Volume 10, Issue 3, March – 2025 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

Study on Real-Time Data Integrity and Security Module Using Machine Learning

Greeva Dinesh Kumar Patel[1]; Kartikeydheer Srivastava[2]; Mansi Mehta[3]

[1]UG Student, Department of CSE, Indus Institute of Technology and Engineering (IITE), Indus University, Ahmedabad, Gujarat, India
[2]UG Student, Department of CSE, Indus Institute of Technology and Engineering (IITE), Indus University, Ahmedabad, Gujarat, India
[3]Assistant Professor, Department of CSE, Indus Institute of Information & Communication Technology (IIICT), Indus University, Ahmedabad, Gujarat, India

Publication Date: 2025/03/06

Abstract: The rapid increase of interconnected virtual ecosystems, pushed by means of IoT devices, cloud infrastructures, and software program-described Networks (SDNs), has amplified the call for for sturdy actual-time information safety and integrity. This studies introduces a real-Time data Integrity and security Module (RTDISM) that leverages system getting to know (ML) to tackle these challenges. by way of integrating SDN architectures, light-weight federated getting to know, and adaptive authentication protocols, the RTDISM provides a scalable, multi-layered defense gadget suitable for diverse environments. Key capabilities include adaptive ML-pushed risk mitigation, low-latency responses, and efficient aid usage. The module is particularly proper for vital domain names together with healthcare, commercial automation, and self reliant systems. Innovat ions include SDN-primarily based security for improved network flexibility, light-weight ML models for aid optimization, and federated getting to know for decentralized, privateness-maintaining operations. Experimental opinions demonstrate the RTDISM's superior overall performance in accuracy, reaction time, and useful resource performance in comparison to present solutions, organising it as a benchmark for subsequent- technology cybersecurity structures.

Keywords: *Real-Time Security, ML, IoT, SDN, Anomaly Detection, Edge AI, Federated Learning, Threat Mitigation.*

How to Cite: Greeva Dinesh Kumar Patel; Kartikeydheer Srivastava; Mansi Mehta (2025). Study on Real-Time Data Integrity and Security Module Using Machine Learning. *International Journal of Innovative Science and Research Technology*, 10(3), 239-245. https://doi.org/10.5281/zenodo.14964519

I. INTRODUCTION

The exponential boom of virtual ecosystems, pushed with the aid of IoT devices, cloud infrastructures, and software program-described Networks (SDNs), has revolutionized information processing while introducing vital vulnerabilities in healthcare, commercial automation, and financial systems[1][2]. IoT gadgets, projected to surpass seventy five billion via 2025, call for sturdy safety answers to combat threats like DDoS assaults, ransomware, and insider breaches[1]. traditional static safety frameworks fail to address these dynamic threats, necessitating adaptive, clever techniques.

Year	Threats Identified	Types of Threats	Mitigation Techniques
2020	120	DDoS, Phishing	Traffic throttling, user training, anomaly detection algorithms
2021	160	Data Breaches, Malware	Encryption protocols, access controls, behavioral analytics
2022	210	Insider Threats, APTs	Real-time monitoring, SVM-based prediction models, response automation
2023	250	Ransomware, Supply Chain Attacks	AI-driven threat detection, Blockchain for supply chain verification
2024	300	IoT Exploitation, Zero-Day Attacks	Multi-layered ML security, Autoencoders, predictive threat modeling

Fig 1 Cybersecurity Threats and Mitigation Techniques (2020-2024)

Machine learning (ML) offers transformative solutions by using autonomously reading datasets, detecting anomalies, and predicting vulnerabilities with strategies like assist Vector Machines (SVM), decision trees (DT), Autoencoders, and Convolutional Neural Networks (CNNs)[1][4]. This look at introduces a real-Time information Integrity and security Module (RTDISM), integrating ML algorithms, federated learning, and edge AI for scalable, adaptive cybersecurity.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

RTDISM minimizes latency and complements privateness through processing records regionally on IoT gadgets and part servers, decreasing reliance on centralized cloud structures[15].

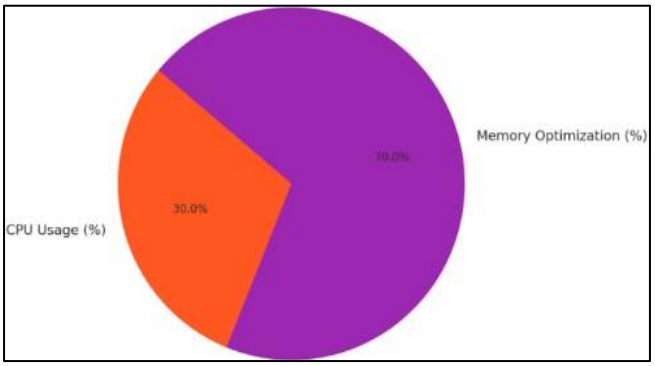

Fig 2 Resource Utilization Breakdown

The RTDISM leverages SDN architectures for centralized manage and dynamic chance mitigation[1][3]. It additionally carries light-weight cryptographic strategies and adaptive authentication mechanisms to guard touchy IoMT-generated health statistics towards man-in-the-middle (MITM) assaults, replay attacks, and impersonation[11]. Empirical evaluations highlight its superior performance in accuracy, response time, and resource efficiency.

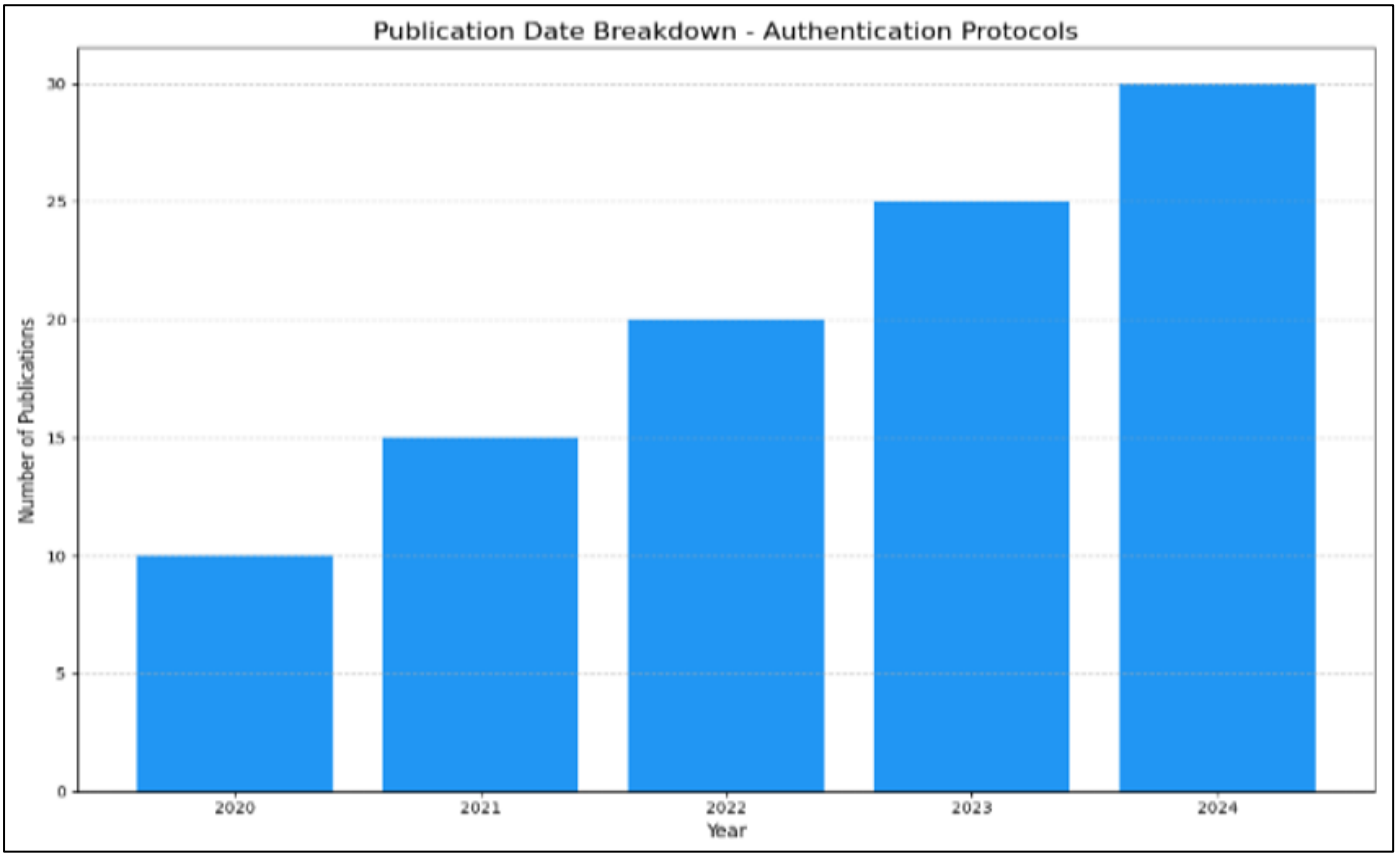

Fig 3 Publication Date Breakdown- Authentication Protocols

By synthesizing advancements in IoT, SDN, and cloud security, RTDISM sets a benchmark for next-generation cybersecurity frameworks, addressing the critical need for real-time data integrity in an interconnected digital ecosystem.

II. SURVEYS ARTICLES FOR THE IOT

IoT security faces precise demanding situations due to device heterogeneity, resource constraints, and fragmented ecosystems, requiring tailor-made answers. Many IoT gadgets lack the computational electricity for traditional cryptographic algorithms, and inconsistent standards amongst providers create vulnerabilities[5].system studying offers dynamic, adaptive processes to hazard detection, with supervised techniques like guide Vector Machines (SVM) and Random forest excelling in established statistics class, at the same time as unsupervised strategies including clustering and Autoencoders efficaciously detectanomalies in unstructured data. These approaches address evolving threats by analyzing behavioral patterns and data anomalies in real time.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

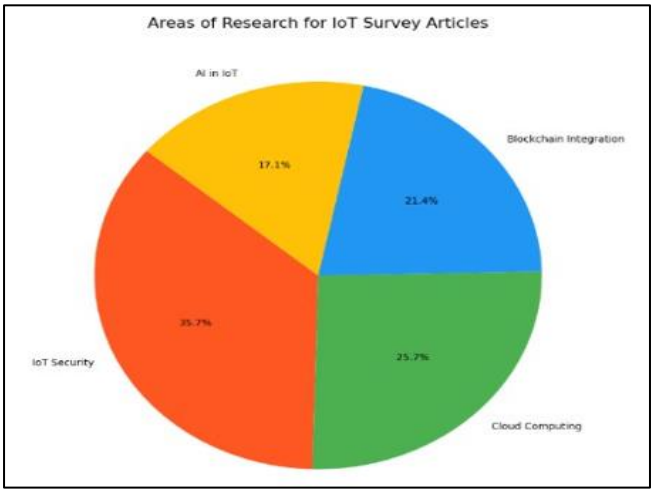

Fig 4 Areas of Research for IOT Survey Articles

Deep learning has advanced cybersecurity by leveraging Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to analyze full-size datasets, discover latent malicious styles, and enhance hazard detection talents. these strategies drastically enhance Intrusion Detection structures (IDS) and malware category frameworks via accomplishing higher detection costs and minimizing fake positives. This integration creates a multi-faceted safety system that successfully addresses the complexity of evolving cyber threats. IoMT systems face demanding situations in securing statistics transmission and garage. [5]proven SDN's capability to decorate community control and safety, integrating device learning to optimize resource utilization, statistics shipping, and real-time routing even as decreasing verbal exchange overhead[5][8][12].

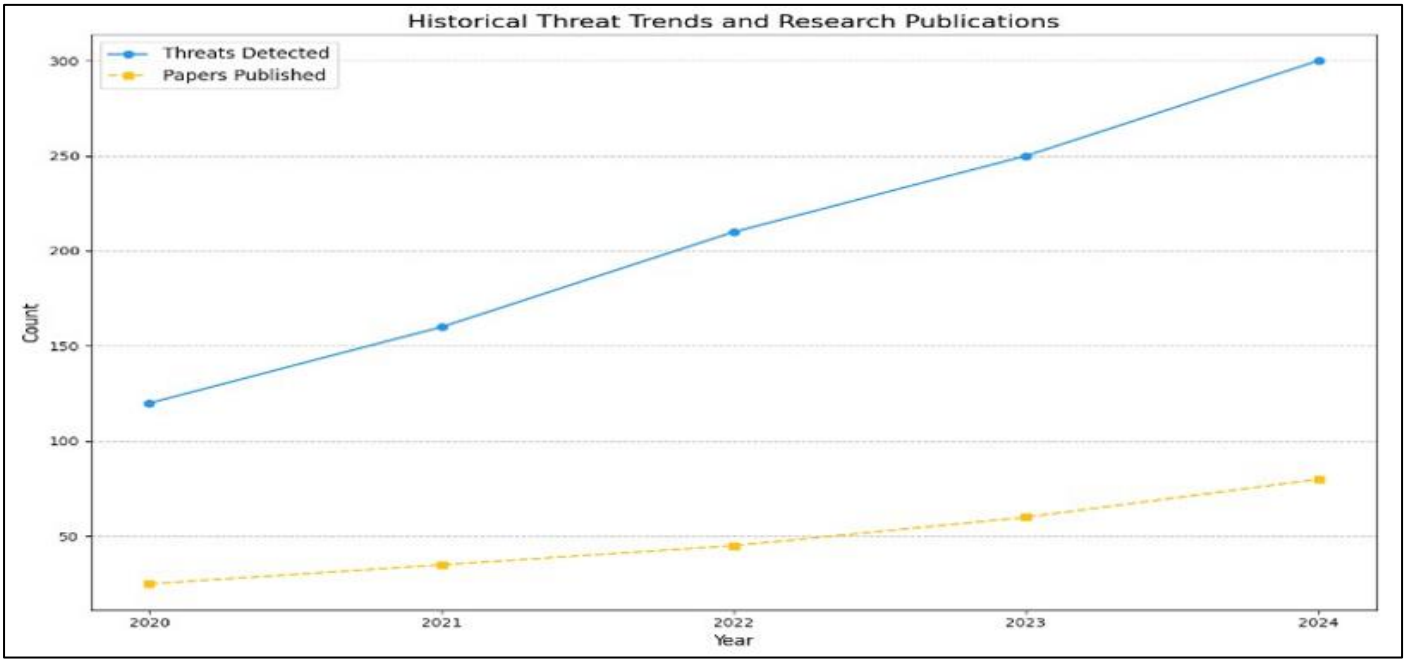

Fig 5 Historical Threats Trends and Research Publication

Research in IoT protection makes a speciality of addressing demanding situations like code injection, IoMT vulnerabilities, and authentication[6]proposed CNN-based fashions for code injection detection, the usage of character-degree n-grams to perceive malicious code patterns. [16] highlighted SDN's position in IoMT structures, combining device studying to optimize actual-time statistics routing, expect useful resource usage, and reduce communication overhead. [18] reviewed over 40 lightweight authentication protocols, emphasizing relaxed methods like ECC for M2M communication and protection towards attacks inclusive of guy-in-the-middle and impersonation.

Anomaly detection frameworks leverage statistical models and superior ML techniques for real-time hazard identity. Blockchain era has been explored for enhancing information integrity and decentralized authentication, though scalability challenges persist. A habitual theme is the want for standardized taxonomies to unify security measures across numerous IoT ecosystems.building on those insights, this examine proposes a strong protection framework utilising ML algorithms and formal verification to make sure data integrity and security throughout present day IoT environments.

III. THREAT MODELS

IoT threat fashions cope with vulnerabilities arising from interconnected, useful resource-confined devices and insufficient security protocols. commonplace threats include network eavesdropping, DDoS attacks, and device spoofing, which take advantage of the heterogeneity of IoT ecosystems. Attackers often use compromised gadgets to infiltrate networks, developing cascading vulnerabilities. The reliance on wi-fi conversation protocols similarly increases risks, as those channels are susceptible to interception and manipulation. advanced system studying algorithms, mainly anomaly detection fashions, play a critical position in figuring out and mitigating these threats in real- time, enabling proactive and adaptive security features[5][16][18].

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

Table 1 Summary of Threats and Mitigation Techniques

Year	Threats Identified	Types of Threats	Mitigation Techniques
2024	320	IoT Botnets, Data Exfiltration	Anomaly detection using ML, predictive analytics, and endpoint security orchestration[14][15].
2023	270	Ransomware 2.0, Cloud Malware Injections	AI-driven behavioral detection, cloud security protocols, and automated incident mitigation[15][17].
2022	230	Zero-Day Exploits, Cross- Site Scripting (XSS) Attacks	Proactive vulnerability scanning, sandboxing, and regular system patching[16][18].
2021	200	Data Breaches, Advanced Persistent Threats (APTs)	Encryption algorithms, realtime threat monitoring, and behavioral analytics[15][16].
2020	160	Supply Chain Attacks, Cloud Misconfigurations	Blockchain verification systems, AI-based misconfiguration analysis
2019	130	Malware, IoT Exploitation, Insider Threats	Secure firmware updates, device authentication, and privilege-based access control[16][18].
2018	100	DDoS, Phishing, Ransomware	Traffic filtering, multi-factor authentication, and robust incident response plans[18][19].

Lightweight authentication protocols, such as Elliptic Curve Cryptography (ECC) and hash-based totally methods, provide sturdy security with minimum computational overhead, making them ideal for IoT environments[1]. ECC supports secure device-to-tool communication, even as symmetric key protocols and public-key infrastructures offer alternatives with alternate-offs in safety and aid performance. Multi-thing authentication, even though useful resource-intensive, complements safety against identity spoofing and unauthorized get right of entry to. real-time anomaly detection is critical for IoT security. [4] and others spotlight device learning methods, which include supervised models using labeled datasets, unsupervised models detecting deviations, and hybrid models combining both for improved accuracy. Autoencoders have shown promise in identifying network intrusions by learning baseline behaviors and flagging deviations. Statistical models are effective for structured data but are increasingly complemented by ML techniques to address dynamic and unstructured IoT environments.

Performance evaluations of the Data Integrity and Security Module emphasize its effectiveness across key metrics: detection accuracy, prediction accuracy, and response latency. These metrics demonstrate its capability to address diverse threat models and safeguard IoT ecosystems in real-time.

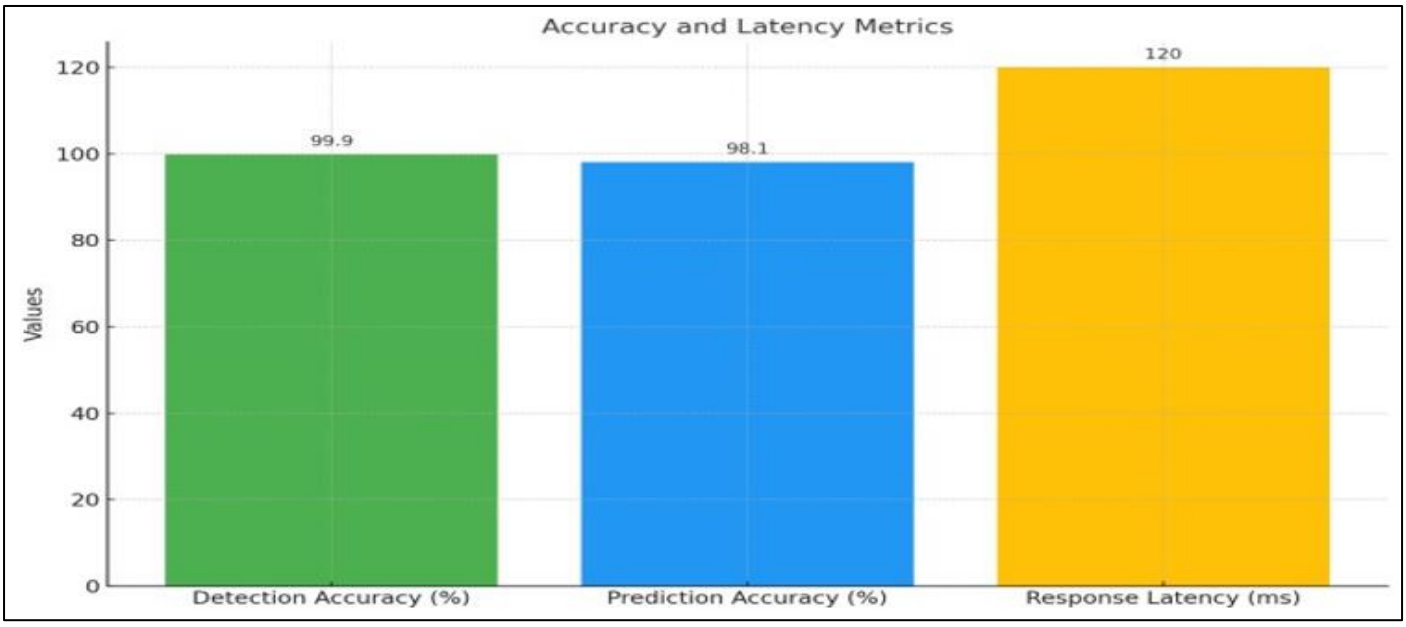

Fig 6 Accuracy and Latency Metrics

The module achieves an great detection accuracy of 99.9%, showcasing its capacity to identify anomalies and complex threats, which include guy-in-the- middle (MITM) and Replay attacks, in actual-time. This excessive precision ensures reliable differentiation between everyday operations and capacity safety breaches, minimizing fake positives and enhancing consider within the system's detection talents.With a prediction accuracy of 98.1%, the module successfully forecasts rising threats by using studying historic information and behavioral patterns. This predictive capability is essential for addressing advanced assault vectors like Sybil and Impersonation assaults. The module's proactive danger anticipation permits the implementation of mitigation strategies earlier than attacks materialize, strengthening the

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

general protection framework[18]. A reaction latency of one hundred twenty milliseconds highlights the module's rapid reaction to recognized threats, a critical feature for actual-time IoT systems. This low latency is particularly massive for mitigating time- touchy assaults along with MITM, ensuring ongoing communications remain comfy and information integrity is preserved.

These metrics validate the module's robust performance in safeguarding IoT ecosystems. The combination of near-perfect detection accuracy, predictive precision, and swift response times ensures comprehensive protection against diverse and evolving threat models, positioning the module as a reliable and adaptive solution for IoT security[17][18][19].

IV. COUNTERMEASURES AND FORMAL SECURITY VERIFICATION

Addressing IoT safety demanding situations requires a multi-faceted technique that mixes superior technical answers with formal verification techniques to create a robust protection against evolving threats. One important degree is the deployment of gadget mastering (ML)-powered Intrusion Detection structures (IDS), which excel in figuring out and mitigating cyber threats in actual time. Autoencoders, for example, examine baseline network behaviors and flag deviations which can indicate anomalies or ability attacks. further, ensemble models, which integrate a couple of algorithms like Random Forests and help Vector Machines (SVMs), improve hazard detection accuracy by way of leveraging their blended strengths. those systems are further more advantageous by adaptive mastering capabilities, letting them evolve constantly by incorporating new information, making sure they continue to be effective against rising attack vectors[4][16].

Lightweight cryptographic techniques are essential for securing data transmission and storage, particularly in resource-constrained IoT environments. Elliptic Curve Cryptography (ECC) is a standout solution, offering robust encryption with minimal computational demands, making it suitable for IoT devices with limited processing power[3]. Symmetric key protocols also play a vital role, providing fast and efficient encryption by utilizing shared secret keys. Advanced dynamic protocols, incorporating timestamps, nonces, and hash functions, further bolster security by preventing common threats like replay attacks and ensuring the integrity of communication sessions. These combined measures create a layered defense framework, addressing the unique challenges of IoT security effectively[17][18].

Dynamic authentication protocols are vital for securing IoT communications with the aid of leveraging techniques like timestamps, random numbers (nonces), and hash features. Timestamps ensure that transactions are clean, stopping replay assaults with the aid of stopping the reuse of intercepted records packets. Nonces introduce randomness to make each session particular, and hash features securely rework facts into fixed-size strings, that are tough to opposite-engineer or mirror. these protocols are particularly powerful in useful resource-constrained IoT environments, providing a lightweight but strong option to cozy communique.

Software-Defined Networking (SDN) enhances IoT security by centralizing network management, allowing for dynamic reconfiguration of the network. SDN separates the control plane from the data plane, enabling quick detection and isolation of compromised devices, preventing attacks from spreading. The programmability of SDN supports the integration of ML algorithms to analyze network traffic patterns, predict potential security breaches, and optimize resource allocation, ensuring both security and efficiency in IoT networks.

Fig 7 Main Features and Challenges of the Framework

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

The chart illustrates the twin nature of IoT security, wherein excessive function significance highlights the framework's strengths, while top notch venture importance points to areas requiring ongoing refinement. This balance emphasizes the evolving nature of developing sturdy IoT security answers, in which strengths should be continuously stepped forward to meet emerging demanding situations. the integration of blockchain generation has received sizable interest for boosting IoT protection. Blockchain's decentralized, immutable ledger guarantees statistics integrity and stops tampering across dispensed networks, making sure duty. [2][7]emphasize its role in facilitating at ease, obvious interactions between IoT devices. lightweight consensus mechanisms, including proof of Authority (PoA) and Delegated evidence of Stake (DPoS), deal with scalability issues in huge networks. moreover, smart contracts automate safety protocols, decreasing the need for manual interventions in risk mitigation

- *Taxonomy and Comparison of Authentication Protocols for the IoT*

This phase delves into the authentication protocols utilized in actual-time statistics integrity and protection fashions for IoT structures. A cohesive taxonomy of threats, countermeasures, and requirements is important to advancing IoT protection. existing literature categorizes IoT threats into three primary layers: device, network, and alertness. device-stage threats regularly involve firmware tampering, whilst community-stage threats encompass eavesdropping and statistics breaches. Mitigation techniques consisting of comfortable boot mechanisms for devices and encryption protocols for networks are hired. Standardization efforts purpose to address interoperability gaps, allowing seamless integration at the same time as ensuring compliance with safety policies. however, the absence of universally ordinary standards remains a assignment, highlighting the want for industry collaboration [9][10].

Authentication protocols play a crucial role in establishing trust within IoT ecosystems. These protocols are categorized based on their cryptographic mechanisms, resource efficiency, and scalability. Lightweight methods, such as Elliptic Curve Cryptography (ECC), are suited for resource-constrained devices, whereas more robust methods like RSA provide higher security levels for critical applications.

The comparative analysis highlights the trade-offs between computational overhead and security effectiveness in IoT authentication protocols. Machine learning (ML) models enhance these protocols by detecting anomalies and unauthorized access without significantly increasing resource demands. Various authentication protocols are designed for specific subdomains, addressing their unique security requirements. This section presents a taxonomy of these protocols, comparing their effectiveness in securing different IoT environments.

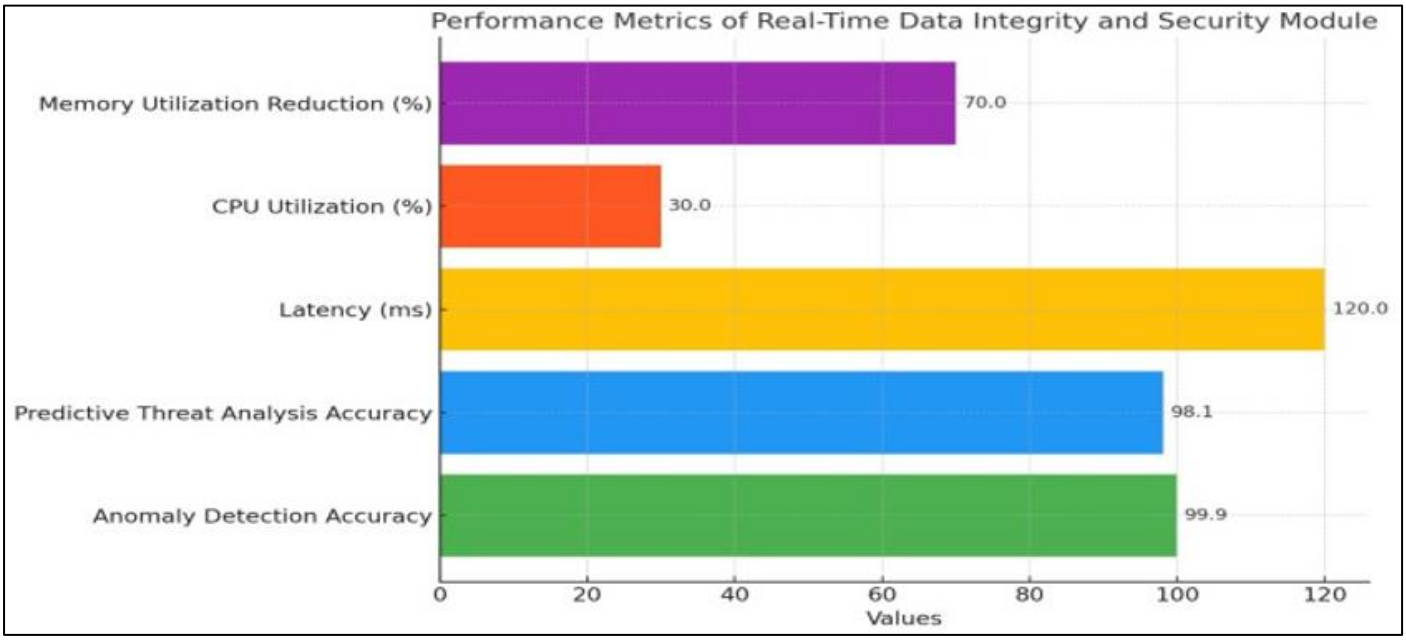

Fig 8 Performance Metrics of Real-Time Data Integrity and Security Module

The class file is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor grouped by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization) [15][16][18].

M2M conversation permits direct device interaction in IoT, emphasizing relaxed and green conversation in spite of resource constraints. light-weight cryptographic strategies like ECC and hash-primarily based protocols are usually used, imparting strong safety while minimizing computational overhead, critical for dynamic and disbursed networks.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

IoV connects vehicles, infrastructure, and entities to improve road safety and traffic management. Authentication protocols in IoV focus on secure data transmission and integrity. PKI, digital certificates, and blockchain technology are key for establishing secure communication and ensuring data immutability and transparency.

IoE integrates IoT in smart grids and energy management. Authentication protocols must support real-time data exchange and secure communication across devices like smart meters and control systems. These protocols are designed to protect against cyber threats, utilizing time-sensitive mechanisms and strong encryption to safeguard energy infrastructures.

IoS involves resource-constrained sensors used in environments like healthcare and environmental monitoring. Authentication protocols focus on minimal resource use while maintaining security. Lightweight techniques, such as symmetric key cryptography and one-time passwords, are used, alongside machine learning models to enhance real-time threat detection and mitigation.

Unique IoT subdomains have unique authentication necessities primarily based on their operational environments. gadget-to-system (M2M) communication requires cozy and green authentication mechanisms to support self reliant device interactions in dispensed networks. lightweight cryptographic techniques like ECC and hash-primarily based protocols are generally employed to make certain safety with out excessive computational overhead. The internet of automobiles (IoV) demands sturdy authentication protocols to allow secure records transmission among motors, infrastructure, and street entities. PKI, digital certificates, and blockchain-primarily based authentication play a extensive position in ensuring transparency and statistics integrity.

In the Internet of Energy (IoE), authentication protocols are designed to secure data exchanges in smart grids and energy management systems. Strong encryption techniques and real-time authentication mechanisms protect against cyber threats while ensuring operational reliability. The Internet of Sensors (IoS) focuses on security solutions for resource-constrained environments, such as healthcare and environmental monitoring systems. Authentication techniques in these domains prioritize low-power consumption, integrating lightweight cryptographic protocols, one-time passwords, and AI-driven threat detection models.

IoT authentication is shaped by rising technologies that enhance safety and flexibility. Federated gaining knowledge of is being explored to allow decentralized authentication, reducing reliance on centralized identification control structures. The 0-believe architecture is gaining traction as a paradigm that assumes no inherent consider within a community, requiring continuous authentication verification at each interaction. With the advent of quantum computing, traditional cryptographic techniques are at danger, necessitating research into submit-quantum cryptography for quantum-resistant authentication mechanisms. artificial intelligence is increasingly being integrated into authentication protocols, supplying adaptive security features and real-time hazard detection through anomaly detection and behavioral analysis.

Future research should focus on developing advanced authentication frameworks that address the evolving challenges of IoT security. Interdisciplinary collaboration among cybersecurity researchers, cryptographers, and AI specialists is essential to designing authentication solutions that balance security, computational efficiency, and scalability. Establishing universally accepted authentication standards will play a crucial role in ensuring interoperability across heterogeneous IoT ecosystems. Research into privacy-preserving authentication mechanisms, such as homomorphic encryption and secure multi-party computation, can further enhance security without compromising user privacy.

By means of integrating cryptographic innovations, artificial intelligence, and scalable authentication architectures, future authentication protocols will offer sturdy and adaptive protection solutions for the dynamic nature of IoT environments. Addressing the safety concerns of IoT ecosystems requires a proactive approach in developing authentication frameworks which could face up to emerging cyber threats at the same time as making sure seamless device interactions [13][16][18].

V. CONCLUSION

This research presents a Real-Time Data Integrity and Security Module designed to tackle the challenges of securing data in dynamic IoT environments. By integrating advanced machine learning (ML) algorithms, the framework effectively mitigates security threats across the device, network, and application layers, ensuring robust data protection in real-time. The use of Convolutional Neural Networks (CNNs) for anomaly detection, Software-Defined Networking (SDN) for adaptive control, and advanced authentication protocols together create a scalable solution capable of addressing evolving cybersecurity threats.

This demonstrates that ML-pushed security mechanisms, mainly anomaly detection models, notably enhance the accuracy and efficiency of danger identification, mitigation, and response. Federated learning permits decentralized safety operations, lowering reliance on centralized cloud infrastructures at the same time as maintaining data privateness. moreover, SDN-based protection solutions enhance network adaptability, allowing for dynamic policy enforcement and actual-time threat intelligence. The RTDISM exhibits tremendous overall performance in detection accuracy, reaction latency, and useful resource optimization, making it well-acceptable for essential applications which includes healthcare, industrial automation, and independent structures.

A comprehensive analysis of authentication protocols highlights the need of standardized protection frameworks tailor-made to aid-constrained IoT environments. The take a

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

look at underscores the significance of submit-quantum cryptography, zero-consider architectures, and AI-pushed safety automation in future cybersecurity techniques. As IoT ecosystems preserve to expand, interdisciplinary collaboration among AI researchers, cybersecurity specialists, and enterprise leaders may be important in growing scalable, sensible safety answers.

By synthesizing improvements in ML, blockchain protection, and adaptive authentication, this studies establishes the RTDISM as a benchmark for subsequent-technology IoT protection frameworks. The version's scalability, real-time adaptability, and precision-driven security features ensure that it offers a resilient foundation for defensive interconnected systems, retaining information integrity, and proactively countering sophisticated cyber threats in an increasingly more virtual landscape.

This study emphasizes the transformative impact of machine learning in modern cybersecurity, demonstrating its potential to safeguard data integrity and security in increasingly dynamic environments. As the digital world evolves, ongoing research and innovation will be crucial in maintaining the security of critical data systems.

ACKNOWLEDGMENT

The authors declare that they have no conflicts of interest.

REFERENCES

[1]. M. Asmar and A. Tuqan, "Integrating machine learning for sustaining cybersecurity in digital banks," Heliyon, vol. 10, p. e37571, 2024. Available: https://doi.org/10.1016/j.heliyon.2024.e37571

[2]. K. Masthan, M. Shabana, and M. Rafi, "Enhancing cloud security using machine learning," Journal of Systems Engineering and Electronics, vol. 34, no. 10, pp. 66–70, 2024. Available: https://www.researchgate.net/publication/386872942

[3]. M. Austin, K. Austin, and M. Osaka, "Machine learning for data security in cloud computing environments," Research Proposal, 2024. DOI: 10.13140/RG.2.2.12840.14088. Available: http://dx.doi.org/10.13140/RG.2.2.12840.14088

[4]. D. Alexander and Z. Chain, "Data Integrity Challenges and Solutions in Machine Learning-driven Clinical Trials," Sher-e-Kashmir University of Agricultural Sciences and Technology of Kashmir, Aug. 2023. [Online]. Available: https://www.researchgate.net/publication/373214664

[5]. E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions," Electronics, vol. 11, no. 3330, Oct. 2022. [Online]. Available: https://doi.org/10.3390/electronics11203330

[6]. T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review," Electronics, vol. 12, no. 3958, Sep. 2023. [Online]. Available: https://doi.org/10.3390/electronics12183958

[7]. S. K. Sahu and K. Mazumdar, "Exploring Security Threats and Solutions Techniques for Internet of Things (IoT): From Vulnerabilities to Vigilance," Frontiers in Artificial Intelligence, vol. 7, no. 1397480, May 2024. [Online]. Available: https://doi.org/10.3389/frai.2024.1397480

[8]. S. B. Masud, M. M. Rana, H. J. Sohag, F. Shikder, M. R. Faraji, and M. M. Hasan, "Understanding the Financial Transaction Security Through Blockchain and Machine Learning for Fraud Detection in Data Privacy and Security," Pakistan Journal of Life and Social Sciences, vol. 22, no. 2, pp. 17782-17803, Dec. 2024. [Online]. Available: http://dx.doi.org/10.57239/PJLSS-2024-22.2.001296

[9]. S. K. Devineni, S. Kathiriya, and A. Shende, "Machine Learning-Powered Anomaly Detection: Enhancing Data Security and Integrity," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 2, pp. 1-9, May 2023. [Online]. Available: http://dx.doi.org/10.47363/JAICC/2023(2)184

[10]. J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," Engineering Applications of Artificial Intelligence, vol. 123, p. 106432, May 2023. [Online]. Available: https://doi.org/10.1016/j.engappai.2023.106432

[11]. F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 167–185, Jan. 2024. [Online]. Available: https://doi.org/10.1016/j.iotcps.2023.12.003

[12]. H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," Scientific Reports, vol. 14, no. 12077, 2024. [Online]. Available: http://dx.doi.org/10.1038/s41598-024-62861-y

[13]. M. Salayma, "Risk and threat mitigation techniques in internet of things (IoT) environments: A survey," Frontiers in the Internet of Things, vol. 2, no. 1306018, Jan. 2024. [Online]. Available: https://doi.org/10.3389/friot.2023.1306018

[14]. L. Doris and R. Shad, "Using machine learning models to identify and predict security-related anomalies in real-time for proactive maintenance," ResearchGate, Dec. 2024. Available: https://www.researchgate.net/publication/386573125_USING_MACHINE_LEARNING_MO DELS_TO_IDENTIFY_AND_PREDICT_SECURITY-_RELATED_ANOMALIES_IN_REALTIME_FOR_PROACTIVE_MAINTENA NCE

[15]. G. Arjunan, "Optimizing Edge AI for Real-Time Data Processing in IoT Devices: Challenges and Solutions," International Journal of Scientific Research and Management (IJSRM), vol. 11, no. 6, pp. 944-953, June 2023. [Online]. Available: DOI:10.18535/ijsrm/v11i06.ec2

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14964519

[16]. A. S. Shaik and A. Shaik, "Code Injection Attack Prevention with AI- Integrated Machine Learning Approach Using CNN," ShodhKosh: Journal of Visual and Performing Arts, vol. 3, no. 2, pp. 848-854, Dec. 2022. [Online]. Available: https://doi.org/10.29121/shodhkosh.v3.i2.2022.3181

[17]. M. Sugadev et al., "Implementation of Combined Machine Learning with the Big Data Model in IoMT Systems for the Prediction of Network Resource Consumption and Improving the Data Delivery," Computational Intelligence and Neuroscience, vol. 2022, Article ID 6510934, 12 pages, July 2022. [Online]. Available: https://doi.org/10.1155/2022/6510934

[18]. M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," Security and Communication Networks, vol. 2017, Article ID 6562953, pp. 1– 41, 2017, [Online]. Available: https://doi.org/10.1155/2017/6562953

[19]. N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," Sensors, vol. 25, no. 79, pp. 1–45, 2025, [Online]. Available: https://doi.org/10.3390/s25010079