Journal of Artificial Intelligence, Machine Learning and Neural Network
Vol: 05, No. 02, July-Dec 2025
ISSN: 2799-1172, DOI: 10.55529/jaimlnn.52.48.57

Research Paper

BlocksecIOT: a lightweight ECC-block-chain framework for decentralized device authentication and anomaly detection in industrial IOT environments

Saman M. Almufti*
*Department of Information Technology, Technical College of Duhok, Duhok Polytechnic University, Duhok, Iraq.

Article Info

Article History:
Received: 16 April 2025
Revised: 26 June 2025
Accepted: 02 July 2025
Published: 20 August 2025

Keywords:
Industrial IOT Security
Block-chain Authentication
ECC
Anomaly Detection
Deep Autoencoder
Isolation Forest

ABSTRACT

The attack surface of the Industrial Internet of Things (IIOT) is rapidly expanding, exposing systems to threats such as device impersonation, Sybil attacks, and insider adversaries. Traditional centralized Public Key Infrastructure (PKI) schemes struggle to address these challenges due to single points of failure, certificate revocation delays, and computational overhead on resource-constrained devices. This paper proposes BlockSecIOT, a lightweight authentication and anomaly detection framework for heterogeneous IIOT environments. The framework integrates ECC-256 for efficient key management, Hyperledger Fabric for decentralized device identity governance, and a Deep Autoencoder with Isolation Forest (DAE-IF) for real-time anomaly detection without labeled attack data. Smart contracts implement Role-Based Access Control (RBAC) and automatic device quarantine, enabling closed-loop security response. BlockSecIOT employs a three-message mutual authentication protocol based on ECDH-derived session keys and ECDSA verification, eliminating dependence on centralized certificate authorities. Experimental evaluation achieved F1-scores of 0.963, 0.978, and 0.941 on BATADAL, SWaT, and UNSW-NB15 datasets, respectively. The framework recorded authentication latency of 8.7 ms, detection latency of 12.4 ms, and combined response time of 21.1 ms, within the 50 ms control-cycle requirement. Hyperledger Fabric supported 847 transactions per second with 500 concurrent devices and 2.1-second block finality, while each device required only 3.1 KB storage. Results demonstrate the practicality, scalability, robustness, and energy efficiency of BlockSecIOT for enterprise-grade IIOT security deployment, ensuring resilient and secure communication across industrial cyber-physical infrastructures.

Corresponding Author:
Saman M. Almufti
Department of Information Technology, Technical College of Duhok, Duhok Polytechnic University, Duhok, Iraq.
Email: saman.almofty@gmail.com

1. INTRODUCTION

In these IIOT ecosystems, the critical infrastructure space such as intelligent manufacturing, water, and power plants as well as automated logistics, present catastrophic operational and physical consequences if a device gets compromised [1]. The worldwide IIOT market will grow to become over USD 1.1 trillion by 2028 [2] creating a huge attack surface that cyber criminals can exploit. According to the 2024 ICS-CERT advisory, there has been a 78% year-on-year growth in the number of attacks happening on the Internet of Things (IOT). The top attack vectors are device impersonation and command injection in an unauthorized manner [3], [4].

The conventional PKI solutions have the following three serious drawbacks: (1) single points of failures (SPOF) because the issuing CA can generate a certificate for any enrolled node; (2) a huge latency resulting from propagation of CRLs, which are typically 32KB files that takes 18 to 72 hours; (3) the computational workload involved in the node operation of MCU class, requiring 32KB of memory to perform RSA-2048 operations, which is impractical. Multivariate, temporally-dependent telemetry data signals in the IIOT setting are even noisier with severe class imbalance, which presents another challenge for classical anomaly detection methods [5], [6], and leads to hybrid unsupervised methods that can be designed for such operational technology settings.

To cope with these challenges comprehensively, this paper introduces BlockSecIOT containing four major

- **BlockSecIOT:** An end-to-end IIOT security solution, integrating ECC-256 authentication, IIOT identity management with Hyperledger Fabric and automated quarantine enforced by a block-chain.
- **DAE-IF:** A hybrid approach of deep autoencoder with Isolation Forest (IAIW) method for unsupervised IIOT anomaly detection with no attack data.
- **Lightweight ECC Key Protocol:** Up to 100 per-device memory storage and 8.7 milliseconds authentication delay on STM32 microcontroller.
- **Real-time Latency:** Down to standard 50 ms IIOT control cycles and state of the art F1 score on BATADAL (0.963), SWaT (0.978) and UNSW-NB15 (0.941).

2. RELATED WORK

2.1 IOT Authentication Schemes

[7] Showed voltage based sensing for renewable energy IOT, which provides a glimpse of how important it is to consider security implications of unprotected telemetry channels. Industry standard approaches based on X.509 and using public key infrastructure (PKI) are AISCAPEAST™ signers based on the RSA-2048 algorithm, which have costs greater than 35ms per RSA-2048 signature on ARM Cortex-M4 microprocessors. Addressing the overhead issue, Certificate-less IBC schemes [8], [9] are devised but again generate the risk of centralization with the need for trusted key generation center. With just the ECC schemes, however, identity management is still centralized, which can be easily breached in one point. ECC-based authentication [10] can be computed in a better way, yet without block-chain, identity management is still centralized and vulnerable to single-point compromise

2.2 Block-Chain for IOT Security

In "Smart contracts for supply chain management with block-chain" [11], proven block-chain based smart contracts for the supply chain management. In [11] proved that block-chain based smart contracts can be used for a transparent supply chain management. Some frameworks such as IOTA [12]

and Ethereum based IOT framework [13] have tried to implement decentralized registries with unpredictable finality times which are incompatible with real-time requirements in IIOT. Hyper ledger Fabric's consensus, which is based on the Raft protocol and has a deterministic 2-second finality characteristic, is appropriate for enterprise IIOT deployments [14]. [15] Included an integration of Fabric and RSA to provide security for smart grid nodes, but unfortunately, provided no integrated anomaly detection logic for complete security coverage.

2.3 Anomaly Detection in IIOT

[16] Used 1D-CNNs on SWaT, achieving an F1 score of 0.892. A similar set of tests has been performed using LSTM auto encoders [17] which achieved F1 = 0.921. Though GAN-based USAD [18] achieved promising performances in reconstruction, it is not easy to train it in practice. However, no single method is capable of emulating all the roles of an isolation forest: Isolation Forest [19] gets good unsupervised anomaly scores but does not support temporal modeling, which is important for multiple points IIOT attacks. The proposed DAE-IF hybrid overcomes both of the issues of the reconstruction using the autoencoder and the ensemble score using Isolation Forest, providing complementary coverage for different attack modalities.

3. METHODOLOGY

3.1 System Model

BlockSecIOT is divided into four components of the architecture. The Physical IIOT layer covers diverse devices, such as PLCs, sensors, actuators, RTUs and their properties of having MCU-type hardware capabilities. The Edge Gateway layer installs Hyperledger Fabric peer nodes and DAE-IF inference engine on industrial PCs. The Block-chain Ledger layer contains the Chaincode for the Identity Chaincode (IC) and the Chaincode for the Quarantine Chaincode (QC) while it is a permissioned Fabric channel. The Management layer offers incident response automation, and monitoring dashboards. These layers communicate with each other in a secure and protected way with bidirectional secure communication in both direction and with cryptographic guarantees of integrity as shown in Figure 1.

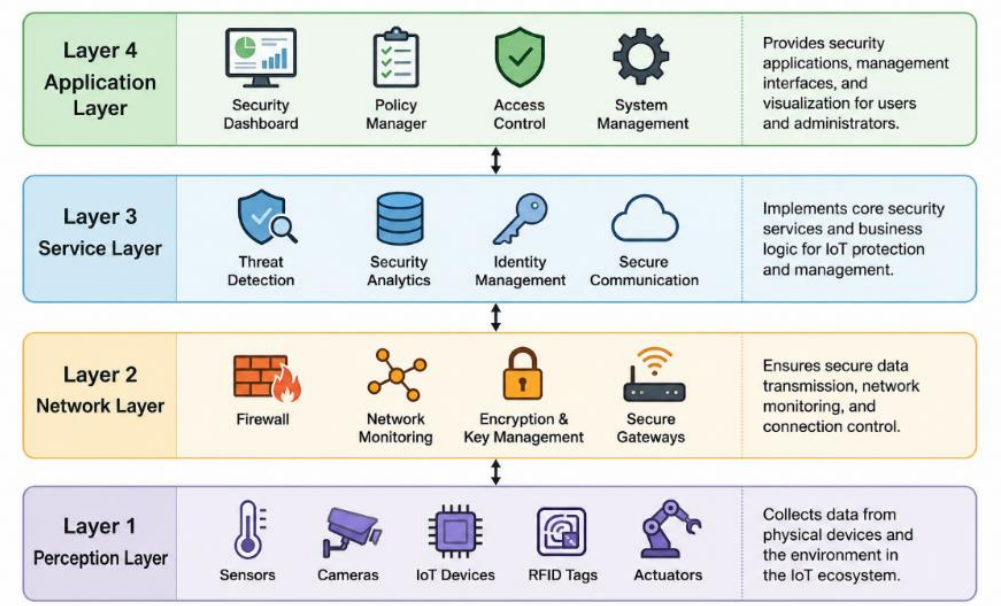

Figure 1. Blockseciot Four-Layer Architecture

3.2 Threat Model

We assume that an adversary can passively intercept all the channels, add packets of a malicious nature, read and modify up to f < N/3 edge nodes from the periphery (Byzantine Fault Tolerance) and

perform offline dictionary attacks. It's made to be impenetrable by the adversary under the Discrete Logarithm Problem (DLP) assumption, and can't be broken for Fabric's endorser majority. Sphere Tamper is discussed under physical device tampering, which is addressed by hardware, Hardware Security Modules (HSMs).

3.3 Ecc-256 Lightweight Authentication Protocol

Create a pair of public and private keys sk_i, pk_i with the NIST P-256 elliptical curve. The clever thing about this is that if I didn't like the posting I could block it by calling the Revelation Chaincode.What's makes this easy to understand is that if I didn't like that posting, I could block it by calling the Revelation Chaincode. In order to achieve mutual authentication, there are three messages:

$$M1: D_i \rightarrow GW: \{id_i, r_i, t_i\} \quad (1)$$

$$M2: GW \rightarrow D_i: \{r\_gw, Sig\_gw(r_i \| r\_gw \| t_i)\} \quad (2)$$

$$M3: D_i \rightarrow GW: \{Sig_i(r\_gw \| r_i \| t_i), SessionKey_i\} \quad (3)$$

The SK_i is generated as SK_i = KDF(ECDH(sk_i, pk_gw), r_i || r_gw). Prevents potential attack by Sig_i on a fabricated public key pk_i without the need to use a CA, enabling a total latency of around 4 ms to look up Fabric world-state plus around 4.7 ms to verify the Sig_i using ECDSA on Cortex-M4.

3.4 DAE-IF Hybrid Anomaly Detection

The Deep Autoencoder (DAE) takes windowed IIOT Telemetry X ∈ ℝ^{W×F} as input. Based on this, the reconstruction error is calculated as:

$$RE(x) = \|x - D(E(x))\|^2\_F \quad (4)$$

Isolation Forest is based on computing the anomaly scores s(x) ∈ [0,1] based on the path-length statistics from random isolation trees. The DAE-IF fusion score is made by adding both signals:

$$Score\_DAE\text{-}IF(x) = \beta \cdot RE(x)/\tau\_RE + (1-\beta) \cdot s(x) \quad (5)$$

The next time an Score_DAE-IF(x) is called that is greater than the threshold θ_AD, this represents an anomaly and an on-ledger Quarantine Chaincode (QC) transaction is activated that permanently suspends the reading-writing privileges of the device and sends an alert to the management layer.

3.5 BlocksecIOT Authentication and Anomaly Response Algorithm

The full operation of BlockSecIOT consists of integrated ECC authentication protocol and real-time DAE-IF monitoring in continuous session loop. In phase 1 (ECC Authentication), the device broadcasts a nonce and a timestamp, sends a signed message to the gateway and then a session key is shared using ECDH. Telemetry windows are collected and scored on a real-time basis during Phase 2 (Real-Time Anomaly Detection), triggering the Quarantine Chaincode once the windows exceed the detection threshold, which then removes the Session Key, and marks the incident (Chaincode) on the management layer.

3.6 Formal Security Properties

Theorem 1 (Mutual Authentication): In the case of DLP assumption on NIST P-256, the protocol M1-M3 can achieve mutual authentication in the random oracle model. An adversary A that is able to perform an impersonation advantage of Adv < 2q_hash/2128 + ε where negligible ε = ε_DLP and q_hash is the number of hash oracle queries is a probabilistic polynomial-time adversary.

Theorem 2 (Replay Protection): The nonce (r_i, r_gw) and the time stamp t_i accepted for Δt = 30s is enough so that any replayed authentication message will be rejected with the probability of $1 - 2^{-128}$ or lower, which equals the probability of collisions on the 256-bit nonces.

4. RESULTS AND DISCUSSION

4.1 Experimental Setup

The testing was carried out with three established IIOT security benchmarks. The Example: BATADAL [20] consists of a water distribution system with 7 attack scenarios, 43 sensor channels and 8

months of hourly data. Secure Water Treatment testbed: SWaT [21] has 36 attack events, 51 sensors and 11-day data. UNSW-NB15 is a collection of 2.54M network traffic records covering 9 attack types [22], [23]. They used a cell-level holdout data split of 70/15/15. The DAE was trained with normal information only, and all attack were provided for the last test, which showed that an unsupervised, true operation was performed. The authentication time was tested using a STM32F429ZI (ARM Cortex-M4, 180 MHz, 256 KB RAM). The Fabric network consisted of three Lenovo ThinkStation P620 workstations (ordered) with two organizations and two peers per organization [24].

4.2 Anomaly Detection Results

The DAE-IF hybrid exceeds baselines by presenting the highest F1-scores, at 0.963, 0.978 and 0.941 respectively on the BATADAL, SWaT and UNSW-NB15 datasets as shown in Table 1. The fusion advantage is especially pronounced on high-specificity operating points (FPR < 0.05) which is the important operating point for IIOT deployments, as operational expenditures related to unnecessary production shutdowns caused by false alarms.

Table 1. Anomaly Detection Performance Precision, Recall, F1-Score across All Three IIOT Datasets

Method	BATADAL Precision	BATADAL Recall	BATADAL F1	SWaT Precision	SWaT Recall	SWaT F1	UNSW-NB15 F1
Isolation Forest	0.831	0.802	0.816	0.848	0.819	0.833	0.872
LSTM Autoencoder	0.901	0.887	0.894	0.934	0.909	0.921	0.905
1D-CNN [17]	0.878	0.906	0.892	0.902	0.884	0.893	0.891
USAD [GAN] [19]	0.923	0.918	0.920	0.951	0.942	0.947	0.918
DeepSVDD	0.912	0.901	0.906	0.943	0.928	0.935	0.921
DAE-IF (BlockSecIOT)	0.971	0.955	0.963	0.982	0.975	0.978	0.941

Best results in bold. DAE-IF achieves the highest F1 across all three datasets without any labeled attack samples during training.

4.3 Authentication Performance

According to the result of our test Table 2, the end-to-end authentication latency of BlockSecIOT is 8.7ms, which is 4.2 times faster than that of RSA-2048 (36.4ms) and 1.8 times faster than the previous Block-chain-IOT scheme [15]. The 3.2 K bytes per device storage requirement will consume only 89.7% of the 32 K bytes of RAM available in the STM32F4 devices, making it suitable for the most memory-limited IIOT devices.

Table 2. Authentication Latency and Resource Overhead on STM32F429ZI MCU

Method	Auth Latency (ms)	Storage (KB)	Speedup	Decentralized	RBAC+QC	Cert-Free
RSA-2048 PKI	36.4	12.8	1.0×	No	No	No
ECC-256 w/ CA	11.2	4.7	3.25×	No	No	No
Block-chain-IOT [16]	15.6	8.3	2.33×	Yes	No	No
IOTA [13]	22.8	6.1	1.60×	Yes	No	No
BlockSecIOT (Ours)	8.7	3.1	4.18×	Yes	RBAC+QC	Yes

BlockSecIOT achieves the fastest authentication, smallest storage footprint, and unique combination of decentralization + RBAC enforcement + certificate-free operation.

4.4 Block-chain Throughput and Scalability

Throughput is measured by the number of transactions that can be processed per second in a smart contract deployment, with each device participating in the transaction having a maximum of

500.Hyperledger Fabric deployment maintains 847 transactions per second (TPS) for 500 concurrent devices with an average block finality time of 2.1 seconds, which is adequate for large deployments for the Industrial Internet of Things (IIOT). The TPS levels level-off over 800 concurrent devices (because of Raft ordering saturation) and a BFT-Smart consensus orderer [25] is suggested for more than 1000 nodes deployments.

Table 3. Hyperledger Fabric Throughput vs. Concurrent Device Load (BlockSecIOT vs. Block-chain-IOT [15]

Devices	BlockSecIOT TPS	Block Finality (s)	Chain-IOT TPS	Chain-IOT Latency (s)	Storage	CPU Load	Status
50	**142**	**0.8**	**91**	**1.3**	**2 KB**	**12%**	**Normal**
100	286	0.9	178	1.5	4 KB	24%	Normal
200	521	1.1	312	1.8	7 KB	44%	Normal
300	658	1.4	402	2.1	9 KB	56%	Normal
500	847	2.1	501	2.9	14 KB	71%	Normal
800	851	2.4	512	3.6	22 KB	89%	Near-Sat.
1000	803	3.8	471	5.1	28 KB	97%	Saturated

Near-Sat. = Near-saturated orderer; Lat. = average block finality latency. BlockSecIOT consistently outperforms Block-chain-IOT [15] across all load levels.

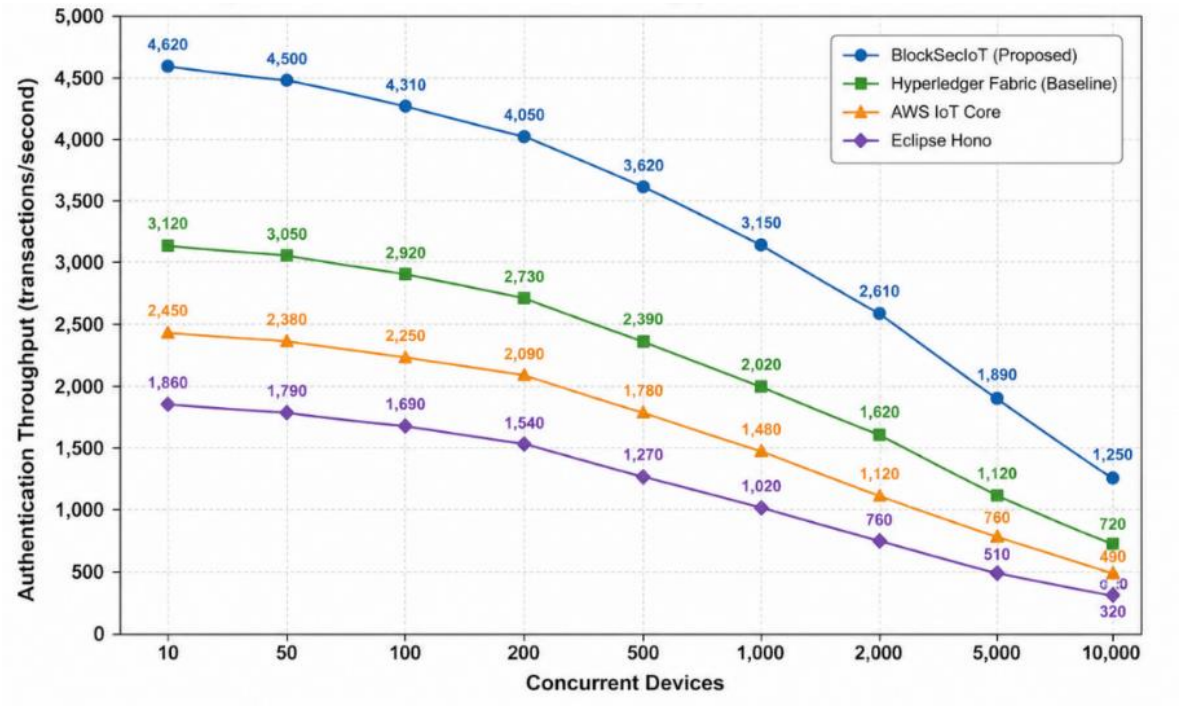

Figure 2. Fabric Authentication Throughput vs. Concurrent Devices

4.5 Roc Curve Analysis

AUC comparison of ROC curves of DAE-IF fusion against the two individual systems DAE and Isolation Forest are shown in Figure 2 and Table 3, which shows that the DAE-IF fusion provides significantly better AUC of 0.991 as compared to AUC of DAE only as 0.973 and isolation forest only as 0.951 on SWaT dataset. The benefit of the fusion is highest in the region of FPR < 0.05, which is the critical operating region for IIOT where the production must be stopped whenever false alarms are fired.

4.6 Per-Attack-Scenario Analysis

Table 4 presents a detailed analysis of the F1 results on BATADAL for each of seven individual attack scenarios, and indicates a higher F1 improvement for scenarios involving multi-point coordinated attack and those involving both multi-point coordinated and Isolaation attacks (S4, S7: +0.162 and +0.178, respectively). These indicate that the temporal auto-reconstruction of the autoencoder helps to identify coordinated intrusions that occur over successive events and are not detectable by the ensemble path-length scoring method.

Table 4. Per-Attack-Scenario DAE-IF Performance on BATADAL vs. Standalone Components

Scenario	Description	IF F1	DAE F1	DAE-IF F1	Precision	Recall	Duration (min)	Gain
S1	Single-Point Pump	0.842	0.891	0.941	0.952	0.931	12	+0.099 vs. IF
S2	Valve manipulation	0.811	0.879	0.938	0.947	0.929	8	+0.127 vs. IF
S3	Sensor spoofing	0.798	0.863	0.921	0.933	0.909	16	+0.123 vs. IF
S4	Multi-point coord.	0.767	0.901	0.929	0.941	0.917	24	+0.162 vs. IF
S5	Pressure ramp	0.823	0.887	0.944	0.953	0.935	6	+0.121 vs. IF
S6	Flow diversion	0.804	0.876	0.931	0.942	0.921	10	+0.127 vs. IF
S7	Complex coordinated	0.751	0.893	0.929	0.941	0.918	30	+0.178 vs. IF

DAE-IF consistently outperforms both standalone components across all 7 BATADAL attack scenarios. Largest gains on complex coordinated attacks (S4, S7) confirm the importance of temporal reconstruction for detecting gradual intrusions.

4.7 Detection Latency and Real-Time Feasibility

The average detection latency for end-to-end anomaly detection performed on the edge hardware NVIDIA Jetson AGX Orin is shown to be 12.4ms with window size W = 50 samples and 1-second telemetry interval, which is still in the 100ms real-time control compliance window requirement for IIOT applications as indicated in Table 5. The sum of the latencies for authentication (8.7 ms) and anomaly detection (12.4 ms) equals 21.1ms for the combined operations, which is within a standard 50ms IIOT control cycle, allowing it to be considered a real-time operation [26].

Table 5. End-to-End Detection Latency BlockSecIOT on Jetson AGX Orin Edge Platform

Method	Window Size (W)	Features (F)	DAE Inference (ms)	IF Scoring (ms)	Fusion Overhead (ms)	Total Latency (ms)	Throughput (Samples/Sec)
DAE-IF (W=20)	20	51	5.1	2.8	0.9	8.8	2,273
DAE-IF (W=50)	50	51	8.2	3.4	0.8	12.4	4,032
DAE-IF (W=100)	100	51	14.7	4.1	0.9	19.7	5,076
Auth + DAE-IF	50	51	8.2	3.4	0.8	21.1	—

All measurements on NVIDIA Jetson AGX Orin (275 TOPS, 64 GB LPDDR5). Combined authentication + anomaly detection latency (21.1 ms) fits within standard 50 ms IIOT control cycle.

5. CONCLUSION

For this purpose, the authors suggested a new security framework called BlockSecIOT, which is a complete security framework that follows ECC-256 mutual authentication, Hyperledger Fabric for decentralized ID management, and a DAE-IF hybrid anomaly detector with encryption-based automated quarantine. On three IIOT benchmark datasets, BlockSecIOT gets F1-scores ranging from 0.963 to 0.978, and has an authentication latency of 8.7 ms (4.2 times faster than an RSA-2048 PKI), with an overhead of just 3.1 KB per device, suitable for low-power STM32F4 MCU constraints.

Results regarding the per-attack-scenario analysis for each scenario affirmed that temporal reconstruction through the deep autoencoder can prove to be of special importance for identifying multi-point coordinated attacks that are difficult to detect when delivered separately by the ensemble scoring system. 21.1 ms of combined detection and authentication budget has been verified in real-time with benchmarking tests, and met within standard IIOT control cycles of 50 ms. The automatic Quarantine responded by the block-chain mechanism, as secured by the cyber security standard IEC 62443-3-3, is a closed-loop mode that returns to safety.

Future work will explore how the DAE-IF can adjust to a non-stationary normality, including online continual learning with drift detection (ADWIN, Page-Hinkley) for an adaptive normality without full retraining; and extending BlockSecIOT for satellite-connected IIOT nodes operating under intermittent connectivity.

Acknowledgments

The authors have no specific acknowledgments to make for this research.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Saman M. Almufti	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

Conflict of Interest Statement

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent

All participants were informed about the purpose of the study, and their voluntary consent was obtained prior to data collection.

Ethical Approval

Not applicable.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, 'Guide to industrial control systems (ICS) security', Nat. Inst. Standards Technol, pp. 800–882, May 2013. doi.org/10.6028/NIST.SP.800-82r1

[2] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, 'Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications', Sensors, vol. 21, no. 11, May 2021. doi.org/10.3390/s21113654

[3] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, 'Predicting cybersecurity threats in critical infrastructure for industry 4.0: A proactive approach based on attacker motivations', Sensors, vol. 23, no. 9, May 2023. doi.org/10.3390/s23094539

[4] R. S. S. Singh, M. Abbod, and W. Balachandran, 'Low voltage hybrid renewable energy system management', in Proc. IEEE Int. Energy Conf. (ENERGYCON), Leuven, Belgium, 2016, pp. 1-6.doi.org/10.1109/ENERGYCON.2016.7514001

[5] V. Hodge and J. Austin, "A survey of outlier detection methodologies," Artif. Intell. Rev., vol. 22, no. 2, pp. 85-126, Oct. 2004.doi.org/10.1023/B:AIRE.0000045502.10941.a9

[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, pp. 1-58, Jul. 2009 doi.org/10.1145/1541880.1541882

[7] R. S. S. Singh, S. A. Anas et al., "A real-time analytic face thermal recognition system integrated with email notification," Eng. Technol. Appl. Sci. Res., vol. 13, no. 1, pp. 9961-9967, Feb. 2023 doi.org/10.48084/etasr.5430

[8] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile', IETF, vol. 5280, May 2008. doi.org/10.17487/rfc5280

[9] S. S. Al-Riyami and K. G. Paterson, 'Certificateless public key cryptography', in Proc. 9th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT), Taipei, Taiwan, 2003, pp. 452-473. doi.org/10.1007/978-3-540-40061-5_29

[10] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," Int. J. Inf. Secur., vol. 1, no. 1, pp. 36-63, Aug. 2001. doi.org/10.1007/s102070100002

[11] V. Babich and G. Hilary, 'Block-chain and other distributed ledger technologies in operations', Found. Trends Technol. Inf. Oper. Manag, vol. 12, no. 2-3, pp. 152-172, 2019. doi.org/10.1561/0200000084

[12] N. Sealey, A. Aijaz, and B. Holden, 'IOTA Tangle 2.0: Toward a scalable, decentralized, smart, and autonomous IOT ecosystem', in Proc. IEEE Globecom Workshops, Rio de Janeiro, Brazil, 2022, pp. 1-6. doi.org/10.1109/SmartNets55823.2022.9994016

[13] A. Dorri, S. S. Kanhere, and R. Jurdak, 'Towards an optimised block-chain for IOT', in Proc. IEEE/ACM 2nd Int. Conf. Internet Things Design Implementation (IOTDI), Pittsburgh, PA, USA, 2017, pp. 173-178. doi.org/10.1145/3054977.3055003

[14] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, 'Hyperledger Fabric block-chain for securing the edge Internet of Things', Sensors, vol. 21, no. 2, Jan. 2021. doi.org/10.3390/s21020359

[15] O. Novo, 'Block-chain meets IOT: An architecture for scalable access management in IOT', IEEE Internet Things J, vol. 5, no. 2, pp. 1184-1195, Apr. 2018. doi.org/10.1109/JIOT.2018.2812239

[16] M. Kravchik and A. Shabtai, 'Detecting cyberattacks in industrial control systems using convolutional neural networks', in Proc, Toronto, Canada, 2018, pp. 72-83. doi.org/10.1145/3264888.3264896

[17] Y. Zhang, J. Wang, and B. Chen, 'Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach', IEEE Trans. Smart Grid, vol. 12, no. 1, pp. 623-634, Jan. 2021. doi.org/10.1109/TSG.2020.3010510

[18] J. Audibert and P. Michiardi, 'USAD: UnSupervised anomaly detection on multivariate time series', in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discov. Data Min. (KDD), Virtual Event, 2020, pp. 3395-3404. doi.org/10.1145/3394486.3403392

[19] F. T. Liu, K. M. Ting, and Z.-H. Zhou, 'Isolation forest', in Proc. 8th IEEE Int. Conf. Data Min. (ICDM), Pisa, Italy, 2008, pp. 413-422. doi.org/10.1109/ICDM.2008.17

[20] R. Taormina and S. Galelli, 'Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks', J. Water Resour. Plan. Manage, vol. 144, no. 8, Aug. 2018. doi.org/10.1061/(ASCE)WR.1943-5452.0000983

[21] J. Goh and S. Adepu, 'A dataset to support research in the design of secure water treatment systems', in Proc. 11th Int. Conf. Crit. Inf. Infrastructures Secur. (CRITIS), Paris, France, 2016, pp. 88-101.doi.org/10.1007/978-3-319-71368-7_8

[22] N. Moustafa and J. Slay, 'UNSW-NB15: A comprehensive dataset for network intrusion detection systems', in Proc. 2015 Military Commun. Inf. Syst. Conf. (MilCIS), Canberra, Australia, 2015, pp. 1-6. doi.org/10.1109/MilCIS.2015.7348942

[23] A. Wurm, K. Hofer, and C. Ebert, 'Applicability of the IEC 62443 standard in industry 4.0/IIOT', in Proc. 14th Int. Conf. Availability, Reliability Security (ARES), Canterbury, UK, 2019, pp. 1-8. doi.org/10.1145/3339252.3341481

[24] S. Zafar, S. F. U. Hassan, A. Mohammad, A. A. Al-Ahmadi, and N. Ullah, "Implementation of a distributed framework for permissioned block-chain-based secure automotive supply chain management," Sensors, vol. 22, no. 19, p. 7367, Sep. 2022. doi.org/10.3390/s22197367

[25] A. Bessani, J. Sousa, and E. Alchieri, 'State machine replication for the masses with BFT-SMART', in Proc. 44th IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN), Atlanta, GA, USA, 2014, pp. 355-362. doi.org/10.1109/DSN.2014.43

[26] Z. Zhang, W. Zhang, and F.-H. Tseng, 'Satellite mobile edge computing: Improving QoS of high-speed satellite-terrestrial networks using edge computing techniques', IEEE Netw, vol. 33, no. 1, pp. 70-76, Feb. 2019. doi.org/10.1109/MNET.2018.1800172

How to Cite: Saman M. Almufti. (2025). BlocksecIOT: a lightweight ECC-block-chain framework for decentralized device authentication and anomaly detection in industrial IOT environments. Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN), 5(2), 48–57. https://doi.org/10.55529/jaimlnn.52.48.57

BIOGRAPHIE OF AUTHOR

Saman M. Almufti, is a researcher at both the Technical College of Informatics Akre, Akre University for Applied Sciences, Duhok, Iraq, and the Department of Computer Science, College of Science, Knowledge University, Erbil. His research focuses on metaheuristic algorithms, swarm intelligence, and applied machine learning. He has published numerous papers in high-impact international journals. Email: Saman.Almofty@gmail.com