniques like automated data log and efficient data indexing, ensuring efficiency even with large datasets.

Unique Value Propositions (UVP) :

- Supports multiple forensic image formats and integrates with existing tools, allowing smooth adoption without disrupting current workflows.
- Built to handle large datasets with ease performance optimizations.
- Automation and key word scanner to extract related data

Secure Mavericks

TECHNICAL APPROACH

SMART INDIA HACKATHON 2024

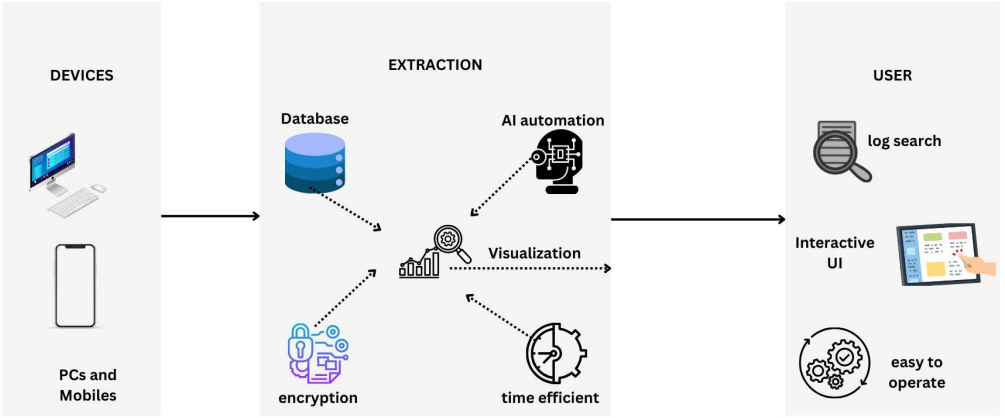
Digital Forensics:
Analyzing **memory dump** and **network traffic**, using **Pytsk3**, **Python-registry** identify important information in a compromised system for intrusion response.

AI/ML integration:
To **automate** the tasks like **extraction of data** for forensics using libraries like **Scikit-learn**, **TensorFlow**,**PyTorch, Pandas** and **NumPy** for data analytics.

Encryption and Security:
Custom encryption algorithm using **TLS/SSL** and **AES-256** secure data transmission and authentication.

Cloud and database Services:
MySQL - Relational database management
AWS Cloud- For large scale storage purposes.

PROCESS FLOW ARCHITECTURE



Product Status: 35% product development is completed and further development is on progress. The libraries alongwith flowchart and algorithms are ready and proceeding with code development.

Secure Mavericks

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

- **Automation:** Existing frameworks and APIs can provide smooth data gathering from multiple sources, including digital devices, networks, and cloud services.
- **AI/ML Integration:** Different libraries and platforms like TensorFlow, PyTorch, and Scikit-learn can provide the necessary infrastructure to develop and train machine learning models used for digital forensic investigations.
- **Interactive Interface:** Modern technologies, such as React or Angular, along with UX design principles, ensure the creation of an interactive and accessible interface.
- **Training and Support:** Minimal training will be needed due to the tool's interactive design. But only comprehensive documentation and customer support services will be available to address any issues or questions.

Secure Mavericks

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

- Potential impact on the target audience
  1. **Computer Forensics Investigator** - Time Efficiency and Management .
  2. **Computer Forensics Enthusiasts** - Easily Understandable and Learnable Modules .
  3. **Information Security Analyst** - Efficient Database Management for Analysis and Visualization.

- Benefits of the solution
  1. **Interactive interface** : Accessible interface makes it easier to use .
  2. **Resource Management** : Data Logs and datasets are effectively managed and saved.
  3. **Security**: Provides a secure environment for carrying out cloning and data extraction .
  4. **Easy To Learn**: New Learners and Cyber security enthusiasts can understand and learn easily.

Secure Mavericks

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

1. Details / Links of the reference and research work IEEE, Scopus, Elsevier , Science Direct

1. **" A Cyber Security Data Triage Operation Retrieval System "** Chen Zhonga,*, Tao Linb, Peng Liub, John Yenb, Kai Chenc,d

2. **" Improving forensic triage efficiency through cyber threat intelligence "** Nikolaos Serketzis, Vasilios Katos, Christos Ilioudis, Dimitrios Baltatzis, Georgios Pangalos

3. **" The industrial control system cyber defence triage process "** Allan Cook, Helge Janicke, Richard Smith, Leandros Maglaras

4. **" A Data Triage Retrieval System for Cyber Security Operations Center "** Tao Lin