 **NOVANECTAR SERVICES PVT. LTD**

**Integrity Checker Project Report**

**Project Title: Integrity Checker**

**ID**: NN/22/2410

**NAME** : S.E.PAVITHRA

**1. Introduction**

In the ever-evolving landscape of cybersecurity, safeguarding sensitive system files from unauthorized modifications is crucial. The **File Integrity Verification System** is designed to monitor and validate the authenticity of critical files using cryptographic hash functions. This system helps organizations detect unauthorized changes, prevent potential cyber threats, and maintain data integrity.

**2. Objectives**

The system is developed to achieve the following key objectives:

* **Generate Baseline Hashes:** Compute and store initial cryptographic hashes of essential system files.
* **Continuous Monitoring:** Regularly scan and compare file hashes to detect alterations.
* **Unauthorized Change Detection:** Identify modifications, additions, or deletions of critical files.
* **Security Alerts:** Provide real-time alerts in case of suspicious file changes.
* **Comprehensive Logging:** Maintain a record of detected changes for auditing and forensic analysis.
* **User Customization:** Enable users to configure directories for monitoring and update hash baselines as required.

**3. Implementation Details**

**3.1 Technologies Used**

* **Programming Language:** Python
* **Libraries Used:** os, hashlib, json, time, datetime, logging
* **Hashing Algorithm:** SHA-256 for file integrity verification
* **Alert Mechanism:** Log-based alerts and notifications

**3.2 Features of the System**

* **Automated File Hashing:** Uses SHA-256 to compute file integrity values.
* **Periodic Scans:** Scheduled scans to detect file alterations.
* **Change Detection:** Alerts administrators when files are modified or removed.
* **Exclusion Mechanism:** Ignores irrelevant system files such as configuration backups.
* **User-defined Directories:** Allows users to specify critical directories for monitoring.

**4. Security Considerations and Enhancements**

To enhance security and reliability, the following measures are integrated:

* **Encryption of Stored Hashes:** Prevents tampering of reference hash values.
* **Access Restrictions:** Ensures only authorized personnel can modify settings.
* **Logging and Audit Trails:** Keeps a detailed history of file integrity checks.
* **Integration with Security Tools:** Supports compatibility with existing Intrusion Detection Systems (IDS).

**5. Project Execution Plan**

1. **Phase 1:** Research cybersecurity risks and define technical requirements.
2. **Phase 2:** Develop core functionalities, including hash generation and comparison.
3. **Phase 3:** Conduct rigorous testing to evaluate accuracy and efficiency.
4. **Phase 4:** Deploy the system and provide comprehensive documentation for users.

**6. Sample Log Output**

[2025-03-01 14:52:10] ALERT: Unauthorized modification detected in C:\SecureFiles\config.ini

[2025-03-01 14:55:30] WARNING: File deleted: C:\SecureFiles\database\_backup.sql

[2025-03-01 15:10:45] NOTICE: New file detected: C:\SecureFiles\security\_policy.txt

**7. Challenges Faced & Solutions**

|  |  |
| --- | --- |
| **Challenge** | **Solution** |
| High resource usage during scanning | Implemented optimized hashing to reduce CPU load |
| False positives in integrity checks | Enhanced exclusion mechanism for irrelevant files |
| Need for real-time notifications | Integrated logging and alert system for instant monitoring |

**8. Potential Future Improvements**

* **User Interface (UI):** Develop a GUI for enhanced user interaction.
* **Cloud-Based Monitoring:** Extend integrity checks to remote storage solutions.
* **Cross-Platform Support:** Ensure compatibility with Linux and macOS.
* **Artificial Intelligence (AI) Integration:** Predict security threats using machine learning models.

**9. Conclusion**

The File Integrity Verification System serves as a robust solution for maintaining data integrity in critical environments. By continuously monitoring file changes, logging activities, and providing timely alerts, the system enhances cybersecurity defenses and helps mitigate risks associated with unauthorized modifications.