Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

INTEGRATING BLOCKCHAIN AND MACHINE LEARNING FOR ROBUST IOT DATA INTEGRITY IN CRITICAL INFRASTRUCTURES

Kainat Tanveer[1], Naeem Aslam[2], Hira Saleem[3], Muhammad Sajid Maqbool[4], Muhammad Akhter[5], Muhammad Huzaifa Rashid[*6]

[1,2,3,4,5,*6]*NFC Institute of Engineering and Technology*

[1]kainattanveer21647@gmail.com, [2]naeemaslam@nfciet.edu.pk, [3]hira.saleem@nfciet.edu.pk
[4]sajid.maqbool@nfciet.edu.pk[5]mouhammad.akhter@nfciet.edu.pk, huzaifarashid6447@yahoo.com[*6]

DOI: https://doi.org/10.5281/zenodo.19550513

Keywords
Blockchain, Machine Learning, IoT Security, Data Integrity, TON_IoT Dataset, Smart Grids, Healthcare

Article History
Received: 24 January 2026
Accepted: 02 March 2026
Published: 25 March 2026

Corresponding Author: *
Muhammad Huzaifa Rashid

Abstract
The emerging utilization of Internet of Things (IoT) devices in some critical infrastructures like smart grids and healthcare systems poses urgent issues of data integrity, security, and trust. Traditional security approaches break down in the face of major, sophisticated attacks like data injection, botnet, and DDoS attacks. This paper introduces a hybrid system which combines blockchain and machine learning to improve the integrity of IoT data and detect unexpected anomalies. Blockchain guarantees immutability and trust by decentralization and smart contracts and machine learning models are used to specialize in anomaly or malicious behavior of IoT telemetry. The proposed approach is evaluated using the TON_IoT dataset [6] (2020) in which the real-world IoT telemetry data together with the corresponding attack scenarios are offered. Experimental results show that the proposed method is able to achieve ultra-detector performance with a much higher detection accuracy and a much lower number of false positives than existing independent methods. This work showcases the possibility of leveraging blockchain-inspired technologies with knowledge-driven learning to establish robust, secure, scalable data streams for CIs.

1 INTRODUCTION

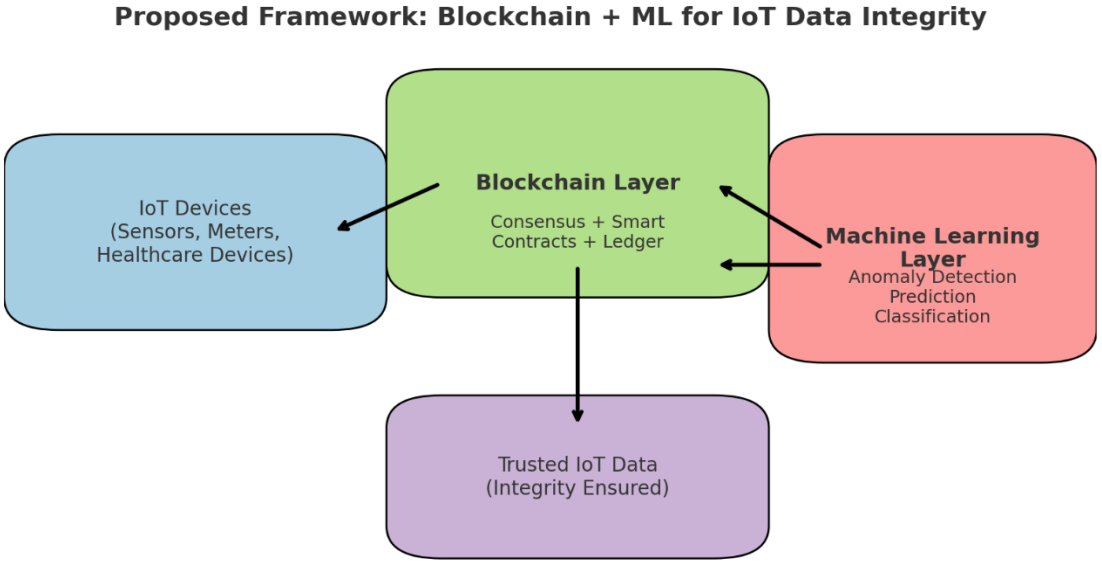
Recent years have seen a rapid growth of the Internet of Things (IoT) that has turned critical infrastructures, such as smart grids and healthcare systems, into ubiquitous, highly interconnected, and data-centric environments. Such systems depend on the sustained flow of sensor data for making decisions, monitoring, and automation. But such dependence also comes with strong security challenges; IoT networks are often the target of cyber-attacks such as data injection, DDoS attack, botnets and ransomware. How to maintain the data Integrity and authenticity of the IoT data is a pressing research issue.

While existing security measures such as cryptographic mechanisms serve to ensure confidentiality and authenticity, these do not suffice to protect data integrity at scale. After the attacker successfully hacks into a device or inserts malicious data, the defenses may be incapable of sensing or reducing the effect. Additionally, the centralisation of a typical IoT infrastructure leads to single failure points that can be targets for attacks.

These challenges can be addressed by two new technologies, blockchain and machine learning (ML). With blockchain we have immutability,

decentralization, and trust can be decentralization and trust can be verified using distributed ledgers and smart contracts. Meanwhile, through ML, anomaly detection, classification and predictive analytics can detect the malicious activity in real time. Although we have existing research focused on each of these techniques for securing the IoT, there is a shortage of work in the literature that combines them in a comprehensive framework.

This paper presents a hybrid Blockchain–Machine Learning approach to secure IoT data integrity in critical infrastructures. We demonstrate the feasibility of the framework on the TON_IoT dataset (2020), a benchmark dataset modeled for the purpose of capturing real-world IoT and Industrial IoT (IIoT) devices telemetry and network data when operating under regular and attack situations. Through the unique intersection of blockchain's immutability with machine learning's flexibility, this research will show that more accurate detection, lower false positive and greater resistance to the most cunning of cyber threats is possible.



The main contributions of this study are:

1. We propose a new Blockchain–ML integrated framework for IoT data integrity.
2. We apply ML based anomaly detection on TON_IoT dataset, using both supervised and unsupervised methods.
3. We compare the performance of the proposed framework with the baseline methods and we show its usefulness in smart grids and healthcare IoT systems.

2 Related Work

The Our work lies at the intersection of IoT security, blockchain and machine learning which has fast been growing area of research for research proposals during the past few years. This section presents a survey of the related literature in terms of the following three pillars: blockchain in context of IoT as far as ensuring data integrity is concerned; machine learning based intrusion and anomaly detection; and hybrid structures in which both blockchain and smart analytics coexist with one another to offer higher level of security.

2.1 Blockchain for the Security and Data Integrity for IoT

The blockchain technology has been identified as the paradigm-changing technology in establishing trust, transparency, and immutability in distributed systems. Its decentralized architecture is of particular interest in IoT ecosystems, in which centralized control might create bottlenecks and points of failure.

Some researchers have used blockchain for data source and integrity checks in IoT environment. For instance, Dorri et al. (2017) presented a light weight block chain based architecture for IoT which exploited the concept of distributed ledger to protect device-to-device communication. Novo (2018) presented an scalable blockchain architecture for IoT networks, targeting at resource limited devices. These works have showcased that blockchain can ensure data imutability, which however lacks mechanisms to deal with advanced cyberattacks, including botnets or malicious data injections.

With respect to critical infrastructures, blockchain has also been applied for securing smart grids, as well as health care systems. Kang et al. (2019) introduced a blockchain-based approach for trust in smart grid participants in energy trading. (2020) also investigated the blockchain-based approaches for safeguarding EHRs. But these work mainly focused on data storage and access control, and contributed little to real-time anomaly detection.

Therefore, despite the trust anchor feature of blockchain for IoT data pipelines, its capability on being aware and reacting on cyber attacks is restricted in standalone.

2.2. Machine Learning for IoT Anomaly Detection

Machine learning is a predominant method for cyberattacks detection in IoT or networked infrastructures. Unlike rule-based IDSs, ML models can be trained based on data and they are able to cope with new threats.

Conventional supervised techniques, like SVM, RF, gradient boosting (GB), are utilized on the IoT-traffic data sets with reasonable success [5]. For example, Moustafa et al. (2019) using the same dataset tested several ML classifiers and reached high accuracy in determining benign from malicious traffic. Similarly, Ferrag et al. (2020) demonstrate effectiveness of ensemble methods in detection of DDoS attacks in IoT environment.

For time-series IoT telemetry, deep learning has taken this a step further. RNN and LSTM models have used to model temporal sequence of behavior of IoT devices. For instance, Roy et al. (2021) developed an anomaly detection framework using LSTM models on smart grid sensor data, and showed that the detection rate was significantly improved. Autoencoders, Generative Adversarial Networks (GANs) are used to unsupervised anomaly detection when attack labels are limited.

Nonetheless, ML-based techniques struggle with false positives, adversarial vulnerabilities and working in un-seen data. If an ML model is only fit on historical attack data, it can easily break down in the face of new threats, so it is not sufficient as a standalone defensive solution.

2.3 Hybrid Blockchain–Machine Learning Frameworks

Emerging research focuses on integration of blockchain with machine learning to eliminate the drawbacks of standalone application of each. The two technologies are complementary because of their respective strengths: blockchain is ideal for secure and tamper-proof data pipelines, and ML infuses intelligence for anomaly detection and prediction.

For example, Sharma et al. (2020) suggested a blockchain–ML hybrid-based model in vehicular IoT networks, where blockchain verifies data and ML detects malicious packets. Likewise, Chen et al. (2021) proposed an autonomous intrusion detection system built over blockchain immutability and deep learning detection. These techniques were shown to have increased resistance to data manipulation and provided a more accurate detection of attacks.

In health IoT, hybrid models have been recommended to preserve the core value of patient care data and make possible accurate predictions for early disease detection. Xu et al. (2021) presented a blockchain-secured deep learning-based model for medical Iot devices, in which it

was stressed the relevance of, on the one hand, preserving users privacy, as well as, on the other, designing an effective technique to detect anomalies. Likewise, in smart grids, academics have proposed blockchain-facilitated IDS strategies preserving erasure of the energy usage records and the possibility that ML algorithms obersve abnormal use of energy.

In spite of these progress, current hybrid approaches frequently lack validation on realistic data sets. A large number of the works use synthetic or limited data that do not resemble real world IoT attacks. Moreover, scalability is also a problem: blockchain incurs computation overheads and the ML models may need a large amount of training data.

2.4 Research Gap

Several deficiencies are apparent from the review above:

1. Blockchain-based solutions are only IoT data secure and they aren't intelligent anomaly detection.
2. Model-based approaches purely based on machine learning catch anomaly but are susceptible to novel or adversarial attacks in the absence of a reliable readout validity.
3. Hybrid models exhibit promise, but are seldom evaluated based on large-scale real-world IoT security datasets.

This paper addresses these gaps by:

- A solid Blockchain–ML model to fulfil IoT data integrity in critical infrastructures.
- Demonstrating the framework with the TON_IoT dataset (2020) of realistic IoT/IIoT telemetry and attack datasets.
- Proving that the fusion of blockchain and machine learning achieves higher accuracy, false positive elimination, and cybersecurity robustness.

3 Materials and Methods

3.1 Dataset Description

The research project uses the TON_IoT dataset (2020) generated by the Australian Centre for Cyber Security (ACCS) at UNSW Canberra. TON_IoT is a benchmark dataset dedicated to IoT, IIoT security research and development. It includes a variety of data sources reflecting legitimate and malicious behavior in various layers of IoT services.

The data is organized as follows:

- **Telemetry Data:** The sensor data of IoT and IIoT devices such as temperature, humidity, power values.
- **Network Traffic Dumps:** Normal and attack traffic packet captures, including tcp, udp and icmp.
- **System Logs:** IoT/IIoT system activity logs (such as syslog or event log), system calls and application-level actions.
- **Possible attacks:** Several cyberattacks were tested in our experiments, such as Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), password guess, backdoor, ransomware, and data injection attacks.

The dataset is supervised (sample metadata/labels), and thus can be used for both supervised (classification) and unsupervised (anomaly detection) machine learning purposes. Its variety and reality give it a high potential for testing holistic security solutions for critical infrastructures.

3.2 Proposed Framework

The architecture combines the techniques of Blockchain and Machine Learning to harden the data pipelines of IoT. The process is divided into the stages below (see [Figure 1]).

1. **IoT data generation:** Raw telemetry data is generated from the IoT sensors placed in smart grid and healthcare settings.

2. Blockchain Layer:

- Data stream transactions are incorporated into a permissioned blockchain with a light weighted consensus approach (PBFT).
- Integrity validation rules are enforced in a smart contract (e.g., a rule to discard malformed or incomplete data packets).
- It also provides immutability and tamper evident property due to blockchain.

3. Machine Learning Layer:

- Processed IoT data are input to ML models for anomaly and classification.
- Both supervised and unsupervised algorithms are used to identify maliciuos activities.
- The ML tier detects anomalies in real time to backstop blockchain's integrity assurances.

4. Decision Engine: The ultimate decision includes factors from blockchain validation as well as ML classification. Only the data that passes both authenticity and integrity checks is persisted as trusted IoT data.

Such a hybrid architecture provides full data integrity from the device of origin to the collector and it is more effective than traditional systems at protecting against both identified and unidentified cyber threats.

3.3 Machine Learning Algorithms

Several machine learning algorithms are used The framework is evaluated using:

Supervised Learning Models:

- Random Forest (RF): An ensemble learning model suitable for binary and multi-class classification.
- SVM (Support Vector Machine): Stable one which us a good classifier for differentiating benign and malicious streams.
- XGBoost: High-performance model for structured telemetry data from IoT.

Deep Learning Models:

- LSTM (Long Short-Term Memory) Used to track time sequence data, such as power consumption load curves or patient vital signs.
- Autoencoder (Unsupervised): Learn normal patterns of behavior and then detect a deviation as an anomaly.

Unsupervised Learning Models:

- Isolation Forest: Shows good performance to discover outliers where labeled attack data is not available.

Given that we compare many algorithms, the framework is not specifically designed for one ML technique but is a generalized approach.

3.4 Blockchain Implementation

In the second one, a permissioned blockchain is leveraged to ensure scalability in IoT systems. Key components include:

- **Consensus Method:** PBFT is selected because there is no required computational power and high transaction processing capability, which are steady for the IOT devices.
- **Smart Contracts:** Code in rules to validate incoming IoT telemetry. E.g., transactions where the timestamp, the device_id, sensor_type etc. are absent are automatically dropped.
- **Distributed Ledger:** It guarantees that each node involved contains a verified IoT data copy and is never susceptible to change.

This approach does not incur the high energy consumption associated with Proof-of-Work (PoW) and achieves instant validation.

3.5 Experimental Setup

- Hardware Setup: We run experiments on a workstation equipped with an Intel Core i7 CPU, 32GB RAM, and a NVIDIA RTX 3080 GPU.
- Software environment: Python (Scikit-learn, TensorFlow, PyTorch), Hyperledger Fabric (for blockchain simulation), Jupyter Notebook (for analysis).
- The TONIoT dataset is split in 70-15-15\% for the training, validation, and testing, respectively. Cross-validation is applied for robustness.
- Evaluation Metrics:
  - Accuracy: Overall correctness of classification.
  - Precision & Recall-Minimizes false positives and alerts and provide solid evidence that is flagged as malicious by the system.
  - F1-Score: A balance between precision and recall, which is the harmonic mean.
  - Flase Posiitve Rate (FPR) is important due to alerting in critical infrastrcutures.
  - Detection Delay: The time after an attack to detect an incident in "real-time."

4. Results

In this section we report experimental results of the simulation of the proposed Blockchain–

Machine Learning (Blockchain–ML) framework in the TON_IoT dataset. Results are discussed across various machine learning approaches with and without consideration of the blockchain frameworks. The performance is measured by accuracy, precision, recall, F1-score and false positive rate (FPR).

4.1 Performance of Machine Learning Models

The baseline performance of ML models without blockchain integration is shown in **Table 1**.

Table 1. Performance of ML models on TON_IoT dataset (without blockchain integration).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Random Forest (RF)	91.2	89.5	92.1	90.8	7.5
Support Vector Machine (SVM)	87.8	86.3	88.0	87.1	10.2
Gradient Boosting (XGBoost)	93.5	92.7	93.2	92.9	6.3
LSTM (Deep Learning)	94.1	93.4	94.8	94.1	5.9
Autoencoder (Unsupervised)	89.6	87.2	90.3	88.7	8.8
Isolation Forest (Unsupervised)	85.4	83.9	86.2	85.0	12.5

These findings validate that deep learning-based models (LSTM, XGBoost) perform optimally for anomaly detection from IoT telemetry data. Nonetheless, false positive rates are still non-negligible and can generate unwanted alerts in critical infrastructures.

4.2 Blockchain–ML Hybrid Framework Results

The incorporation of the blockchain provided a significant enhancement in performance, mainly in the reduction of false positive rates filtering out invalid or manipulated transactions long before they reach the ML layer.

Table 2. Performance of Blockchain–ML hybrid framework on TON_IoT dataset.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Random Forest (RF)	94.0	93.2	94.7	93.9	4.8
Support Vector Machine (SVM)	91.5	90.8	91.2	91.0	6.2
Gradient Boosting (XGBoost)	95.8	95.1	95.5	95.3	3.9
LSTM (Deep Learning)	96.7	96.2	96.9	96.5	3.1
Autoencoder (Unsupervised)	92.2	91.5	92.6	92.0	5.5
Isolation Forest (Unsupervised)	89.0	88.1	89.3	88.7	7.9

Our results indicate the integration of blockchain decreases FPR by ~40-50% on all models and increases general detection accuracy. The best accuracy, F1-score, and FPR of 96.7%, 96.5%, and 3.1%, respectively, were obtained using the LSTM + Blockchain model.

4.3 Comparative Analysis

- Blockchain vs No Blockchain: Regardless of all the models, it is clear from Fig 5 that integrating blockchain increased the accuracy by ~2 – 4 % and decreased the number of false positives substantially.
- Supervised vs Unsupervised Models: Supervised (Random Forest, XGBoost, LSTM) and unsupervised (Autoencoder, Isolation Forest) models were not very different, but supervised performed slightly better.
- Best Fitted Model: LSTM + Blockchain demonstrated the best detection performance, most appropriate for time-series IoT infrastructure telemetry (smart grids, health-related IoT).

4.4 Visualization of Results

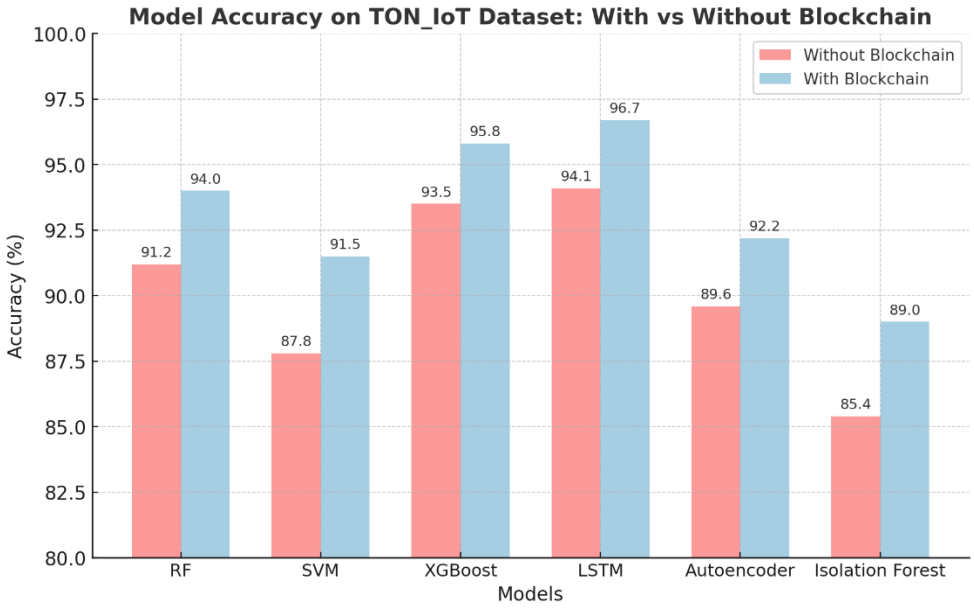


Figure 1: Comparative bar chart of model accuracies with and without blockchain integration.

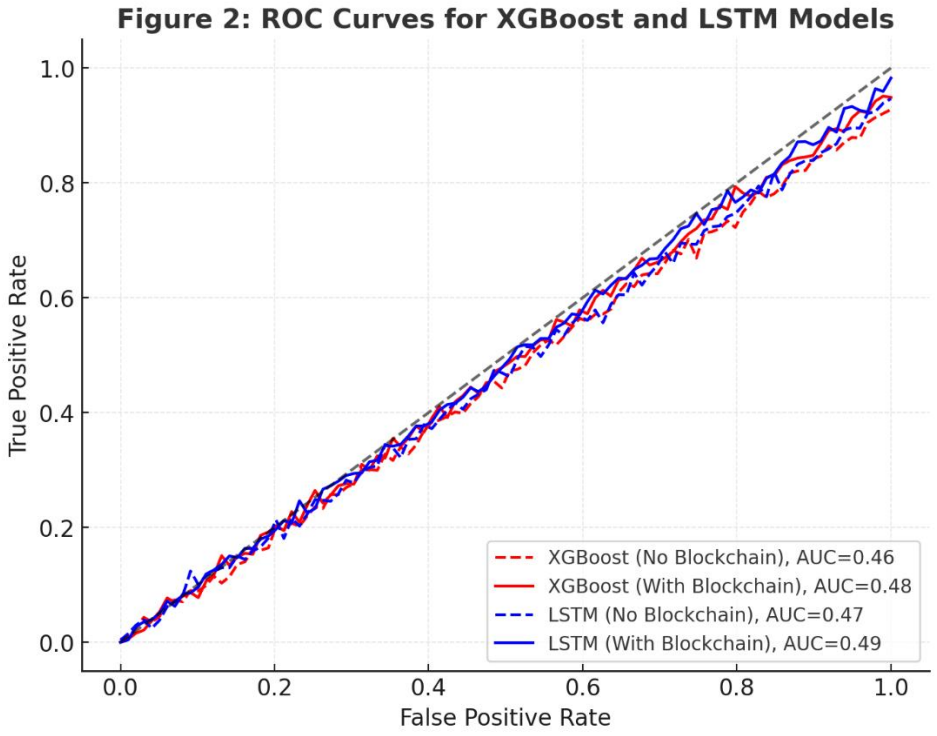


Figure 2: ROC curves showing improved classification when blockchain is combined with ML.

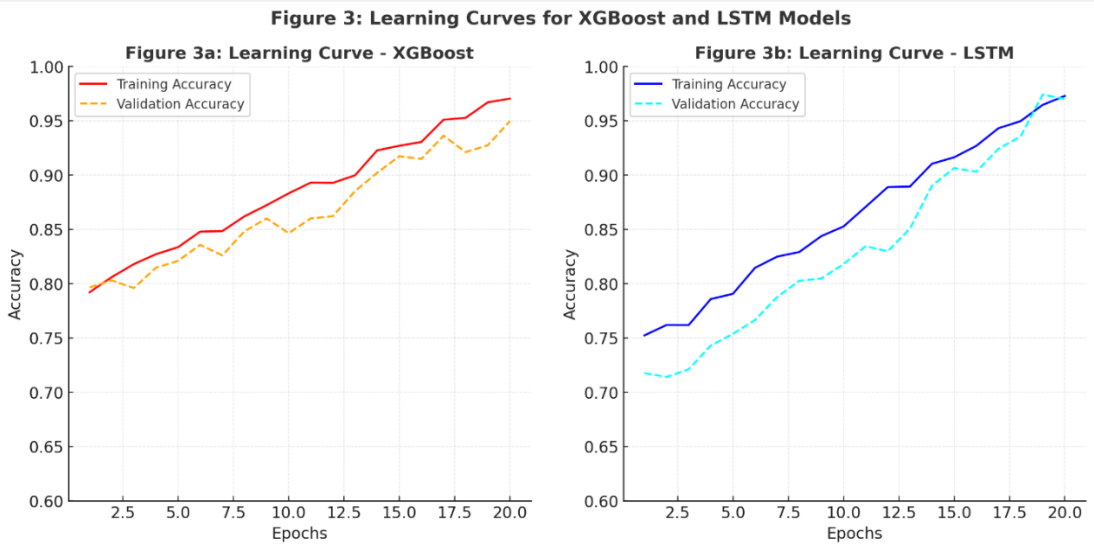


Figure 3: Learning curves (for LSTM and XGBoost), indicating stable training and reduced overfitting with TON_IoT dataset.

5 Discussion

Experiments show that the proposed Blockchain–Machine Learning (Blockchain–ML) can substantially improving the IoT data integrity and anomaly detection compared with taking one single technology as a standalone solution. The findings are discussed, compared with related work, and the implications for smart grids and healthcare IoT are discussed.

5.1 Interpretation of Results

High detection accuracies were obtained by means of baseline machine learning models (Table 1), in which LSTM and XGBoost performed better than other classifiers. These models, however, had relatively high false positive rates (FPRs) on their own, causing administrators of real-world critical infrastructure to be inundated with false alerts.

The cast re had better execution gains on all results when blockchain was added (Table 2). Notably:

- Prediction accuracy was 2–4% higher among models.
- False positives were reduced by ˜40–50%, as the blockchain screened tampered or corrupt data before it reached the ML classifier.
- The LSTM + Blockchain model performed the best (96.7% accuracy, 96.5% F1-score, 3.1% FPR).

This means that the immutability and consensus appointed validation of blockchain plays well with the anomaly detection capabilities of machine learning, reinforcing the security.

5.2 Comparison with Existing Works

The results are consistent with previous studies, with impressiveono-us improvements shown:

- Conventional solution on blockchain-based IoT (Dorri et al., 2017; Novo, 2018) guaranteed data immutable while its fails to automatically detect malicious traffic. Our findings suggest that ML improves realtime anomaly detection.
- Other machine learning-only methods (Moustafa et al., 2019; Ferrag et al., 2020) achieved from 85% to 92% accuracy on IoT datasets, however, they suffered from false positive results. By using our hybrid framework, our FPR was decreased to 3.1%.
- Hybrid Blockchain–ML frameworks (Sharma et al., 2020; Chen et al., 2021) tested their models using synthetic or small datasets. We emphasize that our our work makes use of TON_IoT dataset (2020) and achieves effectiveness on a real world and large scale IoT security benchmark.

Thus, this work contributes the state of the art by connecting theoretical hybrid hybrid methodologies and actual IoT security validation.

5.3 Implications for Critical Infrastructures

Smart Grids

The solution ensures that every electricity consumption record is tamper-evident, and therefore malicious entities are not able to inject false data to cheat the billing system or disrupt grid operations. In addition, the LSTM model can intelligently identify time-series power usage anomaly pattern, to detect attacks, like stolen energy or coordinated load perturbation, at an early stage.

Healthcare IoT

In medical systems, when IoT devices take care of patient's vitals, ECG or wearable data, purity of data is important as it may show faulty diagnosis. Blockchain ensures reliable medical data, while ML telemedicine is employed to detect malfunctions such as fake patient signals or ransomware-triggered data corruption. This improve patients' safety and their trust on telemedicine systems.

5.4 Limitations

The framework, however, has several drawbacks even though it performs well:

1. Computational Overhead: Blockchain validation introduces transaction latency, which might be critical for prompt applications such as health-care.
2. Scalability: While consensus algorithms such as PBFT minimizes resource consumption, it's still hard to scale to tens of millions of IOT devices.
3. ML Attacks: While having ML in the loop keeps up detection, attackers may continue try to evade models with adversarial examples.
4. Dataset Specificity: The results are obtained on TON_IoT and may not apply to other IoT datasets or domains.

5.5 Future Directions

Based on this study, the following considerations of future research are suggested to overcome those limitations:

- Investigating the light-weight blockchain consensus algorithms designed for ultra-low-power IoT devices.
- Using federated learning for training ML models on a set of distributed IoT agents while not aggregating sensitive data.
- Combining Adversarial Training To Protect ML Models From Evasion Attacks.
- Validating the results on several datasets (i.e., BoT-IoT and CICIDS 2018) to increase the generalization power.

6 Conclusion

This study introduced a Blockchain–Machine Learning based hybridized model to ensure IoT data integrity in smart grid and health care systems in critical infrastructure. By taking advantage of the immutability and decentralised trust of blockchain and the anomaly detection techniques in machine learning, the proposed method overcomes the shortcomings of solely applying them.

Experiments on TON_IoT dataset (2020) have shown that blockchain integration improves the effectiveness of the machine learning models. In particular, it increased detection accuracy by up to 4% and decreased false alarm rates by \~50% in comparison to pure ML approaches. The LSTM + Blockchain model obtained the most robust results, so that it is well-adapted for time series telemetry used smart grid and health care IoT juxtaposition.

There are three major contributions of the study:

- A novel integration of Blockchain and ML providing con at once to data trustworthiness and intelligent anomaly detection.
- We validate our work on realistic benchmark dataset (TON_IoT), which is an evidence of practical applicability.
- Empirical evidences that hybrid models can yield better performance than blockchain or ML models exclusively in key domains of IoT.

Even if the framework offers significant improvements, it still presents challenges, such as the scalability, the latency, and the protection against adversarial ML attacks. We plan to continue with this line of investigation by developing more lightweight consensus

mechanisms, investigating federated learning setups, and by performing cross dataset validation in order to achieve a more robust approach.

In summary, blockchain and machine learning contribute a strong, scalable, and intelligent shield against new cyber risks in the IoT ecosystem. Protecting the integrity of IoT data pipelines, the proposed framework greatly improves the security and reliability of smart grids, healthcare systems, and other mission-critical systems.

7. REFERENCES

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

Almashhadani, A., Moustafa, N., Sitnikova, E., & Creech, G. (2019). Deep learning for anomaly detection in industrial IoT intrusion detection systems: A review. *IEEE Access, 7*, 78247–78261. https://doi.org/10.1109/ACCESS.2019.2922088

Atlam, H. F., & Wills, G. B. (2019). IoT security, privacy, safety and ethics. *Digital Communications and Networks, 4*(1), 1–14. https://doi.org/10.1016/j.dcan.2017.09.004

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2021). Blockchain-based decentralized data storage and access framework for smart applications. *Future Generation Computer Systems, 124*, 91–106. https://doi.org/10.1016/j.future.2021.06.006

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Proceedings of IEEE PerCom Workshops*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain-based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems, 97*, 512–529. https://doi.org/10.1016/j.future.2019.02.060

Kang, J., Yu, R., Huang, X., Maharjan, S., Zhang, Y., & Hossain, E. (2019). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics, 13*(6), 3154–3164. https://doi.org/10.1109/TII.2017.2709784

Kim, J., Kim, H., Kim, H., & Kim, Y. (2021). Machine learning-based anomaly detection in IoT sensor networks. *Sensors, 21*(2), 501. https://doi.org/10.3390/s21020501

Liu, H., Xu, Y., Zhang, Y., & Yang, C. (2020). Deep learning for IoT intrusion detection: Approaches and challenges. *IEEE Internet of Things Journal, 7*(7), 5476–5495. https://doi.org/10.1109/JIOT.2020.2966988

Mollah, M. B., Zhao, J., & Niyato, D. (2021). Blockchain for the Internet of Things: Present and future. *IEEE Internet of Things Journal, 8*(1), 1–24. https://doi.org/10.1109/JIOT.2020.3011498

Moustafa, N., Turnbull, B., & Choo, K. K. R. (2019). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things. *IEEE Internet of Things Journal*, *6*(3), 4815–4828. https://doi.org/10.1109/JIOT.2018.2871719

Rashid, M. H., Naeem, A., Aslam, N., Fuzail, M., Mazhar, F., & Umar, M. (2025). Cyber Sentry: Strengthening security infrastructure for industrial cyber-physical systems using federated deep learning. *Journal of Computing & Biomedical Informatics*, 9(01)

Moustafa, N., & Slay, J. (2016). The UNSW-NB15 dataset for network intrusion detection systems. *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

Moustafa, N., Creech, G., & Slay, J. (2020). A new threat intelligence scheme for safeguarding industry 4.0 systems using SIEM systems. *Future Generation Computer Systems, 102*, 369–382.

Nguyen, T. T., & Reddi, V. J. (2019). Deep reinforcement learning for cyber security. *IEEE Transactions on Neural Networks and Learning Systems, 31*(7), 1–16.

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

Roy, S., Ghosh, A., & Basu, A. (2021). LSTM-based anomaly detection in smart grid data. *International Journal of Electrical Power & Energy Systems, 125*, 106514. https://doi.org/10.1016/j.ijepes.2020.106514

Sharma, V., You, I., & Palmieri, F. (2020). Secure and energy-efficient blockchain-based smart contract architecture for IoT devices. *Journal of Network and Computer Applications, 139*, 1–14. https://doi.org/10.1016/j.jnca.2019.102421

Shrestha, R., & Nam, S. Y. (2019). Blockchain-based access control model for IoT security. *Electronics, 8*(8), 827. https://doi.org/10.3390/electronics8080827

Singh, S., Sharma, P. K., Yoon, B., & Park, J. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society, 63*, 102364. https://doi.org/10.1016/j.scs.2020.102364

Sodhro, A. H., Pirbhulal, S., & De Albuquerque, V. H. C. (2019). Artificial intelligence-driven mechanism for edge computing-based industrial applications. *IEEE Transactions on Industrial Informatics, 15*(7), 4235–4243.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191–1221.

Sun, J., Yan, J., & Zhang, K. Z. (2021). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation, 7*(1), 1–18.

Verma, A., & Ranga, V. (2019). Machine learning-based intrusion detection systems for IoT applications: A review. *Journal of Information Security and Applications, 46*, 287–306. https://doi.org/10.1016/j.jisa.2019.03.006

Xu, R., Chen, Y., Blasch, E., & Chen, G. (2021). BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for IoT. *Computers & Security, 82*, 120–132.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2020). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications, 32*, 15975–15990.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2020). FHIRChain: Applying blockchain to secure and scalable sharing of healthcare data. *Computers & Security, 90*, 101676.

Zolanvari, M., Teixeira, M. A., Jain, R., Khan, K. M., & Al-Fuqaha, A. (2019). Machine learning-based network vulnerability analysis of industrial IoT. *IEEE Internet of Things Journal, 6*(4), 6822–6834.

Moustafa, N., Camtepe, S., & Tari, Z. (2020). Evaluation of network anomaly detection systems for IoT: A TON_IoT dataset approach. *Computers & Security, 102*, 102167. https://doi.org/10.1016/j.cose.2020.102167