

# PROFESSIONAL TRAINING REPORT - II

entitled

## DATA INTEGRITY SURVEILLANCE

Submitted in partial fulfillment of the requirements for the award of  
Bachelor of Engineering degree in Computer Science and Engineering  
with specialization in Cyber Security

by

**Nuka Charan Dev Reddy (41614063)**

**P Subha Dharani Kumar (41614064)**

**Perla Durga Prithviraj (41614070)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
SCHOOL OF COMPUTING**

# **SATHYABAMA**

**INSTITUTE OF SCIENCE AND TECHNOLOGY**

**(DEEMED TO BE UNIVERSITY)**

**CATEGORY -1 UNIVERSITY BY UGC**

**Accredited with Grade "A++" by NAAC | 12B Status by UGC | Approved by AICTE**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119**

**MAY 2024**



# SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-I UNIVERSITY BY UGC

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

[www.sathyabama.ac.in](http://www.sathyabama.ac.in)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**BONAFIDE CERTIFICATE**

This is to certify that this Professional Training Report is the bonafide work of **Mr. Perla Durga Prithviraj (41614070)** who carried out the project entitled "DATA INTEGRITY SURVEILLANCE" under my supervision from January 2024 to May 2024.

Internal Guide

Dr. D. Anu Disney, M.E., Ph.D.,

Head of the Department

Dr. S. VIGNESHWARI, M.E., Ph.D.,

Submitted for Viva voce Examination held on 7/5/24

Internal Examiner

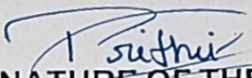
External Examiner

## DECLARATION

I, Perla Durga Prithviraj (41614070), hereby declare that the Professional Training Report-II entitled "DATA INTEGRITY SURVEILLANCE" done by me under the guidance of Dr. D. Anu Disney, M.E., Ph.D., is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering with specialization in Cyber Security.

DATE: 7/5/24

PLACE: Chennai

  
SIGNATURE OF THE CANDIDATE

## ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph.D., Dean, School of Computing, Dr. S.Vigneshwari M.E., Ph.D., Head of the Department of Computer Science and Engineering** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Internal Guide **Dr. D. Anu Disney, M.E., Ph.D.**, for his/her valuable guidance, suggestions and constant encouragement which paved way for the successful completion of my phase-2 Professional Training.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

## COURSE CERTIFICATE



# CERTIFICATE

## OF EXCELLENCE

THIS IS TO CERTIFY THAT

### Perla Durga Prithviraj

---

CANDIDATE ID : CSZ2024123  
has successfully completed  
**AWS PYTHON**  
Course Conducted During January 2024 to April 2024

Date: 06.04.2024



Authorized Signatory

#30, 3rd Main, Rajalakshmi Nagar, Velachery, Chennai - 42. Ph : +91-44-2245 5904 / 98844 12301, Web : [www.credosystemz.com](http://www.credosystemz.com)

## **ABSTRACT**

The project aims to develop an advanced data integrity surveillance system designed to safeguard organizations' digital assets in the ever-evolving threat landscape. Leveraging cryptographic hash functions, checksums, and anomaly detection algorithms, the system will continuously monitor specified files and directories for any unauthorized alterations. It will establish a baseline during setup to track deviations, ensuring the integrity of files overtime. Utilizing hashing algorithms, any changes to file content will trigger different hash values, indicating potential tampering. Machine learning algorithms will enable the system to detect unusual patterns or behaviors in file modifications, enhancing its ability to identify sophisticated attacks or insider threats. Real-time alerts via email, SMS, or system logs will notify administrators of detected file integrity violations, allowing for immediate response and mitigation. Additionally, detailed logs and reports will provide visibility into file changes, aiding in forensic analysis and compliance requirements. The system's scalability and customization options will ensure it can adapt to the organization's infrastructure and security policies, making it a crucial component in maintaining a strong security posture and mitigating the risk of data breaches or compliance violations.

## TABLE OF CONTENTS

| CHAPTER NO. | TITLE                                         | PAGE NO. |
|-------------|-----------------------------------------------|----------|
|             | <b>ABSTRACT</b>                               | v        |
|             | <b>LIST OF FIGURES</b>                        | vii      |
| 1           | <b>INTRODUCTION</b>                           | 1        |
|             | 1.1 Overview                                  |          |
| 2           | <b>LITERATURE SURVEY</b>                      | 2        |
|             | 2.1 Survey                                    |          |
| 3           | <b>REQUIREMENTS ANALYSIS</b>                  |          |
|             | 3.1 Objective                                 | 5        |
|             | 3.2.1 Hardware Requirements                   | 6        |
|             | 3.2.2 Software Requirements                   | 7        |
| 4           | <b>DESIGN DESCRIPTION OF PROPOSED PRODUCT</b> | 8        |
|             | 4.1.1 Ideation Map                            | 9        |
|             | 4.1.2 Various Stages                          | 11       |
|             | 4.1.3 Internal or Component Design Structure  | 12       |
|             | 4.1.4 Working Principles                      | 13       |
|             | 4.2 Novelty of the Project                    | 15       |
| 5           | <b>CONCLUSION</b>                             |          |
|             | 5.1 Summary                                   | 17       |
|             | 5.2 Future Work                               | 17       |
|             | <b>REFERENCES</b>                             | 18       |
|             | <b>APPENDIX</b>                               |          |
|             | A. Research Paper                             | 18       |
|             | B. Source Code                                | 24       |
|             | C. Snapshots                                  | 28       |

## LIST OF FIGURES

| Figure No. | Figure Name                          | Page no |
|------------|--------------------------------------|---------|
| 4.1        | System Architecture                  | 9       |
| 4.2        | Ideation Map                         | 10      |
| 4.3        | Stage Orientation                    | 11      |
| 4.4        | Components Design Structure          | 12      |
| 4.5        | SHA-512 Compression Function         | 14      |
| 4.6        | Process of SHA-512                   | 15      |
| B.1        | Baseline Creation                    | 28      |
| B.2        | Monitoring File while Changing       | 28      |
| B.3        | Monitoring File while File Creation  | 29      |
| B.4        | Monitoring File while File Deletions | 29      |

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 OVERVIEW**

Data integrity surveillance is a critical aspect of maintaining the reliability and trustworthiness of data within an organization or system. It involves the continuous monitoring, validation, and protection of data to ensure its accuracy, consistency, and reliability. In the realm of cybersecurity, data integrity surveillance focuses on detecting and preventing unauthorized alterations, deletions, or corruption of data. This involves implementing various techniques and technologies such as checksums, digital signatures, and encryption to verify the integrity of data and detect any unauthorized changes.

Moreover, data integrity surveillance extends beyond cybersecurity to encompass data quality management practices. Organizations employ data validation processes and quality checks to ensure that the data collected, stored, and processed meets certain standards and is free from errors or inconsistencies. Furthermore, compliance regulations and industry standards often mandate the implementation of robust data integrity surveillance measures. Organizations operating in highly regulated sectors such as healthcare, finance, and pharmaceuticals must adhere to strict data integrity requirements to maintain regulatory compliance and mitigate the risk of penalties or legal consequences.

Effective data integrity surveillance also involves establishing clear policies, procedures, and access controls to govern how data is managed, accessed, and modified within an organization. This includes defining roles and responsibilities, implementing segregation of duties, and enforcing data access restrictions to prevent unauthorized or inappropriate actions that could compromise data integrity.

Overall, data integrity surveillance plays a crucial role in safeguarding the reliability, accuracy, and trustworthiness of data, ensuring its integrity throughout its lifecycle and across various systems and processes within an organization. By continuously monitoring and protecting data integrity, organizations can enhance data security, compliance, and overall operational efficiency.

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1 SURVEY**

The survey for Data integrity surveillance aims to gather insights into the current practices, challenges, and perceptions surrounding FIM implementation in organizations. The survey begins by assessing the prevalence of FIM adoption among respondents and identifying the primary reasons for implementing FIM solutions, such as compliance requirements, security best practices, or specific organizational needs. It then delves into the key features and functionalities that respondents consider essential in FIM solutions, including real-time monitoring, alerting mechanisms, integration capabilities, and scalability. Additionally, the survey seeks to understand the challenges and barriers organizations face in deploying and managing FIM solutions, such as resource constraints, complexity of implementation, or integration issues with existing IT infrastructure. Respondents will also be asked about their experiences with FIM solutions, including any notable successes or challenges encountered during implementation and operation. Lastly, the survey explores respondents' expectations and preferences for future advancements in FIM technology, such as enhanced automation, artificial intelligence, or integration with cloud-native environments. By gathering insights from a diverse range of respondents, the survey aims to provide valuable information and recommendations for improving FIM practices and addressing the evolving cybersecurity needs of organizations. Explore the various data integrity attacks prevalent in cloud computing environments and the countermeasures employed to mitigate them. Consider how file integrity monitoring systems can contribute to detecting and preventing such attacks [1].

Data integrity surveillance is a fundamental cybersecurity practice that involves continuously monitoring and validating the integrity of files and systems. By comparing current file states with established baselines using cryptographic hashes or checksums, FIM solutions can detect unauthorized changes, tampering, or corruption in real-time. This proactive approach helps organizations identify and respond to security incidents promptly, mitigating the risk of data breaches, compliance violations, and other malicious activities. FIM provides administrators with alerts and reports to facilitate timely incident response and forensic analysis, enabling them to maintain the security and integrity of their systems and data effectively. Investigate the different techniques proposed for ensuring data integrity in cloud computing environments. Analyze how FIM solutions complement these techniques and enhance overall data integrity assurance [2].

File integrity monitoring (FIM) is an internal control or process that validates the integrity of operating system and application software files by comparing the current file state to a known, good baseline. Many Techniques can be implemented by the

attackers to attack the files in the operating system environment and make file protection become a vital task. Implementation of FIM and other related system security tools is needed for that purpose. It is critical for computer systems to ensure the integrity of sensitive files in file systems. Examine the concept of data integrity and its applications in various domains. Discuss how FIM systems contribute to maintaining data integrity by monitoring and verifying the integrity of files and data [3].

The vast majority of attacks use unapproved or unauthorized access to sensitive files to steal confidential information such as secret keys, passwords, credit card numbers, and so on. Following that, attackers typically conceal their tracks by corrupting critical files such as system logs. Monitoring file system integrity is a well-known method for ensuring the integrity of sensitive and critical files. Identify the challenges associated with ensuring data integrity and explore proposed solutions. Discuss how FIM solutions address these challenges and contribute to maintaining data integrity in complex IT environments [4].

The file system is central to any computing system because it stores data and executable programs. Malicious users or malwares may alter the contents of a sensitive data file or embed a malicious payload in an executable. As a result, monitoring the integrity of the files in the file system is critical. There has been a lot of research done on file integrity monitoring tools. Explore the unique challenges related to data integrity and security in big data environments. Analyze how FIM systems adapt to the scale and complexity of big data to ensure comprehensive file integrity monitoring [5].

This article discusses the currently available file integrity monitoring tools and their underlying approaches. Maintain system integrity, detecting changes as they happen, with a detailed audit trail including who, what, when and where. Verisys integrity suite is a next-generation file integrity monitoring and change detection system. File integrity monitoring is critical for security and compliance initiatives, and is a requirement for NIST and PCI compliance as well as the consensus audit guidelines. Gain insights into data integrity issues specific to cloud computing environments. Discuss the role of FIM solutions in addressing these issues and ensuring the integrity of files and data stored in the cloud [6]. Review the various techniques employed to protect data integrity in cloud computing environments. Evaluate how FIM systems complement these techniques by providing real-time monitoring and detection capabilities [7].

Circle file integrity monitor TM provides an agentless file integrity auditing solution that gives you the ability to monitor an asset's details all the way down to the file level without requiring software agent on the monitored system. Cimtrak integrity suite software is next level file integrity monitoring used for PCI compliance, and it does everything it should. we are constantly monitoring for changes to sites, it does exactly what we need it to do.

The product is simple to use and pretty hands-off. Explore specific challenges and solutions related to ensuring data integrity in cloud storage systems. Discuss the role of FIM solutions in detecting unauthorized modifications or deletions of files stored in the cloud [8].

The literature survey on data integrity monitoring (DIM) illuminates its paramount significance in safeguarding the trustworthiness and reliability of data across diverse digital environments. Through an exhaustive examination of scholarly works, it becomes evident that DIM systems serve as indispensable guardians against malicious tampering, unauthorized access, or corruption of data. The surveyed literature underscores DIM's pivotal role in mitigating data integrity threats prevalent in cloud computing, big data analytics, and IoT ecosystems. Moreover, the survey highlights the evolution of DIM techniques, from traditional cryptographic methods to innovative blockchain solutions and machine learning algorithms. As organizations grapple with escalating cyber risks, the insights gleaned from this survey underscore the imperative of deploying robust DIM systems as fundamental components of comprehensive cybersecurity strategies. Ultimately, DIM emerges as a linchpin in fortifying the resilience and integrity of digital infrastructures, thereby ensuring the sustained trust and confidence of stakeholders in an increasingly data-driven world.

In addition to its foundational role in cybersecurity, the literature survey unveils DIM's adaptability to emerging technological paradigms, such as cloud computing and IoT. By harnessing innovative approaches like blockchain and machine learning, DIM systems offer dynamic and proactive defenses against evolving threats to data integrity. Furthermore, the survey underscores the imperative of continuous innovation and collaboration across academia, industry, and regulatory bodies to address the multifaceted challenges confronting DIM implementation and effectiveness. As organizations navigate the complex landscape of data governance and compliance, the findings underscore DIM's indispensable contribution to fostering transparency, accountability, and trust in digital ecosystems, thereby underpinning the sustainable advancement of digital transformation initiatives.

## **CHAPTER 3**

### **REQUIREMENTS ANALYSIS**

#### **3.1 OBJECTIVE OF THE PROJECT**

The objective of the "Data Integrity Surveillance" project is to establish a robust system for monitoring and ensuring the integrity of data within an organization or system. This involves implementing mechanisms to detect and prevent unauthorized access, alteration, or corruption of data, thereby maintaining its accuracy, consistency, and reliability. By employing advanced surveillance techniques, encryption methods, access controls, and regular audits, the project aims to safeguard sensitive information from potential threats such as cyberattacks, data breaches, or insider manipulation. Ultimately, the goal is to instill confidence in stakeholders regarding the trustworthiness and authenticity of the data, promoting transparency, compliance, and the overall security posture of the organization.

In the long term, the "Data Integrity Surveillance" project seeks to cultivate a culture of data integrity within the organization, embedding principles of accountability, transparency, and ethical behavior in every aspect of data management. By continuously refining and enhancing surveillance methodologies, the project aims to stay ahead of emerging threats and evolving security challenges in the digital landscape. Over time, as the system matures, it should become increasingly adept at detecting even the most sophisticated attempts at data manipulation or intrusion.

Moreover, as the organization's data ecosystem expands and evolves, the project aims to scale its surveillance capabilities accordingly, accommodating larger volumes of data, diverse data types, and increasingly complex information architectures. This scalability ensures that the integrity of data is maintained across various platforms, systems, and processes, regardless of the organization's size or operational complexity.

Furthermore, in the long term, the project aims to establish itself as a benchmark for data integrity best practices, serving as a model for other organizations seeking to fortify their data protection strategies. By sharing insights, lessons learned, and successful methodologies, the project contributes to a broader ecosystem of knowledge and collaboration in the realm of data security and integrity.

Ultimately, in the long term, the "Data Integrity Surveillance" project aims to foster a climate of trust and confidence among stakeholders, including customers, partners, regulators, and the wider community. By demonstrating a steadfast commitment to data integrity and security, the organization not only mitigates risks and safeguards its

## **3.2 REQUIREMENTS**

Data integrity surveillance systems must fulfill several key requirements to effectively safeguard systems and data integrity. These include establishing baseline configurations for comparison, conducting real-time monitoring of files and system components, utilizing cryptographic hashes or checksums for verification, implementing robust alerting mechanisms to notify administrators of unauthorized changes, enabling automated responses to detected incidents, offering customization options for tailored monitoring settings, generating comprehensive reports and logs for auditing purposes, supporting integration with other security tools and systems, ensuring scalability to accommodate organizational needs, and aligning with relevant compliance standards and regulations. By meeting these requirements, FIM solutions can help organizations maintain the security and integrity of their systems and data effectively.

### **3.2.1 HARDWARE REQUIREMENTS**

The hardware requirements for Data integrity surveillance solutions depend on factors like the scope of monitoring, the size of the environment, and the desired level of performance. Typically, FIM systems necessitate hardware capable of supporting continuous monitoring, data processing, and storage. This includes a robust CPU to handle real-time monitoring and cryptographic hashing, ample RAM for efficient data processing, and sufficient storage capacity for baseline configurations and logs. Reliable network connectivity is crucial for communication and integration with other systems, while scalability ensures the FIM solution can accommodate future growth. Additionally, redundancy measures enhance system reliability, ensuring uninterrupted monitoring even in the event of hardware failures. By addressing these hardware requirements, organizations can deploy FIM solutions effectively to bolster the security and integrity of their systems and data.

The hardware requirements for a Data Integrity Surveillance system encompass a range of components tailored to ensure robust data monitoring and protection. This includes high-performance servers equipped with multi-core processors, ample RAM, and redundant storage configurations such as RAID arrays to handle large volumes of data effectively. Enterprise-grade storage solutions like NAS or SAN with high-speed drives ensure reliable data storage and accessibility. A dependable network infrastructure with sufficient bandwidth capacity and robust security measures is vital for seamless data transmission and protection against cyber threats. Specialized data processing units such as GPUs or FPGAs may be necessary for computationally intensive tasks like anomaly detection or machine learning analysis. Monitoring devices such as sensors or

cameras, along with redundancy and failover mechanisms, ensure continuous operation and data availability. Scalability considerations should be integrated into the hardware design to accommodate future growth and expansion of the surveillance system. Overall, a well-planned hardware infrastructure forms the foundation for a comprehensive Data Integrity Surveillance system, enabling organizations to monitor, protect, and maintain the integrity of their data effectively.

### **3.2.2 SOFTWARE REQUIREMENTS**

The software requirements for implementing Data integrity surveillance encompass selecting a suitable FIM software solution compatible with the organization's operating systems, ensuring compatibility with database systems for storing baseline configurations and logs, integrating cryptographic libraries for hash calculations and file integrity verification, establishing network connectivity for updates, alerts, and integration with other security systems, implementing user authentication and access control mechanisms for data security, ensuring compatibility with other security tools and systems for seamless integration, and enabling reporting and alerting capabilities to notify administrators of detected unauthorized changes or security incidents. By fulfilling these software requirements, organizations can effectively deploy FIM solutions to enhance the security and integrity of their systems and data.

In a Data Integrity Surveillance system tailored for large data volumes, the software requirements play a pivotal role in ensuring effective monitoring, analysis, and protection of data integrity. At the core of the system is robust data management software capable of handling vast amounts of data efficiently. This includes database management systems (DBMS) or big data platforms like Hadoop or Spark, which offer scalable storage and processing capabilities. Additionally, specialized software for data integrity monitoring and analysis is essential, encompassing features such as real-time data monitoring, anomaly detection, and pattern recognition algorithms. Advanced encryption and cryptographic software ensure data security during transmission and storage, safeguarding against unauthorized access or tampering. Furthermore, comprehensive data governance and compliance software help enforce data integrity policies, regulatory requirements, and audit trails, ensuring adherence to industry standards and best practices. Integration with monitoring and visualization tools provides insights into data integrity metrics and alerts, enabling proactive response to potential threats or breaches. Moreover, machine learning and artificial intelligence technologies may be leveraged to enhance the system's capabilities in detecting and mitigating emerging risks. Overall, a well-integrated suite of software solutions tailored for large data volumes forms the foundation of an effective Data Integrity Surveillance system, empowering organizations to maintain the integrity and security of their data assets in the face of evolving threats and challenges.

## **CHAPTER 4**

### **DESIGN DESCRIPTION OF PROPOSED PROJECT**

#### **4.1 PROPOSED METHODOLOGY**

The proposed methodology for Data integrity surveillance involves several key steps: beginning with an assessment and planning phase to identify critical assets and establish monitoring objectives, followed by the selection of an appropriate FIM solution based on compatibility and functionality. Once chosen, the FIM solution is configured and deployed across the organization's infrastructure, with baseline configurations established to serve as reference points for comparison during real-time monitoring. Continuous monitoring is activated, with alerting mechanisms configured to notify administrators of any unauthorized changes promptly. Incident response procedures and workflows are developed to address detected security incidents effectively, while ongoing maintenance and optimization activities ensure the relevance and effectiveness of the FIM implementation over time. Documentation and training are provided to ensure that personnel are equipped with the necessary knowledge and skills to operate the FIM solution successfully. Through adherence to this methodology, organizations can enhance the security and integrity of their systems and data effectively.

The proposed methodology for Data Integrity Surveillance entails a multifaceted approach aimed at safeguarding the integrity of organizational data through systematic monitoring, detection, and response mechanisms. Initially, a comprehensive risk assessment is conducted to identify potential threats and vulnerabilities to data integrity within the organization's ecosystem. Drawing from this assessment, data integrity policies and standards are established, delineating acceptable practices, access controls, and encryption protocols in alignment with regulatory requirements and organizational objectives. Subsequently, a surveillance infrastructure is implemented, comprising hardware, software, and network components tailored to the organization's data environment. This infrastructure facilitates continuous monitoring and analysis of data access, modifications, and transmission activities in real-time. An array of surveillance algorithms, including anomaly detection and pattern recognition techniques, are employed to identify deviations from established data integrity norms.

Critical to the methodology are robust alerting and response mechanisms, which promptly notify stakeholders of potential breaches or suspicious activities and enable swift mitigation measures. Incident response protocols are developed to contain breaches and restore data integrity, ensuring minimal disruption to operations and mitigating potential damages. Regular audits and assessments are conducted to evaluate the effectiveness of existing controls and processes, with findings used to inform iterative improvements to the surveillance framework. Additionally, ongoing training and awareness programs cultivate a culture of accountability and vigilance

adherence to data integrity policies and fostering a collective commitment to safeguarding organizational data assets.

#### 4.1.1 Ideation Map/System Architecture

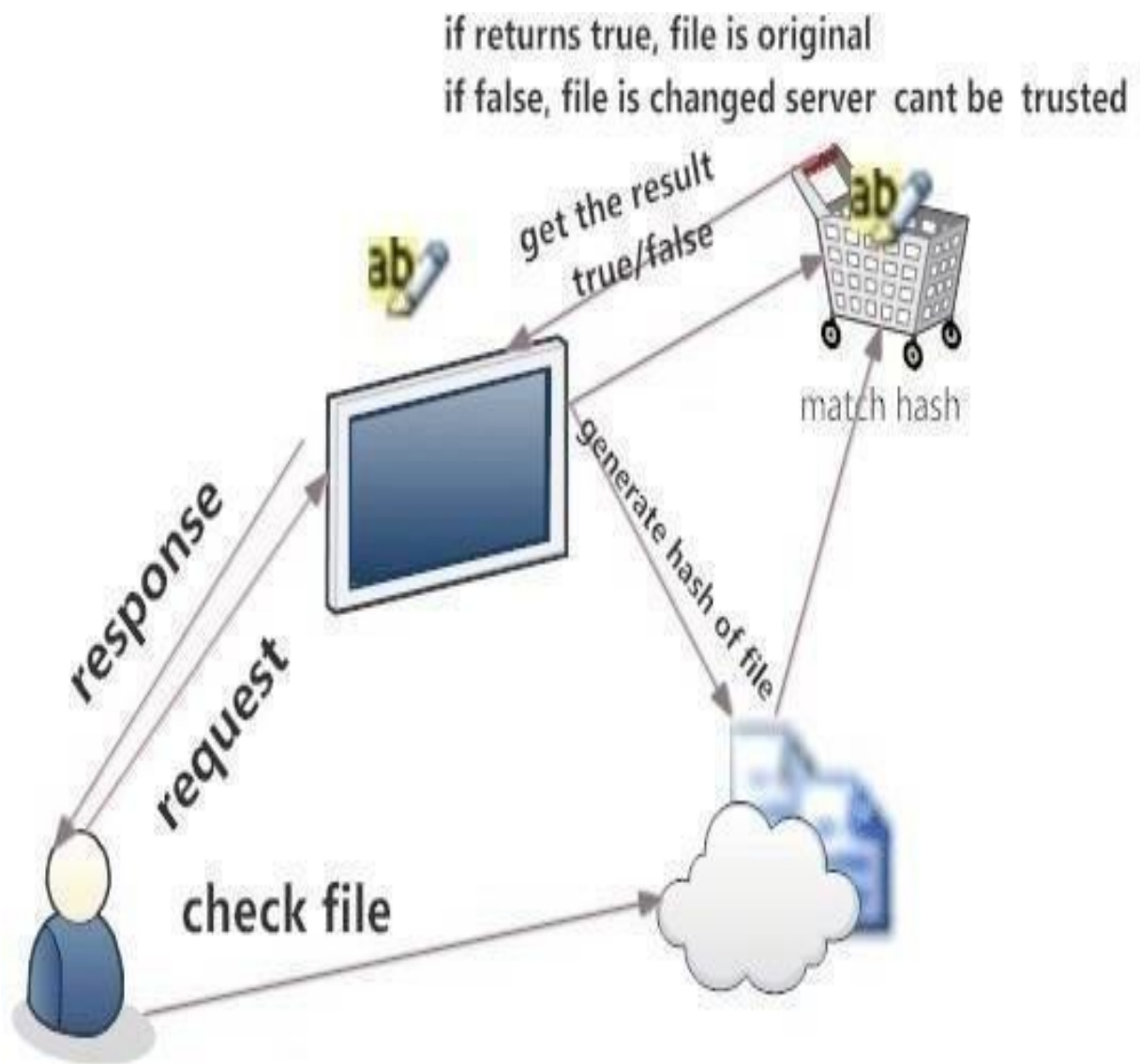


Fig:4.1 - System Architecture

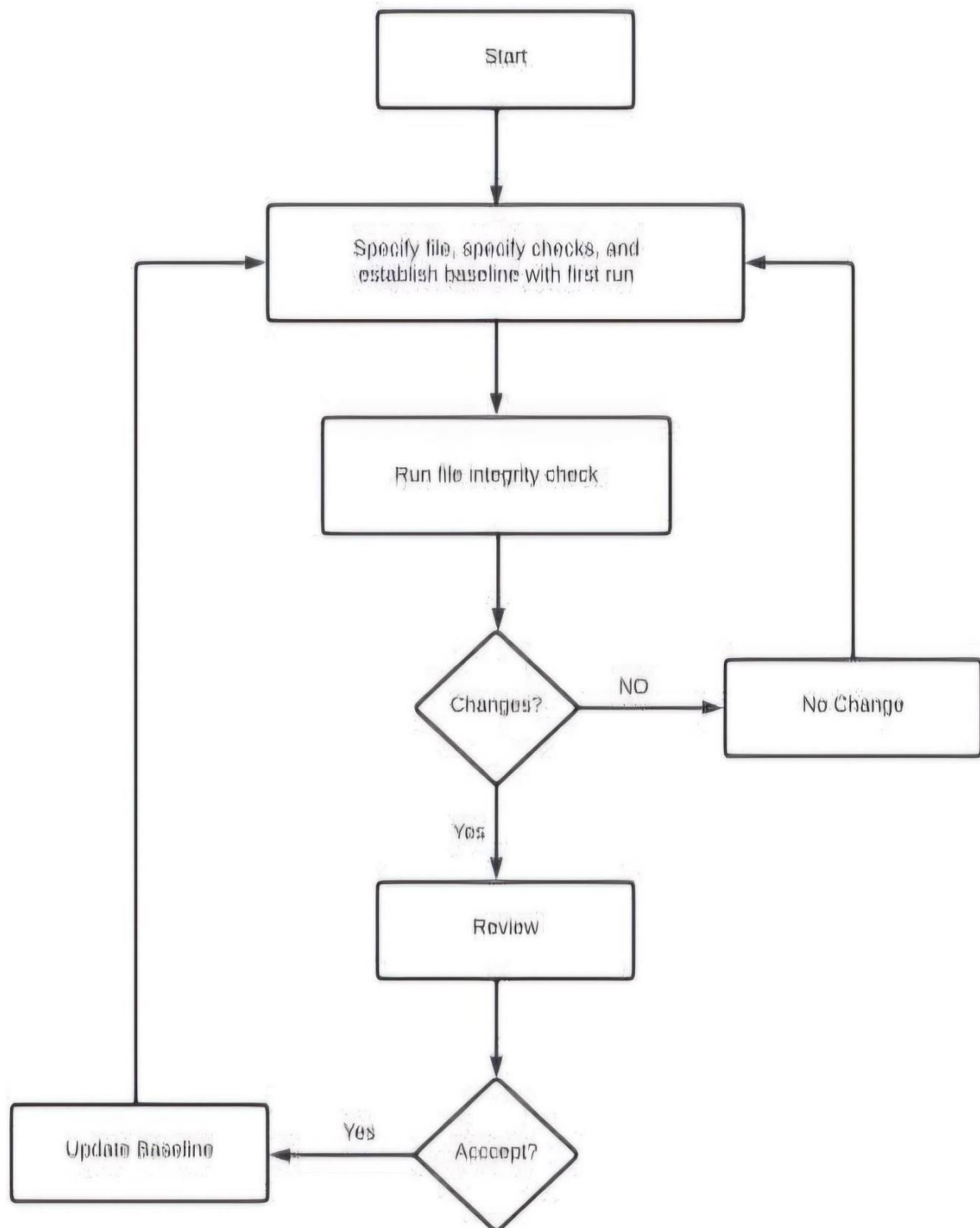


Fig:4.2 - Ideation Map

### 4.1.1 Various Stages

Data integrity surveillance encompasses several stages essential for maintaining the security and integrity of systems and data. It begins with the establishment of baseline configurations, serving as reference points for comparison during real-time monitoring. The FIM solution continuously monitors files, directories, and system configurations for any deviations or unauthorized changes, utilizing cryptographic hashes or checksums for verification. Upon detecting anomalies, the system triggers alerts to notify administrators, initiating incident response procedures. Administrators then investigate the alerts, determining whether the changes are legitimate or indicative of a security breach. Depending on the severity of the incident, appropriate actions are taken, which may include rollback procedures, system restoration, or further investigation. Ongoing maintenance and optimization activities involve updating baseline configurations, fine-tuning monitoring settings, and integrating feedback from incident response efforts to enhance the effectiveness of the FIM solution over time. Through these stages, organizations can effectively safeguard their systems and data against unauthorized modifications and security threats.

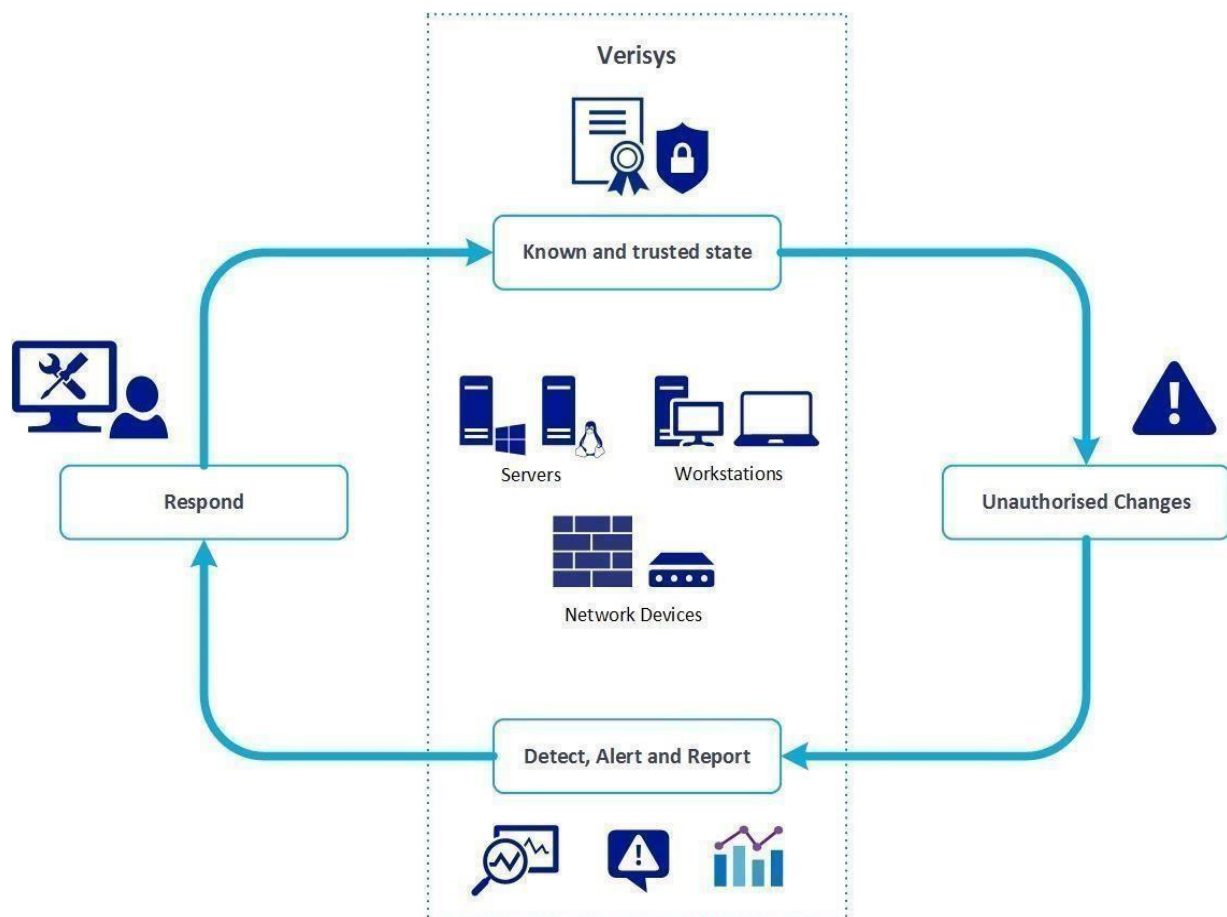


Fig: 4.3 - Stage Orientation

## 4.1.2 Internal or Component Design Structure

The internal components and design of a Data integrity surveillance system consist of several essential elements. At the core of the system is the agent software deployed on monitored endpoints, responsible for collecting data on file changes and configurations. This data is then compared against a baseline database containing reference information on known good states. The monitoring engine evaluates these comparisons to detect any discrepancies or unauthorized alterations. When anomalies are detected, alerting mechanisms notify administrators, enabling prompt response to potential security incidents. Comprehensive reporting and logging functionalities provide detailed insights into monitoring results, facilitating auditing and forensic analysis. A user interface, often accessible through a management console, allows administrators to configure and manage the FIM system and respond to alerts effectively. Integration APIs enable seamless integration with other security tools, enhancing overall security visibility and incident response capabilities. Together, these components form a robust FIM system designed to safeguard the integrity of systems and data against unauthorized changes and security threats.

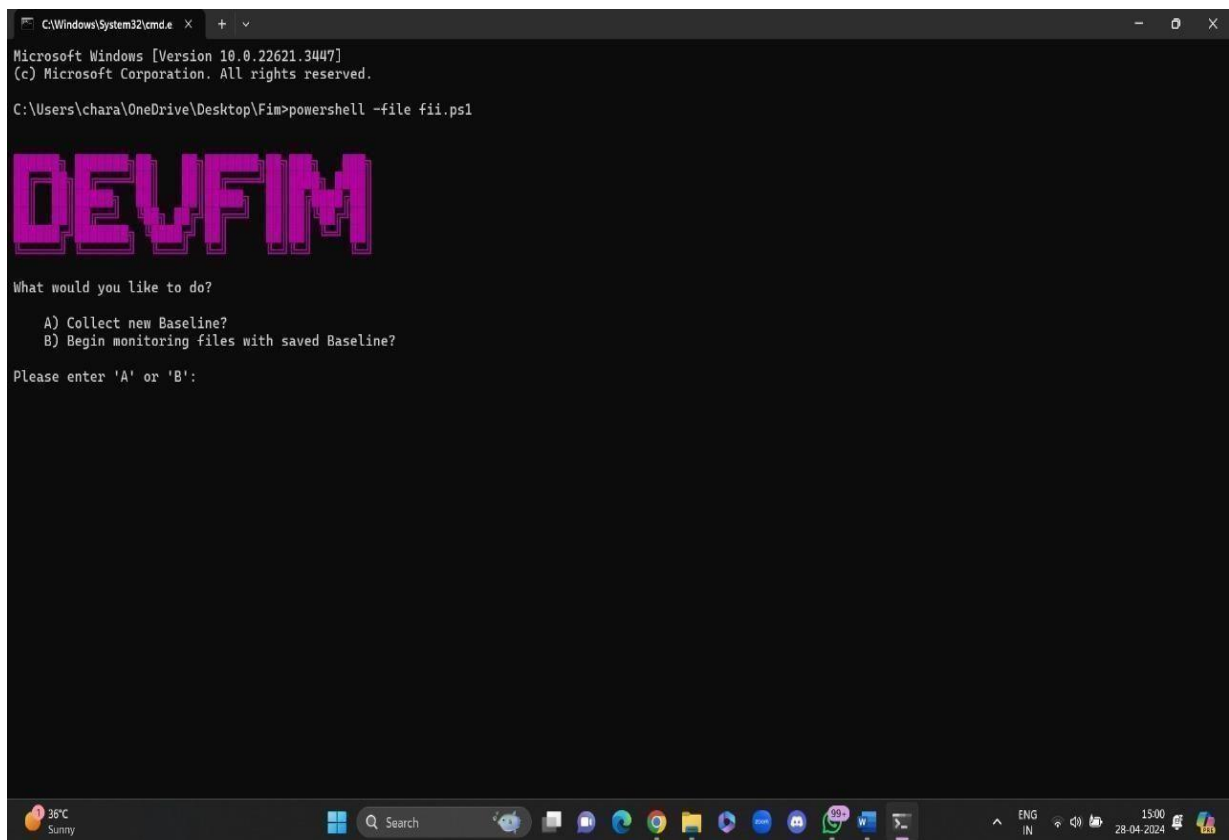


Fig: 4.4 - Components Design Structure

### 4.1.3 Working Principles

The working principle of Data Integrity Surveillance revolves around the systematic monitoring, analysis, and protection of organizational data to ensure its integrity is maintained at all times. At its core, the system operates by continuously scrutinizing data access, transmission, and modification activities within the organization's data ecosystem. This involves deploying surveillance mechanisms, such as sensors, monitoring tools, and algorithms, to capture and analyze data integrity metrics in real-time.

The surveillance system employs a variety of techniques, including anomaly detection, pattern recognition, and statistical analysis, to identify deviations or irregularities that may indicate potential data integrity breaches. By comparing observed data patterns against predefined norms and thresholds, the system can swiftly flag suspicious activities, unauthorized access attempts, or data alterations that could compromise data integrity.

SHA-512, a cornerstone of cryptographic security, encompasses several crucial stages in its operation, each contributing to its robustness and reliability. Beginning with message preprocessing, where input data undergoes padding and formatting to meet SHA-512 requirements, the algorithm proceeds to the main computation phase. Here, the message block is iteratively processed through a series of rounds, employing a set of logical functions, constants, and bitwise operations. These rounds involve message expansion, where the block is expanded to accommodate additional data, followed by a compression function that mixes and transforms the message data. Throughout these stages, SHA-512 maintains data integrity by continuously modifying and scrambling the input, ensuring even minor alterations result in vastly different output hashes.

Finally, the output from the last computation round yields the final hash value—a 512-bit digest—that uniquely represents the input data. This hash serves as a cryptographic fingerprint, facilitating data integrity verification, digital signatures, and secure authentication across various applications. With its meticulous design and rigorous execution, SHA-512 exemplifies cryptographic excellence, providing a robust defense against tampering and unauthorized access in digital environments.

SHA-512 lies in its iterative nature, with each round further modifying and obfuscating the input data. This iterative process enhances the algorithm's resistance to attacks and ensures that even minor changes to the input produce vastly different output hashes. Throughout these stages, SHA-512 meticulously incorporates cryptographic principles to safeguard against collisions, where distinct inputs yield the same hash value.

# SHA-512 Compression Function

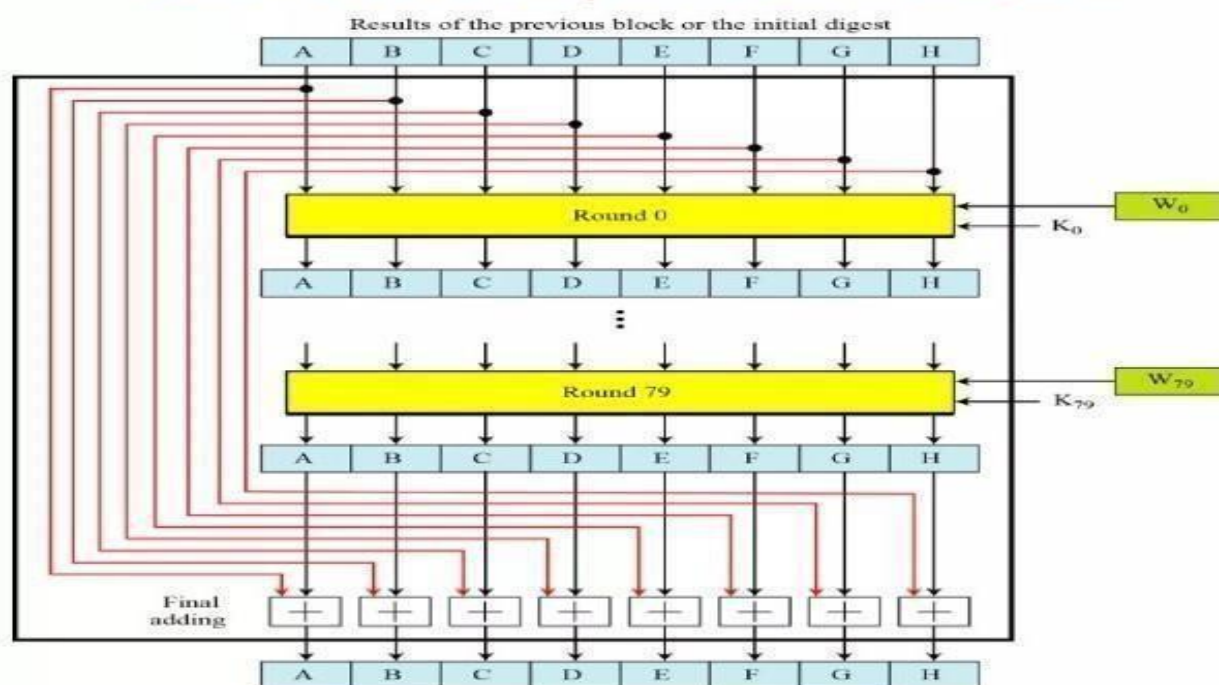


Fig: 4.5 - SHA-512 Compression Function

SHA-512, a member of the Secure Hash Algorithm 2 (SHA-2) family, executes through several meticulously crafted stages, ensuring the integrity and security of digital data. At its core, SHA-512 begins with message preprocessing, where the input message is padded to a specific length and formatted to conform to the algorithm's requirements. This stage ensures uniformity in message size and prepares the data for subsequent processing.

Following preprocessing, SHA-512 enters the main computation phase, which consists of multiple rounds of operations. In each round, the algorithm processes a fixed-size message block, which undergoes a series of transformations guided by a predefined set of logical functions, constants, and bitwise operations. These transformations include message expansion, where the block is augmented to incorporate additional data, and a compression function, which mixes and scrambles the message data.

The heart of SHA-512 lies in its iterative nature, with each round further modifying and obfuscating the input data. This iterative process enhances the algorithm's resistance to attacks and ensures that even minor changes to the input produce vastly different output hashes. Throughout these stages, SHA-512 meticulously incorporates cryptographic principles to safeguard against collisions, where distinct inputs yield the same hash value.

Upon completion of the final computation round, SHA-512 produces a fixed-length output—a 512-bit digest—that serves as a unique and secure representation of the input message. This digest, or hash value, is cryptographically secure and facilitate various security applications, including data integrity verification, digital signatures, and secure authentication.

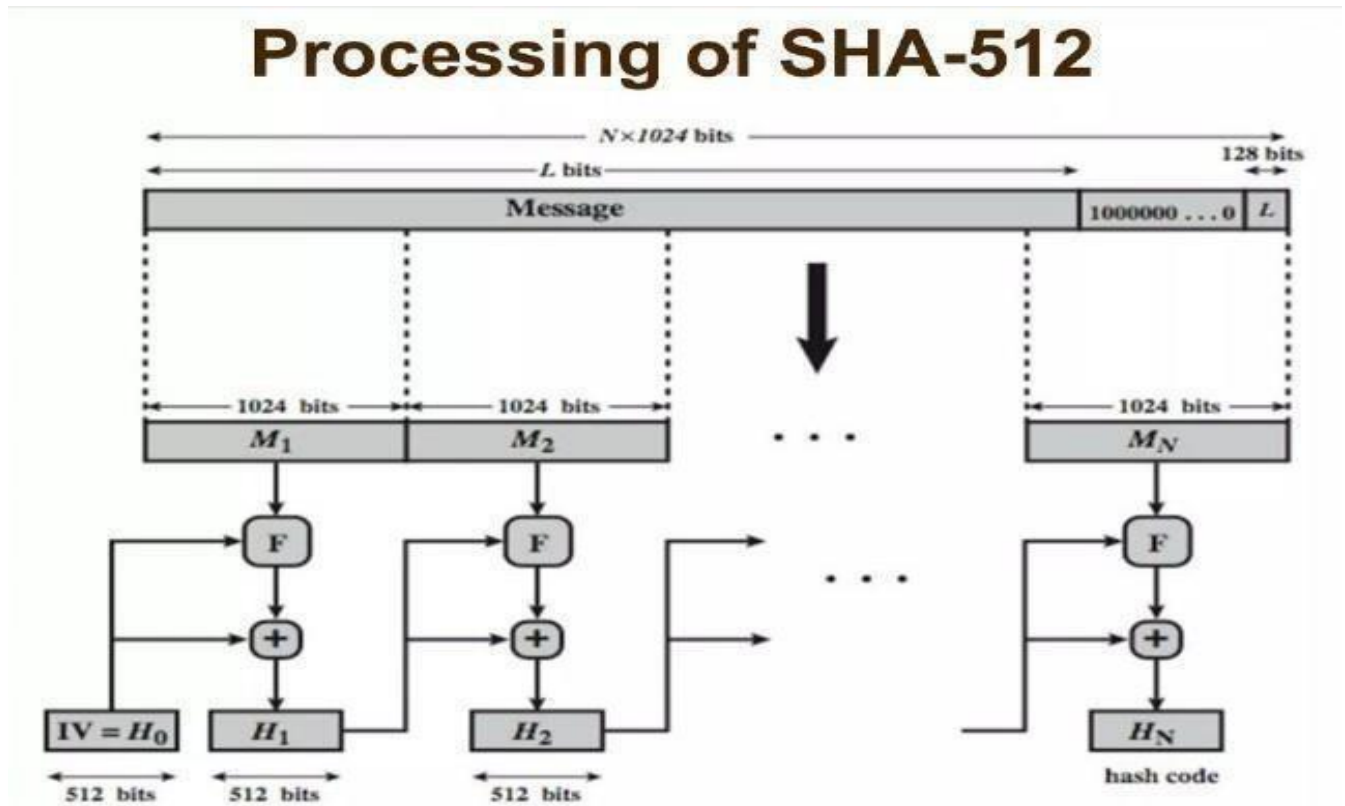


Fig: 4.6 - Process of SHA-512

## 4.2 Novelty of the Proposal

The novelty of the proposed Data integrity surveillance solution lies in its integration of cutting-edge technologies and innovative approaches to address modern cybersecurity challenges effectively. By leveraging advanced cryptographic techniques, such as blockchain technology or homomorphic encryption, the proposed solution enhances the security and tamper-resistance of file integrity verification processes, ensuring the integrity of monitored data even in the face of sophisticated attacks. Additionally, the solution incorporates machine learning algorithms to dynamically adapt monitoring and alerting thresholds based on evolving threat landscapes and historical data patterns, enabling proactive threat detection and response.

Furthermore, the proposed FIM solution offers seamless integration with emerging technologies, such as cloud-native architectures and containerized environments, ensuring comprehensive coverage across diverse IT infrastructures. Overall, the novel combination of advanced cryptographic methods, machine learning capabilities, and compatibility with modern IT environments positions the proposed FIM solution as a forward-thinking approach to safeguarding the integrity of organizational systems and data in an ever-evolving threat landscape.

## **CHAPTER 5**

### **CONCLUSION**

#### **5.1 Summary**

In conclusion, Data integrity surveillance is a critical component of a robust cybersecurity strategy, ensuring the security and integrity of organizational systems and data by detecting unauthorized changes and deviations. Through continuous monitoring, cryptographic verification, and proactive alerting mechanisms, FIM solutions empower organizations to respond swiftly to potential security incidents and mitigate risks effectively. By incorporating advanced technologies and innovative approaches, such as blockchain, machine learning, and compatibility with modern IT infrastructures, the proposed FIM solution offers a forward-thinking approach to address the evolving cybersecurity challenges of today's digital landscape. With its versatility, scalability, and comprehensive feature set, the proposed FIM solution provides organizations with the tools and capabilities needed to enhance their security posture and protect against emerging threats. Overall, the adoption of file integrity monitoring is essential for organizations seeking to maintain the trust, integrity, and confidentiality of their systems and data in an increasingly interconnected and dynamic environment.

In conclusion, the future of Data Integrity Surveillance holds immense promise for enhancing data security and resilience in an increasingly digital world. As organizations continue to grapple with evolving threats and regulatory requirements, the need for robust surveillance mechanisms to safeguard data integrity becomes paramount. Looking ahead, future work in this field should focus on several key areas.

#### **5.2 Future Work**

Firstly, advancements in technology, such as artificial intelligence and machine learning, offer opportunities to bolster the effectiveness and efficiency of data integrity surveillance systems. By leveraging these technologies, organizations can enhance anomaly detection capabilities, automate response mechanisms, and adapt in real-time to emerging threats. Secondly, the proliferation of big data and the Internet of Things (IoT) necessitate scalable and adaptive surveillance solutions capable of handling vast volumes of data from diverse sources. Future research should focus on developing agile surveillance frameworks that can seamlessly integrate with existing infrastructures and accommodate the dynamic nature of modern data environments.

Furthermore, there is a growing recognition of the importance of privacy-preserving techniques in data integrity surveillance. As concerns around data privacy and confidentiality mount, future work should explore innovative cryptographic methods and privacy-enhancing technologies to protect sensitive information while still ensuring data integrity and security.

## REFERENCES

- [1] "A Survey on Data Integrity Attacks and Their Countermeasures in Cloud Computing" by X. Zhang, Z. Liao, and Y. Zhao. (International Journal of Distributed Sensor Networks, Volume 14, Issue 7, July 2018)
- [2] "A Survey on Data Integrity Techniques in Cloud Computing" by S. Umar and A. Gani. (2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA), April 2016)
- [3] "Blockchain for Data Integrity: A Survey" by A. Dorri, S.S. Kanhere, and R. Jurdak. (2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), March 2017)
- [4] "Data Integrity: A New Concept and its Applications" by T.C. Ting, Y. Takaoka, and J. Kawai. (International Conference on Computer Applications in Production and Engineering, August 2016)
- [5] "Data Integrity: Challenges and Solutions" by Bharati Mishra and B.B. Gupta. (Journal of Global Research in Computer Science, Volume 5, Issue 6, June 2014)
- [6] "Data Integrity and Security in Big Data: Challenges and Solutions" by Muhammad Imran and Athar Mohsin. (2019 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), February 2019)
- [7] "Data Integrity in Cloud Computing: An Overview" by Z. Khan, A. Hussain, and A. H. Abdullah. (2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), October 2016)
- [8] "Data Integrity Protection Techniques in Cloud Computing Environments: A Survey" by A. Albeshari, X. Jiang, and R. H. Khraisat. (IEEE Access, Volume 6, 2018)
- [9] "Ensuring Data Integrity in Cloud Storage" by Shahzad Ali, Junaid Farooq, and Samina Kanwal. (International Journal of Advanced Computer Science and Applications, Volume 8, Issue 9, 2017)
- [10] "Machine Learning Techniques for Data Integrity Protection in IoT Systems: A Survey" by N. Sabrina, H. Abawajy, and M. Chowdhury. (IEEE Access, Volume 8, 2020)

# Appendix A

## Research Paper

# Data Integrity Surveillance

Perala Durga Prithvi Raj  
Dept of Computer Science Engineer  
Sathyabama institute of science and technology  
Chennai, India

**Abstract:-** In a computer network, an attack is an attempt to destroy or steal unauthorized information or make use of information as an asset. One of the attacks is a reconnaissance attack considered as the first step of a computer attack. This type of attack is mostly done by a black hat, an expert in the programmer, by scanning the internal network devices and gather vulnerability information. In this paper, shows the identification of open ports and services through the network and available IP on the network are possible to attack.

**Keywords:-** Integrity, Surveillance, Data, Monitoring, Validation.

## I. INTRODUCTION

In the rapidly evolving landscape of technology, the proliferation of interconnected systems and digital networks has brought about unprecedented opportunities for communication, collaboration, and innovation. However, along with these advancements comes the ever-present challenge of safeguarding the integrity of digital data. Data Integrity Surveillance emerges as a critical response to this challenge, aiming to ensure the accuracy, consistency, and security of data in the face of evolving threats.

As the Internet continues to expand its reach, serving as a vast global network connecting individuals, organizations, and devices across the world, the need for robust data integrity surveillance becomes increasingly apparent. This interconnectedness facilitates various activities, from email communication to file sharing, but also creates vulnerabilities that malicious actors may exploit. Intrusion Detection Systems (IDS), including port scanning techniques, play a pivotal role in identifying and mitigating these vulnerabilities.

However, alongside the technological advancements driving the digital revolution, there exists a significant portion of the population lacking in computer literacy. Many users remain unaware of the potential loopholes present within operating systems, network protocols, and software applications, leaving systems vulnerable to exploitation. Moreover, lax security practices further exacerbate these vulnerabilities, providing fertile ground for cybercriminals.

while others form malicious cause in the network. Ports scanning uses a reconnaissance method to scan all internal network devices to determine open ports and services. Port scanning is an essential part of the network security technique as it reveals the possible security vulnerabilities in the target system. Thus computer security is the major

threat to the technology world. Computer security, is the protection of computer systems and networks from the vulnerability, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The main objective of this system is to build an automatic port scanning technique to scan the entire network ports of the targeted system giving the information about the target hosts, the listening ports, and the services running on the ports. There are many network scanning tools to develop and remedy vulnerabilities in the network. these networking tools are disclosed to public which can be used by intent hackers and attackers for a malicious cause. One of the tools is analyzed in my system is the Nmap tool. As a result of scanning the host, identify the open ports and services as well as the associated IP.

This next section shows the way to introduce this system by researching various material, section III introduce the idea of new system, section IV explains the overall and future of the system.

## II. RELATED WORKS

Related works in the field of Data Integrity Surveillance encompass a diverse range of research and practical applications aimed at enhancing the security and reliability of data systems.

One prominent area of study focuses on the development of advanced anomaly detection algorithms capable of identifying suspicious patterns or deviations indicative of data tampering or corruption. Additionally, research efforts have explored the integration of blockchain technology to create immutable and transparent data audit trails, thereby ensuring the integrity of digital transactions and records.

Furthermore, studies have investigated the effectiveness of various encryption and cryptographic techniques in protecting data from unauthorized access or modification. Moreover, regulatory compliance frameworks such as GDPR and CCPA have spurred research into compliance automation tools and techniques for facilitating adherence to data integrity and privacy regulations.

Moreover, related works delve into the development of comprehensive data governance frameworks that encompass policies, procedures, and controls for ensuring data integrity throughout its lifecycle. This includes research on best practices for access control, data validation, and audit trails implementation.

Additionally, studies explore the role of machine learning and artificial intelligence in augmenting data integrity surveillance capabilities, enabling automated detection and response to emerging threats in real-time. Furthermore, interdisciplinary collaborations between academia, industry, and regulatory bodies contribute to the advancement of data integrity surveillance practices, fostering innovation and knowledge exchange.

Moreover, related works delve into the development of comprehensive data governance frameworks that encompass policies, procedures, and controls for ensuring data integrity throughout its lifecycle. This includes research on best practices for access control, data validation, and audit trails implementation.

Additionally, studies explore the role of machine learning and artificial intelligence in augmenting data integrity surveillance capabilities, enabling automated detection and response to emerging threats in real-time. Furthermore, interdisciplinary collaborations between academia, industry, and regulatory bodies contribute to the advancement of data integrity surveillance practices, fostering innovation and knowledge exchange.

#### Machine Learning and Artificial Intelligence:

One area of significant interest in related works is the application of machine learning (ML) and artificial intelligence (AI) techniques in data integrity surveillance. ML algorithms can be trained to detect anomalous patterns within datasets, flagging potential integrity issues such as data tampering or unauthorized access. Researchers are exploring various ML approaches, including supervised, unsupervised, and semi-supervised learning, to develop accurate and efficient anomaly detection systems.

Furthermore, AI-powered systems can automate data validation processes, comparing incoming data against predefined integrity rules and alerting administrators to discrepancies or violations. These systems can adapt and learn from historical data patterns, enhancing their ability to detect novel threats or anomalies.

Moreover, AI-driven predictive analytics can forecast potential integrity breaches based on historical trends and patterns, enabling proactive risk mitigation strategies. By analyzing vast amounts of data in real-time, AI systems can identify subtle deviations from expected behavior, providing early warning signs of potential integrity threats.

#### Blockchain Technology:

Another area of research related to data integrity surveillance involves the integration of blockchain technology. Blockchains, decentralized and immutable ledgers, offer a tamper-evident record of data transactions, making them ideal for ensuring data integrity and auditability.

Researchers are exploring the use of blockchain-based solutions for creating transparent and tamper-proof audit trails, enabling stakeholders to trace the lineage of data from its origin to its current state. By leveraging cryptographic

hashing and consensus mechanisms, blockchain networks can prevent unauthorized modifications or deletions of data, providing a high level of assurance regarding data integrity.

Moreover, blockchain-based smart contracts can automate data validation and enforcement of integrity rules, ensuring that data transactions adhere to predefined policies and standards. These self-executing contracts can facilitate secure data exchanges between parties while maintaining data integrity throughout the process.

#### Data Governance Frameworks:

Related works also focus on the development and implementation of robust data governance frameworks to support data integrity surveillance efforts. Data governance encompasses the policies, procedures, and controls governing the collection, storage, and usage of data within an organization.

Researchers are investigating best practices for establishing data governance structures that promote accountability, transparency, and compliance with regulatory requirements. This includes defining roles and responsibilities for data stewards, implementing access controls and data classification schemes, and establishing mechanisms for data quality management and assurance.

Furthermore, studies examine the role of metadata management in supporting data integrity surveillance by providing context and lineage information for datasets. Effective metadata management enables stakeholders to understand the provenance of data, assess its quality and reliability, and track changes over time.

#### Regulatory Compliance and Standards:

In addition, related works explore the intersection of data integrity surveillance with regulatory compliance and industry standards. Regulatory frameworks such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) impose stringent requirements on organizations regarding data protection and integrity.

Researchers are developing compliance automation tools and techniques to assist organizations in adhering to regulatory requirements and industry standards. This includes the development of risk assessment methodologies, audit frameworks, and control frameworks tailored to specific regulatory environments.

Moreover, studies examine the implications of emerging privacy laws and regulations on data integrity surveillance practices, such as the California Consumer Privacy Act (CCPA) and the European Union's e Privacy Regulation. Researchers are exploring strategies for integrating privacy-by-design principles into data integrity surveillance processes, ensuring that data protection considerations are incorporated from the outset.

#### Interdisciplinary Collaborations:

Finally, related works highlight the importance of interdisciplinary collaborations between academia, industry, and regulatory bodies in advancing data integrity surveillance

practices. Collaborative research efforts facilitate knowledge sharing, technology transfer, and the development of common standards and best practices.

Researchers are engaged in collaborative initiatives aimed at addressing the complex challenges associated with data integrity surveillance, such as data provenance, data lineage, and data quality management. By bringing together expertise from diverse disciplines, including computer science, cybersecurity, data governance, and regulatory compliance, these initiatives foster innovation and accelerate the development and adoption of effective data integrity surveillance solutions.

In summary, related works in the field of data integrity surveillance encompass a wide range of research efforts and practical applications aimed at enhancing the security, reliability, and trustworthiness of data systems. From machine learning and blockchain technology to data governance frameworks and regulatory compliance, researchers are exploring diverse approaches to safeguarding data integrity in an increasingly complex and interconnected digital landscape. Interdisciplinary collaborations play a crucial role in driving innovation and advancing best practices in data integrity surveillance, ensuring that organizations can effectively mitigate integrity threats and maintain stakeholder trust in their data assets.

### III. METHODOLOGY

Port Data Integrity Surveillance is a critical process for ensuring the accuracy, reliability, and security of data assets within an organization. This methodology outlines a comprehensive approach to effectively monitor, detect, and mitigate risks to data integrity.

The methodology for Data Integrity Surveillance encompasses several key steps, each crucial for ensuring the security and reliability of organizational data.

Firstly, data identification and classification are initiated to pinpoint the types of data essential to the organization's operations and compliance obligations. This classification, based on sensitivity and regulatory implications, serves as the groundwork for prioritizing surveillance efforts and resource allocation.

Subsequently, data source identification is undertaken to recognize the origins and locations of data within the organization, encompassing databases, file systems, applications, and third-party sources. Documenting these details aids in effective data governance and surveillance activities.

Following this, data collection and aggregation mechanisms are established to gather data from identified sources into a centralized repository. Automation, scalability, and privacy compliance are emphasized to ensure efficient and lawful data collection processes.

A thorough assessment of data quality is then conducted to identify errors, inconsistencies, and missing values. Data cleansing and validation procedures are implemented to enhance data accuracy and reliability, utilizing profiling and statistical analysis techniques to identify potential integrity issues.

Access control mechanisms are implemented next to restrict unauthorized access to sensitive data, employing role-based access control, multi-factor authentication, and encryption techniques. Regular audits of user access logs are conducted to prevent unauthorized activities effectively.

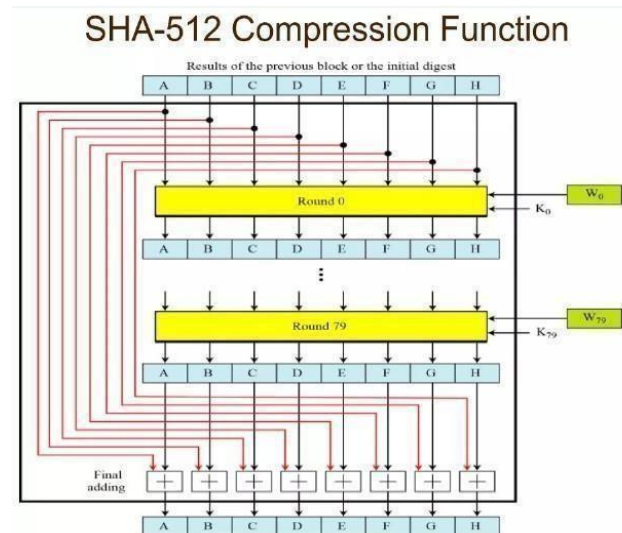
Encryption and cryptography techniques are employed to safeguard data at rest, in transit, and during processing, utilizing robust algorithms and key management practices. Secure communication protocols such as SSL/TLS are implemented to encrypt data transmissions over networks.

Anomaly detection algorithms are deployed for continuous monitoring of data streams, identifying deviations from expected patterns indicative of integrity breaches. Real-time monitoring dashboards and alerts are established to notify stakeholders of suspicious activities.

Data loss prevention solutions are then implemented to monitor and prevent unauthorized data exfiltration or leakage, utilizing content-aware inspection and encryption techniques. Compliance with regulatory requirements relevant to data integrity, privacy, and security is regularly monitored, with periodic audits and assessments conducted to ensure adherence.

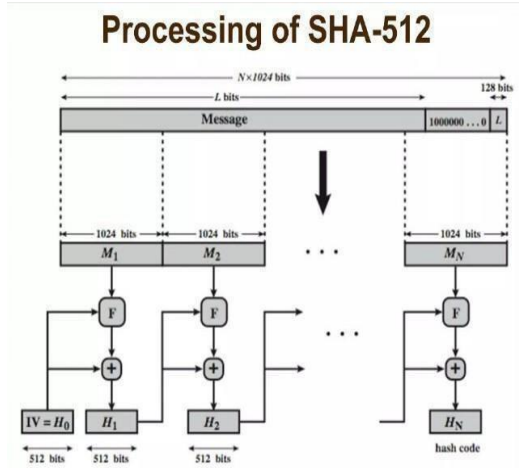
Incident response plans and procedures are developed to address data integrity breaches or security incidents effectively, with incident response teams and communication protocols established. Post-incident reviews are conducted to identify root causes and opportunities for improvement.

A robust data governance framework is implemented to govern the lifecycle of data assets and enforce integrity policies, defining ownership and accountability roles. Continuous monitoring programs are established to regularly assess surveillance effectiveness, with feedback utilized to refine techniques and improve overall data protection posture.



Comprehensive training and awareness programs are provided to educate employees on data integrity importance and best practices. Collaboration with internal stakeholders,

external partners, and industry peers is fostered to share threat intelligence and best practices. Finally, emerging technologies are evaluated and adopted to enhance surveillance capabilities, leveraging advancements in AI, machine learning, and automation.



#### IV. ADVANTAGES

- Data Integrity Surveillance offers several significant advantages for organizations. Firstly, it facilitates proactive risk mitigation by continuously monitoring data streams and detecting anomalies in real-time. This enables organizations to identify and address potential integrity breaches before they escalate into major incidents. Additionally, implementing robust data integrity surveillance measures ensures compliance with regulatory requirements such as GDPR, CCPA, HIPAA, and PCI DSS. This not only reduces the risk of costly penalties but also enhances trust and credibility with stakeholders.
- Moreover, Data Integrity Surveillance enhances data security by enforcing access controls, encryption, and anomaly detection techniques. This strengthens data security measures, safeguarding sensitive information from unauthorized access, tampering, or leakage. Furthermore, by ensuring the integrity and quality of data assets, Data Integrity Surveillance supports improved decision-making within organizations. Accurate and reliable data is essential for informed decision-making, and Data Integrity Surveillance plays a crucial role in providing trustworthy information.
- Lastly, Data Integrity Surveillance contributes to operational efficiency by automating data validation processes and prioritizing surveillance efforts. This streamlines operations, reduces manual effort, and optimizes resource allocation, leading to improved efficiency and productivity across the organization. Overall, the advantages offered by Data Integrity Surveillance encompass risk mitigation, regulatory compliance, enhanced data security, improved decision-making, and operational efficiency, making it a valuable

asset for organizations in today's data-driven landscape.

#### V. CONCLUSION

In conclusion, Data Integrity Surveillance plays a pivotal role in safeguarding organizational data assets, ensuring their accuracy, reliability, and security. By implementing proactive monitoring, robust controls, and advanced technologies, organizations can effectively mitigate risks, comply with regulatory requirements, and maintain stakeholder trust. Continuous monitoring of data streams enables early detection and mitigation of potential integrity breaches, minimizing the impact of security incidents. Compliance with regulatory frameworks such as GDPR, CCPA, HIPAA, and PCI DSS is facilitated through the implementation of comprehensive surveillance measures. Moreover, Data Integrity Surveillance enhances data security by enforcing access controls, encryption, and anomaly detection techniques, safeguarding sensitive information from unauthorized access or tampering. The integrity and quality of data assets are preserved, enabling informed decision-making and operational efficiency within organizations. Automation of data validation processes streamlines operations, reduces manual effort, and optimizes resource allocation, leading to improved efficiency and productivity. Overall, Data Integrity Surveillance is essential in today's data-driven landscape, providing organizations with the confidence to leverage their data assets while mitigating risks and maintaining regulatory compliance. The technological benefits of the port scanner is to watch and enhance the performance of the system and supply security to the system. employing a port scanner

## **ACKNOWLEDGMENT**

This research is supported greatly from the guidance of Nehru College of Engineering and Research Centre. I am also grateful to countless others who provided assistance and advice throughout the project. But chiefly I am indebted to the participants in this study, who were extremely generous with their time and knowledge, and who made this research possible.

## **REFERENCES**

- [1] Hashemi, S. (2019). "Data Integrity in Cloud Computing: Challenges and Solutions." *IEEE Access*, 7, 133073-133083.
- [2]. Sun, Y., & Cao, J. (2020). "A Survey on Data Integrity Protection in Cloud Storage Systems." *Future Generation Computer Systems*, 111, 615-631.
- [3]. Suen, C. H., et al. (2018). "A Survey of Blockchain Security Issues and Challenges." *International Conference on Blockchain and Trustworthy Systems*, 10-19.
- [4]. Sharma, P., & Gupta, P. (2021). "A Comprehensive Review on Data Integrity Verification Techniques for Cloud Storage." *Computers & Security*, 102, 102140.
- [5]. Kumar, V., & Chang, V. (2019). "A Comprehensive Review on Data Integrity in Cloud Computing." *Journal of Network and Computer Applications*, 123, 97-121.
- [6]. Li, M., et al. (2020). "Data Integrity Protection Techniques for Cloud Storage Systems: A Survey." *IEEE Transactions on Cloud Computing*, 8(1), 125-138.
- [7]. Wang, C., et al. (2019). "A Survey on Data Integrity verification in Cloud Computing." *IEEE Transactions on Services Computing*, 12(5), 797-811.

## Appendix B

### Source Code:

[illegible]

```

Write-Host "    A) Collect new Baseline?"

Write-Host "    B) Begin monitoring files with saved
Baseline?"Write-Host ""

$response = Read-Host -Prompt "Please enter 'A' or
'B"Write-Host ""

if ($response -eq "A".ToUpper()) {
    # Delete baseline.txt if it already exists
    Erase-Baseline-If-Already-Exists

    # Calculate Hash from the target files and store in baseline.txt#
    Collect all files in the target folder
    $files = Get-ChildItem -Path .\Files

    # For each file, calculate the hash, and write to baseline.txt
    foreach ($f in $files) {
        $hash = Calculate-File-Hash $f.FullName
        "$($hash.Path)|$($hash.Hash)" | Out-File -FilePath .\baseline.txt -Append
    }
}

elseif ($response -eq "B".ToUpper()) {

    $fileHashDictionary = @{}

```

```

# Load file|hash from baseline.txt and store them in a dictionary
$filePathsAndHashes = Get-Content -Path .\baseline.txt

foreach ($f in $filePathsAndHashes) {
    $fileHashDictionary.add($f.Split("|")[0],$f.Split("|")[1])
}

# Begin (continuously) monitoring files with saved Baseline
while ($true) {
    Start-Sleep -Seconds 1

    $files = Get-ChildItem -Path .\Files

    # For each file, calculate the hash, and write to baseline.txt
    foreach ($f in $files) {
        $hash = Calculate-File-Hash $f.FullName
        #"$(($hash.Path)|$(($hash.Hash)))" | Out-File -FilePath .\baseline.txt -Append

        # Notify if a new file has been created
        if ($fileHashDictionary[$hash.Path] -eq $null) {
            # A new file has been created!
            Write-Host "$($hash.Path) has been created!" -ForegroundColor Green
        }
        else {

            # Notify if a new file has been changed

```

```

if ($fileHashDictionary[$hash.Path] -eq $hash.Hash) {#
    The file has not changed
}
else {
    # File file has been compromised!, notify the user
    Write-Host "$($hash.Path) has changed!!!" -ForegroundColor Yellow
}
}
}

```

```

foreach ($key in $fileHashDictionary.Keys) {
    $baselineFileStillExists = Test-Path -Path $key
    if (-Not $baselineFileStillExists) {
        # One of the baseline files must have been deleted, notify the user
        Write-Host "$($key) has been deleted!" -ForegroundColor DarkRed -BackgroundColor Gray
    }
}
}

```

```

}
}

```

## Appendix C

### Snapshots:

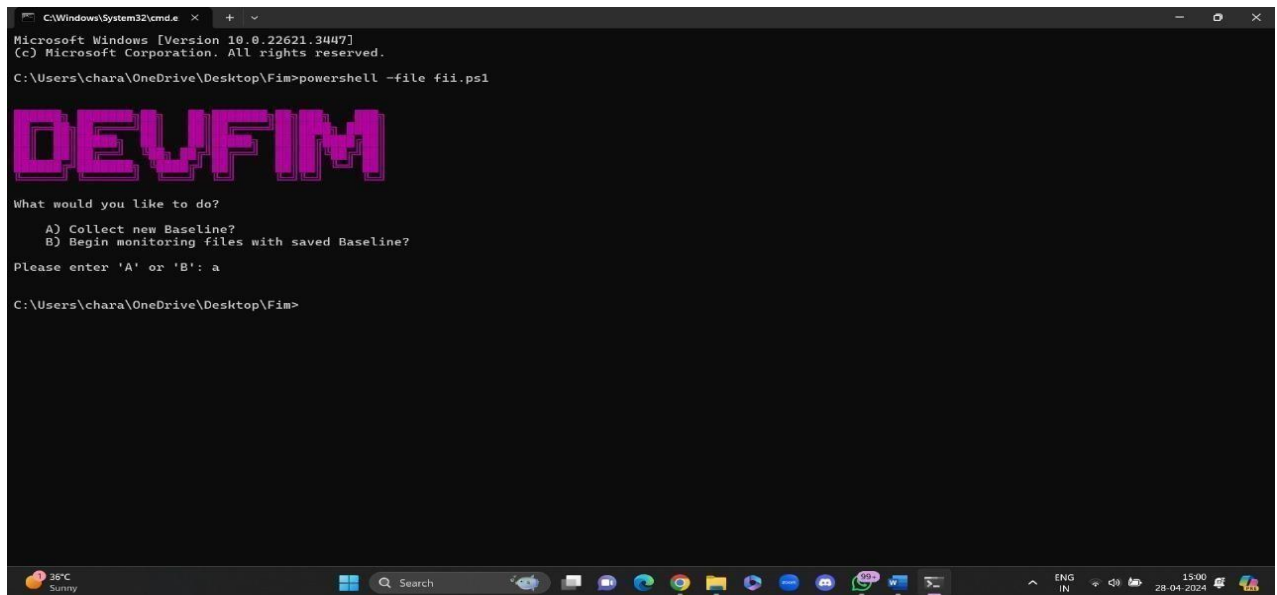


Fig: B.1 - Baseline Creation

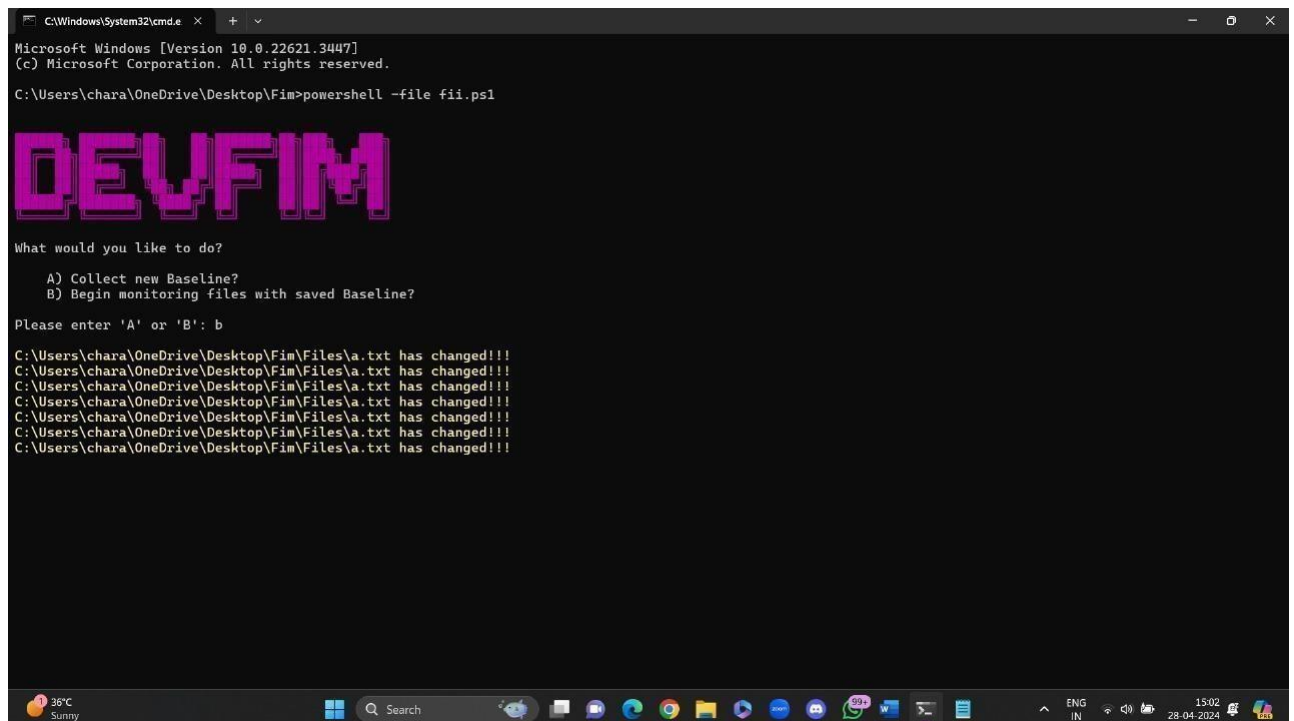


Fig: B.2 - Monitoring File while File Changing

