Blockchain-based solutions for privacy in the Internet of Things Smart Environment

Author: Shubhankar Darbari[1] , **Supervisor: Miray Ayşen**[1] , **Responsible Professor: Zekeriya Erkin**[1]

[1]Cyber Security Group
Department of Intelligent Systems
Delft University of Technology

Abstract

The expansion of the Internet and wireless access has led to a widespread increase of Internet of Things applications. These smart devices are becoming a daily aspect of our lives. All the convenient and automated services provided by smart devices come from a centralized service provider. This service provider has access to all the personal data associated with the devices and hence, poses a threat to users' data privacy. Blockchain-based applications provide many desirable features for the IoT infrastructure, for example, decentralization, trust, and immutability. This paper discusses the integration of blockchain and IoT while expanding upon existing studies in a smart home environment where privacy needs immediate attention. Furthermore, different privacy-preserving mechanisms used in blockchain-based IoT solutions were classified and analyzed. The evaluation reflects that cryptographic solutions enhance overall privacy in terms of data confidentiality and untraceability but are low utility solutions for resource-constrained IoT. An effective balance can be found in data manipulation solutions. Finally, suggestions and future research directions on the subject of privacy in blockchain-based IoT systems are offered as a result of this review.

1 Introduction

The term 'Internet of Things' or IoT was first observed in 1999 [1]. Now, it is a modern technology that allows various devices to connect to the Internet and communicate with one another. It is expected to grow to 50 billion devices by the end of 2025 [2]. This steady growth can be explained by the expansion of the Internet and wireless access. An IoT smart environment is an ecosystem of smart devices. These devices are permeating many aspects of our daily life and automating tasks for us [3].

One such example of an IoT smart environment is the smart home system, it consists of all the smart appliances in our home, like smart lights, entertainment system, and more. Despite the multiple benefits of IoT, personal data and information are often stored, mishandled, and misused, posing a threat to users' data privacy. Smart home appliances can record the users' offline activities in their personal space and transmit data about them to the Internet [4]. State-of-the-art IoT systems are centralized which means the services provided by the smart devices are obtained from a centralized server. Sending highly sensitive data to centralized companies poses a significant threat to users' privacy as they have little knowledge of the whereabouts of their data [5]. In addition to the privacy concerns, the current devices are expected to address challenges such as higher costs, single point of failure for data (centralized clouds), and inefficiency due to the expansion of IoT [2]. A decentralized private-by-design IoT architecture is required for efficient resource utilization and protection of users' right to privacy [6] as it eliminates the need of entrusting data to centralized companies.

Blockchain is one of the different types of distributed ledger technology. It is, in essence, a decentralized, distributed, and immutable ledger that can be seen as a potential solution to the IoT challenges. The integration of the two technologies can be advantageous as blockchain delivers better security and privacy for the user and device data by utilizing sophisticated cryptography algorithms and providing a secure computing environment. However, there are some issues when combing blockchain with IoT [7] that need to be looked into. The blockchain network must meet the demand for increasing user privacy, taking into account the limited resources of IoT devices and the adaptability of itself in IoT.

In this paper, we answer the following sub-questions:

- What are the current challenges in IoT devices and what role can blockchain play in the integration of these technologies?
- What are the privacy requirements in IoT devices?
- What are the different methods for preserving privacy in blockchain-based decentralization for IoT smart homes, and how do they work?
- What evaluation methodology can be implemented on industry-based use cases for privacy assessment in blockchain-based IoT frameworks?
- What blockchain-based IoT frameworks have an efficient privacy-preserving method that justifies overhead of blockchain in IoT devices?

Keeping in mind the sub-questions and motivation of en-

hancing privacy in IoT, here are the main contribution of this research:

- Chronological assessment of trends in literature from the past 5 years.
- Comparative analysis of real-time industry-based use cases or case study implementation of privacy-preserving frameworks.
- Identification of the privacy-preserving mechanisms in blockchain-based applications
- Exploration into the extent to which data privacy could be improved in blockchain-based IoT applications.

The work presented in this paper builds on previous research to explore the available privacy mechanism in a blockchain-based IoT smart home system. The remainder of the paper is organized as follows. Related works are discussed in Section 2 followed by Section 3 that presents the methodology of the research. Section 4 provides the necessary background information. A detailed analysis of different privacy-preservation mechanisms is presented in Section 5. Section 6 discusses the evaluation of the research. Furthermore, Section 7 discusses responsible research. Finally, conclusions with future research directions are explored in Section 8.

2 Related works

In recent years, IoT and blockchain have keened the interests of researchers. In this section, some of the researched works are discussed with an updated view of insights gained from them which includes solutions for the IoT environment, and potential challenges of a decentralized IoT.

In [8], a thorough review of how can blockchain be adapted to meet the requirements of IoT is presented. The paper addresses the current challenges and optimizations regarding many aspects of a Blockchain-based IoT (BIoT) application, where privacy is one of the aspects. It discusses the main challenges of privacy as the auditability of blockchain in IoT since smart devices can reveal personal or private user data that could be stored on the blockchain. The mechanisms compared in this paper are also discussed in the later section of this paper. Furthermore, it concludes with future research directions for the optimized BIoT designs as IoT devices can be resource-constrained. In [7], the authors discussed the research challenges and opportunities in this field along with different integration schemes for blockchain and IoT. In addition, the study in [7] presents a detailed analysis of recent research efforts in IoT privacy where the integration with blockchain is proven to have a meaningful impact. Authors of [9] proposed a lightweight blockchain by eliminating the consensus mechanism to account for the limitations in IoT devices in smart homes. According to the researchers, this is the first study aimed at optimizing blockchain in the context of smart homes. However, it mainly discusses the overhead of blockchain and not an in-depth review of privacy in smart homes. From a recent paper [10], privacy challenges were discussed in the physical layer of IoT architecture where the devices collect a large volume of data from the environment and how privacy preservation techniques are needed to be designed.

3 Methodology

Since this paper is a comparative study, research takes precedence in the methodology. Blockchain, being a nascent research topic, requires rigorous and traceable study and design for creating or writing frameworks and case studies. This research follows the recommendations as stated in [11]. As a research project, this paper follows the guidelines as described in [12] for evaluation and iteration within the scope of this research. The paper will follow the following guidelines by Hevner *et al.*:

- This study produces a practical artifact in the structure of a method.
- This study aims to develop technology-based solutions to a relevant business problem.
- This study's quality is rigorously demonstrated by a well-executed evaluation method.
- This study provides transparent and verifiable contributions.
- This study is based on the use of rigorous procedures in both the production and assessment of the artifact.
- This study makes use of existing resources to achieve desired results while adhering to the laws of the problem environment.
- This study effectively communicates to both technology-oriented and management-oriented audiences.

Furthermore, the search strings "Blockchain AND IoT AND Privacy ["review", "literature review" OR "survey"]", "Blockchain AND IoT AND Privacy AND smart home [interval: 2017-2021]" were used in Google Scholar to obtain the data set for the research and to achieve the stated results, the paper aims to review the technologies generated from the search result, as well as implementations in the industry. The solutions will be compared in the aspects of privacy features such as data confidentiality, untraceability, user anonymity, and privacy risks such as data misrouting, linkability, and performance of blockchain in the Section 5.2.

4 Background

In this section, we discuss blockchain and IoT technology. The first subsection focuses on blockchain, its feature, types, and applications. This is followed by an overview of IoT technology, then privacy in the current IoT model, integration of blockchain in an IoT smart environment, and lastly, the challenges of privacy that need to be addressed.

4.1 Overview of Blockchain

Blockchain is a database that documents transactions among participating parties in an immutable ledger. The blockchain network is a peer-to-peer network, which means there are no centralized clouds. After a transaction has been acknowledged and cryptographically verified by other network participants or nodes, it is added to the blockchain as a 'block'. A

block contains information about the transaction's time of occurrence, previous transactions, and transaction details. Since the blocks contain the previous node's hash, it forms a 'chain' of blocks where the first block is known as the genesis block. This digital ledger is duplicated and distributed across the entire network of computer systems on the blockchain [13].

Features of Blockchain

According to [14], the most important features of blockchain technology are summarized as follows.

- *Decentralization*: In a blockchain-based system, there is no trusted central authority that validates the transactions or data exchange like in that of a centralized network infrastructure.
- *Persistency*: One of the main features of Blockchain is to create an immutable ledger. All network participants agree upon a decentralized consensus, which makes the blockchain tamper-resistant. Since all the nodes are immutable, an attacker would need to alter the majority of nodes in the blockchain for a successful attack, otherwise, any change would be easily detected.
- *Auditability*: The ledger is distributed across the network. This allows transparency among the participating parties to acknowledge any data exchange of a particular blockchain address.
- *Anonymity*: The users can have a self-generated address for any interaction with the blockchain. Furthermore, they can generate a list of addresses ahead of time in order to conceal their identity. The decentralized nature of blockchain also prevents the user's real identities to be exposed from a single point of failure. In this way, blockchain protects user privacy to a certain extent.

Types of Blockchain

Blockchain can be categorized into three types based on authentication and control mechanisms [5].

- *Public Blockchain*: Blockchain in which all members can access and add to the ledger content. Public blockchains are termed *permissionless* as it allows everyone in the network to keep a copy of the ledger. Bitcoin is an example of a public blockchain.
- *Private Blockchain*: Compared to that of public blockchains, a private blockchain is termed as *permissioned*, and every network node is a recognized member of a particular organization.
- *Consortium Blockchain*: A consortium blockchain is also a permissioned blockchain network. It can encompass many organizations and aid in maintaining transparency among the stakeholders involved.

Blockchain-based Platforms for IoT

Industries that employ blockchain technology, such as Unilever, Walmart, Visa, and others, have reaped benefits in terms of transparency, security, and traceability. [15]. Among these various domains is the IoT system.

For implementing blockchain with IoT systems, the primary step is to choose the blockchain-based platform which can be adapted to merge with IoT. The most widely used platforms that can be utilized in the implementation of BIoT are Ethereum, Hyperleder, and IOTA as in addition to being open-source, the platforms efficiently connect blocks with minimal overhead for transactions [16].

- *Ethereum*: A multipurpose blockchain that is used to develop blockchain-based applications. Ethereum claims itself as the 'world's first programmable blockchain'.
- *Hyperledger*: An open-source blockchain-based platform focused on developing permissioned, enterprise-grade blockchain solutions. Fabric is one of Hyperledger's sub-projects.
- *IOTA*: A Tangle-based distributed ledger technology which is not considered as one of the blockchain-based platforms but reviewed in this paper due to its relevance to IoT.

4.2 Overview of Internet of Things

Internet of Things abbreviated as IoT is the future of communication technology [3]. It is a network of physical objects connected and communicating through the Internet. The 'things' that connect and exchange data over the internet are primarily embedded with sensors, nanotechnology, software, and other relevant technologies without requiring any human-to-machine or human-to-human interaction [17].

Goyal *et al.* [17] categorize the challenges faced by IoT devices into the following categories: privacy, security, accountability, legal and general. The privacy issues arise from the sensitive data stored and exchanged by IoT-enabled devices. This data should not be used without the consent of the owner. Security issues arise due to the limited resources in IoT. Accountability and legal issues arise due to the lack of trust in these devices. A general concern in IoT devices is the centralized nature of this technology. If the cloud server fails, the whole network bears the repercussions [2].

Privacy in Centralized IoT

In the state-of-the-art IoT ecosystem, all the convenient services come from a centralized service provider, which analyses and manages sensor or appliance data gathered from the smart home system. The centralized nature of smart home appliances presents privacy concerns for users' data. The sheer volume of data being collected, transmitted, stored, and potentially being sold [5].

Users are required to put their trust in the companies that provide Internet-based services. They have little to no understanding of the personal data that is transmitted, stored, or sold to third-party entities. Users must not only trust centralized services to protect their privacy, but they must also trust that their data is handled in a secure way. Malicious parties can eavesdrop and acquire data without authorization when dealing with unprotected data [5].

The state-of-the-art privacy-preserving solution involves users passing via a privacy broker [18], which is essentially an intermediate entity between the consumer and the IoT network which can be prone to threats [5].

Blockchain-based Smart Home

One of the most common IoT use cases is the smart home, which has already established itself as an integral part of

the digital revolution [19]. A smart home generally consists of devices like lighting, temperature, and entertainment controls, with the goal of automating tasks and providing smart services to the residents of the home. However, these devices pose a threat to users' privacy as the IoT data processed in smart homes is mainly personal. The current architecture depends upon the centralized cloud services with a single access point for data management and consequently originate data transparency, privacy, and trust issues [20].

Researchers have proven that most smart home devices lack fundamental security measures and could be easily compromised [21]. Blockchain functionality can improve the security and privacy of personal data in smart homes by enabling trustworthy, transparent, and secure sharing services [19]. Blockchain offers several advantages to IoT, but it must also meet security and privacy standards in order to be appropriate for integration.

The scope of this paper is limited to the privacy requirements of a blockchain-based smart home. According to [19], the privacy requirements can be summarized as:

- Implementation of permissioned and restricted configuration is required to secure sensitive IoT data from unauthorized entities.
- Adaptation of appropriate cryptographic primitives for the resource-constrained IoT devices.
- Addition of several privacy-enhancing techniques depending on the context of the application.
- Consideration of data rights on processing of an individual's personal data.

Section 5.1 discusses the privacy-preserving mechanisms in relation to the relevant blockchain platforms and frameworks.

Privacy challenges in BIoT

Users are subject to privacy threats such as linking attacks and illicit data mining, as a result of the distributed nature of blockchain and the sensitive data stored by IoT. An attacker tries to find information connected to a user's private data in a linking attack [22]. This data may be used to create user profiles or anticipate patterns. In this section, privacy concerns are generalized into user-oriented and device-oriented privacy [23]. As shown in Figure 1, each category of the privacy challenges is divided into subcategories which are explained as follows.

- *User profiling*: Profiling is the process of describing a user's activity, for instance, their daily routines or activities. In a BIoT system, a user's future pattern or profile can be anticipated based on the data published by the devices on the blockchain. For example, a smart home system may be aware of a user's absence according to their schedule, or it may convey future energy usage of a device [24].
- *User identification*: Similar to user profiling, users can be identified based on the information supplied by the devices in the smart environment [23].
- *Device profiling*: As more and more smart devices get connected to the Internet, more private and sensitive data will be produced. Misuse of information pertaining to the ownership, identification, and capabilities of devices may result in device profiling issues [23].
- *Targeted advertisements*: User's private logged data can be used by malicious members (for example, a service provider) in the smart environment to send customers targeted advertisements [25]. This information can be derived from a particular IoT device making this a device-oriented privacy issue.

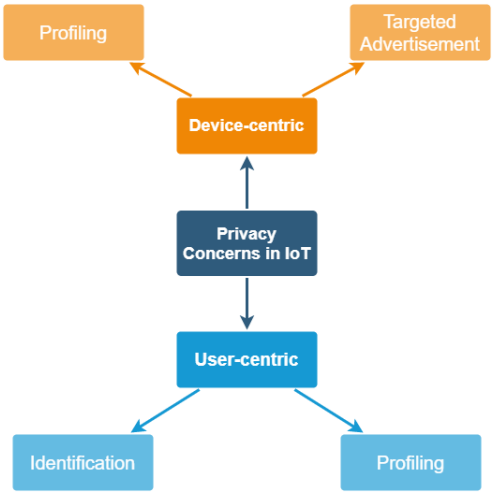

Figure 1: Privacy challenges in blockchain-based IoT

5 Analysis

In this section, different privacy-preserving mechanisms are described followed by an evaluation based on privacy features and risks. The mechanism can be divided into three categories, namely cryptographic solutions, data manipulations, and trust-based solutions.

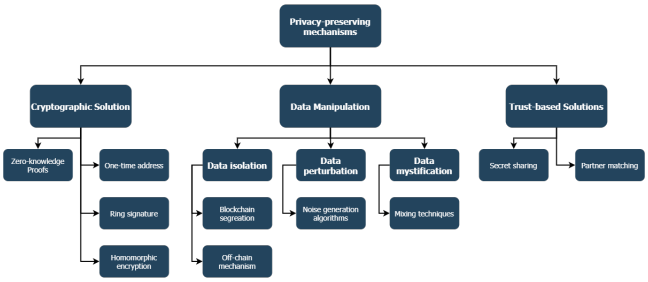

Figure 2: Privacy-preserving mechanisms in Blockchain-based IoT frameworks

5.1 Privacy-preserving mechanisms

As shown in Figure 2, the mechanisms are discussed by a short description followed by the framework or platform employing it and lastly, a general analysis of the mechanism. Pseudonymization technique is available in all frameworks, hence excluded from the figure.

Pseudonymization

Pseudonymization is the processing of private data in such a way that the data is no longer linked or ascribed to the specific user without the use of any extra information [19]. Usually, user identifiers are replaced by pseudonyms in order to achieve pseudonymization.

This technique can be seen in a public financial transaction where there is no straightforward way to map the amounts of cryptocurrency to an individual [19]. Similarly, in any blockchain application, pseudonymous data can be stored on the ledger. For instance, a user's identifiers can be replaced with pseudonyms in a smart environment. This pseudonymous data is still personal data and depending on the technique and the information available, it can be linkable to the user. For instance, Bitcoin [26], a blockchain-based digital currency had 3760 traced cases of bitcoin transactions by a former federal agent over 12 months [27].

One-time address

The one-time address refers to the technique of establishing an unique or 'stealth' address for each transaction or data with a particular user. More precisely, by appropriately using cryptographic algorithms in order to enhance untraceability for the latter [28].

The author of [28] performed a theoretical analysis on the proposed solution of faster Dual-Key Stealth Address Protocol (DKSAP) especially for IoT devices which can achieve at least 50% performance improvement on the original DKSAP. DKSAP uses two cryptographic keys namely, 'scan' and 'spend' keys and computes a one-time address for each transaction.

It can be observed that the classical one-time address might not be a practical solution in IoT devices, as the devices need to transmit data constantly which imposes a heavy computational burden by generating new addresses for every transaction.

Mixing techniques

The mechanism of the mixing technique enables multiple users to shuffle multiple transactions making them unlinkable [29]. Coin-Shuffle [29] is an example of this technique in the context of blockchain. It can be used to hide the history of a particular user as the 'mixed' transactions correspond to multiple senders and receivers making the data linkability for a single user difficult.

Despite the untraceability, mixing techniques have lower user anonymity levels and can be compromised by intersection attacks [30]. Furthermore, a notion of added complexity is introduced by mixing transmitted data.

Ring signature

Ring signature refers to the public verification of the signature by a group member without exactly identifying the actual signer [31]. Authors of [31] presented a lightweight ring signature technique for resource-constrained networks such as IoT networks. Each signature has added uniqueness for enhancing protection. The study in [32] shows that the implied privacy is directly proportional to the group size 'r'.

Although the user or group anonymity can be preserved by using ring signatures, the transaction ledge is not confidential which can lead to linkability of the signature and receiver [33].

Homomorphic encryption

Homomorphic encryption is a type of encryption that includes the ability to compute over encrypted data without knowing the secret key. [34]. The output generated by the computation over encrypted data is the same as the output by the same operation over plain text. Ethereum has an AZTEC protocol, which is based on cryptographic solutions like homomorphic encryption over the inputs and outputs of a transaction, along with testing the logical correctness of the encryptions [19].

In the proposed solutions by [35], a homomorphic consortium blockchain model is presented for the smart home system. The model largely guarantees the security of data and was evaluated thoroughly.

Despite the high privacy preservation provided by homomorphic encryption, it usually has limited homomorphic operation [34]. In addition, IoT devices also need to handle the computational burden imposed by this encryption.

Zero-knowledge proofs

A zero-knowledge proof (ZKP) is a cryptographic solution that allows a party or an entity to prove to another party that they possess knowledge without conveying any computational information [45]. In the context of blockchain, ZKPs are being re-explored and utilized to construct confidential transactions. Blockchain platforms like Ethereum employ ZKP as one of their protocols [19].

Unfortunately, the high computation and memory usage of ZKPs limits their suitability with blockchain-based IoT. As stated in [37], Zerocoins transaction is longer than 45kB and requires 450ms for verification.

Zerocash [37], a ledger-based currency based on decentralized anonymous payments leveraged zero-knowledge proofs. Apart from providing anonymous transactions, the transaction details are also hidden in Zerocash. The framework of Zerocash uses the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge which means that the proofs can be verified within a few milliseconds and the proof consists of a single message from the prover. Less expensive cryptographic solutions can ensure data compression and verifiability between many parties but it is still a constantly evolving field [19].

Differential privacy

Differential privacy (DP) is a form of data perturbation, and it can maintain the confidentiality of data without endangering data leakage [30].

In the survey [39], Hassan *et al.* discuss the efficient perturbation methods to enhance privacy in the blockchain. It also states how DP can be used in the current blockchain platforms and architecture. The survey compares various DP solutions in blockchain-based applications, where the IoT domain is also one of the discussed applications. To the best of our knowledge, there are not many DP solutions for blockchain-based smart homes but it can be said with high assurances that these solutions are an effective solution for IoT domains [39] including smart homes.

Table 1: Comparison of the aforementioned mechanisms

Privacy mechanism	Proposed solution/platform(s)	Feature(s)	Risk(s)
One-time address	[28], Ethereum	• User Anonymity • Untraceable data	• Computational burden • Unencrypted data
Mixing technique	[29], IOTA [36]	• Untraceable data	• Increased complexity • Low anonymity
Ring signature	[31]	• User Anonymity • Untraceable data • Encrypted data	• Signature reuse • Address correlation
Homomorphic encryption	[35], Ethereum	• User Anonymity • Untraceable data • Encrypted data	• Computational burden
Zero-knowledge proof	[37], Ethereum, Fabric [38]	• User Anonymity • Untraceable data • Encrypted data	• Data misrouting • Computational burden
Differential privacy	[39]	• Lightweight • Confidential data	• Trade-off b/w privacy & accuracy
Off-chain mechanism	[40], [41], IOTA [36], Fabric [38]	• User Anonymity	• Linkable data • Traffic correlation
Partner matching	[42]	• User Anonymity • Confidential data	• Address correlation
Secret sharing	[43]	• User Anonymity • Confidential data	• High memory usage • Computational burden
Editable blockchain	[44]	• Blockchain features • Right to be forgotten	• Still in development

In the context of BIoT application, data perturbation-based mechanisms can be leveraged in the privacy preservation of IoT nodes' data. Although DP is a lightweight technique that can be utilized in the implementation of various BIoT applications, it comes with a choice of enhancing privacy or improving accuracy due to the added amount of noise [30].

Off-chain mechanism

In the case of the IoT ecosystem, not only peer-to-peer connection is required but also machine-to-machine transactions. Adding these transactions can increase the transaction processing and chances of compromising the user's privacy. The off-chain mechanisms refer to the deployment of an off-chain ledger linked to the on-chain ledger, which conserves the blockchain resources and conceals the personal data included in the off-chain ledger [40].

The authors of [41] presented an Exonum-based health data ecosystem. Exonum uses the principle of off-chain mechanism. In this example, the data is divided into two components - open and closed. The closed component stores the medical data whereas the open component stores the patient's identifier. Another example is the proposed solution by [46] which combines a blockchain (with access control enabled) with off-chain storage to store users' personal data.

It can be observed that with the introduction of a new chain/storage, the problems of increased cost, limited capacity of the new chain, and routing security are bound to occur.

Partner matching

Partner matching is the mechanism of matching an individual to another based on the preferences provided by that individual, privacy information is disclosed or shared when partners match. A simple instance that describes this mechanism would be the matching between buyers and sellers [42].

An example of this mechanism in a BIoT application is [47]. Laszka *et al.* introduced a trading algorithm in a distributed setting. By leveraging access control, offer and matches are made among users (prosumer) while preserving anonymity using mixing of transaction.

It can be observed that this type of matching relies heavily on the matching algorithm in terms of security, and computational overhead.

Secret sharing

In secret sharing, the hidden and sensitive value or information is "encrypted with a one-time secret with the receiver and attached to the transaction" [23]. According to [34], the main idea behind secret sharing was to partition the document between N users and only when *t* out of N users cooperate, the document can be reconstructed.

Authors of [43] put forward an attribute-based signature scheme with multiple authorities, "the patient endorses a message according to the attribute while disclosing no information other than the evidence that has been attested to it" [43]. Diffie-Hellman's (DH) key exchange is a way to securely generate cryptographic keys and it was used in the aforementioned solution to achieve privacy and become effective against predict attacks [23].

Editable blockchain

As the name implies, an editable blockchain is a blockchain that challenges the inherent immutable property of the blockchains. This immutability characteristic of blockchains leads to a data protection problem known as the 'right to be forgotten'. Although there are certain exemptions to this right, one should always consider how to handle such cases.

Authors of [44] explore the possibility of creating an editable blockchain (alias redactable blockchain) by using a certain hash function (chameleon hash function) to edit or delete data. This type of blockchain which is editable and preserves the other properties of blockchain can be desirable for IoT applications but unfortunately, it is a newly evolving research area of blockchains which is not been implemented yet.

5.2 Evaluation methodology

The following evaluation criteria are used to assess the quality of privacy provided by the aforementioned solutions. The criteria decided for this study were inspired from the evaluation framework in [23] and divided into two groups where the first group is the *features* that aim to enhance the overall privacy of the system whereas the other group is the *risks* associated with the mechanism. These criteria were mainly determined by studying the gaps in the literature with a focus on protecting user data in a smart home system. The groups are divided in such a way that they account for the privacy concerns discussed in Figure 1.

To the best of our knowledge, the features of a privacy mechanism in the scope of this research are:

- *Data confidentiality*: This criterion is a part of transaction privacy. It denotes the extent of confidentiality of the data which includes data encryption, obfuscation, or separation.
- *Data untraceability*: This criterion refers to the condition where an adversary is unable to find information about a transaction's content or the users or devices involved in the transaction.
- *User anonymity*: This criterion refers to different methods of hiding a user's identifier.

The risks are:

- *Performance concerns*: This criterion considers the capacity and size of a transaction along with the computational requirements of the solution.
- *Data linkability*: This criterion is basically the potential to correlate data from various sources.
- *Data misrouting*: This criterion refers to the risk of data leakage, token or signature reuse, and transaction misrouting.

Table 1 summarizes the main properties of the discussed privacy-preserving mechanism and their corresponding framework or platform. The pseudonymization feature is available in all frameworks, hence excluded from the table. It can be seen that the higher the privacy, the higher will be the computational, and resource consumption. From this observation, Section 6 aims to provide potentially higher utility privacy solutions for IoT smart homes.

6 Results and Discussions

From the Table 1, we observed the general qualities of a privacy-preserving mechanism. It can be said with confidence that achieving higher user and user data privacy requires high resource consumption, computational burden, and delayed response. Here are the highlighted results from this evaluation:

- Cryptographic solutions enhance overall data privacy and can be used in various domains of IoT. This solution requires the devices to handle the high computational burden for encryption and decryption of private data, leading to a lower utility solution for IoT devices. Many of the evaluated mechanisms are being optimized for the integration with IoT such as ZKP which might be an option in the near future.
  - The ring signature benefits outweigh the costs as observed in the Table 1 and it demonstrates that this mechanism could be a suitable match for IoT devices as there are no performance limitations. According to the study in [34], it can be seen that this mechanism is a high maturity solution and provides transaction privacy but it has a disadvantage of difficult management of several signers. As a suggestion, a 'ring' or group can be made with the composition of similar functionalities of home appliances.

- Data manipulation solutions showed an effective balance in the solution's utility and suitability with IoT devices. Although they are mostly traceable and unencrypted, they enhance overall privacy with low resource consumption. A hybrid approach of data manipulation solutions can be used in resource-constrained devices like IoT and maintain privacy to a much greater extent.
  - Differential privacy shows great prospective in the IoT domain. According to the authors of [30] and [39], DP can be easily implemented in a BIoT system with a trade-off between accuracy and privacy. No DP implemented BIoT solution was discovered in the scope of this paper but it should be highly recommended to expand research in it.
- Trust-based solutions create a secure link or group between 'trusted' parties to exchange data. Although user anonymity and data confidentiality are available in these mechanisms, the anonymity is limited to the pseudonymous feature (Section 5.1), which makes them susceptible to linking attacks. Moreover, the partner's limitation can account for operability in the system. In secret sharing, high computational power needs to be considered for generating cryptographical keys. The importance of performance outweighs the benefits of this type of solution, making it unsuitable for IoT devices.
- From the platforms discussed in the scope of this paper, IOTA and Hyperledger Fabric are a better choice for integrating with IoT devices as observed from the result and Table 1 that Ethereum uses high computational burden solutions as compared to others. There is no 'one-fits-all' platform for solving the privacy issues, in order to get high privacy sometimes a lower utility solution can also be acceptable.

The evaluation methodology used in this paper compares the mechanisms on two main criteria of features and risks where most of them are qualitative. To improve this evaluation, more quantitative criteria can be introduced. In addition to that, improved analysis of the performance of these mechanisms can be done by testing them on a blockchain-based platform with the same configurations.

The limited subset of mechanisms and platforms is far from complete to conclude this paper. The mechanisms were chosen from survey papers and implementations of the BIoT applications. The sets of mechanisms and platforms can be extended for future evaluations.

7 Responsible Research

This section discusses the research's ethical implications as well as its reproducibility.

7.1 Research Integrity

Considering the ethical conduct of responsible research, this research is in a safe space of ethical aspects as no human interaction or data was needed for the evaluation. This research aims to analyze and compare different privacy mechanisms in blockchain-based IoT frameworks. Although blockchain technology raises some ethical issues, the most prominent problem is its effect on the environment and potential criminal activity [48]. In this paper, blockchain-based frameworks for IoT devices that require low computation power were analyzed. This will consequently decrease the energy used, having a low impact on the environment. Moreover, the focus of this paper is the privacy of users' sensitive data with the objective of mitigating the potential criminal activities related to IoT data.

7.2 Research Reproducibility

The methodology used in the system is general guidelines of a design science research by Hevner *et al.*, making it reasonably straightforward to reproduce. Furthermore, based on the information in this paper, any reader should be able to retrace the sources of the described mechanisms and evaluations. Besides, the documents referring to the framework and literature that mentioned the presented privacy mechanisms are provided.

8 Conclusions and Future Work

Data privacy is the right of a user on controlling how their personal data is collected and used. This privacy concern raises with the emergence of IoT devices storing our data in large volumes from our daily activities. A smart home environment is one such example where data privacy needs attention. We aim to tackle this concern by making the IoT decentralized and private-by-design. Through this study, we compared and classified privacy mechanisms based on the criteria that were focused on mitigating privacy concerns in the smart home system. The main privacy requirements of IoT include implementation in a permissioned setting along with the appropriate privacy-preserving solutions.

The evaluation stated that the set of cryptographic solutions provide the most privacy features compared to the other solutions but need high computational resources making them slightly unsuitable for IoT devices. Solutions involving manipulating data such as perturbation, isolation, or mystification can provide a practical privacy solution for the IoT. Another set of solutions known as trust-based solutions don't seem like a good fit for the smart home system due to the added overhead. Three blockchain-based platforms, IOTA, Hyperledger, and Ethereum, were also briefly discussed in terms of their available privacy option and suitability with IoT. To sum up, it can be said that there is no 'one-fits-all' solution.

In the future, evaluations can be done with quantitative criteria instead of qualitative measures used in this study. The limited set of mechanisms and platforms can be expanded for identifying suitable features and techniques. Furthermore, the suggestions could be taken into consideration when developing or expanding research in BIoT applications.

References

[1] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and internet of things (biot):

requirements, working model, challenges and future directions," *Wireless Networks*, vol. 27, no. 1, p. 55–90, 2021.

[3] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 1, 2019.

[4] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," 2017.

[5] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[6] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Peer to peer for privacy and decentralization in the internet of things," in *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, pp. 288–290, 2017.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[8] T. M. Fernandez-Carames and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, p. 32979–33001, 2018.

[9] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, IEEE, 2017.

[10] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of iot using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881–888, 2021.

[11] H. Treiblmaier, *Toward more rigorous blockchain research: Recommendations for writing blockchain case studies*. Springer, 2020.

[12] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[13] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, p. 15, 2016.

[14] Z. Zheng and et al., "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018.

[15] S. Afreen, "Why is blockchain important and why does it matters," Apr 2021.

[16] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and ai," *Big Data and Cognitive Computing*, vol. 4, no. 4, p. 28, 2020.

[17] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of things: Applications, security and privacy: A survey," *Materials Today: Proceedings*, vol. 34, pp. 752–759, 2021.

[18] G. V. Lioudakis, E. A. Koutsoloukas, N. Dellas, S. Kapellaki, G. N. Prezerakos, D. I. Kaklamani, and I. S. Venieris, "A proxy for privacy: the discreet box," in *EUROCON 2007 - The International Conference on "Computer as a Tool"*, pp. 966–973, 2007.

[19] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for iot applications: Architectures, security, privacy, and performance," *Computer Networks*, vol. 191, p. 108005, 2021.

[20] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, *Managing Smart Home Appliances with Proof of Authority and Blockchain*, p. 221–232. Communications in Computer and Information Science, 2019.

[21] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Computers & Electrical Engineering*, vol. 83, p. 106585, 2020.

[22] C. Matte, J. P. Achara, and M. Cunche, "Device-to-identity linking attack using targeted wi-fi geolocation spoofing," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, (New York, NY, USA), Association for Computing Machinery, 2015.

[23] M. D. Firoozjaei, R. Lu, and A. A. Ghorbani, "An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms," *Security and Privacy*, vol. 3, no. 6, 2020.

[24] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in iot-based transactive energy systems using distributed ledgers," 2017.

[25] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security Privacy*, vol. 8, no. 1, pp. 11–20, 2010.

[26] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[27] J.-H. Lee, "Rise of anonymous cryptocurrencies: Brief introduction," *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, p. 20–25, 2019.

[28] X. Fan, "Faster dual-key stealth address for blockchain-based internet of things systems," 2018.

[29] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in *Computer Security - ESORICS 2014* (M. Kutyłowski and J. Vaidya, eds.), (Cham), pp. 345–364, Springer International Publishing, 2014.

[30] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based iot systems: In-

tegration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, p. 512–529, 2019.

[31] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[32] M. Daghmehchi Firoozjaei, A. Ghorbani, H. Kim, and J. Song, "Hy-bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in internet-of-things platforms," *Sensors*, vol. 20, no. 3, p. 928, 2020.

[33] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[34] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[35] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving," *IEEE Access*, vol. 7, p. 62058–62070, 2019.

[36] I. Foundation, "Introducing masked authenticated messaging," Dec 2020.

[37] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, pp. 459–474, 2014.

[38] "Private and confidential transactions with hyperledger fabric."

[39] M. Ul Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," *Journal of Parallel and Distributed Computing*, vol. 145, p. 50–74, 2020.

[40] S. Zhao, B. Wang, Y. Li, and Y. Li, "Integrated energy transaction mechanisms based on blockchain technology," *Energies*, vol. 11, no. 9, p. 2412, 2018.

[41] I. Kotsiuba, A. Velvkzhanin, Y. Yanovich, I. S. Bandurova, Y. Dyachenko, and V. Zhygulin, "Decentralized e-health architecture for boosting healthcare analytics," in *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 113–118, 2018.

[42] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019.

[43] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, p. 11676–11686, 2018.

[44] D. Grigoriev and V. Shpilrain, "Rsa and redactable blockchains," 2020.

[45] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, no. 2, p. 77–94, 1988.

[46] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, pp. 180–184, 2015.

[47] S. Eisele, T. Eghtesad, K. Campanelli, P. Agrawal, A. Laszka, and A. Dubey, "Safe and private forward-trading platform for transactive microgrids," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, p. 1–29, 2021.

[48] "5 blockchain problems: Security, privacy, legal, regulatory, and ethical issues," Jun 2020.