DLT-Based Approach for Secure and Cyber Resilient Resource Constrained IoT Devices: A Survey on Recent Advances

Sthembile Mthethwa[1][a], Moses Dlamini[2][b] and Edgar Jembere[1][c]

[1]*School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Durban, Westville, South Africa*

[2]*Defence and Security, Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa*

Keywords: Resource Constrained, IoT Devices, DLTs, Security, Cyber Resilient.

Abstract: Distributed Ledger Technologies (DLTs) are advancing various fields such as the financial sector, supply chain management, Internet of Things (IoTs), etc. Through its characteristics, DLTs have the potential to solve some of the challenges encountered by IoT devices as the number of connected devices continues to grow tremendously. These characteristics includes but not limited to decentralisation, traceability, security, transparency, immutability, non-repudiation, etc. There has been an increase in the body of knowledge in relation to the convergence of DLTs and IoTs. This paper examines how DLTs can enhance the security of resource-constrained IoT devices, which have limitations that prevent the implementation of traditional security measures like encryption due to size and computational power. This paper consolidates existing research by comparing techniques, technologies used, and results achieved over the years. Finally, the research identifies knowledge gaps for future exploration.

1 INTRODUCTION

The Internet of Things (IoT) is a rapidly growing technology, with the capability of revolutionising a wide range of industries such as agriculture, health care, oil and gas, utilities, etc. This technology development is centered around Operational Technology (OT) and other cyber-physical digital devices such as Internet-enabled sensors that can now interact and exchange data with other sensors, computational services, end users, and digital objects. Therefore, the continual increase in the usage and connection of OT Internet-enabled sensors or devices to the world-wide Internet, demands for more robust cybersecurity controls to protect these devices and the data they collect or transmit.

Typically, OT Internet-enabled sensors or devices have limited resources to compute, process and store data (Jin et al., 2022). For example, limited processing power essentially impacts the sensors' ability to provide immediate or real-time responses on complex computations. Low memory limits data storage, negatively impacts managing firmware updates, and implementing computationally intensive cybersecurity protocols like encryption, authentication etc. These devices are very conservative with regards to energy consumption. This is because they are often reliant on batteries or low-power sources. Therefore, frequent data transmissions, computationally intensive processing tasks, and maintaining operational longevity presents a huge challenge. Though there are workarounds for certain issues like encryption; whereby lightweight encryption may be adopted, this challenge persists with other devices (Jin et al., 2022). Therefore, OT Internet-enabled devices running without computationally intensive cybersecurity controls are usually more susceptible to cyber-attacks than other endpoint devices with more computing power.

The integration of emerging technologies, such as Distributed Ledger Technologies (DLTs), quantum computing, Artificial Intelligence (AI) and Machine Learning (ML) to IoT, has the potential (when integrated correctly) to enhance the security of OT Internet-enabled sensors or devices. Presently, cloud-based information systems have become the norm for

[a] https://orcid.org/0000-0001-7961-5240
[b] https://orcid.org/0000-0001-8109-2979
[c] https://orcid.org/0000-0003-1776-1925

Mthethwa, S., Dlamini, M. and Jembere, E.
DLT-Based Approach for Secure and Cyber Resilient Resource Constrained IoT Devices: A Survey on Recent Advances.
DOI: 10.5220/0013202100003944

In *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025)*, pages 199-206
ISBN: 978-989-758-750-4; ISSN: 2184-4976

managing IoT data. IoT data is often untrusted, of questionable integrity and has unverified origin or lack provenance. This is mainly due to OT sensors or devices' limited resources and lack of a centralised administrative control. Current IoT services often lack data integrity and traceability. Therefore, adopting DLTs could address these cybersecurity challenges, by leveraging DLT features (Jin et al., 2022); the cybersecurity aspect of IoT sensors or devices can be managed and cyber threats targeting them can be detected and mitigated.

Several researchers (Jin et al., 2022; Farahani et al., 2021; Pescetelli et al., 2022) have already started looking at the role of DLTs in securing IoT sensors and/or devices and the data they create, collect or exchange. For example, (Farahani et al., 2021) proposes a DLT framework for ensuring the security and privacy of IoT infrastructure in the context of smart communities. Authors of (Pescetelli et al., 2022) proposes a framework for IoT based on DLT and decentralised identifiers. Although IoT and DLT are distinct technologies that have evolved independently over the years, they are somehow complimentary (Jin et al., 2022). The convergence of IoT and DLTs offers new opportunities to address some of the major challenges of IoT, such as the lack of data integrity or provenance failures, non-auditability, lack of transparency, and insecure data sharing (Jin et al., 2022). There is a significantly growing body of knowledge and research community that are now focusing on this convergence.

While much research has focused on the adoption of DLTs for IoT applications in various sectors; minimal research work has been focused on using DLTs to enhance OT Internet-enabled sensors or devices security. This paper aims to consolidate existing research on this topic, through comparing the different techniques or approaches, technologies used, and results achieved over the years. This is meant to gain a comprehensive understanding of the current-state-of-the-art in this area and identify some of the research gaps that exists.

The paper is structured as follows. Section 2 provides a background that lays out the foundation of the study. It examines security challenges of IoT and presents an overview of the key DLT features. Section 3 focusses on the current state-of-the-art with respect to the convergence of IoT and DLTs. Section 4 identifies and unpack the existing research gaps in the common body of knowledge. Finally, Section 5 concludes the study and provides pointers for future research that will address some of the identified research gaps and move IoT technology beyond the current state-of-the-art.

2 BACKGROUND

IoT has transformed how we interact with the world, creating opportunities to build powerful, ubiquitous computing platforms by integrating sensing and connectivity into everyday objects (di Vimercati et al., 2016). IoT systems consist of small, smart devices with sensors and actuators, applied across various sectors like healthcare, energy, industry, agriculture, OT, and smart homes. The IoT penetration in many aspects of our lives brings together data to improve infrastructure, public utilities, and services, as well as giving rise to smart cities' development.

The use of IoT devices has seen exponential growth over the years. According to Statista, the number of IoT devices worldwide is forecast to be close to 30 billion in 2030 which is portrayed in Figure 1 (Vailshery, 2024). The rapid growth of IoT is also proliferated by the development of communication technologies such as 5G and data analytics using AI and ML. IoT brings a greater prevalence of such smart objects with higher connectivity and the ability to collect data in real-time (Vailshery, 2024; Vailshery, 2024).

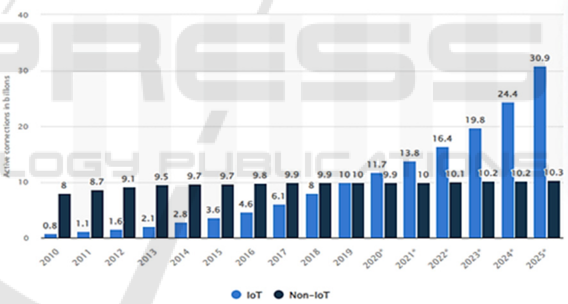


Figure 1: The number of connected IoT and non-IoT Devices (Vailshery, 2024; Vailshery, 2024).

However, the innovative nature brought by IoT devices has allowed manufactures to solely focus on that plus the ease of use introduced by these devices to capture their audience in the market. This means that less efforts are invested towards ensuring the security aspect of these devices (Ebad, 2023). Security concerns for IoT devices are due to resource-constraints in terms of energy consumption, storage capacity, computational power, battery lifetime etc. This means that conventional security measures like antivirus, encryption, etc cannot be directly applied to IoT devices due to resource constraints. Therefore, OT Internet-enabled devices are usually more vulnerable to cyber-attacks than other endpoint devices with more computing power.

It is anticipated that Industrial applications may see a rise in IoT integration with the convergence of AI, augmented reality, and massive deployment of private 5G networks to seamlessly integrate digital twins to existing processes within an industry. With this integration, emerging technologies, (DLTs, and Digital Identity) have the potential (when integrated correctly) to enhance the security of OT Internet-enabled sensors or devices. Presently, cloud-based information systems have become the norm for managing IoT data, which is untrusted due to the centralised administrative control. Hence, it fails to guarantee the integrity of IoT data and traceability of operations to achieve transparency within organisations. Therefore, the adoption of DLTs can be a key enabler to solve many IoT device security challenges, by tapping into some of the features offered by both DLTs and Digital Identities.

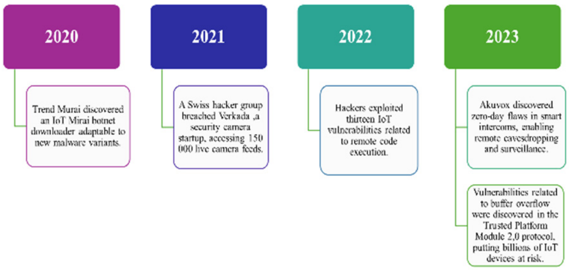
2.1 IoT: State-of-the-Art

According to (Perscheid et al., 2023), IoT is a network of connected devices, sensors and control entities that enable communication among various objects. IoT connects previously unconnected objects to the Internet, offering diverse services and providing IoT devices with advantages like higher manageability and reachability (Na & Park, 2021). This allows for IoT devices to collect, process, and transmit large amounts of real-time data about patients, property, traffic, electricity, etc. As the number of devices increases, data produced by the devices will continuously increase requiring the network to have greater capacity to administer and manage the data (Perscheid et al., 2023). IoT enables the interconnectivity of several heterogeneous (diversity and variety of devices, communication protocols, and data) devices and networks using different communication technologies. The connectivity nature of IoT network allows for device communication which may occur between machine-to-machine (M2M) or thing-to-thing (T2T), human-to-thing (H2T) or human-to-human (H2H) (Khanam et al., 2020).

Despite IoT benefits, security, legal and regulatory issues remain. Key challenges and vulnerabilities include the following:

- Privacy concerns: IoT devices constantly collects and shares large amounts of sensitive personal data which can result in regulatory penalties if compromised or stolen.
- Centralisation: concentrating control and decision making to a single entity, resulting to issues of single point of failure due to a compromise and may lead to privacy issues as one entity has full access to sensitive data.
- Security vulnerabilities: this is a key challenge for legacy IoT systems and devices – especially those that can no longer be supported. Most IoT devices are resource-constrained that often lack the necessary computing power to take updates/upgrades to firmware/software and can hardly integrate traditional security features making them susceptible to attacks. This creates multiple attack vectors for IoT networks. For example, communication channels can be compromised via eavesdropping (Ebad, 2023). In addition, user authentication is an underlying security mechanism to verify the users' validity between the entities connected in the network (Rao & Deebak, 2023). Data authentication: "is also crucial to store sensitive information on cloud services that must be securely transferred to networks" (Dhar et al., 2024).

Other issues exist like interoperability, identity management, and lack of standardisation (Mthethwa, 2023). This paper focuses on the security aspect for resource constrained IoT devices. Figure 2 illustrates several IoT security breaches over the past years. A common denominator of these breaches are the existing vulnerabilities and zero-day flaws that may be exploited by cyber threat actors to access confidential information. These incidences highlight IoT devices as vulnerable targets and remains a low hanging-fruit for threat actors to exploit. Therefore, as organisations rely heavily on IoT devices, it is important to evaluate the safety of information systems, and the data they process to ensure cyber resilience against cyber-attacks.



Trend Murai discovered an IoT Mirai botnet downloader adaptable to new malware variants.

A Swiss hacker group breached Verkada ,a security camera startup, accessing 150 000 live camera feeds.

Hackers exploited thirteen IoT vulnerabilities related to remote code execution.

Akuvox discovered zero-day flaws in smart intercoms, enabling remote eavesdropping and surveillance.

Vulnerabilities related to buffer overflow were discovered in the Trusted Platform Module 2,0 protocol, putting billions of IoT devices at risk.

Figure 2: Recent notable IoT security breaches and IoT hacks.

To address these challenges, the security of resource-constrained devices and networks is studied from various perspectives where various solutions are explored. These solutions incorporate elements such as device authentication, secure communication protocols, and robust encryption algorithms specifically tailored for resource-constrained IoT devices (Dhar et al., 2024). Recent advancements in IoT devices and sensors have led to more efficient sensors with extended battery life, smart capabilities, equipped with onboard processing power, promoting edge computing, and reducing reliance on centralised processing. These advancements integrated with AI and ML enable decision making, predictive analytics and automated anomaly detection (Karma, 2024).

A countermeasure for addressing IoT issues is the introduction of lightweight solutions for resource-constrained devices. There is a need for plausible solutions to manage vulnerabilities in the IoT devices. Unlike IT environments, vulnerability management in OT/IoT requires distinct approaches. This research explores the use of DLTs as a countermeasure to secure resource-constrained IoT devices.

2.2 Overview of DLTs

DLT is an emerging technology that eliminates the need for a central entity and allows for the recording of data or transactions of assets and stores it in multiple places simultaneously thus fulfilling the distributed nature of a ledger (Jnr et al., 2023). The DLT network consists of various nodes responsible for the authentication and validation of transactions through a consensus mechanism i.e., Proof of Stake (PoS), Proof of Work (PoW), etc. The nature of DLT makes it immutable, decentralised, fault-tolerant, transparent, verifiable, auditable, and trustworthy (Gugueoth et al., 2023). These key characteristics are the fundamentals of the uniqueness of DLTs. There are different types of DLTs, namely Blockchain, Hashgraph, Holochain, Directed Acyclic Graph (DAG), and Tempo (Radix) (Chowdhury et al., 2019).

DLTs can be classified as public or permissionless (accessible to everyone), private or permissioned (accessible only to verified parties or nodes), and consortium or hybrid (a combination of public and private) (Chowdhury et al., 2019). Originally used for cryptocurrencies, DLTs have evolved to offer solutions beyond this scope. Key features of DLTs includes decentralisation, distributed, anonymity, security, immutability, traceability, transparency, consensus, and auditability. Thus, making them useful for addressing information security challenges and enabling secure communication and interaction among IoT devices.

3 DLT FOR IOT SECURITY: RELATED WORKS

The nature of DLT has made it possible for it to be applied to various sectors to solve different challenges and this has also been the case for IoT. This is evident through the recent studies towards the implementation of DLTs in IoT. Several security frameworks have been proposed in the IoT space (Eghmazi et al., 2024; Raj & Ghosh, 2023; Gowda et al., 2023; Wu et al., 2023; Qi et al., 2023; Chen et al., 2022; Yin et al., 2022; Wickström et al., 2020; Le & Mutka, 2019). In (Dhar et al., 2024), the authors focus on securing multimedia data (audio, video, and images) from IoT devices using blockchain and quantum cryptography. However, issues like scalability, privacy, interoperability, and energy efficiency remain. Moreover, real-world implementation and validation have yet to be conducted. These aspects must still be addressed to strengthen the framework's security (Dhar et al., 2024).

Authors (Patruni & Saraswathi, 2022) proposed a framework for securing and monitoring IoT devices using blockchain, focusing on access control and strong authentication mechanisms to enhance privacy and security. Several studies (Papageorgiou et al., 2020; Tegane et al., 2023; Kaven & Skwarek, 2023) also explore access control with DLTs to secure IoT devices and data. The work of (Patruni & Saraswathi, 2022) could be extended by using the quantum cryptography approach from (Dhar et al., 2024).

Integrating DLTs with IoTs is challenging due to complexities like consensus mechanism, throughput delays, high computational costs, etc. These challenges are even more pronounced for resource-constrained IoT devices. To address this, researchers have proposed lightweight DLT solutions tailored for resource-constrained IoT networks and devices. A study conducted by (Mershad & Cheikhrouhou, 2023) present a taxonomy of lightweight blockchain solutions, identifying five key areas: architecture, device authentication, cryptography model, consensus algorithm, and storage method. The authors explore various methods used in each area, highlighting gaps and identifying areas for improvement, to effectively address these challenges.

Researchers have focused on DLT-based authentication for IoT devices across various use cases like smart grids, vehicles, group key agreements etc (Wu et al., 2023; Abubakar, 2023; Wang et al., 2023; Yao et al., 2019; Naresh et al., 2022; Wang et al., 2020). While these studies present promising approaches, further work is still required to develop highly secure systems that satisfies anonymity,

Table 1: Summary of related works.

Ref.	Purpose	Technologies Used	Findings
(Eghmazi et al., 2024)	Presents a Blockchain as a Service (BaaS) application to address IoT security and privacy challenges. It introduces a new data structure with encryption based on public/private keys.	Hyperledger Fabric, Kafka, & InterPlanetary File System (IPFS)	The platform links numerous IoT devices with blockchain, using a scalable data structure ensuring strong security and effective device management, advancing secure, scalable IoT blockchain networks.
(Dhar et al., 2024)	Focuses on fortifying the security of multimedia data, encompassing audio, video, and images, obtained from IoT devices.	Blockchain, cloud technology, quantum cryptography, Zero-Knowledge Proofs (ZKPs), lightweight ring signatures	The framework ensures secure data handling in IoT systems, protecting against eavesdropping, man-in-the-middle, data tampering, and Sybil attacks, while ensuring communication authenticity and integrity.
(Sharma & Goveas, 2023)	Provides secure and flexible access control to prevent unauthorised access and ensure only authorised users can interact with IoT device.	Non-Fungible Tokens (NFTs) & Solana Blockchain	Requires minimal computational power and milliseconds of delay, making it ideal for resource-constrained devices. NFTs offers a secure and flexible solution for IoT systems.
(Raj & Ghosh, 2023)	Proposes Fusion Chain-S, designed to create a lightweight and secure framework for IoT networks irrespective of their limitations.	IPFS, Constrained Application Protocol (CoAP), Blockchain	Provides enhanced storage and access policies for every data element and considered fault-tolerant, lightweight, and secure compared to other peer models.
(Kyriakidou et al., 2023)	Explores the SSI benefits in IoT, while addressing associated challenges and reviews existing SSI-based systems for managing authentication, authorisation, and access control in resource-constrained IoT devices.	SSI, DIDs, VCs, DLT	A comprehensive analysis regarding the contributions of DIDs and VCs, the two main pillars of SSI, to enhance privacy and security for IoT.
(Gowda et al., 2023)	Proposes a Blockchain-based Secured Key Management in a Fog Computing Environment (BSKM-FC), a decentralised system, utilises a one-way hash chain for key generation and Elliptic Curve Cryptography (ECC) for secure key sharing.	Private blockchain technology	The performance analysis using MIRACL shows the proposed scheme meets security requirements and improves efficiency. It reduces computation, communication, and storage overhead by 7-14%, 9-18%, and 7-17%, respectively, while decreasing block preparation time by 14-28%.
(Wu et al., 2023)	Proposes a lightweight anonymous authentication scheme for patients and medical servers in Internet of Medical Things (IoMT), ensuring mutual authentication and privacy protecting.	Consortium Blockchain, biometric technology and fuzzy extraction technology	Results shows that the scheme achieved the designed security goals and better performance in computation and communication overhead. It is an efficient mutual authentication protocol.
(Karthika & Jaganathan, 2023)	Presents the Winner of Guess (WoG) consensus and the iLEDGER framework for resource-constrained IoT applications, enabling data sharing.	Blockchain, Smart contract	It provides lightweight architecture based on Validate-Execute with minimal communication overhead.
(Qi et al., 2023)	Introduces a lightweight PoW for IoT, with a trust evaluation mechanism,	Proof of Work, blockchain	Results show that the method has a lower energy consumption and higher security.
(Chen et al., 2022)	Proposes a Lightweight Blockchain with Low Communication Overhead (LBLCO) and a new consensus algorithm, Proof of Repute Score based on Hidden Block (HBPORS).	Blockchain	Experimental tests show that LBLCO can meet the requirements of large number of nodes and fast response speed in IoT.
(Yin et al., 2022)	Proposes SmartDID, a blockchain-based distributed identity for establishing SSI with strong privacy preservation.	Digital Identity, SSI, DIDs, Blockchain, Smart contract, ZKPs	Presents a distributed identity management system for IoT consisting of an identity system.
(Patruni & Saraswathi, 2022)	Designed a new framework application for securing and monitoring IoT devices through Blockchain technology	Ethereum Blockchain, Radio Frequency Identification (RFID), Smart contracts	Achieved an efficient access control mechanism and secure data sharing through different IoT devices.
(Al Oliwi et al., 2021)	Addresses security and data privacy in smart homes by integrating IoT, blockchain, and smart contracts for access control.	Lightweight Scalable Blockchain (LSB). Ethereum Smart Contract	The framework effectively addresses security and data privacy issues in smart homes, prevent unauthorised access to IoT devices.
(Wickströ et al., 2020)	Securing IoT device deployments and means for communicating securely with devices.	Ethereum, Smart contracts & Oracles	The protocol enhances security for IoT devices by using smart contracts to enforce security policies.
(Le & Mutka, 2019)	Enables IoT devices to validate blockchain data without a central server by randomly selecting network witnesses for access control validation.	Ethereum, Smart contracts, consensus & Bloom filters	A lightweight method enabling resource-constrained IoT devices to validate blocks using Bloom filters and network witnesses, bypassing complex computation.

traceability, and non-repudiation properties, while producing acceptable processing, communication, and delay overhead.

In (Panda et al., 2020), the authors classify how IoT systems can leverage DLT attributes to address privacy and security challenges. The five classifications are: privacy preservation, trust, authentication and access control, integrity, and availability. They note the current DLT-based solutions are still in early stages, requiring further research. Table 1 provides a critical and systematic analysis of the related work on using DLT to enhance security of IoT devices and networks, focusing on their purposes, technologies and key findings.

From the technologies or approaches in Table 1, most works utilise smart contracts which are a program that consists of a set of Scenario-Response procedural rules and logic, deployed on a DLT. It allows for certain tasks to be executed automatically once the predefined conditions are met (Wang et al., 2018). By inheriting DLT properties, smart contracts enable flexible and customisable rules for IoT device authentication.

With the shift towards decentralised identity and Self-Sovereign Identity (SSI), Table 1 shows papers incorporating these approaches alongside DLTs. The fundamental premise of SSI is that individuals have sovereignty over their digital identities and thus, have control over their data.

In this model, users are granted full control over their identities, enabling them to decide when, if, and how they wish to disclose or modify their data. SSI is enabled by emerging technologies such as DLTs (to effectively eliminate the need for central authorities and foster a trustless environment), Decentralised Identifiers (DIDs) (ensuring every IoT device is uniquely identified by DID, linked to a key pair that is under the direct management of the IoT device owner and can assist in improving privacy (Kortesniemi et al., 2019)), and Verifiable Credentials (VCs) (which promotes interoperability thus supports accountability) (Mazzocca et al., 2024; Schardong & Custódio, 2022).

4 EXISTING RESEARCH GAPS

This paper analyses existing DLT-based solutions for enhancing IoT security. Based on the systematic literature review conducted, the authors have identified the following research gaps (and give a brief narrative) that should be addressed in future research work.

- *Research Gap 1 – Insufficient Research Work that Moves Beyond the Current State of The Art*: There is a need for research beyond the proof-of-concept solutions that are proposed in current literature. Researchers must implement, test, and pilot these solutions and others in real-life scenarios. Future research must focus on transforming the proposed proof-of-concepts into actual products for testbed deployment, whilst evaluating their efficiency and effectiveness. Additionally, there is a lack of research that examines progress beyond the current state-of-the-art in DTL for securing IoT.
- *Research Gap 2 – Lack of Use and Misuse Cases:* A research gap exists in the lack of use and misuse cases for leveraging DLTs to enhance IoT devices security and cyber resilience. While some use cases exist, there is no focus on malicious use or misuse cases of DLTs on IoT devices. Therefore, researchers must employ misuse cases that will test such systems for cyber resilience.
- *Research Gap 3 – Lack of Performance Benchmarks:* Research is needed to compare the performance of different approaches, particularly those with similar approaches.
- *Research Gap 4 – Lack of Reviews that Unpack Key Features*: A research gap exists for studies to review and analyse the features of each proposed solution in detail.
- *Research Gap 5 – Lack of Testing and Evaluation*: Rigorous testing is crucial for optimisating IoT devices. Thus, there is a need to test and evaluat the proposed approaches for their appropriateness and performance.
- *Research Gap 6 – Lack of Comprehensive Solutions*: There is a need for solutions that integrate some of the existing proposals to create more comprehensive solutions applicable across different contexts.

The above points highlight just a few of the knowledge gaps identified by the authors, and this list is not exhaustive. These gaps indicate areas that require further research to advance the field. Thus, using DLT to enhance IoT device security remains an emerging field with several unanswered questions.

5 CONCLUSIONS

This paper presents a critical and systematic review of using DLT to enhance the security of resource-constrained IoT devices with limited storage and processing power. It examines how DLT features, such as decentralisation, can secure IoT devices and networks. Several challenges including interoperability, processing capabilities, scalability, availability, and security, hinder successful deployment of applications in IoT devices. It was observed that smart contracts are mostly used and now the rise of SSI has introduced the use of decentralised identities in IoT. However, SSI adoption is still in its early stages, requiring further investigation into integration challenges, such as scalability, reliability, performance concerns, etc. Most reviewed works do not explicitly address these challenges in their analysis.

REFERENCES

Jin, W., Lim, S., Woo, S., Park, C., & Kim, D. (2022). Decision-making of IoT device operation based on intelligent-task offloading for improving environmental optimization. Complex & Intelligent Systems, 8(5), 3847-3866.

Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. Journal of Network and Computer Applications, 177, 102936.

Pescetelli, G., Petrosino, L., Della Valle, S., Ronga, G., Merone, M., & Vollero, L. (2022, June). Framework for IoT ecosystems based on distributed ledger technologies and decentralized identifiers. In 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0&IoT) (pp. 87-91). IEEE.

di Vimercati, S. D. C., Livraga, G., Piuri, V., Samarati, P., & Soares, G. A. (2016, April). Supporting Application Requirements in Cloud-based IoT Information Processing. In IoTBD (pp. 65-72).

Vailshery, L.S., (2024, February). Internet of Things (IoT) - statistics & facts. Statista. https://www.statista.com/topics/2637/internet-of-things/#topicOverview (accessed Jan. 20, 2024).

Vailshery, L. S. (2022, September). Global number of connected IoT devices 2015-2025. Statista. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed Jan. 20, 2024).

Ebad, S. A. (2023). On Quantifying of IoT Security Parameters-An Assessment Framework. IEEE Access.

Perscheid, G., & Moormann, J. (2023, October). Towards a Framework for Analyzing the Suitability of DLTs for Integration in the IoT. In 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA) (pp. 208-214). IEEE.

Na, D., & Park, S. (2021). Fusion chain: A decentralized lightweight blockchain for IoT security and privacy. Electronics, 10(4), 391.

Khanam, S., Ahmedy, I. B., Idris, M. Y. I., Jaward, M. H., & Sabri, A. Q. B. M. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE access, 8, 219709-219743.

Rao, P. M., & Deebak, B. D. (2023). A Comprehensive Survey on Authentication and Secure Key Management in Internet of Things: Challenges, Countermeasures, and Future Directions. Ad Hoc Networks, 103159.

Dhar, S., Khare, A., Dwivedi, A. D., & Singh, R. (2024). Securing IoT devices: A novel approach using blockchain and quantum cryptography. Internet of Things, 25, 101019.

Mthethwa, S. (2023, August). Securing Internet of Things (IoT) Devices Through Distributed Ledger Technologies (DLTs) and World Wide Web Consortium (W3C) Standards. In The International Conference on Deep Learning, Big Data and Blockchain (pp. 119-128). Cham: Springer Nature Switzerland.

Karma, M.R. (2024, February). The future trends and Innovations in IOT sensor technology, Sigma Wire. Available at: https://sigmawire.net/future-trends-iot-sensor-technology (Accessed: 06 March 2024).

Jnr, B. A., Sylva, W., Watat, J. K., & Misra, S. (2023). A Framework for Standardization of Distributed Ledger Technologies for Interoperable Data Integration and Alignment in Sustainable Smart Cities. Journal of the Knowledge Economy, 1-44.

Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585.

Chowdhury, M. J. M., Ferdous, M. S., Biswas, K., Chowdhury, N., Kayes, A. S. M., Alazab, M., & Watters, P. (2019). A comparative analysis of distributed ledger technology platforms. IEEE Access, 7, 167930-167943.

Patruni, M. R., & Saraswathi, P. (2022). Securing Internet of Things devices by enabling Ethereum blockchain using smart contracts. Building Services Engineering Research and Technology, 43(4), 473-484.

Mershad, K., & Cheikhrouhou, O. (2023). Lightweight blockchain solutions: Taxonomy, research progress, and comprehensive review. Internet of Things, 24, 100984.

Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT Data Security: Using the Blockchain to Boost Data Integrity and Privacy. IoT, 5(1), 20-34.

Sharma, R. K., & Goveas, N. (2023, March). Use of Blockchain in Securing IoT systems with Resource Constrained Devices. In 2023 IEEE 20th International Conference on Software Architecture Companion (ICSA-C) (pp. 216-223). IEEE.

Raj, R., & Ghosh, M. (2023, March). A Lightweight Blockchain Framework for secure transaction in resource constrained IoT devices. In 2023 5th International Conference on Recent Advances in Information Technology (RAIT) (pp. 1-7). IEEE.

Kyriakidou, C. D. N., Papathanasiou, A. M., & Polyzos, G. C. (2023). Decentralized Identity With Applications to Security and Privacy for the Internet of Things. Computer Networks and Communications, 244-271.

Gowda, N. C., Manvi, S. S., Malakreddy, B., & Lorenz, P. (2023). BSKM-FC: Blockchain-based secured key management in a fog computing environment. Future Generation Computer Systems, 142, 276-291.

Wu, A., Guo, Y., & Guo, Y. (2023). A decentralized lightweight blockchain-based authentication mechanism for Internet of Vehicles. Peer-to-Peer Networking and Applications, 1-14.

Karthika, V., & Jaganathan, S. (2023). Iledger: A lightweight blockchain framework with new consensus method for IoT applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022EAP1088.

Qi, L., Tian, J., Chai, M., & Cai, H. (2023). LightPoW: A trust based time-constrained PoW for blockchain in internet of things. Computer Networks, 220, 109480.

Chen, C., Liu, M., Mo, P., Yuan, C., & Dai, P. (2022, July). LBLCO: A Lightweight Blockchain with Low Communication Overhead for Internet of Things. In Proceedings of the 2022 4th Blockchain and Internet of Things Conference (pp. 92-99).

Yin, J., Xiao, Y., Pei, Q., Ju, Y., Liu, L., Xiao, M., & Wu, C. (2022). SmartDID: a novel privacy-preserving identity based on blockchain for IoT. IEEE Internet of Things Journal, 10(8), 6718-6732.

Al Oliwi, H. H., Al Husain, Z., & Rafeh, R. (2021, November). Integrating Blockchain and Internet of Things for Smart Homes. In 2021 Computing, Communications and IoT Applications (ComComAp) (pp. 77-82). IEEE.

Wickström, J., Westerlund, M., & Pulkkis, G. (2020). Rethinking IoT security: a protocol based on blockchain smart contracts for secure and automated IoT deployments. arXiv preprint arXiv:2007.02652.

Le, T., & Mutka, M. W. (2019, June). A lightweight block validation method for resource-constrained iot devices in blockchain-based applications. In 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 1-9). IEEE.

Papageorgiou, A., Mygiakis, A., Loupos, K., & Krousarlis, T. (2020, June). DPKI: a blockchain-based decentralized public key infrastructure system. In 2020 Global Internet of Things Summit (GIoTS) (pp. 1-5). IEEE.

Tegane, S., Semchedine, F., & Boudries, A. (2023). An extended Attribute-based access control with controlled delegation in IoT. Journal of Information Security and Applications, 76, 103473.

Kaven, S., & Skwarek, V. (2023, May). Poster: Attribute Based Access Control for IoT Devices in 5G Networks. In Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (pp. 51-53).

Abubakar, M. A. (2023). Blockchain-based Authentication and Access Control Mechanism for Internet of Things (IoT) (Doctoral dissertation).

Wang, S., Huang, K., Ma, K., Xu, X., & Hu, X. (2023). A lightweight encryption and message authentication framework for wireless communication. IET Communications, 17(3), 265-278.

Yao, Y., Chang, X., Mišić, J., Mišić, V. B., & Li, L. (2019). BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 6(2), 3775-3784.

Naresh, V. S., Allavarpu, V. D., & Reddi, S. (2022). Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN. The Journal of Supercomputing, 1-25.

Wang, W., Huang, H., Zhang, L., Han, Z., Qiu, C., & Su, C. (2020, December). BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid. In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 1332-1338). IEEE.

Panda, S. S., Mohanta, B. K., Dey, M. R., Satapathy, U., & Jena, D. (2020, July). Distributed ledger technology for securing IoT. In 2020 11th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-6). IEEE.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F. Y. (2018, June). An overview of smart contract: architecture, applications, and future trends. In 2018 IEEE Intelligent Vehicles Symposium (IV) (pp. 108-113). IEEE.

Kortesniemi, Y., Lagutin, D., Elo, T., & Fotiou, N. (2019). Improving the privacy of iot with decentralised identifiers (dids). Journal of Computer Networks and Communications, 2019.

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2024). A Survey on Decentralized Identifiers and Verifiable Credentials. arXiv preprint arXiv:2402.02455.

Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. Sensors, 22(15), 5641.