information

Article

Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions

Burhan Ul Islam Khan [1,*], Khang Wen Goh [2], Mohammad Shuaib Mir [3,*], Nur Fatin Liyana Mohd Rosely [2], Aabid Ahmad Mir [4] and Mesith Chaimanee [5]

[1] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2] Faculty of Data Science and Information Technology, INTI International University, Nilai 71800, Malaysia
[3] Department of Management Information Systems, College of Business, King Faisal University, Al-Ahsaa 31982, Saudi Arabia
[4] Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Kuala Lumpur 50250, Malaysia
[5] Faculty of Engineering and Technology, Shinawatra University, Pathum Thani 12160, Thailand
* Correspondence: burhankhan@um.edu.my (B.U.I.K.); mmir@kfu.edu.sa (M.S.M.)

Abstract: As the Internet of Things (IoT) continues to revolutionize value-added services, its conventional architecture exhibits persistent scalability and security vulnerabilities, jeopardizing the trustworthiness of IoT-based services. These architectural limitations hinder the IoT's Sensor-as-a-Service (SEaaS) model, which enables the commercial transmission of sensed data through cloud platforms. This study proposes an innovative computational framework that integrates decentralized blockchain technology into the IoT architectural design, specifically enhancing SEaaS efficiency. This research contributes to an optimized IoT architecture with decentralized blockchain operations and simplified public key encryption. Furthermore, this study introduces an advanced SEaaS model featuring innovative trading operations for sensed data among diverse stakeholders. At its core, this model presents a unique blockchain-based data-sharing mechanism that manages multiple aspects, from enrollment to validation. Evaluations conducted in a standard Python environment indicate that the proposed SEaaS model outperforms existing blockchain-based data-sharing models, demonstrating approximately 40% less energy consumption, 18% increased throughput, 16% reduced latency, and a 25% reduction in algorithm processing time. Ultimately, integrating a lightweight authentication mechanism using simplified public key cryptography within the blockchain establishes the model's potential for efficient and secure data-sharing in IoT.

Keywords: Internet of Things (IoT); Sensor-as-a-Service (SEaaS); lightweight cryptography; decentralized data-sharing; secure data transactions; blockchain-enhanced IoT

Citation: Khan, B.U.I.; Goh, K.W.; Mir, M.S.; Mohd Rosely, N.F.L.; Mir, A.A.; Chaimanee, M. Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions. *Information* **2024**, *15*, 212. https://doi.org/10.3390/info15040212

Academic Editor: Kun She

Received: 4 January 2024
Revised: 14 March 2024
Accepted: 2 April 2024
Published: 10 April 2024

1. Introduction

The continuous evolution and integration of the Internet of Things (IoT) into various sectors has brought about an era of unprecedented connectivity and data exchange, representing a transformative shift in networks, analytics, and automation [1]. IoT efficiently connects physical devices, software, and technologies, facilitating ubiquitous applications in smart homes, healthcare, industrial IoT, logistics, energy management, and more [2–5]. Essentially driven by its ability to link physical and digital components, the IoT stands out as a fully connected digital ecosystem that enhances efficiency through high-level data collection and analytical methodologies. This paradigm allows for the real-time monitoring and management of devices and fosters the development of informed, decision-centric services, leading to enhanced process optimization and customer experiences [6,7].

Despite its significant impacts and increased adoption, the core architectural framework of IoT still faces significant challenges, especially in terms of the scalability, security,

and diversity of data. Despite the architectural variances in IoT systems, the conventional models generally consist of layers such as perception, network, middleware, application, business, and user layers, with the occasional addition of cloud and edge computing layers [8]. These layers, though customizable, are consistently influenced by factors like scalability, latency, security, connectivity, and regulatory compliance, amongst others [9,10].

The Sensor-as-a-Service (SEaaS) model is central to IoT's operational efficiency, a paradigm that has increased as a vital business instrument in the IoT landscape [11]. SEaaS facilitates the acquisition of essential data through IoT sensors, thereby facilitating data exchange on a commercial level. This model relies significantly on utilizing cloud systems, serving as the foundation for critical operations, such as data collection, transmission, and accessibility, without relying on extensive hardware or infrastructural frameworks [12].

Despite its immense potential, the SEaaS model faces fundamental and inherent challenges, predominantly reflecting the fundamental issues affecting the broader IoT architecture, such as data heterogeneity, decentralized environment complexity, security vulnerabilities, and traffic management difficulties [13–15]. Such challenges amplify in scenarios involving extensive buyer–seller interactions necessitating synchronized, secure data transactions. The conventional architecture of an IoT cannot provide an effective platform for supporting the practical agenda of SEaaS owing to the heterogeneity of data issues, complexity in maintaining a decentralized environment, security threats, traffic management, etc. [16,17]. Such a problem becomes more challenging when many buyers must be synchronized with the seller's data and comply with security standards. Hence, the proposed study seeks to address the following research questions:

- How can effective data-sharing methods be developed to enhance SEaaS within a large and decentralized network?
- What procedures can be implemented to enhance accountability among all stakeholders involved in SEaaS, while maintaining cost-effectiveness?
- How can a system model of SEaaS be developed to facilitate practical deployment within an IoT environment?

In exploring fair solutions to the above-mentioned research questions, this study proposes an innovative technique to improve the SEaaS model within the IoT domain. The originality of the contributory research objectives linked to the proposed model, distinguishing it from the existing literature, is outlined as follows:

- Designing a simplified and lightweight IoT architecture that integrates the decentralized operation of blockchain technology with simplified public key encryption;
- Developing a novel SEaaS model featuring exclusive trading operations for sensed data conducted by sellers, buyers, service providers, and blockchain entities;
- Introducing a pioneering blockchain-based data-sharing process encompassing enrollment, sale, request, feedback management, and validation procedures;
- Benchmarking the proposed SEaaS model against recent standard blockchain-based data-sharing methodologies to demonstrate its effectiveness across multiple performance parameters.

The manuscript is organized as follows: Section 2 explores the related works; Section 3 identifies the research problems; Section 4 discusses the research methodology and the development of the SEaaS algorithm; a comparative analysis of our results with other data-sharing models is performed in Section 5; and Section 6 concludes the discussion.

2. Related Work

This section discusses various existing research methodologies undertaken to improve the data-sharing process in the IoT environment. All the prominent recent research publications associated with data-sharing mechanisms in IoT have been studied. Further, they were filtered to narrow down the manuscript samples based on the inclusion and exclusion criteria. The inclusion criteria for choosing the manuscript were the research papers with a vivid discussion of blockchain implementation and its associated methods for investigating

the data-sharing process. The exclusion criteria for filtering the manuscripts were research papers without illustrative algorithms and result discussion. Conventionally, there are various data-sharing methods, viz., the publish/subscribe model, request/response model, edge computing model, data marketplaces, blockchain for data integrity, and consent management. To simplify the understanding of existing approaches, the discussion of numerous research methods in this section is carried out with respect to several methods. e.g., architecture, encryption, distributed operation, data-driven, and miscellaneous.

- Architecture-focused methods: These methods aim to develop IoT architectures for managing large volumes of sensing data in real time [18]. Chiti and Gandini [19] focused on enhancing interoperability in IoT architecture through distributed ledger services, which may need further attention to the complexities in maintaining a decentralized environment. Jin and Kim [20] developed a rule-based scheme to integrate devices, IoT services, rule services, and clients within a heterogeneous IoT architecture, addressing complex control issues but lacking comprehensive solutions for security challenges.
- Encryption-focused methods: Secure data-sharing methods in blockchain or non-blockchain environments often rely on encryption-based operations. He et al. [21] introduced a data-sharing mechanism integrating attribute-based encryption with smart contracts, offering nuanced control over data access, but may require enhancements for computational efficiency and scalability due to attribute-based encryption's complexity. Sun et al. [22] proposed a methodology aiming to enhance user experience in data access but raised concerns about the practicality of homomorphic encryption due to its computational intensity. Researchers like Razzaq et al. [23] and Albualyhi and Alsukayti [24] utilized the Ethereum blockchain to facilitate open frameworks in IoT architectures, facing challenges such as network congestion and scalability. Fukuda et al. [25] presented a modular design for distributed data-sharing using streaming services to enable distributed processing tasks. Various encryption-based and blockchain-based data-sharing models have been proposed, including chaotic RSA encryption (Priyadharshini et al. [26]), attribute-based encryption (Zhang et al. [27]), public key encryption with a ring signature (Wu et al. [28]), software-defined blockchain with a Byzantine algorithm (Shi et al. [29]), and homomorphic encryption with hashing (Zhang et al. [30]). However, this approach's primary limitation lies in its focus on a centralized operational approach, which may only partially meet the needs of large-scale applications requiring decentralized management.
- Distributed-operation-focused methods: These methods primarily support large-scale data-sharing services in IoT and often incorporate machine-learning, artificial intelligence, and blockchain technologies. Debauche et al. [31] introduced an integrated machine-learning scheme to process blockchain data at the cloud level for improved data streams, while Olaniyi et al. [32] emphasized the need for enhancing blockchain security for real-time applications. However, these models need to comprehensively address the practical implications and computational demands of integrating these complex technologies. Zichichi et al. [33] proposed another decentralized data-sharing mechanism using smart contracts and a distributed hash table for smart query management on a ledger in the blockchain. Despite advancements, this approach's implementation using a hypercube-distributed hash tree increases the routing complexity with a tree dimension expansion, suggesting the need for more scalable systems. Fallatah et al. [34] discussed personalized data stores for service relaying, highlighting challenges in managing large-scale informatics linked with personal data. Palaiokrassas et al. [35] developed a platform for managing sensory data in smart cities, while Almstedt et al. [36] explored the use of small-scale blockchains. However, these blockchain models operate with latency due to consensus mechanisms, limiting real-time data-sharing applications.
- Data-driven methods: These methods model adversaries to address threats in specific data-processing scenarios. Bentahar et al. [37] and AI Ma-hamid et al. [38] introduced

key agreement and middleware schemes for authentication and data management in IoT environments. Despite their contributions, a comprehensive approach to address the security, scalability, and real-time processing challenges in IoT transactions remains necessary. The integration of fog with cloud and IoT offers a wider range of applications, improving service relaying [39]. Various techniques for disseminating information using sensing technologies, such as in public transportation scenarios, have been discussed [40]. Othman et al. [41] proposed a unique sensing-as-a-service model using a search optimization algorithm for a virtual sensing environment. However, the lack of flexible interaction among entities may increase overhead during real-time data-sharing, particularly in virtualized cloud environments.

- Miscellaneous methods: Mathew et al. [42] and Hoque et al. [43] explored novel areas in IoT, including crowdsensing and airborne-based data services. Mathew et al. developed a crowdsourcing model integrated with smart city services to bridge the gap between consumers and data collectors, while Hoque et al. [43] proposed IoT service relaying using drones, particularly in smart agriculture. Woodward [44] proposed a blockchain-based big data transmission model, and Grupac and Negoianu [45] discussed augmented reality applications. Both studies investigated the relationship between multi-sensor fusion, dynamic routing technologies, and blockchain-enhanced Sensor-as-a-Service (SEaaS) in IoT. While these explorations are valuable, further research is needed to ensure the reliable, quality, and secure transmission of diverse data forms. Additionally, these models should provide supportive evidence for managing spatial and temporal data dynamics, which present significant challenges in dynamic environments.

In synthesis, while each referenced work contributes uniquely to advancing IoT architectures and data-sharing methodologies, a common shortcoming pervades—a tendency toward specialization, often neglecting a comprehensive evaluation concerning scalability, security, and practical applicability in dynamic, real-world IoT ecosystems. Thus, this literature review highlights the need for a holistic and integrative research approach. The agenda is to move beyond the current limitations of specialized focus areas to unfold a more universally applicable, resilient, and efficient SEaaS model in IoT.

Before addressing the identified research problem, it is crucial to acknowledge the importance of offering sensing data as an IoT service. From the existing studies discussed in this section, it was observed that cloud environments require a comprehensive examination of various aspects, particularly those related to blockchain technology and the inherent challenges in the IoT environment. Numerous prevalent research issues and challenges are yet to be resolved, such as routing problems, traffic management, security concerns, and resource allocation. These interconnected challenges are vital for achieving effective sensing as a service in IoT systems. Hence, this section narrows down all the challenges and highlights only those challenges that are addressed in the proposed scheme, as follows:

- **Lack of accountability:** Existing research studies have implemented blockchain (both centralized and distributed, e.g., Ethereum) [24], which offers better fairness while performing data-sharing with high-quality information. However, there must be a dedicated model which supports accountability. Consequently, these models often compromise with privacy and accountability, especially when handling simultaneous transactions between buyers and sellers.
- **Less study towards sensing as a service:** It should be noted that approaches towards data-sharing can be used for systems towards sensing as a service; however, they are not explicitly meant to carry out this specific task. There are a significantly smaller number of standard research models in which data-sharing methods are integrated with sensing as a service over an IoT environment [26–30].
- **Stale IoT architecture:** While designing a decentralized blockchain operation [33], it is essential to modify the architecture of the IoT without changing the core layer-based operation. This demands more extensibility and flexibility in authentication, data access, and updating tasks. The currently deployed mechanism in the IoT architecture

needs to explore its holistic architectural potential. Our prior work has addressed these issues [46]; however, more extensive modeling is required.

- **Complex data/block management:** A practical modeling of sensing as a service requires consideration of the buyer and seller with a lightweight, flexible sales management scheme. Only some studies have addressed this issue. Existing problem solutions are witnessed to use a complex key management approach that offers better security but at the cost of the computational burden [21,22]. Hence, lightweight data/block management must be carried out so that data sharing can be performed without degrading computational efficiency.

With the growing trend of IoT applications, the challenges associated with security concerns have also increased manifold. Recent state-of-the-art methods towards a secure data-sharing operation have made some progressive contributions; however, the effectiveness of the solutions presented in existing studies needs to be improved to mitigate the increasing number of threats in IoT. The more significant problems associated with data-sharing and management in IoT still include device vulnerabilities, the inappropriate selection of data encryption, and weaker authentication policies. All the unattended security loopholes in IoT also lead to a higher degree of vulnerability in accessing sensor data. As the SEaaS model involves more about the facilitation of accessing the sensor data on subscription, the identified research gap impedes the accomplishment of optimal security.

The endeavor to implement SEaaS in IoT and cloud environments unveils a labyrinth of challenges primarily rooted in blockchain technology and the intrinsic issues of the IoT framework. Despite the myriad ongoing research initiatives to navigate these complexities, substantial impediments, such as routing problems, traffic management, security concerns, and resource allocations, persistently obfuscate the seamless realization of SEaaS in IoT. Central to the research problem is the glaring deficit in accountability within existing blockchain implementations [24]. Although infused with a semblance of fairness in data-sharing, current models require more dedicated mechanisms to bolster accountability. As a result, the environment becomes vulnerable to privacy breaches and reliability compromises during concurrent buyer–seller transactions [23,28].

Adding to this complexity is the need for more scholarly attention toward SEaaS. There is a clear need for dedicated research models that seamlessly integrate data-sharing methods with SEaaS in an IoT environment [37,38].

Additionally, the prevalent IoT architectures require a degree of obsolescence and rigidity, necessitating urgent revitalization to accommodate the innovative decentralization introduced by blockchain technologies [18–45]. The urgent need for architectures that exhibit extensibility and flexibility, especially in pivotal domains such as authentication, data access, and updating, emerges as a pressing research priority.

Further complicating the research terrain is the prevailing complexity of data/block management strategies. Current models, albeit security-robust, are characterized by unwieldy computational burdens attributed to intricate key management protocols [22,26,29]. This highlights a critical research imperative: developing lightweight, efficient frameworks that foster effortless data-sharing without compromising computational agility or security integrity. Our research aims to navigate these multifaceted challenges to unveil groundbreaking solutions that rejuvenate the SEaaS landscape in IoT through the innovative integration of blockchain technology. This approach is pertinent for addressing the current limitations and paving the way for future advancements in IoT systems. By converging the gaps explored in the existing methodologies, research problems were identified and discussed in the next section.

3. Problem Description

To enable secure and reliable data-sharing in IoT, conventional methodologies (described in the previous section) use access control, which is mainly centralized. Such forms of access controls are not feasible for data owners to gain complete control using their deployed IoT devices/appliances in the context of SEaaS. Therefore, the primary problem

in designing the SEaaS framework is overcoming the dependencies of the centrality control system. From the context of blockchain deployment incorporated within data-sharing in an IoT environment, it is a sub-optimal idea to refer to existing methods for evolving as a candidate solution. This is because the existing blockchain [18–45] and encryption-focused methods [21–30] do not balance data-sharing with transparency, especially with respect to the sales management system. Therefore, the secondary problem relates to developing a solution for data-sharing with regard to large-scale distributed and decentralized blockchain architectures. One fair possibility for solving this will be redesigning the smart contract system to support secure sale management in a complex IoT architecture.

Hence, a closer look into the above-mentioned problems will foretell the prominent issues regarding decentralized blockchain operation and the demand for effective data-sharing to incorporate more responsible attributes and design structures to facilitate better system accountability. Therefore, the prime problem statement of the proposed study can be summarized as follows—*including a higher degree of accountability of reliable data transmission in IoT using conventional blockchain*.

4. Materials and Methods

This section explains the research methodology and innovative design approach leveraging the blockchain technology in the proposed SEaaS scheme. Four pivotal actors comprise the operational dynamics of this model: seller, service provider, buyer, and blockchain.

Seller: Sensing devices play a crucial role as sellers, capturing diverse environmental data in the IoT context. Governed by unique encryption mechanisms and key management techniques, these devices prioritize security, enabling authorized access. Owners possess the authority to modify device configurations and customize them for commercial gains or enhanced service experiences.

Service Provider: This intermediary strengthens the framework by managing the interactions between owners (sellers) and clients (buyers). The service provider administers enrollment, aligning buyers and sellers based on data requirements and meticulously tracking transactional records to mitigate potential disputes. This actor operates on the foundations of blockchain's smart contracts or ledgers, upholding the integrity and fluidity of operational transactions despite the inherent risks of privileged content disclosures.

Buyer: Representing the client, the buyer, be it a person or an entity, has eyes on the services offered within the IoT spectrum. With a level of adaptability similar to cloud-based services, the SEaaS model makes it easy for buyers to access services from the owners. Structured on a comprehensive payment mechanism including pre-paid and post-paid paradigms, the model ensures a streamlined financial transaction flow. Prioritizing simplicity, it adopts a conventional payment methodology calibrated against the delivery of relayed services.

Blockchain: By deploying the potential capabilities of the distributed Ethereum blockchain, the proposed system manages core operations centered around smart contracts. The architecture places significant emphasis on smart contract operations, manipulating buyers' and sellers' interactions with anonymous attributes, thereby ensuring a robust enrollment process under the vigilant supervision of the service provider. As a savvy intermediary, the smart contract oversees financial transactions, fostering a resilient and dynamic transactional ecosystem.

Each actor, characterized by distinct roles and responsibilities, converges to develop a unified, secure, and efficient SEaaS model enhanced by the decentralized virtues of blockchain technology.

4.1. Transactional Block for SEaaS

This section discusses the essential operations required to implement the proposed SEaaS model. The proposed scheme is examined using a case study of smart appliances in

an IoT environment. Referring to the graphical representation in Figure 1, consider that a user owns a smart device that operates on an external power supply.

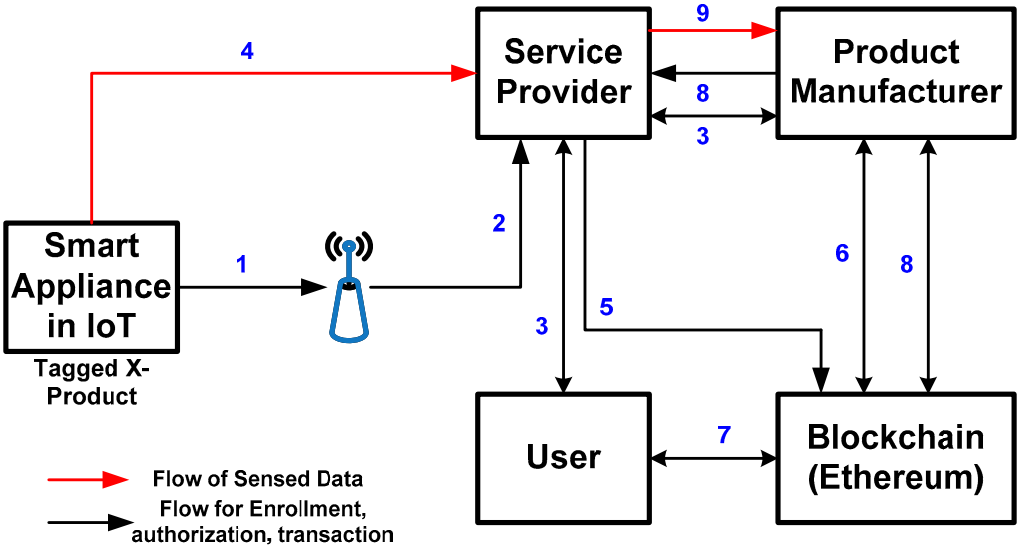

Figure 1. The transactional flow of the proposed method.

The discussion of the above-mentioned transactional flow exhibited in Figure 1 with steps of flow represented by numerals is as follows: The study considers that a user possesses a smart device that works on an external power supply. The task shown in step 1 is connecting the smart appliance with wireless hotspots, followed by linking with the service provider as a task in step 2. The inbuilt sensing devices within the smart appliances capture their designated surrounding information precisely. The service provider then asks the user if the sensed data are permitted to be specifically collected and if the user is interested in selling the collected sensed data in step 3. Suppose the user responds by playing the role of the seller; then, they are facilitated with the blockchain bearing all the sale data. In such circumstances, the enrollment of the new seller (user) is carried out while the new seller is also required to furnish additional information to the service provider associated with their smart appliances, viz., identity, components, operational configuration, settings, price, etc. At the same time, there is also a fair likelihood that certain manufacturers of objects hosted by smart appliances (also within the smart appliances) are enrolled via the same service provider.

In step 4, as shown in Figure 1, the service provider acquires the aggregated sensed information from the agreed smart appliances by the new seller. It should be noted that public key encryption can be used to encrypt the sensed data while forwarding the data. The encrypted data is stored locally by the service provider on the permission acknowledged by the new seller and issues the smart contract, which maintains the information related to these sales within a blockchain to the user in step 5. The study also assumes that the manufacturer can act as a new buyer and, hence, could be interested in the new sensed information in encrypted form within the secured captivity of the service provider. The new buyer further proceeds to purchase this sensed encrypted data from the service provider. In step 6, the new buyer (manufacturer) pays the price towards the smart contract and further updates the blockchain. The new seller uses the public key of the new buyer to encrypt its sensed data. The system also computes a proof to provide evidence for this cryptographic operation using the new buyer's public key. In step 7, the new seller submits the legitimate information to the smart contract to acquire the price money towards these successful sales in an IoT environment. The new buyer then acquires the encrypted symmetric key from the smart contract and generates a request to acquire encrypted data from the service provider in step 8. In step 9, the service provider forwards the encrypted data after confirming the

request, where the new buyer decrypts the encrypted data to access the actual sensed data of the new seller.

Referring to Figure 1, the entire set of operations essential for developing the proposed method emphasizes the implementation of a decentralized blockchain operation. This decentralization is instrumental and involves various actors, such as users, service providers, and product manufacturers. A strategically designed smart contract leverages this blockchain operation, facilitating many explicit functions crucial for the enrollment process, updating process, sales management, request, response management, and validation in the proposed SEaaS model.

The compositional framework of the proposed smart contract S_c is expressed as follows:

$$S_c = \sum_{i=1}^{m} \mu_i \quad (1)$$

The above empirical expression (1) represents the design of a smart contract, S_c, which consists of m number of internal operations μ towards its blockchain operation, especially keeping decentralization in mind. The proposed scheme considers ten different types of internal algorithmic operations (m = 10, i.e., μ_1, μ_2, ..., μ_{10}) by varying the functionalities of the operations μ to cater to the objective of the proposed SEaaS model. The briefing of all the involved internal operations represented by μ_i in expression (2) (i.e., μ_1, μ_2, ..., μ_{10}) is as follows:

- **Data-Sharing Operation (μ_1):** This is the default operation of the data-sharing process, activated when the blockchain is applied and deployment of S_c is carried out.
- **Enrollment Management (μ_2/μ_3):** This operation consists of (i) Store Enrollment Data (μ_2) and (ii) Acquire Enrollment Data (μ_1) that carries out storing and acquiring all transactional information about the enrollment process to create clear accountability towards each operation.
- **Sale Management (μ_4/μ_5):** This operation consists of (i) Sale-Updating Operation (μ_4) and (ii) Acquire Sale Data (μ_5) that are responsible for facilitating and acquiring all the undertaken sales-based information in the SEaaS model.
- **Request Management (μ_6/μ_7):** This operation consists of (i) Request-Storing Operation (μ_6) and (ii) Acquire Request Information (μ_7) that carry out storing and acquisition of all forms of requests based on a purchase order of sensory services in IoT. It should be noted that Request-Storing Operation (μ_6) is given more importance as it relates to the allocation of incentive α for providing correct feedback.
- **Feedback Management (μ_8/μ_9):** This operation consists of (i) Feedback-Storing Operation (μ_8) and (ii) Acquire Feedback Information (μ_9) that carry out storing and acquisition of feedback (or acknowledgment). It should be noted that the study model offers more importance to Feedback-Storing Operation (μ_8) as the seller (or owner of a service) can acquire a service fee upon invoking Feedback-Storing Operation (μ_8), which is underscored for its capability to enable the seller (or service owner) to increase service fees concurrent with the provision of legitimate feedback, also facilitating the withdrawal of service fees by the buyer.
- **Validation Operation (μ_{10})**: This operation, dedicated solely to verifying the authenticity and accuracy of feedback information provided by various participants, is crucial to maintaining the integrity and reliability of the SEaaS model's operational framework.

4.2. Algorithm Implementation

This section discusses the core algorithmic implementation in which unique key management is used to further secure the blockchain-based holistic architecture in IoT. As the proposed model mainly targets formulating a scheme that facilitates an effective data-sharing scheme over a decentralized environment of the SEaaS model, the security and integrity of the data to be shared are of utmost importance. Hence, before understanding blockchain-based data-sharing in SEaaS, it is essential to describe its encryption operation briefly. The complete encryption operation is carried out in four steps: (i) the first step

is associated with the secure token generation, where a public key cryptography-based encryption can be utilized to generate a pair of public and private keys; (ii) the second step is to perform an encryption operation using the generated secure token in the prior step to generate encrypted data $Enc \rightarrow A_1.A_2$, where A_1 represents $(1+f).O_{data}$ and $(rand)^f.|f^2|$, where f is a variable obtained by the product of two random prime numbers, O_{data} is original data, and $rand$ is any random natural number; (iii) the next step is performing a decryption operation to acquire the original data $O_{data} = g(Enc^Z, |f^2|)$, where the variable Enc represents encrypted data, variable z represents the lowest common multiplier between $(p-1)$ and $(q-1)$, assuming p and q are two prime numbers selected in first steps, and the function $g(x)$ applied on them represents $g(x) = \Delta\psi/f$, where $\Delta\psi = \psi - 1$ and $\psi = |f|$, and, hence, the decrypted data are obtained; and iv) an extra layer of randomness $rand_1$ is added to the generated encrypted data to offer an extended layer of security, where $rand_1 = Enc.A_3.A_4$. The variable A_3 and A_4 represents $(1+f)^{o_{data}}$ and $|f^2|$, respectively.

The above-mentioned encryption operational steps are carried out in the algorithmic process toward sharing the data and services from various actors involved in the proposed scheme. The complete procedure is developed to support the decentralized operation of the blockchain operation, and to support relaying seamless services over the IoT ecosystem.

The core operations involved in the proposed scheme for sharing data in the SEaaS model are stated as Algorithm 1.

Algorithm 1 For Blockchain-Based Data-Sharing in SEaaS.

Input: S_{attr} (system attributes)
Output: O_{data} (delivery of original data from seller to buyer)
Start
1. Init $S_{attr} \rightarrow (\beta, k_1, k_2, I)$
2. $S_{conf} \rightarrow S_{attr}$
3. $STG \rightarrow (\sigma_1, \sigma_2)$
4. $\eta = k_1(l_{tok}||d_{iden})$
5. $Eval(\sigma_1, \sigma_3, \sigma_4, \tau)$
6. **if** $auth(\sigma_1, \sigma_3, \sigma_4, \tau) = F$
7. $\rightarrow$ $Flag \rightarrow$ Reject request
8. **else**
9. $\rightarrow V_{iden} = k_1(\lambda)$
10. $\mu_2(\sigma_1, V_{iden})$
11. $device \rightarrow (s_{data})$
12. **if** $k_1(s_{data1}) = v_{inf}$
13. $(\mu_2, \mu_3) \leftarrow$ Store $data$
14. perform $\mu_4 \rightarrow S_c(I)$
15. **end**
16. $\mu_5 \leftarrow I$
17. Obtain (e_k, d_k)
18. Perform μ_5, $\mu_6(\alpha)$
19. $\mu_7 \rightarrow seller(I)$
20. $\mu_8 \rightarrow seller(\Phi(I))$
21. Validate Φ
22. $\mu_9 \rightarrow buyer(I)$
23. $\mu_{10} \rightarrow (O_{data})$
End

The discussion of the aforementioned algorithmic operation of the proposed system extends to multiple operational blocks as follows:

- **Configuration Stage:** This is the first step of operation, which is related to the configuration of the proposed approach towards blockchain-based data-sharing in SEaaS. The implementation initiates by declaring the system attributes. S_{attr} consists of $\beta, k_1, k_2,\ I$ representing public attribute generated by the first step of encryption, first secret key, second secret key, and identity of the smart appliance, respectively (Line 1 and Line 2).

It is noted that k_1 and k_2 are two different hash keys whose key size is restricted to 256 bits and the highest natural number. This means that the proposed scheme is intended to accommodate the secure hashing of any size of data. Apart from this, all the actors involved in the proposed system yield a specific form of private record (σ_1, σ_2) using the secret token generator STG (Line 3). This is meant to facilitate transactional information within the blockchain, while a leader security token, l_{tok}, is used for enrollment. To perform validation of the smart appliance's legitimacy bearing the identity d_{iden} in the blockchain, the service provider further computes a verification key η (Line 4).

- **Enrollment Process:** After the configuration stage is accomplished, the following line of action is directed toward the enrollment process, which is necessary for utilizing the SEaaS model by various actors in the IoT environment. One of the essential steps in the enrollment process is to evaluate some crucial information to ascertain the genuineness of the smart appliances in IoT. For this purpose, the algorithm constructs a method $Eval$ to assess some of the essential information $(\sigma_1, \sigma_3, \sigma_4, \tau)$ that represents public information of the actor's account, the real identity of smart appliances, supporting attribute σ_4 to prove the genuine identity of smart devices and signatures, respectively (Line 5). The signature attribute is generated as $\tau = ds(\sigma_1, \sigma_3, \sigma_4)$, where the method ds represents the Elgamal signature. The service provider initially assesses the genuineness of signature attribute τ by verifying the public key attribute σ_1, original identity attribute σ_3, supporting attribute σ_4, and signature attribute τ (Line 5). The algorithm authenticates all these attributes, and if they are violated (Line 6), then the algorithm denies the request for data-sharing (Line 7). Otherwise, the algorithm computes the virtual identity attribute V_{iden} (Line 9). During this computation of V_{iden}, the algorithm applies its primary hash key k_1 to a matrix λ using the leader token l_{tok} (Line 9). The variable matrix λ is formed by concatenating the leader token l_{tok}, public key σ_1, and the original identity of smart appliances σ_3. Further, the algorithm forwards σ_1 and V_{iden} information to the smart contract to reposition it using the Store Enrollment Data μ_2 operation (Line 10). It should be noted that the service provider uses the local database to store all the lists of V_{iden} information that could be used for future reference. Another essential factor towards this enrollment operation of the proposed algorithm is that the system permits the enrollment process, provided σ_1 and V_{iden} are already indexed in the identity of smart contract I.
- **Managing Sensed Information in IoT:** Consider that the new seller utilizes its virtual identity, V_{iden}, to initiate the selling process to the enrolled service provider. In such cases, the sensed information from the seller's smart appliances must be securely forwarded to the new buyer via the service provider. The service provider acquires the seamless transmission of a specific set of information from the smart appliances of the new seller (Line 11). The information captured by the service provider includes (i) the device's identity d_{iden}, (ii) start time of data collection t_s, (iii) total duration of data collection t_d, (iv) verification code of source information $v_c = (k_1(s'_t||O_{data}))$, (v) encrypted data $Enc_1 = Enc(s'_t||(t_s + i.t_d))$, and (vi) verification information evaluated by the algorithm $v_{inf} = k_1(\gamma)$, where the variable γ represents the concatenation of user verification key η, device identity d_{iden}, t_s, t_d, v_c, and Enc_1. Further, it should be noted that s_t and s'_t represent the key owned by the sensor owner for a long time and the secret key for that particular session, respectively. The computation of s'_t is performed by applying the primary hash key k_1 to the concatenated value of s_t and the session time t_s. The service provider computes the verification key η_1 using primary hash key k_1 over the concatenated value of the leader token l_{tok} and the device identity d_{iden}. This computation is performed over s_{data1} to check its validity with verification information v_{inf} (Line 12). The variable s_{data1} bears concatenated information on the service provider verification key η_1, device identity d_{iden}, t_s, t_d, v_c, and Enc_1. For the matching conditional logic stated in Line 12 of the algorithm, the system stores the following information locally, device identity d_{iden}, t_s, t_d, v_c, and Enc_1, followed by the

Sales-Updating Operation μ_4 for relaying sales information to the smart contract $S_c(I)$ where I represents the identity of the smart contract (Line 13 and Line 14). The sales information will further consist of concatenated information on device identity d_{iden}, V_{iden}, $cost$, t_s, t_d, and $data$, where the new variables, $cost$ and $data$, relate to anticipated service cost by seller and content of data being sold, respectively.

- **Request Management:** The next part of the algorithmic implementation is associated with the buyer's request to obtain the sensed information as a service from the buyer. For this purpose, the implementation uses the operation of acquiring sales data μ_5 to obtain information on the device identity d_{iden}, the virtual identity of the seller V_{iden}, $cost$, t_s, t_d, and $data$ utilizing the smart contract S_c with identity I (Line 16). Further, the first step of encryption is implemented to generate the security token as e_k and d_k, representing the buyer's public and private keys (Line 17). In the following line of operation, the algorithm uses the Request-Storing Operation μ_5, where the algorithm obtains information on the device identity d_{iden}, new and prior virtual identity of the seller, instantaneous time, and public key of the buyer that are finally forwarded to S_c (Line 18). Further, the algorithm executes a Request-Storing Operation μ_6 while allocating α incentive for appropriate transactional information.
- **Feedback Management:** The algorithm uses Acquire Request Information μ_7 to obtain requests from the smart contract S_c, where the requested information consists of device identity d_{iden}, the old and new virtual identities of the seller, the instantaneous time of receiving the request, and the public key of the buyer e_k (Line 19). To generate feedback on the newly acquired request, the seller uses the primary session token s_t to create a secondary session key s'_t. This operation is carried out as $s'_t = k_1(B)$, where the variable B represents the concatenation of the primary session token s_t and the total duration of data collection t_d. Further, the public key of the buyer is used to encrypt the secondary session token s'_t by the seller, followed by generating feedback Φ (Line 20) using the Feedback-Storing Operation μ_8 that is forwarded to the smart contract S_c with the identity I.
- **Authentication of Service Relaying:** This is the final operation of the proposed algorithm, which involves validating the feedback Φ (Line 21). The algorithm uses Acquire Feedback Information μ_9, where the buyer verifies the information from the data owned at that time by the smart contract S_c with identity I (Line 22). Finally, the algorithm retrieves the original data O_{data} using the validation operation μ_{10} (Line 23). In the final stage of the operation, the generated request and compliance using the generated feedback are cross-checked by the service provider from the smart contract. The system indexes the successful transaction as a record upon finding a valid request. Hence, the algorithm completes its operations towards a completely decentralized data-sharing mechanism using a distributed blockchain in the IoT architecture.

5. Result Discussion

This section provides a detailed analysis of the results of implementing the algorithm discussed in the previous sections. To achieve the objectives of SEaaS, the proposed system model has been coded in Python. It elaborates on the evaluation environment, the strategy, and a comprehensive discussion of the outcomes achieved during the study implementation.

5.1. Assessment Environment

The assessment environment is designed in a planned manner to map its applicability to real-world cases of blockchain deployed in a large environment. In all real-world cases, there is an eventual anticipation for autonomous and continuous operations to be performed by smart contracts without involving human interaction. A discussion of such a form of real-time design methods has also been carried out in the existing literature (e.g., Deniziak et al. [18], He et al. [21], and Albulayhi and Alsukayti [24]) where it was learned that a smart contract executes its actions upon fulfillment of its specified conditions.

Regarding the proposed SEaaS model, a smart contract must also be investigated in similar scenarios to prove its applicability in real-time environments. To fulfill this agenda, the model is initially required to consider IoT devices in the form of standard sensor nodes with a specific area to carry out an observation. Apart from this, the sensors must be represented as core actors in the proposed SEaaS model (i.e., buyer and seller), where the model implements the algorithm discussed in the previous section. This is the primary justification for designing the test environment and undertaking the initialized values of the parameters involved in the assessment.

A use case illustrated in Figure 1 was developed in this subsection. A hypothetical model of 200 sensor nodes dispersed over 1000 m $\times$ 1000 m was conceived for simulation purposes, representing a smart city region. Table 1 lists the simulation parameters used in the experiment.

Table 1. Adopted simulation parameters.

Parameters	Values
Total sensors/smart appliances	200
Number of sellers	5–10
Number of buyers	10
Number of service provider	2
Data packets	50 gigabytes
Size of control message	10 bits
Bandwidth	5 gigabytes per second
Initialized energy of nodes	10 J

Of the 200 sensors, a scheme was devised in which a minimum of five and a maximum of ten seller nodes were randomly selected. These nodes express interest in selling the sensed data. Concurrently, the model considers another set of ten randomly chosen buyer nodes. Both sellers and buyers undergo a verification process, culminating in confirmation only after completing their enrollment.

Two service providers were incorporated into the model, tasked with facilitating synchronized transactions between buyers and sellers. The choice of assigned values is driven by the intention to develop a controlled research environment within the scope of a smart city. The sellers' and buyers' numbers can grow exponentially in this environment.

The algorithm commences its experimentation with these predefined values. These values are subject to incremental adjustments in alignment with escalating traffic loads in the IoT environment, facilitating an efficient evaluation of the system's operational performance. The goal is to interpret the system's capabilities and adaptability in response to varying network demands, offering insights into its functional robustness and scalability within a dynamic smart city ecosystem.

5.2. Assessment Strategy

This assessment strategy of the proposed study is primarily based on two key components: (i) a comprehensive IoT architecture and (ii) blockchain. These components function in a synchronized manner to achieve the unified objective of seamless data sharing, an essential aspect in realizing the vision of the SEaaS model. To conduct a comprehensive benchmark analysis, this study thoroughly investigates influential research studies aligning with a common purpose. A range of models are listed below, each followed by a detailed examination of their similarities and differences in relation to the proposed SEaaS:

- **SDS (Secure Data-Sharing):** The model developed by Priyadharshini and Canessane [26] aims to address existing security challenges in blockchain technology. It presents a notable integration of the Rivest–Shamir–Adleman (RSA) algorithm and a chaotic

map, enhancing the security of data sharing within the IoT environment, marked by many devices.

- Congruence with SEaaS: A significant use of public key encryption is employed to strengthen blockchain-based data-sharing in IoT.
- Distinctiveness: The SEaaS model introduces a novel approach by orchestrating sales transactions using smart contracts, a functionality that is notably absent in the SDS framework.

- **BaDS (Blockchain-augmented Data-Sharing):** Developed by Zhang et al. [27], this exceptional architecture improves data sharing in the IoT framework by utilizing an attribute-based signature encryption combined with a ciphertext policy.
  - Congruence with SEaaS: A shared adherence to using smart contracts as instrumental components in promoting secure data-sharing within IoT architectures.
  - Distinctiveness: The SEaaS ecosystem operates in an environment where equal importance is given to device and user (seller/buyer) identities, growing into a more decentralized setting. This contrasts with BaDS, which prioritizes the device identity through control tables.
- **ADS (Anonymized Data-Sharing):** Developed by Wu et al. [28], this model adopts public key encryption to enhance anonymity. This is a popular model for strengthening authenticity, accountability, and privacy in the context of data sharing.
  - Congruence with SEaaS: A unified step towards utilizing blockchain, public key encryption, and signatures, thereby constructing a stronghold of anonymity.
  - Distinctiveness: SEaaS navigates the anonymity landscape through the decentralized management of encrypted device and user (seller) virtual identities. This approach is less cumbersome than the exclusive dependence on signatures, as ADS advocates.
- **SLTA (Secure and Lightweight Trust Architecture):** Developed by Shi et al. [29], the SLTA model presents a system of selective data sharing with privileged owners in a distinct, trust-oriented IoT architecture. Oracle is used for facilitating data collection, followed by tamper prevention by edge devices, along with identity management in a distributed manner.
  - Congruence with SEaaS: A collective ode to distributed identity management in the blockchain-empowered data-sharing.
  - Distinctiveness: SEaaS establishes an innovative route through simplified mathematical methodologies enhanced by multilayered security protection without complex orchestrations, a deviation from SLTA's trust-centric identity management principles.
- **EDS (Efficient Data-Sharing):** Developed by Zhang et al. [30], this model introduces an innovative payment channel network within blockchain technology, incorporating hashing and homomorphic encryption. This approach aims to overcome conventional obstacles related to transaction success rates and overhead challenges. The model also claims a decreased overhead while adopting a multi-path routing scheme.
  - Congruence with SEaaS: A mutual commitment to incorporating hashing into the fabric of transaction processes.
  - Distinctiveness: SEaaS was developed by introducing a new IoT architecture with innovative system features, stimulating a dynamic data-sharing ecosystem. This approach contrasts with EDS's preference for orchestrating multi-hop routing.

A significant insight gained from reviewing the models mentioned above is the conspicuous absence of a dedicated case study focused on data-sharing schemes. In contrast, the SEaaS model excels with its deep consideration of trading sensing services within a decentralized environment, enhanced by an updated IoT architecture. A key feature of SEaaS is its departure from the complexities associated with traditional public key encryption,

resulting in a system characterized by reduced computational iterations and lower memory requirements during the SEaaS trading process. The established models and the proposed scheme were evaluated in a uniform simulation environment for a robust assessment, exploring factors such as energy consumption, throughput, latency, and processing time. The numerical results, comparing the SEaaS model with various existing models, are presented in Table 2, offering a clear and detailed comparison.

Table 2. Numerical outcomes of comparative assessment.

Approaches	Energy Used	Throughput	Latency	Processing Time
Proposed	3.188	8.529	0.917	1.087
SDS	8.271	5.615	3.19	5.096
BaDS	8.022	7.188	2.09	3.817
ADS	7.912	6.672	2.89	3.588
SLTA	6.193	6.987	2.61	3.118
EDS	6.025	6.996	2.26	2.671

The discussion of the accomplished numerical outcomes concerning its rationale is carried out next.

5.3. Discussion of Outcomes

The efficiency and applicability of an IoT architecture are fundamentally reflected in the prolonged sustainability of the sensors deployed within smart appliances. An essential measure to evaluate this aspect is to assess the cumulative energy consumption of smart devices throughout the entire operation of the data-sharing mechanism. This approach is instrumental in highlighting the operational efficiency and sustainability of the implemented architecture, thereby providing valuable insights into its overall performance and viability. The consequential outcomes of this evaluative measure are comprehensively illustrated in Figure 2.

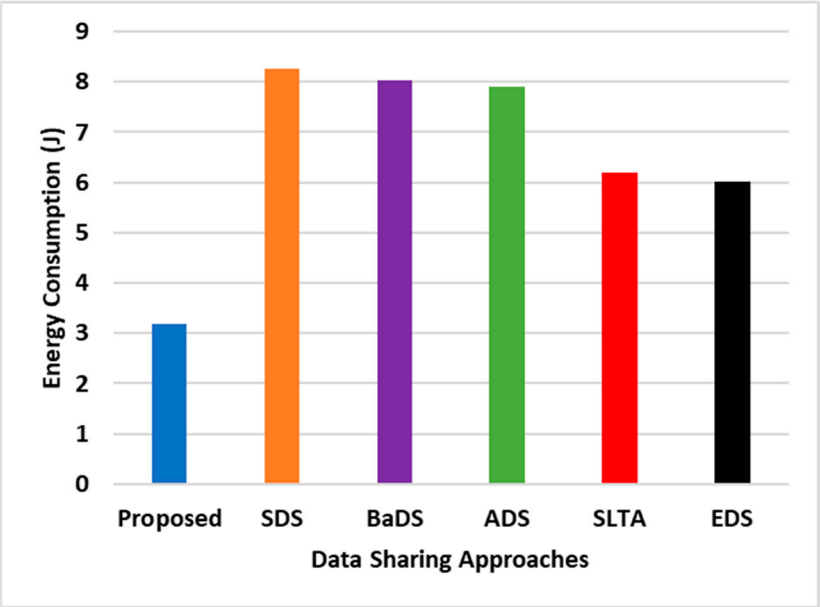

Figure 2. Comparative assessment of energy consumption.

A meticulous examination of Figure 2 reveals that the proposed SEaaS model yields a reduction in energy consumption of approximately 40% compared to the existing blockchain-

based data-sharing models under consideration. The dominant factors contributing to this enhancement are outlined as follows:

The models such as SDS, BaDS, and ADS demonstrate a considerably elevated level of energy consumption. This is primarily attributed to their reliance on sophisticated public key encryption, requiring a complex key management mechanism. Unlike these models, the SLTA and EDS models do not encounter the complexities associated with key management, resulting in nearly equivalent performance levels. Specifically, SLTA employs a blockchain constructed using a software-defined structure, while EDS utilizes hashing, contributing to marginally reduced energy consumption relative to SDS, BaDS, and ADS.

The proposed SEaaS model minimizes energy consumption owing to its extensive deployment of logical operations and a more streamlined utilization of encryption steps. The service provider facilitates the interaction between the seller and buyer, simplifying the task of assessing compliance or contradictions within the smart contract. This refinement leads to accelerated computations and reduced energy consumption, resulting from the reduced reliance on more resource-intensive encryption operations.

Moving forward to the throughput assessment, this includes the exchange involving requests, responses, and the acquisition of original data by the buyer. An optimized IoT architecture attempting for a lightweight operation should demonstrate a well-structured, scalable, and highly accessible form of blockchain, provided that its throughput demonstrates significant enhancement. Figure 3 displays the comparative results, presenting the throughput performance of the proposed SEaaS model relative to the existing blockchain-based data-sharing schemes. This comparative analysis highlights the effectiveness and efficiency of the proposed model, affirming its suitability and robustness in the context of contemporary IoT architectures.

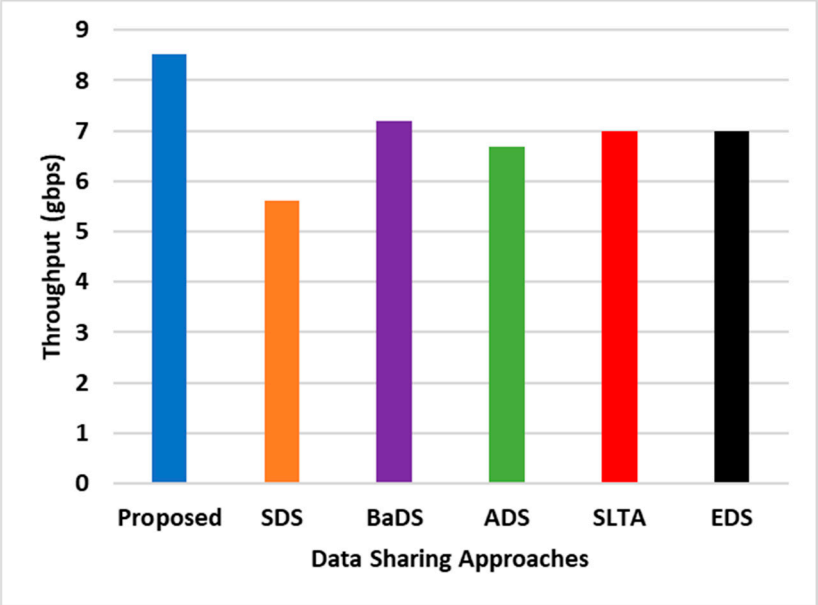

Figure 3. Comparative assessment of throughput.

An in-depth examination of Figure 3 reveals that the proposed SEaaS model demonstrates an approximate 18% increase in throughput compared to existing data-sharing models. To understand the rationale behind this enhancement, it is necessary to consider the critical factors affecting data transmission performance. These factors are predominantly associated with the structure and management of the blockchain within a decentralized IoT architecture, including the size and timing of the blockchain, network latency, congestion, resource availability, and smart contract complexities.

Most existing models, such as SDS, BaDS, ADS, SLTA, and EDS, have been established for identity management, accompanied by extensive cryptographic operations. Although

this approach enhances security, it concurrently hampers data transmission, potentially diminishing throughput. Conversely, the SEaaS model introduces a meticulously structured smart contract management system in a decentralized format. This structure, complemented by the service provider's autonomous validation of transactional sales, ensures that the throughput remains resilient and unaffected by such decentralized blockchain operations. Latency, another crucial performance metric, measures the efficacy of the transmission rates between buyers and sellers. An ideal IoT architecture should proficiently manage the latency. As the bandwidth remains relatively constant, prioritizing streamlined and accelerated operational procedures is essential for effective data transactions within the IoT-cloud environment. Figure 4 illustrates the latency performance outcomes, where the proposed scheme demonstrates superior results compared to the pre-existing models.

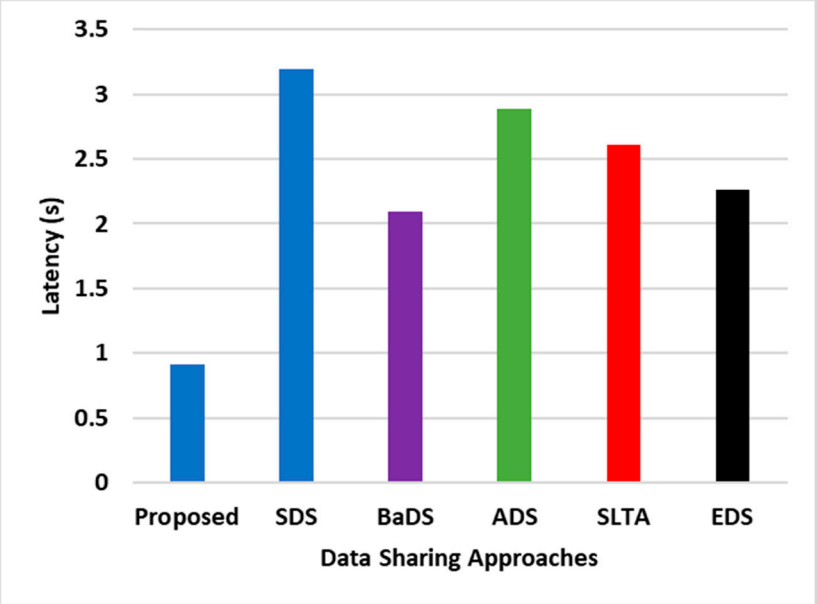

Figure 4. Comparative assessment of latency.

Figure 4 illustrates that SEaaS reduces latency by about 16% compared to other analyzed data-sharing models. Factors contributing to latency in blockchain-based IoT architectures include data volume, blockchain scalability, transaction processing speed, network latency, and block confirmation times. While SDS enhances security with chaotic maps and RSA algorithms, it complicates storage, retrieval, and computational processes, increasing data transmission times. Conversely, the SEaaS model employs structured, decentralized blockchain operations, facilitating flexible and rapid transactional assessment and enhancing path and route determinacy, thus reducing latency.

Lastly, Figure 5 focuses on the algorithm-processing time, which is crucial for evaluating computational efficiency. SEaaS demonstrates approximately a 25% reduction in processing time compared to other models, primarily due to transaction validation and confirmation times. Different blockchain forms may vary in confirmation times, affecting processing times. SEaaS supports concurrency and parallelism within smart contract design, offering performance not typically observed in conventional data-sharing schemas.

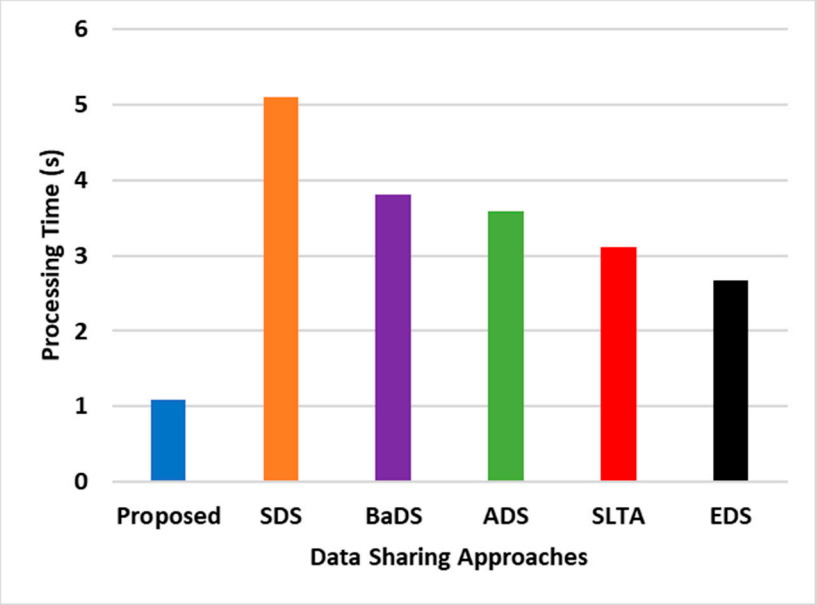

Figure 5. Comparative assessment of processing time.

6. Discussion and Conclusions

This manuscript has presented an insight into a novel arena of highly networked and structured business processes associated with the sensory data and services currently protected by the blockchain. Reviewing the existing literature, various loopholes have been noted in catering to sensing as a service in IoT, viz., the lack of accountability, a smaller number of prominent studies towards sensing as a service, the adoption of stale IoT architecture, and complex data/block management. Such forms of identified research challenges have been addressed in the proposed study model. Therefore, it acts as the overall relevance of the discussed model in which the identified issues are solved by introducing a novel data-sharing process using a decentralized blockchain with unique internal operations involved in smart contracts.

The proposed study model significantly addresses the prevailing challenges of delivering sensing as a service, revealing a novel IoT architecture enhanced by decentralized blockchain operations. This architectural innovation improves the Sensor-as-a-Service (SEaaS) model, ensuring enhanced accountability and effective block management, thereby facilitating an efficient relay of services within the IoT environment. The SEaaS framework, strategically designed for adaptability within a smart city context, co-ordinates synchronized interactions between sellers, buyers, and service providers to ensure secure and trustworthy transactions. At its core, the study unveils a systematically developed smart contract design rich in exclusive operations such as data-sharing, enrollment management, and diverse aspects of transaction validation, ensuring a seamless and effective trading process within SEaaS. This innovative approach is strengthened by a distinct configuration and enrollment management process, a crucial improvement designed to enhance the accountability of each blockchain transaction, addressing a significant gap in current research paradigms. A sophisticated management strategy further distinguishes the model, allowing for a fine-tuned multi-level identification of actors and an efficient transaction process, all achieved without imposing undue computational burdens on constrained sensor resources. Benchmark evaluations of this innovative scheme highlight its superiority, demonstrating remarkable improvements in throughput, energy consumption, latency, and processing time. Apart from this, it is also essential to offer a brief overview of the research questions and their solutions obtained from the study.

- RQ1: How can effective data-sharing methods be developed to enhance SEaaS within a large and decentralized network?

- Solution: The proposed system introduces a highly interconnected and collaborative network system in which the seller's information is subjected to better exposure by prospective buyers and protected using a simplified encryption operation. A specific attribute μ_1 has been used for performing data-sharing operations, which is also an integral part of the smart contract system. Apart from this, the adoption of decentralized Ethereum has been shown to use a specific configuration stage using public key attributes. Moreover, the proposed model also involves a particular module for managing sensed information in IoT, which makes the data and its associated computation much easier and faster, even for concurrent buyers.

- RQ2: What procedures can be implemented to enhance accountability among all stakeholders involved in SEaaS, while maintaining cost-effectiveness?
  - Solution: The complete system is developed using a 'no trust'-based approach where all the actors involved in the system are subjected to an enrollment process. This process uses the public key, original identity, supporting, and signature attributes. Further, the Elgamal signature is used to secure the attributes. When subjected to Ethereum, all these attributes are computationally complex to be unnoticed in case of malicious activity. Hence, it is a robust trapdoor function that offers higher forward/backward secrecy and maintains higher accountability for all the actors involved. It is cost-effective and can be justified by the lower algorithm processing time obtained in the benchmarked outcomes.
- RQ3: How can a system model of SEaaS be developed to facilitate practical deployment within an IoT environment?
  - Solution: The proposed system has developed an analytical model whose deployment scenario is chosen to work in a distributed and decentralized manner. For this purpose, a practical case study of a manufacturing firm (shown in Figure 1) has been used for modeling, while this architecture offers omnidirectional connectivity to all the actors with robust security rules using Ethereum. Hence, any individual actor or organization can easily use this environment without involving potential re-engineering processes in their existing networks.

The far-out consequences, as well as potential advantages of employing the presented scheme, are as follows:

- The proposed SEaaS model introduces an explicit operation towards relaying sensing data as a service, considering four prominent actors, viz., the seller, buyer, service provider, and blockchain, in a more comprehensive manner. This architectural deployment can be carried out by various users ranging from personal individuals to corporate service providers or the manufacturing industry.
- The proposed deployment architecture is designed flexibly, which any industry can adopt without demanding a complex re-engineering process. The ideal setting is to follow the data-sharing protocols, and the rest of the internal operations are autonomously carried out by the proposed study model.
- One of the most beneficial consequences and advantages of the proposed model is associated with sale management, request management, feedback management, and the validation operation, which not only enhances the current productivity of sales but also offers potential security against any uncertain threats.
- The proposed model is deployed with a unique configuration process and enrollment management, which is meant to retain a maximum level of accountability for every transaction process suitable for both the buyer and seller, irrespective of any domain of services being offered via IoT.
- The cost-effectiveness of the proposed model can be realized owing to its inclusion of the unique management of sensed information where a multi-level identification of

actors and various transaction processes is carried out without inducing any computational burden on resource-constrained sensors.

A possible limitation of the proposed model is the need for a dedicated module for optimizing the performance of the blockchain to more complex networks. Future advancements are anticipated to refine the blockchain's smart contract management within the SEaaS model, targeting enhanced optimization and sustainability. An investigation into deep learning is expected to reveal advanced predictive analytics, fostering optimal convergence and improving performance. Emphasis will also be directed toward minimizing computational efforts through complex data augmentation strategies aligned with prevailing market demands. Additionally, significant efforts will be made towards developing robust security infrastructures to neutralize emergent threats such as AI-driven cyber-attacks, ensuring uninterrupted and secure data transactions within the enhanced SEaaS ecosystem.

Author Contributions: Conceptualization, methodology, validation, and writing—review and editing: B.U.I.K., K.W.G. and M.S.M.; formal analysis, and investigation: A.A.M., M.C. and N.F.L.M.R.; writing—original draft preparation: B.U.I.K. and K.W.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the INTI IU Research Seeding Grant Phase 1/2023 initiative under Project Number: INTI-FDSIT-01-01-2023, and the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Project Grant 6,177.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors express their appreciation for the effort of Bisma Rasool in proofreading and editing the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ashraf, Q.M.; Tahir, M.; Habaebi, M.H.; Isoaho, J. Toward autonomic internet of things: Recent advances, evaluation criteria, and future research directions. *IEEE Internet Things J.* **2023**, *10*, 14725–14748. [CrossRef]
2. Li, J.; Liang, W.; Xu, W.; Xu, Z.; Li, Y.; Jia, X. Service home identification of multiple-source IoT applications in edge computing. *IEEE Trans. Serv. Comput.* **2023**, *16*, 1417–1430. [CrossRef]
3. Olanrewaju, R.F.; Khan, B.U.I.; Hashim, A.H.A.; Sidek, K.A.; Khan, Z.I.; Daniyal, H. The Internet of Things Vision: A Comprehensive Review of Architecture, Enabling Technologies, Adoption Challenges, Research Open Issues and Contemporary Applications. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2022**, *26*, 51–77. [CrossRef]
4. Chen, F.; Xiao, Z.; Xiang, T.; Fan, J.; Truong, H.-L. A full lifecycle authentication scheme for large-scale smart IoT applications. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 2221–2237. [CrossRef]
5. Alobaidy, H.A.H.; Jit Singh, M.; Behjati, M.; Nordin, R.; Abdullah, N.F. Wireless transmissions, propagation and channel modelling for IoT technologies: Applications and challenges. *IEEE Access Pract. Innov. Open Solut.* **2022**, *10*, 24095–24131. [CrossRef]
6. Schrettenbrunner, M.B. Artificial-intelligence-driven management: Autonomous real-time trading and testing of portfolio or inventory strategies. *IEEE Eng. Manag. Rev.* **2023**, *51*, 65–76. [CrossRef]
7. Abeysekara, P.; Dong, H.; Qin, A.K. Edge intelligence for real-time IoT service trust prediction. *IEEE Trans. Serv. Comput.* **2023**, *16*, 2606–2619. [CrossRef]
8. Mazon-Olivo, B.; Pan, A. Internet of things: State-of-the-art, computing paradigms and reference architectures. *IEEE Lat. Am. Trans.* **2022**, *20*, 49–63. [CrossRef]
9. Liu, Y.; Yu, W.; Rahayu, W.; Dillon, T. An evaluative study on IoT ecosystem for smart predictive maintenance (IoT-SPM) in manufacturing: Multiview requirements and data quality. *IEEE Internet Things J.* **2023**, *10*, 11160–11184. [CrossRef]
10. Siddiqui, S.; Hameed, S.; Shah, S.A.; Ahmad, I.; Aneiba, A.; Draheim, D.; Dustdar, S. Toward software-defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects. *IEEE Access Pract. Innov. Open Solut.* **2022**, *10*, 70850–70901. [CrossRef]

11. Martin, S.; Soldatos, J.; Cousin, P.; Maló, P. Internet of things experimentation: Linked-data, sensing-as-a-service, ecosystems and IoT data stores. In *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*; River Publishers: Gistrup, Denmark, 2022; pp. 261–277.
12. Vermesan, O.; Friess, P. *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*, 1st ed.; River Publishers: New York, NY, USA, 2022.
13. Ekman, K.; Weilenmann, A. Behind the scenes of planning for public participation: Planning for air-quality monitoring with low-cost sensors. *J. Environ. Plan. Manag.* **2021**, *64*, 865–882. [CrossRef]
14. Symeonaki, E.; Arvanitis, K.; Piromalis, D. A context-aware middleware cloud approach for integrating Precision Farming facilities into the IoT toward Agriculture 4.0. *Appl. Sci.* **2020**, *10*, 813. [CrossRef]
15. Albreem, M.A.; Sheikh, A.M.; Alsharif, M.H.; Jusoh, M.; Mohd Yasin, M.N. Green internet of things (IoT): Applications, practices, awareness, and challenges. *IEEE Access Pract. Innov. Open Solut.* **2021**, *9*, 38833–38858. [CrossRef]
16. Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Blockchain for the Internet of Vehicles: A decentralized IoT solution for Vehicles communication using Ethereum. *Sensors* **2020**, *20*, 3928. [CrossRef] [PubMed]
17. Arshad, Q.-U.-A.; Khan, W.Z.; Azam, F.; Khan, M.K.; Yu, H.; Zikria, Y.B. Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges. *Complex Intell. Syst.* **2023**, *9*, 6155–6176. [CrossRef]
18. Deniziak, S.; Płaza, M.; Arcab, Ł. Approach for designing real-time IoT systems. *Electronics* **2022**, *11*, 4120. [CrossRef]
19. Chiti, F.; Gandini, G. Distributed ledger as a service: A Web 3.0-oriented architecture. *J. Sens. Actuator Netw.* **2023**, *12*, 57. [CrossRef]
20. Jin, W.; Kim, D. Distributed rule-enabled interworking architecture based on the transparent rule proxy in heterogeneous IoT networks. *Sensors* **2023**, *23*, 1893. [CrossRef] [PubMed]
21. He, Q.; Liu, Y.; Jiang, L.; Zhang, Z.; Wu, M.; Zhao, M. Data sharing mechanism and strategy for multi-service integration for smart grid. *Energies* **2023**, *16*, 5294. [CrossRef]
22. Sun, S.; Du, R.; Chen, S. A secure and computable blockchain-based data sharing scheme in IoT system. *Information* **2021**, *12*, 47. [CrossRef]
23. Razzaq, A.; Altamimi, A.B.; Alreshidi, A.; Ghayyur, S.A.K.; Khan, W.; Alsaffar, M. IoT data sharing platform in web 3.0 using blockchain technology. *Electronics* **2023**, *12*, 1233. [CrossRef]
24. Albulayhi, A.S.; Alsukayti, I.S. A blockchain-centric IoT architecture for effective smart contract-based management of IoT data communications. *Electronics* **2023**, *12*, 2564. [CrossRef]
25. Fukuda, H.; Gunji, R.; Hasegawa, T.; Leger, P.; Figueroa, I. DSSM: Distributed Streaming data Sharing Manager. *Sensors* **2021**, *21*, 1344. [CrossRef] [PubMed]
26. Priyadharshini, K.; Canessane, A. Security in data sharing for blockchain-intersected IoT using novel chaotic-RSA encryption. *Int. J. Inf. Secur. Priv.* **2022**, *16*, 1–15. [CrossRef]
27. Zhang, Y.; He, D.; Choo, K.-K.R. BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 2783658. [CrossRef]
28. Wu, T.; Wang, W.; Zhang, C.; Zhang, W.; Zhu, L.; Gai, K.; Wang, H. Blockchain-based anonymous data sharing with accountability for internet of things. *IEEE Internet Things J.* **2023**, *10*, 5461–5475. [CrossRef]
29. Shi, P.; Wang, H.; Yang, S.; Chen, C.; Yang, W. Blockchain-based trusted data sharing among trusted stakeholders in IoT. *Softw. Pract. Exp.* **2021**, *51*, 2051–2064. [CrossRef]
30. Zhang Yue Gai, K.; Xiao, J.; Zhu, L.; Choo, K.-K.R. Blockchain-empowered efficient data sharing in Internet of Things settings. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 3422–3436. [CrossRef]
31. Debauche, O.; Nkamla Penka, J.B.; Hani, M.; Guttadauria, A.; Ait Abdelouahid, R.; Gasmi, K.; Ben Hardouz, O.; Lebeau, F.; Bindelle, J.; Soyeurt, H.; et al. Towards a unified architecture powering scalable learning models with IoT data streams, blockchain, and open data. *Information* **2023**, *14*, 345. [CrossRef]
32. Olaniyi, O.M.; Alfa, A.A.; Umar, B.U. Artificial intelligence for demystifying blockchain technology challenges: A survey of recent advances. *Front. Blockchain* **2022**, *5*, 927006. [CrossRef]
33. Zichichi, M.; Ferretti, S.; Rodríguez-Doncel, V. Decentralized personal data marketplaces: How participation in a DAO can support the production of citizen-generated data. *Sensors* **2022**, *22*, 6260. [CrossRef] [PubMed]
34. Fallatah, K.U.; Barhamgi, M.; Perera, C. Personal Data Stores (PDS): A review. *Sensors* **2023**, *23*, 1477. [CrossRef] [PubMed]
35. Palaiokrassas, G.; Skoufis, P.; Voutyras, O.; Kawasaki, T.; Gallissot, M.; Azzabi, R.; Tsuge, A.; Litke, A.; Okoshi, T.; Nakazawa, J.; et al. Combining blockchains, smart contracts, and complex sensors management platform for hyper-connected SmartCities: An IoT data marketplace use case. *Computers* **2021**, *10*, 133. [CrossRef]
36. Almstedt, L.; Bleeke, K.; Mahhouk, M.; Jehl, L.; Kapitza, R.; Wolf, L. ContractBox: Realizing accountable data sharing on the edge using a small scale blockchain. *Comput. Netw.* **2023**, *229*, 109768. [CrossRef]
37. Bentahar, A.; Meraoumia, A.; Bradji, L.; Bendjenna, H. Sensing as a service in Internet of Things: Efficient authentication and key agreement scheme. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5493–5509. [CrossRef]
38. Al Mahamid, F.; Lutfiyya, H.; Grolinger, K. Virtual sensor middleware: Managing IoT data for the fog-cloud platform. In Proceedings of the 2022 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Halifax, NS, Canada, 18–20 September 2022. [CrossRef]

39. Mohamed, N.; Al-Jaroodi, J.; Lazarova-Molnar, S.; Jawhar, I. Applications of integrated IoT-fog-cloud systems to smart cities: A survey. *Electronics* **2021**, *10*, 2918. [CrossRef]
40. Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Sensing technologies for crowd management, adaptation, and information dissemination in public transportation systems: A review. *IEEE Sens. J.* **2023**, *23*, 68–87. [CrossRef]
41. Othman, R.A.; Darwish, S.M.; Abd El-Moghith, I.A. A multi-objective crowding optimization solution for efficient sensing as a service in virtualized wireless sensor networks. *Mathematics* **2023**, *11*, 1128. [CrossRef]
42. Mathew, S.S.; El Barachi, M.; Kuhail, M.A. CrowdPower: A novel crowdsensing-as-a-service platform for real-time incident reporting. *Appl. Sci.* **2022**, *12*, 11156. [CrossRef]
43. Hoque, M.A.; Hossain, M.; Noor, S.; Islam, S.M.R.; Hasan, R. IoTaaS: Drone-based internet of things as a service framework for smart cities. *IEEE Internet Things J.* **2022**, *9*, 12425–12439. [CrossRef]
44. Woodward, B. Remote big data management and visual imagery tools, multisensor fusion and dynamic routing technologies, and 3D space mapping and object recognition algorithms on blockchain-based metaverse platforms. *Linguist. Philos. Investig.* **2023**, *22*, 60–76. [CrossRef]
45. Grupac, M.; Negoianu, A.E. Immersive extended reality and sensor-based object recognition technologies, socially-oriented location tracking and simulation modeling tools, and artificial vision and haptic augmented reality systems in the metaverse interactive environment. *Rev. Contemp. Philos.* **2023**, *22*, 226–243. [CrossRef]
46. Olanrewaju, R.F.; Khan, B.U.I.; Goh, K.W.; Hashim, A.H.A.; Sidek, K.A.B.; Khan, Z.I.; Daniyal, H. A holistic architecture for a sales enablement sensing-as-a-service model in the IoT environment. *Information* **2022**, *13*, 514. [CrossRef]