A SURVEY ON REAL-TIME FILE INTEGRITY DETECTION SYSTEM

E.RAJKUMAR
Department of Cyber Security
SRM Valliammai Engineering College
Tamilnadu,India
rajkumar.cys@srmvalliammai.ac.in

D.HARIHARAN
Department of Cyber Security
SRM Valliammai Engineering College)
Tamilnadu,India
hariharan@gmail.com

S.J. SANTHOSH
Department of Cyber Security
SRM Valliammai Engineering College)
Tamilnadu,India
santhoshsrinivasan2005@gmail.com

M.SARANRAJ
Department of Cyber Security
SRM Valliammai Engineering College)
Tamilnadu,India
saranrajmuthukuma@gmail.com

***Abstract*— A Survey on Real-Time File Integrity Detection System (RT-FIDS) is designed to monitor, detect, and manage file integration across diverse computing environments in real time. This system provides continuous monitoring of file exchanges between different systems or applications, ensuring that any file integration whether automated or manual is captured instantaneously. The system generates alerts via email, SMS, or dashboard notifications whenever a file modification occurs, ensuring that administrators or users are promptly informed. By employing machine learning techniques, RT-FIDS can learn from historical data and adapt to new types of file integration behaviors, improving its accuracy over time. This capability helps prevent data breaches, ensure data consistency, and enhance system security, especially in industries dealing with sensitive information, such as finance, healthcare, and government.**

Keywords: **Real-Time Detection,System Security, Cybersecurity, File Integrity**

I. INTRODUCTION

In today's digital landscape, securing sensitive files and ensuring their integrity is crucial for individuals and organizations alike. File integrity monitoring (FIM) systems play a vital role in cybersecurity by detecting unauthorized modifications, deletions, or alterations of important files. These systems help prevent data breaches, unauthorized access, and cyberattacks that

could compromise critical information. metadata in the form of a NFT contract. The NFT metadata is stored on a private blockchain to prevent unauthorized modifications. When accessing the file, the Merkle root is recalculated and compared to the original. The File Integration System is designed to track changes in files using cryptographic hash functions like SHA-256. By continuously monitoring files, the system can detect any unauthorized modifications and trigger an alert via SMS notifications using the Twilio API. This real-time alert mechanism enhances security by immediately informing users about potential threats or suspicious activities. NFT metadata in the form of a NFT contract. The NFT metadata is stored on a private blockchain to prevent unauthorized modifications. When accessing the file, the Merkle root is recalculated and compared to the original. If the Merkle root is not matched, original contents are restored. Only the owner of the NFT is allowed to modify the file. This enforces access control and file ownership verification. This decentralized approach provides a secure file integrity solution. This decentralized method uses cryptographic hashing and blockchain immutability to offer a safe file integrity solution.

II. LITERATURE SURVEY

A. Real-Time Dectection

The current detection and intervention capabilities of technologies operate through realtime detection systems. Real-time detection

 DOA:01.12.2025 / DOP: 10.12.2025 ISSN: 3048-619X
Volume 2 Issue 3 [Sep – Dec 2025] DOI:

operates as an essential security technology that works with industrial monitoring together with healthcare diagnostics alongside surveillance systems to protect operations. Real-time detection systems employ technological elements of automated detection with artificial intelligence (AI) and machine learning (ML) and big data analytics to analyze extensive data volumes for pattern recognition which leads to quick automated alerts or automatic responses.

Real-time network monitoring with intrusion detection systems detects unauthorized access attempts together with malware and unexpected activities in cyber security environments. Artificial Intelligence models collaborate with behavior-based analytics to detect threats at their minimal size before causing serious harm. Real-time anomaly detection systems protect industrial equipment through sensor analysis which determines needed maintenance operations beforehand. A smart factory monitoring system uses present-time operations to detect equipment anomalies that protect operational safety and maintain efficiency.

Healthcare facilities underwent extensive transformation in their medical diagnostic systems through implementing real-time detection techniques. Together AI-powered imaging systems and biosensor technologies enable doctors to spot diseases immediately thus establishing better early detection methods. Wearable healthcare devices track vital signs to both notify doctor specialists and users about dangerous heart situations and declining oxygen concentrations.

Real-time detection systems encounter two main difficulties when receiving huge datasets and requires quick actions that preserve exact results. Engineers employ edge computing with optimized network systems to develop advanced algorithms which solve real-time detection problems to enable the technology to function better across different industrial sectors. Real-time detection will preserve its

essential status in critical applications while developing security enhancements and operational efficiency as well as improved decision-making capacity through technological advancements.

B. System Security

The multi-layered system security framework functions as a defense mechanism to protect computer systems and networks and sensitive information from unauthorized access along with cyberattacks and maintains operational continuity. Access control methods and encryption tools along with intrusion detection join incident responses to protect digital assets through system security while maintaining availability and confidentiality and integrity. Critical systems use MFA authentication joined with biometric verification and RBAC access controls to secure them from unauthorized entry points. Organizations protect their networks from DDoS attacks and MITM intrusions and malware through three core security elements which include firewalls and VPNs and IDPS systems.

Individual device protection under endpoint security requires endpoint detection and response solutions, application whitelisting features and antivirus software for defense against malware attacks. TLS with AES encryption establishes a secure data transfer which prevents both unauthorized parties from accessing the data flow and protects data from modification attempts. AI anomaly detection systems monitor both real-time activities and network data for user conduct anomalies that enable threat detection leading to prevention of cyberattacks.

Preventing system attacks necessitates examination of system weaknesses through penetration testing and continuous software updating because these actions prevent attackers from exploiting security vulnerabilities. Correct data protection against cyber attacks requires organizations to establish detailed incident response plans through threat containment

practices and forensic probing and disaster recovery protocols. Zero-trust architectural models coupled with artificial intelligence threat assessment capabilities face new defense system challenges that arise from zero-day vulnerabilities alongside both insider threats as well as evolving attack methods.

The expansion of system security protection towards the future depends on automation combined with behavioral analytics and cloud-native security solutions that fight against growing complex cyber threats. Systems security protection in upcoming years requires organizations and individual users to develop strategic security measures and conduct periodic system maintenance which combines protection against existing cyber attacks. System security protects digital trust and resilience by having effective policies linked with advanced technology users are aware of within current networked societies.

C. Cybersecurity

The discipline of securing digital systems through networks and sensitive information from unapproved access while defending against cyberattacks coming from unauthorized attackers is known as cybersecurity. The necessary security framework contains multiple elements that cover network security and endpoint protection and data encryption management and threat detection in real-time and identity protection services. The continuous monitoring and counteraction of cyber risks depends on organizations that use firewalls combined with intrusion detection and prevention systems (IDPS) and security information and event management (SIEM) solutions. Both Multi-factor authentication (MFA) with zero-trust security models and biometric verification strengthen identity protection because they enable authorized users to reach critical systems.

Data security operates as an essential cybersecurity principle that helps shield confidential information from unapproved

access and data disclosure. Data security during rest time and while being transmitted benefits completely from AES encryption protocols along with SSL/TLS security methods. Endpoint security protects individual devices using combined defense approaches that include antivirus applications and endpoint detection and response (EDR) technologies and application whitelisting systems to prevent unauthorized access and malware threats on computers as well as smartphones and IoT devices.

The essential usage of real-time monitoring through artificial intelligence (AI) and machine learning (ML) tools emerged due to escalating complex cyber threats. The AI-driven security tools scan massive network traffic records to detect particular deviations that AI applications eliminate before threats can lead to substantial harm. Insider threat detection happens through machine learning tools which track unusual data movement patterns and atypical login events. Ransomware protection holds an essential position because criminals now force organizations of all types to pay ransoms to regain access to encoded information.

Robust security frameworks have failed to stop zero-day vulnerabilities together with phishing attacks and persistent threats we call APTs despite their presence. Attack and pre-emptive assault strategies that exploit software vulnerabilities happen concurrently with hacker attempts to acquire user credentials and persistent infrastructure system attacks. Security battles can be won through continuous security learning programs in addition to repeated penetration assessments and planned incident response strategies.

The cybersecurity field is expanding because of cloud computing development alongside the implementation of remote work systems and Internet of Things (IoT). Organizations receive protection for their remote access solutions and decentralized IT systems through the combination of cloud security frameworks and secure access service edge (SASE) architectural designs along with endpoint security solutions. The implementation of rich data security

standards must comply with mandatory regulations such as GDPR and CMMC requirements that governments through regulatory bodies require businesses to follow.

Automation technology combined with quantum-resistant encryption alongside AI threat sensors must be developed to achieve security standards that match attackers capabilities in upcoming cybersecurity times. Security practices in digital environments as zero-day vulnerabilities, phishing attacks, and advanced persistent threats (APTs). Cybercriminals exploit software flaws before they are patched, use deceptive tactics to steal login credentials, and launch prolonged attacks on critical infrastructure. To combat these evolving threats, organizations must implement continuous security awareness training, regular penetration testing, and incident response planning.

The rise of cloud computing, remote work, and the Internet of Things (IoT) has further expanded the cybersecurity landscape. Cloud security frameworks, secure access service edge (SASE) architectures, and endpoint security solutions help mitigate the risks associated with remote access and decentralized IT environments. Governments File integrity is a crucial aspect of cybersecurity that ensures digital files remain unaltered, accurate, and protected from unauthorized modifications, corruption, or malicious tampering. It plays a vital role in safeguarding sensitive information, maintaining system stability, and ensuring compliance with regulatory requirements. Organizations implement File Integrity Monitoring (FIM) solutions to detect.

The security practice of file integrity functions as a primary cybersecurity element to protect digital files from unauthorized modification and ensure their accuracy while defending against tampering incidents. Digital security operations heavily depend on file integrity because it helps to protect information.

 DOA:01.12.2025 / DOP: 10.12.2025 ISSN: 3048-619X
Volume 2 Issue 3 [Sep – Dec 2025] DOI:

protect fundamental assets that include financial assets together with personal information and intellectual properties of corporations and national security infrastructure. Digital system resilience depends on combining budgetary commitments towards advanced cybersecurity solutions with extensive user education about cyber threats.

D. File Integrity

The fundamental method of file integrity verification relies on cryptographic hashing through hash value generation that uses SHA256, SHA-512, and MD5 algorithms. FIM systems generate alerts when any modification occurs however small to a file because the modification changes the hash value of the file. The security team can promptly respond after detecting unauthorized file modifications and malware intrusions and ransomware contaminations using this approach. Digital signatures along with checksum verification enable the maintenance of transmission file authenticity while detecting unauthorized alterations.

File integrity protection delivers defense against unauthorized modifications through the combination of role-based access controls (RBAC), audit logging and version control systems which work together for data preservation after compromise occurs. Organizations need to implement minimum authorization rules which grant modifying access rights only to authorized applications and system users. Security teams use automatic alert systems and forensic management tools to monitor current file modifications which create thorough documentation trails for standards assessment including ISO 27001, NIST 80053, PCI-DSS and HIPAA compliance.

Data protection demands file integrity preservation because this practice maintains both operational continuity and cybersecurity resilience. To protect their digital assets from unauthorized modifications organizations should deploy access controls together with monitoring systems that use cryptographic verification and automated security systems.

File integrity systems serve as prime targets for attackers who wish to conduct data breaches and ransomware attacks along with persistent advanced threats (APTs). System files attacked by adversaries generate backdoor gateways and security settings adjustments while encrypting information for extortion purposes. Success within organizations needs active prevention of and reduced integrity violations through the deployment of real-time FIM solutions that operate automatically and employ AI-powered anomaly detection to detect potential violations and manage automated updates.(with Identifier cloud computing and Internet of Things and remote work environments) it has become more challenging to uphold file integrity. Cloud-based FIM solutions monitor distributed systems through integration capabilities which track elements from containers applications and DevOps operations and hybrid environments. Blockchains' tamper-proof decentralized ledgers stand out as revolutionary technology for file integrity verification because they enhance security measures.

Data protection demands file integrity preservation because this practice maintains both operational continuity and cybersecurity resilience. To protect their digital assets from unauthorized modifications organizations should deploy access controls together with monitoring systems that use cryptographic verification and automated security systems. Advanced machine learning and artificial intelligence driven cybersecurity solutions have emerged as essential tools for detecting integrity violations since both technology approaches protect against evolving data manipulation and cyberattacks.

The security team can promptly respond after detection unauthorized file modifications and malware intrusions and ransomware contaminations using this approach.Digital signatures along with check verification enable cyber security.

III. CONCLUSION

Based on the study of the survey papers, we can conclude that real-time detection, file integrity monitoring and artificial intelligence driven anomaly detection are the most prominent technologies to protect system security, data integrity and rapid threat mitigation. Real-time detection identifies all unauthorized access and malicious activities, FIM ensures the integrity of critical files and AI driven anomaly detection enhances threat detection by analyzing behavioral patterns and network traffic. It can be used in cyber threat prevention, intrusion detection, regulatory compliance and forensic analysis. However, there are challenges like scalability, accuracy, false positive. Current research in machine learning-based threat prediction and blockchain-based file integrity, decentralized systems for security architecture provide new solutions to increase the accuracy for detection and resilience in the system.

REFERENCES

[1] M. A. Helmiawan, E. Julian, Y. Cahyan and A.Saeppani , "Experimental Evaluation of Security Monitoring and Notification on Network Intrusion Detection System for Server Security," in *IEEE Transactions on Information Forensics and Security*,pp.1-6, doi: 10.1109/ CITSM52892. 2024.88988.

[2] R. Zeng et al., "Bi-Level Resilient Control Solution for Distributed Feeder Automation System Under Hybrid Attack," in *IEEE Transactions on Smart Grid*, vol. 16, no. 1, pp. 301-312

[3] H. O. S. Varshith, S. Sural, J. Vaidya and V. Atluri, "Efficiently Supporting AttributeBased Access Control in Linux," in *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp.

[4] T. Zhu et al., "APTSHIELD: A Stable, Efficient and Real-Time APT Detection System for Linux Hosts," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 6, pp. 5247-5264

[5] R. Somers, S. Cunningham, S. Dart, S. Thomson ,C.Chua and E. Pickering ,"Assignment Watch: An Automated Detection and Alert Tool for Reducing

Academic Misconduct Associated With FileSharing Websites," in *IEEE Transaction on Learning Technologies*, vol. 17, pp. 310-318

[6] H. Goyel and K. S. Swarup, "Data Integrity Attack Detection Using Ensemble-Based Learning for Cyber–Physical Power Systems," in *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1198-1209

[7] W. Shen, C. Gai, J. Yu and Y. Su, "KeywordBased Remote Data Integrity Auditing Supporting Full Data Dynamics," in *IEEE Transactions on Services Computing*, vol. 17, no. 5, pp.2516-2529

[8] W. A. Bhat, "Performance- Baseline Estimation of File System Operations for Linux- Based Edge Devices," *in IEEE Transactions on Industrial Informatics, vol.* 20, no. 5, pp.7537-7544

[9] S. Wu, H. Luo, S. Yin, K. Li and Y. Jiang, "AResidual-Driven Secure Transmission and Detection Approach Against Stealthy CyberPhysical Attacks for Accident Prevention," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5762-5771.

[10] He, C. Tang, W. Li, T. Li, L. Chen and X. Lan, "BR-HIDF: An Anti-Sparsity and Effective Host Intrusion Detection Framework Based on Multi-Granularity Feature Extraction," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 485-499

[11] M. Prudjinski, I. Hadar and G. Luria, "Exploring the Role of Team Security Climate in the Implementation of Security by Design: A Case Study in the Defense Sector," in *IEEE Transactions on Software Engineering*, vol. 50, no. 5, pp. 1065-1079

[12] G. Duan, H. Lv, H. Wang, G. Feng and X. Li, "Practical Cyber Attack Detection With Continuous Temporal Graph in Dynamic Network System," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4851-4864

[13] A. Naser, A. Lotfi, M. D. Mwanje and J. Zhong, "Privacy-Preserving, Thermal Vision With Human in the Loop Fall Detection Alert System," in *IEEE*

Transactions on Human-Machine Systems, vol. 53, no. 1, pp. 164-175

[14] Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo and O. Kaynak, "Monitoring and Defense of Industrial Cyber-Physical Systems Under Typical Attacks: From a Systems and Control Perspective," in *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 192-207

[15] M. -E. Vasile, G. Avolio and I. Soloviev, "Performance Evaluation of Modern Time- Series Database Technologies for the ATLAS Operational Monitoring Data Archiving Service," in *IEEE Transactions on Nuclear Science*, vol. 70, no. 6,pp.1131- 1135

[16] Y. Xue, J. Pan, Y. Geng, Z. Yang, M. Liu and R. Deng, "Real-Time Intrusion Detection Based on Decision Fusion in Industrial Control Systems," in *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 143-153

[17] J. Li et al., "LightFS: A Lightweight Host- CSD Coordinated File System Optimizing for Heavy Small File Accesses," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 11, pp. 3527-3538

[18] N. Nissim, A. Cohen and Y. Elovici, "ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 631-646

[19] P. K. Roy, A. Singh, J. V. Desai and S. K. Singh, "Healthcare Data Security Using Lightweight Protocol for Cyber Physical System," in *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2597-2606

[20] Y. Chen, Y. Li, Z. Pan, Y. Lu, J. Chen and S. Ji, "URadar: Discovering Unrestricted File Upload Vulnerabilities via Adaptive Dynamic Testing," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1251-126