MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3841-3843

TRUST - AWARE IOT ARCHITECTURES: INTEGRATING ANOMALY DETECTION WITH DEVICE-LEVEL PROVENANCE

Dr. S. Amutha
Professor, Department of Computer Science and Engineering, School of Computing,
Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,
Chennai, Tamil Nadu, India
dramuthas@veltech.edu.in
Dr. A. Jayanthi,
Associate professor, Department of Management Science,
Hindusthan college of Engineering and Technology, Coimbatore, India thirujayanthi2@gmail.com,
Orc id: https://orcid.org/0009-0001-7862-111X
Wasim Raja A,
Assistant Professor, Department of Artificial Intelligence and Data Science,
Sri Krishna College of Engineering and Technology, Coimbatore, India
wasimrajaa@skcet.ac.in
S. MOHAN,
Assistant professor, Department of Computer Science Engineering,
V.S.B. COLLEGE OF ENGINEERING TECHNICAL CAMPUS, COIMBATORE, India
smohanckr@gmail.com
N. TAMILARASI
Assistant Professor, Department of CCE
Nehru institute of Technology, India
nittamilarasi@nehrucolleges.com
M. Priyadharshan
Assistant Professor, Department of Artificial intelligence and Data science.
Nehru Institute of Engineering and Technology, Thirumalayampalayam, Coimbatore, India
m.priyadharshan@gmail.com

Abstract
The article is talking about aware IoT architectures, which combine anomaly detection and device-level provenance to enhance the security, trust and reliability of a system. It expounds on architectural foundations, methods of detection, provenance and the role of these three different methods in data integrity and real-time monitoring. The article also explains the problem of integration and future trends in scalable and intelligent IoT systems.

Keywords: IoT Security, Anomaly Detection, Data Provenance

1. Introduction

The swift development of the Internet of Things (IoT) has altered the contemporary digital ecosystem because it allows devices, sensors, and systems to exchange information in real-time, and it includes smart cities, healthcare, and industrial automation among other areas (Jot and Sharma, 2023). This has resulted in a huge increase in the number of connected devices, which has played a major role in boosting data generation and the complexity of systems and has opened up various opportunities to enhance efficiency and innovation. Critical threats are also presented by this growth in terms of security, data integrity, and trust. IoT devices are frequently prone to hacking, old software, and low computing power, which are highly susceptible to cyberattacks, data breaches, and manipulation of the system (Jose and Judith, 2024).

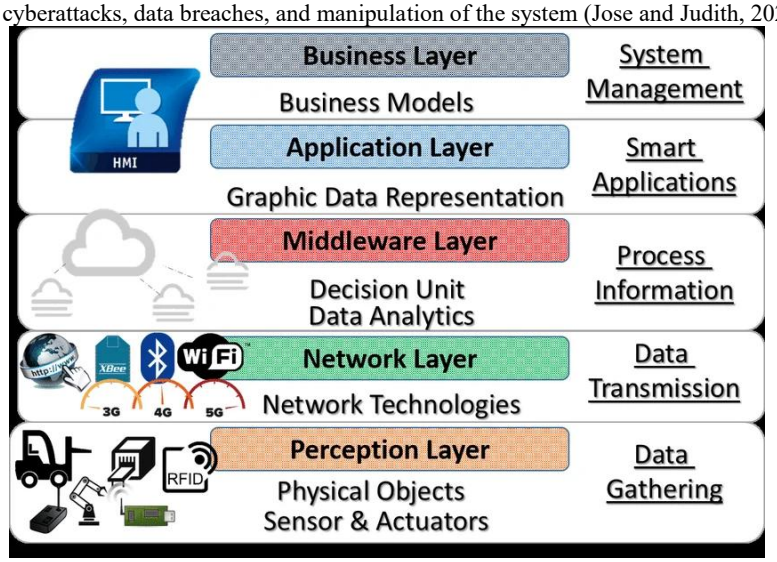

Figure one: Five Layer IoT Architecture
Source: Antãoe *et al.,* 2018

To resolve these problems, we have seen the emergence of the idea of aware IoT architectures, which are based upon context-aware and self-monitoring systems that can dynamically respond to changes in the environment and operations. The intelligent mechanisms do form part of such architectures to observe the behaviour of devices and to maintain the reliability of the system. Anomaly detection is therefore vital in this context because it can detect abnormal patterns or malicious actions in the IoT networks, thus improving security and operational efficiency. Besides, device-level provenance offers the data sources and device actions provenance traceability, enhancing system transparency and trust (Haider *et al.,* 2025). The proposed article focuses on analysing how anomaly detection and device-level provenance are incorporated into the aware IoT architecture. It discusses their synergistic potential to enhance security, reliability, and trust, and stipulates the critical issues and future research perspectives in this developing area.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3841-3843

2. Foundations of Aware IoT Architectures

Aware IoT architectures are made to introduce context-awareness, flexibility, and autonomy in the work of systems. Context-awareness is a concept describing how systems perceive the environmental conditions and user contexts in a dynamic manner and make intelligent decisions. These types of architectures make systems more responsive by continuously observing data and making changes to behaviour depending on changes in situations. The main features are the real-time interpretation of the data, self-configuration, and autonomous control, which facilitate the efficient and scalable IoT environments (Augusto *et al.,* 2022).

The IoT systems are also planned to have multiple layers, including the device (perception) layer, the edge/fog layer, and the cloud layer. The device layer has sensors and actuators that gather information, whereas the edge/fog layer processes information nearer to the origin to minimise the latency. Cloud layer carries out mass storage and analytics. The communication protocols like Wi-Fi, 5G, and Bluetooth among these layers allow data flow and make the connection and information transfer seamless and in real-time (Kawthekar *et al.,* 2025).

Irrespective of these developments, IoT systems have serious security and trust threats. Distributed architectures contribute to the exposure to data manipulation, unauthorised access, and not being transparent. Lack of strong authentication tools and disparity in device settings also make the security control more difficult, which demonstrates the necessity of strong trust systems and encryption-based communication protocols (Mansour *et al.,* 2023).

3. Anomaly Detection in IoT Systems

The anomalies in the IoT systems are usually categorised as point, contextual and collective anomalies. The point anomalies are cases of single data that strongly differ from the general trends, whereas contextual anomalies are scenarios that rely on a certain condition, like time or place (Al-Amri *et al.,* 2021). Collective anomalies are the presence of a group of data that acts abnormally as a pattern. Statistical techniques are used as anomaly detectors and can be modelled as normal behaviour, and anomalies noted, and machine learning or deep learning algorithms used, e.g. neural networks and clustering algorithms, which are more effective detectors of anomaly in complex IoT data (DeMedeiros *et al.,* 2023). Detection may be implemented through cloud-based systems to analyse on a massive scale or an edge-based method to give a faster and real-time analysis. Cloud solutions have a risk of introducing latency, whereas edge computing is faster in response time but limited in resources, which is problematic in terms of scalability in an IoT setting (Ngo *et al.,* 2020).

4. Device-Level Provenance in IoT

IoT Data and device provenance Data and device provenance denotes a record of the provenance of data produced by devices, wherein it is possible to trace the provenance of data across the system with confidence. Provenance has been beneficial in preventing the identity of data and identifying malicious intent in distributed IoT settings (Hu *et al.,* 2020).

The provenance information may be gathered with the help of logging, metadata tagging, and the use of blockchain-based tracking. A blockchain allows documenting the operations of data in an unalterable way, with each purchase being recorded on data creation and modification ensuring integrity and verifiability (Honar Pajooh *et al.,* 2021).

Provenance on a device level provides better trust, traceability and accountability because it keeps track of transparent data histories and avoids unwarranted manipulation of data. There are also storage overhead, scalability concerns, and privacy threats, not to mention that vast amounts of metadata need to be safely stored and processed on the complex IoT networks (Partida, 2024).

5. Integration of Anomaly Detection and Provenance

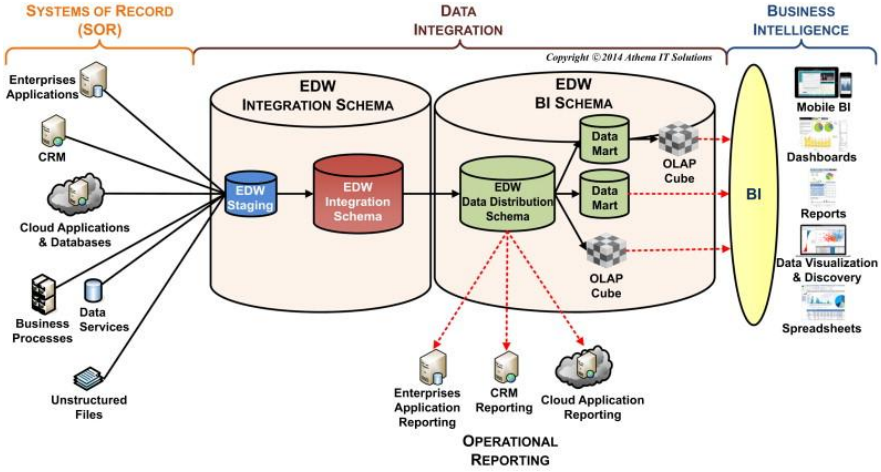

Figure two: Integration Architecture

Source: Van't Wout *et al.,* 2010

Layered and hybrid architectural designs are normally used to implement the integration of anomaly detection and provenance within IoTs. These systems use detection systems together with provenance tracking, both at device, edge and cloud levels, which allows synchronised monitoring and verification. Modern focuses on solution middleware that combines detection and response and auditing capabilities in the middleware to enhance resilience and scalability (Ortiz-Garcés *et al.,* 2025). Moreover, hybrid models frequently use blockchain to guarantee the security and integrity of the records of device operations as well as to define efficient and decentralised anomaly identification surveillance among networks (Almasabi *et al.,* 2025).

A provenance record is beneficial to the detection of anomalies because it supports contextual provenance and provenance history, allowing systems to more readily differentiate legitimate and malicious behaviour. Studies have shown that AI-based detection, together with secure data monitoring, will increase detection and minimise false positives through the provision of data integrity and reliability (Reis, 2025).

In smart cities, healthcare internet of things, and industrial internet of things, embedded systems facilitate real-time tracking, safe data transmission and instant threat assistance. The systems can be used to increase reliability in operations and cybersecurity, as they allow it to detect anomalies continuously and verify large-scale deployments of IoT transparently (Haider *et al.,* 2025).

6. Discussion

Recent methods incorporating anomaly detection and provenance in IoT show that much has been achieved, especially in AI-based and federated learning frameworks that are more accurate in detecting anomalies and preserving privacy. These systems also have constraints associated with data heterogeneity, model robustness, and constraints on real-world deployment, and the fact that available solutions are not yet sufficiently mature and can only be widely adopted by large amounts of data (Alqazzaz, 2026).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 3841-3843

One of the most important issues in question is the balance between performance, privacy and scale. Centralised systems provide a high capacity of computation at the cost of privacy, whereas decentralised systems, like federated learning, keep the data private but cause communication overheads and latency problems. Scaling is yet to be improved because of the device constraints as well as the complexities of the IoT networks within large ecosystems (Deshmukh *et al.,* 2025).

There are still major gaps in the research, especially in interoperability and standardisation. The existing IoT systems tend to work on isolated systems that have incompatible protocols; they lack cross-platform integration and effective sharing of data among each other. The future research directions are based on AI-based adaptive architecture, federated learning, and zero-trust IoT architecture. Such solutions will enable decentralised intelligence, continuing verification and safe collaboration amongst heterogeneous devices, which ultimately promotes resilience, trust, and scalability in the upcoming systems in the IoT (Kaushik *et al.,* 2026).

7. Conclusion and Recommendations

To summarise, conscious IoT architectures incorporating anomaly detectors with device-level provenance are a sound solution to the main issues regarding security, trust, and data integrity. Real-time detection of anomalies and transparent provenance tracking contribute to increasing the reliability of the system as they allow identifying threats correctly and tracing the data.

To enhance the strength of the IoT ecosystems, hybrid edge-cloud infrastructures with low latency and computational efficiency are suggested to be implemented. Lightweight AI models can also be used to aid the real-time monitoring of resource-constrained environments. In addition, it is possible to use safe provenance, including blockchain, to ensure no data is tampered with. Lastly, it is necessary to establish standard frameworks and regulatory policies to enhance interoperability, scalability, and trust on various IoT systems (Pokhrel *et al.,* 2024).

References

Al-Amri, R., Murugesan, R.K., Man, M., Abdulateef, A.F., Al-Sharafi, M.A. and Alkahtani, A.A., 2021. A review of machine learning and deep learning techniques for anomaly detection in IoT data. *Applied Sciences*, *11*(12), p.5320.

Almasabi, A.M., Alkhodre, A.B., Khemakhem, M., Eassa, F., Abi Sen, A.A. and Harbaoui, A., 2025. Internet of things-based anomaly detection hybrid framework simulation integration of deep learning and blockchain. *Information*, *16*(5), p.406.

Alqazzaz, A., 2026. SecuFL-IoT: an adaptive privacy-preserving federated learning framework for anomaly detection in smart industrial networks. *Scientific Reports*.

Antão, L., Pinto, R., Reis, J. and Gonçalves, G., 2018, April. Requirements for testing and validating the industrial internet of things. In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (pp. 110-115). IEEE.

Augusto, J.C., Quinde, M.J., Oguego, C.L. and Giménez Manuel, J., 2022. Context-aware systems architecture (CaSA). *Cybernetics and Systems*, *53*(4), pp.319-345.

Deepali Kawthekar, Pallavi Dakhore, Kalyani Shevatekar , Bharat Shelke, Prajkta More, 2025. *A Comprehensive Survey on Internet of Things (IoT), Architecture, Protocols, and Applications*. https://doi.org/10.22214/ijraset.2025.73169

DeMedeiros, K., Hendawi, A. and Alvarez, M., 2023. A survey of AI-based anomaly detection in IoT and sensor networks. *Sensors*, *23*(3), p.1352.

Deshmukh, A., de la Rosa, P.E., Rodriguez, R.V. and Dasari, S., 2025. Enhancing privacy in IoT-enabled digital infrastructure: Evaluating federated learning for intrusion and fraud detection. *Sensors*, *25*(10), p.3043.

Devin Partida, 2024. *The Role of Data Provenance in Securing IoT Ecosystems*. https://www.iotforall.com/the-role-of-data-provenance-in-securing-iot-ecosystems

Haider, Z.A., Zeb, A., Rahman, T., Singh, S.K., Akram, R., Arishi, A. and Ullah, I., 2025. A Survey on anomaly detection in IoT: Techniques, challenges, and opportunities with the integration of 6G. *Computer Networks*, *270*, p.111484.

Haider, Z.A., Zeb, A., Rahman, T., Singh, S.K., Akram, R., Arishi, A. and Ullah, I., 2025. A Survey on anomaly detection in IoT: Techniques, challenges, and opportunities with the integration of 6G. *Computer Networks*, *270*, p.111484.

Honar Pajooh, H., Rashid, M.A., Alam, F. and Demidenko, S., 2021. IoT Big Data provenance scheme using blockchain on Hadoop ecosystem. *Journal of Big Data*, *8*(1), p.114.

Hu, R., Yan, Z., Ding, W. and Yang, L.T., 2020. A survey on data provenance in IoT. *World Wide Web*, *23*(2), pp.1441-1463.

Jewan Jot, Prof. Lalit Sen Sharma, 2023. *Study of Anomaly Detection in IoT Sensors*. https://doi.org/10.22214/ijraset.2023.55226

Jose, J. and Judith, J.E., 2024. Unveiling the IoT's dark corners: anomaly detection enhanced by ensemble modelling. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *65*(2), pp.584-596.

Kaushik, D., Gulia, P., Gill, N.S., Yahya, M., Shukla, P.K. and Shreyas, J., 2026. Synergizing blockchain and AI to fortify IoT security: a comprehensive review. *Artificial Intelligence Review*, *59*(2), p.41.

Mansour, M., Gamal, A., Ahmed, A.I., Said, L.A., Elbaz, A., Herencsar, N. and Soltan, A., 2023. Internet of things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions. *Energies*, *16*(8), p.3465.

Ngo, M.V., Chaouchi, H., Luo, T. and Quek, T.Q., 2020. Adaptive anomaly detection for IoT data in hierarchical edge computing. *arXiv preprint arXiv:2001.03314*.

Ortiz-Garcés, I., Villegas-Ch, W. and Luján-Mora, S., 2025. Autonomous cyber-physical security middleware for IoT: anomaly detection and adaptive response in hybrid environments. *Frontiers in Artificial Intelligence*, *8*, p.1675132.

Pokhrel, S.R., Yang, L., Rajasegarar, S. and Li, G., 2024, August. Robust zero trust architecture: Joint blockchain based federated learning and anomaly detection based framework. In *Proceedings of the SIGCOMM Workshop on Zero Trust Architecture for Next Generation Communications* (pp. 7-12).

Reis, M.J., 2025. AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. *Electronics*, *14*(12), p.2492.

Van't Wout, J., Waage, M., Hartman, H., Stahlecker, M. and Hofman, A., 2010. *The integrated architecture framework explained: why, what, how*. Springer Science & Business Media.