Name : Aditya Prashant Nikam
Class: BE (AI & DS)
Roll no.: 31
Subject : Cyber Security

GROUP B (ASSIGNMNET NO.: 08)

Title:
Design and implement the program for detecting tampering of data at storage at IoT.

Problem Statement :
Design and implement the program for detecting tampering of data at storage at IoT.

Outcome:
The implemented program successfully detects and reports any tampering or unauthorized alterations to data stored on IoT devices. It utilizes data integrity checks, hashing algorithms, and regular audits to ensure the data's integrity and security. This tamper detection solution enhances the overall reliability of IoT systems by promptly identifying and mitigating data tampering, safeguarding the accuracy and trustworthiness of the stored information.

Theory:

1. Introduction:

- Discuss the significance of detecting data tampering in IoT systems to ensure data integrity and security.
- Outline the primary objectives of the assignment: to develop a program that can identify unauthorized alterations to stored IoT data.

2. Data Tampering Challenges in IoT:

- Explain the specific challenges related to data tampering in IoT, such as the distributed nature of devices and the need for real-time detection.

3. Data Integrity Mechanisms:

- Describe key data integrity mechanisms and techniques essential for IoT, including cryptographic hashing, checksums, and digital signatures.
- Explain the importance of these mechanisms in identifying unauthorized data alterations.

4. Designing Data Tampering Detection Program:

- Outline the architecture and components of the program responsible for detecting data tampering.
- Discuss the choice of data integrity techniques, algorithm selection, and real-time monitoring.

5. Data Hashing and Digital Signatures:

- Explain how the program uses cryptographic hashing to create data fingerprints for stored information.
- Detail the use of digital signatures to verify data authenticity.

6. Real-time Monitoring:

- Describe how the program continuously monitors data integrity in IoT devices and systems.
- Discuss how it can promptly detect any unauthorized changes or tampering.

7. Response and Alerting:

- Explain the program's response mechanisms when data tampering is detected.
- Detail how it can send alerts, take automated actions, or notify administrators.

8. Implementation and Integration:

- Provide technical insights into implementing the data tampering detection program on IoT devices and integrating it into the IoT ecosystem.
- Address resource utilization and compatibility considerations.

9. Testing and Validation:

- Detail the testing procedures to validate the program's effectiveness in detecting data tampering.
- Describe how it responds to simulated tampering attempts.

10. Case Studies and Use Cases:

- Present practical examples of how the data tampering detection program can be applied to specific IoT scenarios, such as industrial control systems or smart cities.

11. Future Enhancements (Optional):

- Suggest potential improvements or future developments for the data tampering detection program, such as implementing blockchain-based tamper-proofing or AI-enhanced anomaly detection.

Conclusion:

- Summarize the key takeaways from the assignment, emphasizing the critical role of data tampering detection in ensuring the integrity and security of IoT data.
- Highlight the program's contribution to enhancing the overall data security of IoT ecosystems.