Author(s): Frantti, Tapio; Şafak, Ilgın

Title: An Architecture for Enabling Collective Intelligence in IoT Networks

Year: 2023

Version: Accepted version (Final draft)

Please cite the original version:

Frantti, T., & Şafak, I. (2023). An Architecture for Enabling Collective Intelligence in IoT Networks. In N. T. Nguyen, J. Botzheim, L. Gulyás, M. Núñez, J. Treur, G. Vossen, & A. Kozierkiewicz (Eds.), Computational Collective Intelligence : 15th International Conference, ICCCI 2023, Budapest, Hungary, September 27–29, 2023, Proceedings (pp. 29-42). Springer. Lecture Notes in Computer Science, 14162. https://doi.org/10.1007/978-3-031-41456-5_3

An Architecture for Enabling Collective Intelligence in IoT Networks*

Tapio Frantti[1*] and Ilgın Şafak[2]

[1] University of Jyäskylä, Jyväskylä, Finland
tapio.k.frantti@jyu.fi
[2] Fibabanka R&D Center, Istanbul, Turkey
ilgin.safak@fibabanka.com.tr

Abstract. Proliferation of the Internet of Things (IoT) has fundamentally changed how different application environments are being used. IoT networks are prone to malicious attacks similar to other networks. Additionally, physical tampering, injection and capturing of the nodes are more probable in IoT networks. Therefore, conventional security practices require substantial re-engineering for IoT networks. Here we present an architecture that enables collective intelligence for IoT networks via smart network nodes and blockchain technology. In this architecture, various security related functionalities are distributed to network nodes to detect tampered, captured and injected devices, recognize their movements and prevent networks' use as an attack surface. Nodes interact with signaling, security information and data traffic. Security information aids to distribute cyber-security functionalities across the IoT network based on the device and/or application type. Every node in the proposed IoT network does not need to have all the cyber-security functionalities, but the network as a whole needs these functionalities.

Keywords: Distributed IoT networks · architecture · blockchain · AI · network security.

1 Introduction

The Internet of Things (IoT) is one of the most important technologies of the last decades enabling data collection, data exchange, communication and control actions between people, processes, and things. We can connect to the Internet and control industrial and everyday objects. According to forecasts, the use of IoT devices will continue to increase with time. For example, Cisco estimates 500 billion devices to be connected to the Internet by 2030, [4]. IoT Analytics counts the number of IoT devices to exceed 30.9 billion units in year 2025, [11]. Statista forecasts that end-user spending on IoT solutions worldwide in 2025 will be 1567 billion US$ [15]. However, the number of security threats targeting IoT devices and the occurrence of cyber security incidents have also increased. The susceptibility to cyber threats is a serious concern for IoT networks and

* Corresponding author.

overlaid complex systems and forces the IoT actors to take countermeasures against hostile cyber actions and attacks. Adversaries may penetrate networks, disrupt or defeat the system defense using exploits available on the Internet, hang on systems for a long time, and utilize data available on the systems. Therefore, the growth of IoT usage will increase the need of new cyber security solutions.

Artificial intelligence (AI) could be used in enabling IoT networks and devices to become smarter and ensure the IoT network's security autonomously. AI-based IoT applications with continuous machine learning (ML) algorithm are capable of continually learning, interacting, and enhancing real-time cognition capabilities of devices.

IoT edge networks do not yet formalize and exploit collective intelligence (CI). CI encompasses task and information distribution, computational load balancing, code offloading, as well as instructing how and where to run CI. However, there are also several significant challenges that must be addressed in CI. These include the quality of data, the distribution of the computational workload and functionalities, mathematical models of the CI, and the scalability and portability of the solution.

Another critical cyber-security concern is related to the deployment of large-scale IoT systems. The centralized architecture of existing IoT systems have weaknesses such as single point of failure, high-cost of transmission and computation, and data loss. Additionally, due to the massive number of devices that can belong to several users, the IoT systems need to ensure data ownership, so that they can exercise complete control over the shared data. The coexistence and collaboration of different technologies and the open standards and protocols employed by the IoT may pose additional security risks. Despite the heterogeneity and inherent computational power constraints of the IoT devices and large scale of the IoT network, there is an increasing interest in autonomic computing for device management, where each device is allowed to make significant decisions without the consent of others. In this case, sensors and devices need to communicate with each other in a distributed way. This in turn leads to many design challenges including limited scalability and high latency. These challenges can be addressed by a secure and supervised distributed architecture where the security platform intelligently divides processing load among the nodes of the network. For this purpose, distributed ledger technology (DLT), such as blockchain, may be utilized. According to [8] blockchain provides advantages including decentralization, transparency, immutability, enhanced security, anonymity, cost reduction and autonomy. DLT transactions are validated using trust-free consensus algorithms that allow every node to participate in the consensus, which increases the robustness and reliability of transactions compared to absolute consensus methods used in centralized methods. Usage of DLT in IoT networks eliminates the need of a single trusted authority, thereby enhancing the potential for scalability and reliability.

Here we present a distributed IoT security architecture, SENTIENCE[3], that enables collective intelligence for IoT networks. The problem statement may be

[3] EPO patent number EP23155296.9 pending.

formulated as *Can we and how do we embed satisfactory security controls for computationally restricted heterogeneous network nodes to enable reliable, secure and resilient platforms for rich ecosystems by applying computational intelligence?*. The main contributions of the paper are as follows.

- A private-by-design and scalable blockchain-based collective intelligence system with distributed blacklisting and trust scoring protocol.
- An AI-based signaling protocol that enables collective intelligence.
- A security analysis of the presented architecture.

The organization of the rest of the paper is as follows. Section 2 presents an overview of AI-based distributed IoT security solutions available in the literature. Section 3 presents the proposed system architecture, blacklisting and signaling protocol. Section IV provides a discussion on advantages and disadvantages of the presented solutions. Section V presents the conclusions of the paper.

2 Literature review

Mohamudally [12] provides a comparative study of mathematical models for CI and a discussion of their suitability for implementation on mobile devices. Additionally, a framework for modeling CI systems using graph theory and artificial neural networks is proposed. Radanliev et al. [14] proposes a dynamic and self-adaptive cyber risk analytics system using AI/ML as well as real-time intelligence. The usage of edge computing nodes and AI/ML technology migrated to the periphery of the Internet, along with local IoT networks, enables a comprehensive and systematic understanding of the opportunities and threats. Joseph et al. [6] proposed a self-organizing IoT system architecture that relies on blockchain and its related features in order to achieve aspects of end-to-end IoT security.

Konstantinos et a. [9] propose a design method and cognitive platform that incorporate various technologies including Public Key Infrastructure (PKI), blockchain, and AI to support a unified and integrated approach towards data privacy, security and safety of Industrial IoT systems. The proposed system analyzes the IoT topology and signal metadata in relation to the relevant safety profiles. The aim is to exploit the cyber-physical representation of the system-of-systems in conjunction with security and safety policies to provide real-time risk mapping for static analysis and continuous monitoring to assess safety issues and take appropriate response actions.

An et al. [1] proposes a novel blockchain based anomaly detection architecture and method for IoT networks to overcome the problems of data resource sharing and collective learning in IoT. IoT devices with abnormal HTTP traffic are detected efficiently and accurately using the proposed clustering and autoencoder methods. This architecture allows detection models to be shared among users, effectively solving the problem of collective learning. Multiple joint detection methods can also be effective in improving the ability to detect anomalies.

Li et al. [10] examines network architectures that may be utilized in future 6G networks to support intelligent IoT. Furthermore, in order to facilitate the sharing of learning and training results in the intelligent IoT, the authors introduce and adopt a novel method called collective reinforcement learning (CRL) that is inspired by the collective learning of humans. Blockchain, mobile edge computing and cloud computing are applied to enhance data security and computing efficiency.

An et al. [1] provide a mechanism for sharing detection models and Li et al. [10] sharing training models. None of the aforementioned works study study collective intelligence by AI signaling, distributed blacklisting via anomaly detection and blockchain network, the mitigation of security threats, or the disaster recovery, which are addressed in this paper.

3 An Architecture for Collective Intelligence

3.1 System Architecture

Here we propose a secure, blockchain-based architecture for enabling collective intelligence in zero-trust IoT networks. In the proposed system, resource constrained nodes combine jointly cyber-security information and defend against cyber threats. Intelligent security related computing, detection, and prevention algorithms are distributed to network nodes. Nodes interact with signaling, AI and data traffic (see Fig. 1).

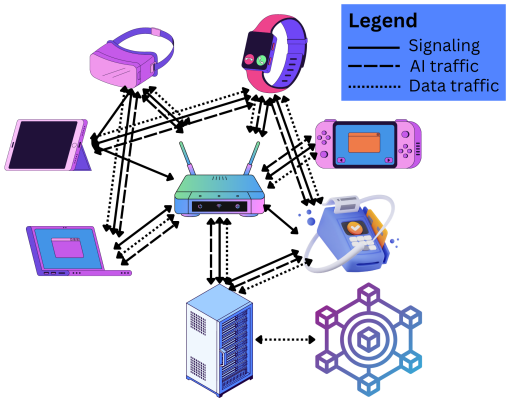

Fig. 1. Network nodes with signaling, data and AI traffic.

Data traffic refers to the actual payload, such as sensor readings, being transmitted over the network. Signaling refers to the exchange of control information between network elements to establish, maintain, or modify communication. AI traffic consists of information analyzed from received traffic and information

from security algorithms. Analysis of the traffic is performed in the cloud servers, routers and IoT nodes. Solid lines in Fig. 1 describe signaling traffic. Signaling traffic of the external connections is not shown. Dashed and dotted lines describe AI and data traffic, respectively.

The usage of IoT and blockchain with AI enable collective intelligence and allow real-time decision making. This facilitates the identification and mitigation of cyber-security threats, reduction of system failures, optimization of data flow, and provides re-routing options for disaster recovery. This is achieved with the *IoT device registration to the network, collection of data from devices, detection of threats from the data anomalies, security incident publication to blockchain,* and *collective actions on detected threats*. Collective action on detected security threats includes, *e.g.*, blacklisting and removing malicious IoT devices from the network, applying load balancing rules to divide computation, retrieving back-up data and re-routing the data flow.

The main components of the system architecture include IoT clients, communication and blockchain network, distributed monitoring, threat detection / prevention, blockchain, CI, zero-trust, load balancing and recovery systems. The system architecture is designed in according to the Zero-Trust Architecture (ZTA) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. ZTA requires users of the network to be authenticated, authorized, and validated before being granted access to applications and data. Here this is achieved by *identity and access management*, *network segmentation*, *least priviledge principle*, *microsegmentation*, *continuous monitoring and analytics*, *endpoint security*, *data encryption*, *zero-trust access*, *device behavior analytics*, and *incident response*. The NIST Cybersecurity Framework was used to assist risk identification, secure delivery of services, and detection of and response to incidents.

The layers of the system architecture with the main functionality of the each layer is depicted in Fig. 2. Security algorithms and computational load are distributed between AI-blockchain nodes, routers and IoT clients to decentralize the computational load. Distribution is guided by time, computational capability and energy principles. Traffic monitoring and detection is distributed to different network nodes by time and energy division based scheduling. Nodes receive alarm information by the AI traffic.

3.2 AI Information Signaling and AI Layer

In the SENTIENCE architecture, intelligent security related functionalities are distributed to different network nodes, where each node has one or more cyber-security functionalities. The aim is to avoid each node requiring to have unnecessarily all the functionalities, but the network as a whole has the functionalities. The network awareness, collective intelligence, is distributed among the nodes. The AI layer handles AI messages between IoT devices and the cloud. It defines how AI messages are sent and received by nodes, as well as the cyber-security functionalities each device possesses, where these functionalities and the device status are kept track of in the cloud.

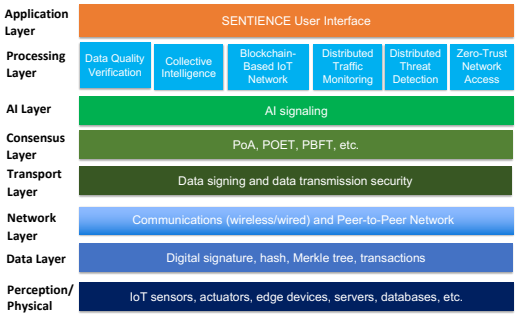

Fig. 2. Layered architecture.

AI plays a critical role in improving the security and reliability of IoT networks through the data analysis. This allows IoT networks to proactively identify and respond to abnormal behavior or potential security threats. In order to detect anomalies and assign trust scores to devices, AI algorithms can learn from historical data, adapt to changing conditions, and continuously enhance their accuracy with time.

AI messages include device fingerprint, battery level, feedback about interactions with other network nodes, average processor load, tampering information, misuse and anomaly detection information, port scanning information, traffic latency, nodes responsiveness, smart contract information, network configuration information, location data, error logs, and optional fields for forthcoming use.

A device fingerprint may include device specific information such as device type, supported security and communications protocols, and MAC address. It is required for AI level topological device grouping and work load distribution. Battery level and processor(s) load are needed for work load distribution. Tampering information note if the node is on the target of side channel attack, tampering or movement. Nodes detect intrusions by misuse and anomaly detection techniques and they report all the security events in AI messages. IoT nodes have also built-in feature to do port scanning and they report all the unnecessary open ports. Latency and nodes responsiveness are included to the traffic information fields of the AI message. AI signaling messages are also used for smart contract information delivery and configuration of information delivery. There are also reserved fields for the forthcoming use.

AI messages are used in securing the IoT network by updating network access rules, keeping the disaster recovery configuration up-to-date, detecting and mitigating security attacks in real-time, sharing feedback about other nodes in the network, and re-routing network traffic for disaster recovery. AI messages are encrypted and hashed.

3.3 A Scalable, Private by Design Blockchain Architecture

Blockchain is an attractive option for the decentralized secure architecture. Its' transactions are validated by trust-free consensus algorithms that allow every node to participate in the consensus, which increases the robustness and reliability of transactions as well as scalability and reliability compared to absolute consensus methods.

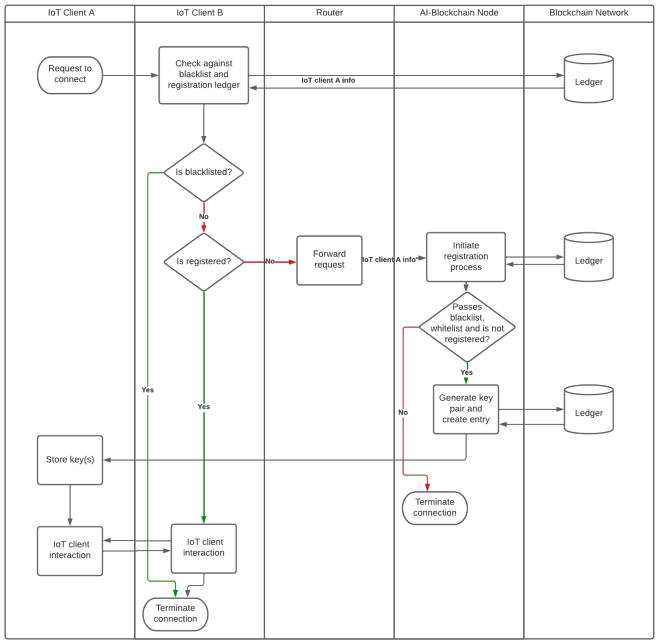

Fig. 3. Sequence chart of AI traffic for an injected IoT client.

The two most popular consensus algorithms, Proof of Work (PoW) and Proof of Stake (PoS), are computationally intensive and not suitable for IoT scenarios. Therefore, lightweight consensus algorithms are required for IoT–blockchain integration. A simple voting mechanism, *e.g.*, Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), or Proof of Elapsed Time (PoET) could be used as the consensus algorithm for the block validation and transactions creation, where public-key cryptography is used as an encryption mechanism. The Lightning Network, a "layer 2" payment protocol designed to be layered on top of a blockchain-based cryptocurrency, such as bitcoin, could also be utilized to meet resource and power constraints of IoT networks, [13]. It has several desirable properties by design and was conceived to enable scalability and high transaction rates.

The SENTIENCE utilizes the private-by-design blockchain architecture based on [7] that ensures the intelligent supervision of all the necessary events in the consensus protocol distributed across the IoT network. This traceability is necessary to guarantee reliability and robustness of the system. Smart contracts are used in enabling and automating interactions between the system and the IoT devices. A separate virtual database is used for logging interactions between IoT devices and the blockchain.

The consensus mechanism classifies the IoT device transactions as public and private. Public transactions are visible to every node in the IoT network, whereas private transactions are accessible only to the nodes that are a part of the transactions. Nodes in the private blockchain network are pre-authenticated using the security protocol described in 3.5 prior to joining the network. Therefore, maintaining consensus does not require complex proof to be carried out. A simple voting mechanism is used as the consensus algorithm for the block validation and creation for both public and private transactions. Network traffic and device data that could be used by malicious actors for exploiting weaknesses of the network, like trust scores of IoT nodes, are stored privately in a private database in the AI-blockchain nodes, whereas the list of blacklisted devices is kept publicly on the public blockchain database. By applying this approach, strict controls are enforced and lateral movement within the network is limited, thus reducing the impact of a potential security breach.

The Transaction Manager is a key module mainly responsible for storing and allowing access to encrypted transaction data. Every AI-blockchain node, whether sender or receiver, has its own transaction manager. It performs anomaly detection and acts as a gateway to distribute private information to other nodes in the network that will encrypt private transactions and handle IoT transactions. The encryption and decryption module will encrypt and decrypt the payload by generating the asymmetric keys and returning them to Transaction Manager. To process the public and private transactions by the AI-blockchain nodes, working layers of blockchain are modified so that for private transactions only the allowed authorized node takes part in communication. Similarly, block validation and block generation logic are modified so that instead of using global root check, it uses global public state root in the blockchain header. For private transaction block validation and creation, logic is altered to handle private transactions. However, still each node is able to demonstrate that it has the same set of transactions as other nodes, since the block validation process also includes a check of the global transaction hash, namely, the hash of all transactions in a block, both public and private ones.

For scalability purposes, a sharding mechanism, such as the one proposed in [3], could be utilized. Blockchain sharding refers to the division of the entire blockchain network into several smaller sub-networks, known as shards. Each shard contains data that is unique to it, as well as being independent of other shards on the network. Each sub-network has its own consensus process for creating blocks. Due to the multiple shards in the network, blocks are generated faster than they would be in a network without shards. The number of shards can

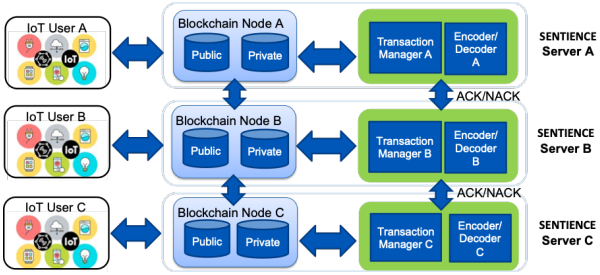

Fig. 4. A private-by-design blockchain architecture based on [7]

be increased as demand for the application grows, thereby allowing the system to allocate resources dynamically.

3.4 Zero Trust, Blacklisting, Trust Scoring and Anomaly Detection

Once an IoT client is registered in the IoT network, it can communicate with other IoT clients. Based on our previous work in [16] and [2], malicious IoT clients are blacklisted in a distributed way by AI-blockchain nodes via the blockchain-based IoT network security system using anomaly detection techniques and the blockchain network.

Fig. 3 describes a case when a malicious client is injected to the IoT network. The malicious client (client A) requests to connect to a registered neighboring IoT client (client B). The client B checks whether the malicious IoT client is blacklisted or registered to the IoT network against the ledger via the blockchain network. If the client A is blacklisted, client B terminates the connection. If the client A is already registered, client B connects and interacts with it. If the client A is not blacklisted and is not registered to the IoT network, client B forwards the request to the AI-blockchain node via the router. After receiving the registration request from the registered client B, the AI-blockchain node initiates the registration process of client A. Firstly it performs a blacklist and registration check. If the client A is not blacklisted and is not registered, it then performs a whitelist check. If the client A passes the device whitelist check, it adds the client A to the IoT network by assigning a public key pair and creating an entry in the ledger. The AI-blockchain node shares the key pair with client A and completes the registration process. After registration is completed, the malicious IoT client can access the IoT network.

All network traffic is continuously monitored by AI-blockchain nodes. If any AI-blockchain node detects an anomalous behavior of the malicious IoT node, it publishes its finding on the ledger via the blockchain network. If and when AI-blockchain nodes have consensus on the anomalous behavior, then the malicious IoT client is added to the blacklist via the blockchain network. Similarly, AI-blockchain nodes may detect an IoT client to be offline, *e.g.*, due to a physical attack or battery depletion. If this client is not detected for a predefined period,

then it is added to a list of compromised clients. Therefore, it is required that clients inform the AI-blockchain server about their presence in the network.

A malicious client may stay silent without advertising itself and eavesdrops communication. Therefore, the data traffic is encrypted for confidentiality reasons and to prevent eavesdropping and man in the middle (MitM) attacks. Additionally, in order to prevent registered malicious IoT clients from adding new malicious IoT clients, the AI-blockchain node also performs regular blacklist and registration checks. Power deprivation attacks are also possible by increased radio interference. The malicious client may also attempt to detect the topology of the networks by listening to the signaling traffic. The network depicted in Fig. 1 is assumed to consists of the trusted clients. The network itself can be analyzed using a trust metric to rate individual clients as well as AI-blockchain nodes.

3.5 Threat Detection

The SENTIENCE architecture provides distributed threat and incident detection solution for misuses, malware and anomalies. In traditional host-based anomaly detection systems, a system call sequence is analyzed in order to model normal behavior of an application. Using the model, the current sequence is examined for anomalous behavior, which may indicate an attack. However, it is shown that sequence-based systems are susceptible to evasion. As a mitigation method, multiple anomaly detection methods, including host-based event anomaly detection, signature-based anomaly detection, and network traffic-based anomaly detection could be jointly used.

4 Security Analysis of the SENTIENCE Architecture

Blockchain threat models relevant to IoT network security can be categorized as identity-based, manipulation-based, cryptanalytic, reputation-based and service-based attacks [5]. The SENTIENCE architecture is potentially resilient to all attack types based on the security analysis provided in Table 1. The channel model is depicted in Fig. 5.

5 Discussion about SENTIENCE Architecture

The presented architecture enables a cyber-secure IoT ecosystem. The intelligent IoT network nodes collectively detect malicious IoT devices, monitor traffic, detect and prevent threats, secure transactions, protect data and deliver awareness information among the nodes. The system also prevents its' use as an attack surface and performs disaster recovery.

The architecture has the several advantages. It *enhances security* with strong access control and real-time identification of malicious or suspicious activities. Its' blacklisting decisions are *fair, transparent and reliable. The immutability*

Table 1. Security analysis of the SENTIENCE architecture

Threat	Description	Guarantee	Proof	Assumptions
Identity	Forged identities masquerading as authorized users to gain access to the system and manipulate it. Includes key, replay, Sybil and impersonation attacks.	1. Immutable device identity. 2. Secure identity verification. 3. Strong access controls. 4. Resilience against Sybil attacks.	1. A PUF session key: authentication and non-repudiation. 2. Device's public key is linked to its identity. 3. Access control through the ZTNA, blacklisting, cryptography, and PUF keys. 4. Only authorized participants can reach consensus.	1. Each device is assigned a cryptographic identity (public-private key pair). 2. A PUF session key cannot be cloned. 3. ZTNA system assigns appropriate access levels. 4. The blockchain network withstands Sybil attacks.
Manipulation	False-Data Injection, Tampering, Overlay, Modification, and MitM attacks.	1. Immutable identity. 2. Identity verification. 3. Strong access controls. 4. Immutable transaction history	Proofs of guarantees 1-3 are the same as above. 4. A block cannot be modified after being added to the blockchain.	Assumptions of guarantees 1-3 are the same as above. 4. IoT data transmitted and stored on the blockchain is cryptographically secured and cannot be tampered with.
Cryptanalytic	Uncover the private key. Includes Side-Channel and Quantum attacks.	1. Secure Cryptographic Algorithms 2. Key management 3. Randomness generation 4. Side-channel mitigation	1. Strong cryptographic algorithms. 2. Robust key management. 3. Cryptographically secure random number generators. 4. PUF key to prevent key theft.	1. Cryptographic algorithms are secure. 2. Robust key management. 3. The RNGs are cryptographically secure. 4. Copying the session key generation function is not possible.
Reputation	Agents manipulate their reputations. Includes Hiding Block and Whitewashing attacks.	1.Robust Reputation Scoring 2. Transparent Trust Evaluation	1. Nodes with high trust scores have more impact on decisions. 2. Only authorized users access the trust scores. 3. Blacklisting decisions are on the blockchain.	1. Trust scoring is performed for all nodes. 2. The blacklist and the trust scores is stored on the public and the private blockchain database.
Service attacks	The purpose is either to disable or to alter the service. DoS/DDoS, Refusal to Sign, Double Spending, and Collusion attacks.	1. DDoS Mitigation 2. Scalability and Load Balancing 3. Resource Monitoring and Management 4. Secure Communication Channels 5. Intrusion Detection and Prevention	1. Traffic monitoring and analysis for DDoS mitigation. 2. Sharding for scaling the blockchain. Load balancing for high traffic loads. 3. Detection of resource exhaustion and abnormal usage by anomaly detection. 4. Data protection by encryption. 5. Traffic monitoring to detect malicious activity.	1. Services to mitigate DDoS attacks. 2. Traffic loads are handled by scalability. 3. Prevention of disruptions through proactive resource management. 4. Encryption, handshake protocol, ZTNA and key management protects the communication channels. 5. IDS/IPS monitor traffic, logs, and behavior.

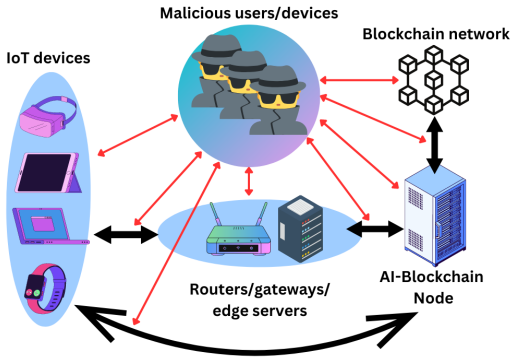

Fig. 5. Channel model

and tamper-resistance of transactions and device identities are ensured by leveraging blockchain technology and device fingerprinting based on Physical Unclonable Functions (PUFs). The use of consensus algorithms, such as PoA and PoET strengthens the network's *resilience to Sybil attacks*. Network node provides feedback about other nodes in the network by monitoring and evaluating *QoS* metrics, such as latency, throughput, reliability, and availability.

The architecture also has some challenges. Despite the distributed load, increased activities of the IoT nodes increase *energy consumption*. As a mitigation technique, energy harvesting may be an option. Collective decision making, consensus protocols and inter-device communications, particularly with the blockchain network, introduces *latency*. Blockchain-based systems have also higher *computational costs* due to consensus and cryptographic operations. As traditional systems do not involve distributed consensus, their computational cost is generally lower. Lightweight consensus algorithms, such as PoA and POET, and sharding can be used to reduce the complexity. *Security and privacy* issues may arise as a result of increased interaction of IoT devices in the blockchain. This could be mitigated by developing new standards for blockchain-based IoT communications and security protocols. Blockchain-based systems may incur a higher *storage cost*. Nodes participating in the blockchain network maintain a copy of the entire blockchain, resulting in data redundancy. The *governance and administration* of SENTIENCE, including distribution of cyber-security functionalities across the network, trust scoring and blacklisting decisions, require careful management.Therefore, it is essential to establish governance policies, dispute resolution mechanisms, as well as ensuring transparency and accountability.

6 Conclusions

This paper presents an architecture to enable collective intelligence in distributed IoT networks. The architecture is based on the zero-trust and NCSF guide-

lines. In the presented solution, various intelligent security functionalities are distributed amongst nodes, where each node has one or more cyber-security functionalities. Nodes interact not only with signaling and data traffic but also with the AI traffic, to transfer security information in the network.

The architecture introduces networking and processing overheads for inter-device communications and collective decision making with AI signaling and the blockchain network. Challenges may arise from managing and optimizing the distribution of tasks amongst nodes and minimizing power consumption and latency.

Future work includes the creation of performance and accuracy metrics for the architecture and the validation of the architecture, as well as contributing to the standardization of blockchain-based IoT communications and improved security protocols that are suitable for IoT devices.

References

[1] Yufei An et al. "An HTTP Anomaly Detection Architecture Based on the Internet of Intelligence". In: *IEEE Transactions on Cognitive Communications and Networking* (2022), pp. 1–1.

[2] C. A. Baykara, I. Şafak, and K. Kalkan. "SHAPEIOT: Secure Handshake Protocol For Autonomous IoT Device Discovery and Blacklistıng Using Physical Unclonable Functions and Machine Learning". In: *13th International Conference on Network and Communications Security (NCS 2021)*. Toronto, Canada, 2021.

[3] Yang-Wai Chow et al. "Visualization and Cybersecurity in the Metaverse: A Survey". In: *Journal of Imaging* 9.1 (2023). ISSN: 2313-433X.

[4] Cisco. *Cisco IoT Solutions*. `https://cisco.com/c/en/us/solutions/internet-of-things/overview.html`. Accessed: 2022-09-07.

[5] Mohamed Amine Ferrag et al. "Blockchain Technologies for the Internet of Things: Research Issues and Challenges". In: *IEEE Internet of Things Journal* 6.2 (2019), pp. 2188–2204. DOI: `10.1109/JIOT.2018.2882794`.

[6] Ajayi Oluwashina Joseph et al. "Securing Self-organizing IoT Ecosystem: A Distributed Ledger Technology Approach". In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. 2019, pp. 809–814. DOI: `10.1109/WF-IoT.2019.8767182`.

[7] Muhammad Kashif and Kubra Kalkan. "BCPriPIoT: BlockChain Utilized Privacy-Preservation Mechanism for IoT Devices". In: *2021 Third International Conference on Blockchain Computing and Applications (BCCA)*. 2021, pp. 201–209. DOI: `10.1109/BCCA53669.2021.9657016`.

[8] Minhaj Ahmad Khan and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges". In: *Future Generation Computer Systems* 82 (2018), pp. 395–411.

[9] Loupos Konstantinos et al. "Cognition Enabled IoT Platform for Industrial IoT Safety, Security and Privacy — The CHARIOT Project". In: *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. Sept. 2019, pp. 1–4.

[10] Meng Li et al. "Intelligent Resource Optimization for Blockchain-Enabled IoT in 6G via Collective Reinforcement Learning". In: *IEEE Network* (2022), pp. 1–19.

[11] Knud Lueth. *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. {https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/}. Accessed: 2022-09-07.

[12] Nawaz Mohamudally. "Paving the Way Towards Collective Intelligence at the IoT Edge". In: *Procedia Computer Science* 203 (2022). 17th International Conference on Future Networks and Communications / 19th International Conference on Mobile Systems and Pervasive Computing / 12th International Conference on Sustainable Energy Information Technology (FNC/MobiSPC/SEIT 2022), August 9-11, 2022, Niagara Falls, Ontario, Canada, pp. 8–15. ISSN: 1877-0509.

[13] Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network*. Tech. rep. Lightning Network, Jan. 2010.

[14] P. Radanliev et al. "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains". In: *Cybersecurity, Springer Nature* 3 (13 2020).

[15] Statista. *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. {https://www.statista.com/statistics/976313/global-iot-market\\-size/}. Accessed: 2022-09-07.

[16] O. Tarlan, I. Şafak, and K. Kalkan. "DiBLIoT: A Distributed Blacklisting Protocol for IoT Device Classification Using the Hashgraph Consensus Algorithm". In: *The 36th International Conference on Information Networking (ICOIN) 2022*. Jeju Island, Korea, 2022.