Privacy Implications of IoT: Data Protection and Consent in a Connected World

Article · December 2023

CITATION
1

READS
379

2 authors:

Oluwatoyin Adeniji
Bournemouth University
11 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Chinaza Ifeji
Bournemouth University
3 PUBLICATIONS **1** CITATION
SEE PROFILE

Privacy Implications of IoT: Data Protection and Consent in a Connected World

Chinaza Virginia Ifeji
Faculty of Science and Technology
MSc. IoT with Cybersecurity
Bournemouth University
s5553971@bournemouth.ac.uk

Oluwatoyin Adeniji
Faculty of Science and Technology
MSc IoT with Cybersecurity
Bournemouth University
s5532082@bournemouth.ac.uk

***Abstract* - The Internet of Things (IoT) technologies have metamorphosed communication among humans across the globe. However, regardless of the multiple advantages associated with its use, particularly in convenience and efficiency, significant concerns about data privacy and consent have been raised. This article examines the privacy implications of IoT, with a focus on data protection and the need for informed consent in a connected world. The obstacles, regulatory frameworks, and potential solutions to safeguard the privacy of individuals in an IoT ecosystem are analysed.**

Keywords - Internet of Things (IoT), security, privacy, data, security, cyberattacks, IoT data, IoT device, consent.

I. INTRODUCTION

Contemporary years introduced a period of technological improvement, among which is the rise of IoT, revitalizing human interactions with digital devices [1]. IoT technologies have brought about convenience, even though the downsides are major concerns about data privacy and the consent of users [2]. The Internet of Things incorporates a massive network of everyday devices and objects that are impeccably interconnected through the Internet, enabling the collection and exchange of data for one form of service or the other. This innovative interconnection has brought about ground-breaking changes across diverse sectors, from healthcare to transportation, to smart homes and what have you [3]. IoT has become popular as a result of its importance in the daily lives of users who constantly use this technology to monitor home security, remotely control vehicles, or manage household appliances [4]. There are currently several billions of interconnected devices as indicated by Fig. 1 below, which predicts that the total number of interconnected devices will reach 75 billion devices in the year 2025 [5].

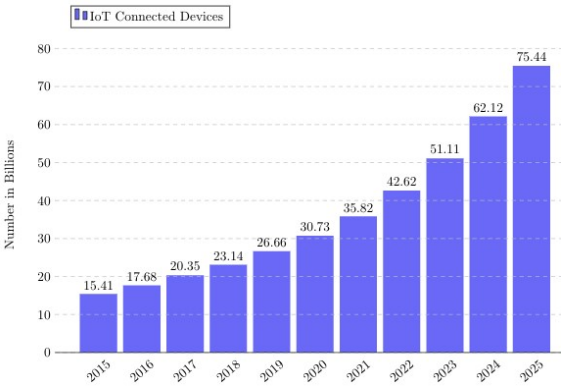

Figure 1: Population of Interconnected Devices

The paper has a dual-purpose mission, the first of which is to evaluate the privacy concerns found within the extensive IoT ecosystem due to the relentless growth in the number of connected devices leading to numerous standards and protocols. These standards and protocols present complexities such as device incompatibility, and notable security vulnerabilities. Secondly, the paper aims to thoroughly discuss data protection and consent inherent in the IoT industry, focusing on the challenges experienced and the potential solutions to safeguard individual privacy [6].

II. LITERATURE REVIEW

Recently, web security became a topic of interest due to the proliferation of the Internet of Things (IoT), accompanied by a rise of privacy concerns, necessitating experts to find solutions through rigorous research. IoT is categorized by seamless data

transfer among devices, making the job of data security a serious challenge [4]. Current literature suggests the pressing need for the industry to provide a balance between tech innovation and individual privacy, especially as it concerns the IoT network [6]. Studies from numerous investigations discovered the implications of widespread data collection through IoT devices, bringing potential threats that may arise due to the misuse of sensitive personal/private information [7]. However, there is a necessity for a careful approach to ensure that the benefits of IoT innovation are enjoyed while creating solutions to privacy risks [8]. Several known challenges are major factors surrounding the issues of IoT privacy. One of these challenges is the absence of standard security protocols implanted across IoT devices. As a result of this, the complexity and incompatibility of devices increase the range of security vulnerabilities [9]. Then again, the enormous amount of data generated by IoT devices, usually without plain user consent, is a significant privacy risk that must be considered [2]. Another concern worthy of note is the possibility of unauthorized access, data breaches, and the inadvertent misuse of personal information by bad actors [10]. However, there are legal frameworks responsible for shaping data privacy and its perceptions within the industry. Scholars have analytically explored the application of existing frameworks such as the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) [11].

The General Data Protection Regulation (GDPR) framework was established by the European Union to protect the privacy of users. This framework borders on personal data, protection of individual rights, and provides regulations that data controllers and processors are obliged to adopt for their platforms especially where it involves the use of personal information [12]. In the United States, state of California, the CCPA regulation endows privacy rights to residents/users and enforces compulsory laws for businesses for the collection and use of personal data [13].

The GDPR, designed to protect personal data, has been observed to extend its view across a variety of IoT items such as healthcare gadgets and wearables, smart homes, and interconnected industrial tools [14]. Even though the CCPA was not specifically crafted for IoT, the principles guiding it have implications for the protection of user privacy [13]. It has been suggested that for these regulations to be applied, it requires a careful consideration of the diversity of IoT applications deployment [15]. For example, healthcare IoT solutions involving sensitive patient data should unequivocally fall within the purview of GDPR, while smart home applications may also warrant scrutiny under pertinent data protection regulations [13]. There are various consent models employed in IoT applications among which is the informed consent model, a foundational principle in data privacy that involves users being comprehensively informed about the purposes for which their data is collected and how it will be used [16]. This model is demonstrated in Fig. 2 below [17].

According to reference [18], the sheer volume and complexity of data flows in interconnected ecosystems pose challenges for users to fully comprehend and control the utilization of their data. Furthermore, the imperative for lightweight and user-friendly consent mechanisms is needed for a widespread adoption and compliance [19].

Concerning the implementation of consent mechanisms, emphasizes the need for interoperable

mechanisms to facilitate seamless communication between devices, platforms, and users [20]. Challenges to this implementation include the development of user-friendly interfaces, transparent communication of data usage purposes, and the establishment of mechanisms that align with evolving privacy regulations [6].

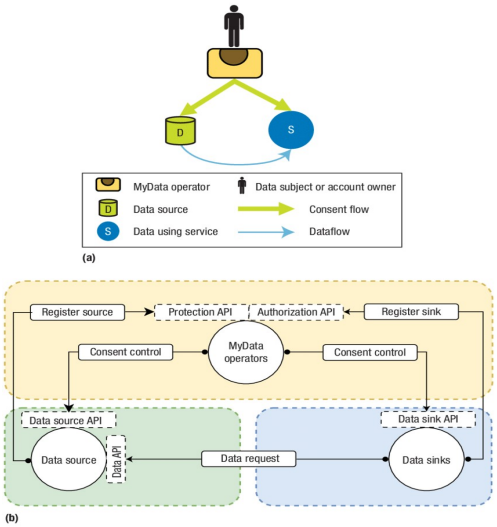

Figure 2: The Informed Consent Model

III. PRIVACY THREATS AND CHALLENGES IN IOT

In scholarly discussions, the ethical dimensions of data collection within the Internet of Things (IoT) have been found to create a prominent focal point, demanding a rigorous and academic evaluation. IoT technologies are pervasive hence, the rise of ethical concerns/implications that go beyond traditional considerations of data privacy [21]. For instance, the deployment of smart home devices which keeps a detailed record of the daily routine of users, emphasize the need for examining the depth of user consent and the broader societal consequences arising from this comprehensive data compilation [22]. There have been reports of practical case studies where a smart television manufacturer recorded users' audio conversations within homes. This serves as distressing illustrations that highlight the elaborate balance between technological convenience and the ethical preservation of individual privacy [23].

In a recent PSA Certified 2023 Security Report, reveals that over 67% of consumers indicate concerns regarding the privacy implications associated with smart devices in their homes [24]. This statistical revelation summarizes the escalating anxieties among users, highlighting the need for more robust ethical frameworks to safeguard their privacy.

Further, biometric data in IoT presents a unique and extremely personal category of information that introduces an additional layer of privacy risks [25]. The widespread adoption of biometric data, including fingerprint recognition in smartphones and facial recognition in smart cameras, further expands these challenges [26]. An instance of this is where a widely used IoT biometric access control system exhibited vulnerabilities leading to unauthorized access, broadly exemplifying the concrete risks associated with the deployment of biometric data in IoT scenarios [27]. These types of occurrence buttress why it is essential for a thorough comprehension of the technical vulnerabilities inherent in these systems so as to find ways of curtailing them [2]. Exploring privacy threats and challenges within the IoT industry demands an academically rigorous approach, integrating practical examples, statistical insights, and visual aids to better understand the challenges.

IV. DATA PROTECTION IN IOT

There is a need to protect privacy of users due to the massive data generated by IoT systems ranging from personal biometrics to behavioral patterns [4]. With several tools and regulations available to achieve this, such as encryption protocols, authentication, audit

requirement etc [28], this paper examines the multifactored proportions of data collection, security vulnerabilities, and the importance of informed consent.

A. Data Encryption and Safety Protocols

Employing robust encryption and security protocols is paramount for safeguarding data whether in transit or otherwise. To achieve this, a good way is to perform retrieval of stored information on encrypted data. This technique became famous in year 2000 and is called Searchable Encryption (SE) [29]. The AES and the RC4 can be used as alternative forms of encryption even though they do not provide equal levels of security. In context, RC4 encryption is faster than the AES [30].

B. Authentication

Verification measures are known to establish secure communication channels among interconnected devices [31]. Cryptographic protocols, such as PKI and digital certificates verify the authenticity of devices and ensure the integrity of data exchanges [32]. Biometric authentication adds an extra layer of security by leveraging unique physiological or behavioral traits for user verification. Multifactor authentication strategies, combining knowledge and possession factors, strengthen the overall security posture [33]. Because most IoT devices are lightweight and resource-constrained, simple authentication protocols are designed to provide efficient service without conceding security [34]. Standardized frameworks and initiatives like the Online Trust Alliance and the Internet of Things Security Foundation provide guidelines to ensure robust authentication, safeguarding IoT ecosystems against unauthorized access and potential threats [35].

C. Secure Device Management

Notably, the development of security architectures for devices, networks, and systems simultaneously with the device manufacturing process is better than trying to implement said security at some later time. Making sure that devices are always up-to-date with patches and firmware helps to disable non-essential services from running, as well as closes open ports that can be exploited by hackers [36].

It is expected that IoT devices should have perpetual alignment with network standards security frameworks/policies, as these are paramount for data security and the safeguarding of devices from loopholes that can be exploited [37].

D. Consideration for Audit Requirement

There are different types of audit requirements that IoT services need to align with. These requirements involve the device users, companies, and government/agencies. Developers as stakeholders are also required to participate to ensure compliance and functionality of IoT devices. For example, users can be granted access to manage their devices through a local hub [38]. This method builds trust among users, helps them to trust IoT policies, and prevents intrusion into the systems.

V. DATA PROTECTION FRAMEWORKS

A. The GDPR – General Data Protection Regulation

The GDPR comprises core values thus; private information, personal rights, data controllers and processors, and global impact [62]. Even though some IoT devices and apps like the Industrial Internet of Things (IIoT) do not collect private data, many other device types do collect personal information, like the

ones used in healthcare delivery. Often, this includes names, diagnoses, addresses, and other private data [4]. Hence, the data generated by such devices/applications lie under the control of the GDPR framework, just as other devices that collect private information do such as such as smart meters, smart home appliances, smart vehicles, etc [23].

B. Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA is another framework responsible for establishing laws to regulate the security of Private Health Information. Private Health Information (PHI) exists in diverse formats such as physical and digital documents, or verbal communications/records [39]. PHI only deals with information derived from patient health records, including images/scans, patient names, associated email addresses, and any other information peculiar to the patient [63]. Using digital technologies, healthcare establishments have been able to minimize cost and improve patient outcomes. Hence, it becomes necessary to embed the HIPAA framework within healthcare delivery systems as it relates to IoT technologies.

C. Industrial Internet Consortium (IIC)

Created in 2014, the IIC was established with the sole aim of regulating the Industrial Internet of Things (IIoT) and provide practical guidelines to mitigate device breaches [63]. To foster collaboration among industries, educational institutions, and government organizations for the construction of practical test environments, the IIC leads by facilitating the exploration and implementation of innovative technologies and solutions to energize progress in the IoT industry. It is almost impossible for all IoT devices to implement tight security solutions all-round. Therefore, it becomes necessary to clearly define and indicate the unique contexts that are relevant, so that the expected security outcome desired the stakeholders can be achieved [64].

D. IoT Security Foundation (IoTSF)

Founded with security in mind, the IoT Security Foundation (IoTSF) is responsible for addressing IoT-related security challenges and promoting secure adoption among users [65]. IoTSF undertakes the mission of providing knowledge and industry best practices to Build Secure, Buy Secure, and Be Secure devices/applications. This organization offers its users guidelines that align with international standards through the IoT Security Assurance Framework. This is all in a bid to help companies and individuals make conscious security decisions.

VI. CASE STUDIES ON IOT PRIVACY INCIDENTS

Recorded incidents provide hindsight into notable privacy breaches that occurred over time to pick valuable insights. In 2018, it was recorded that a widely used smart home security camera system suffered an attack that resulted in unauthorized access to live camera feeds [39]. This incident typifies the vulnerability of IoT devices to bad actors, necessitating a thorough examination of the technical, ethical, and legal dimensions that caused such breaches [40]. Another example relates to a popular wearable fitness tracker transmitting unencrypted user data, leading to unauthorized access and potential compromise of sensitive health information [41]. The consequences and aftermath of IoT privacy breaches extend across various industries. Instances, where compromised data resulted in identity theft, unauthorized surveillance, or physical security threats, require thorough evaluations. From a synthesis of past incidents, some lessons learned are that academia

focuses on extracting insights crucial for comprehending the evolving landscape of IoT security. The recurring themes, such as inadequate encryption protocols, lax authentication mechanisms, or insufficient user awareness, have been commonly identified through research [42]. The proposed strategies for preventing the recurrence of similar incidents represent a proactive stance within academic discourse. As a result, lessons from previous occurrences can be used to ideate new and innovative ways of dealing with such breaches such as advocating for robust regulatory frameworks and enhancing user education.

VII. THE ROLE OF REGULATORY FRAMEWORKS IN IOT PRIVACY

There exist efficient regulatory frameworks used in mitigating privacy concerns within the Internet of Things (IoT) industry. To evaluate the impact and effectiveness of current privacy regulations addressing IoT concerns, frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have made significant strides in safeguarding individual privacy [11] [13]. These regulations outline principles for data processing, consent mechanisms, and user rights, establishing a foundation for privacy protection. Nonetheless, the complex and evolving nature of IoT introduces unique challenges that existing regulations are likely not to satisfactorily address [43]. Gaps are often observed in areas such as the interoperability of regulations across jurisdictions, the tough implementation of consent mechanisms across diverse IoT applications, and the delineation of responsibilities among the myriad entities involved in IoT ecosystems [44].

Before these gaps can be addressed, changes to existing frameworks or the creation of entirely new ones specifically tailored to the IoT industry need to be done. Refining consent mechanisms to align with the diversity of IoT applications is a good example of this, to institute clear guidelines for data ownership and responsibility, and foster transparent communication between stakeholders [31]; potential areas for regulatory enhancement.

Stressing the essence of global collaboration in regulatory efforts is necessary to comprehend the cohesive approach to IoT privacy [45]. Nguyen and Tran [46] posit that as a result of the inherently global nature of IoT systems, regulatory bodies and policymakers must collaborate. This is because a collective approach enhances clarity for businesses operating across borders and reinforces the effectiveness of regulatory measures [2]. More so, the development of best practices through shared insights is promoted. This fosters a collective response to the dynamic challenges experienced by IoT [47].

VIII. USER AWARENESS AND EDUCATION

A. Importance of User Education

The role of user awareness in decreasing the risk of any exposure to breaches and abuse of personal information cannot be overemphasized [48]. This is as a result of its significant importance in educating users about IoT privacy concerns and best practices for interacting with their devices [49]. The need for the awareness of user safety is sacrosanct for users to navigate safely with interconnected devices. This awareness is particularly essential in educating users on how to mitigate privacy risks [49] [16]. Data sharing, consent mechanisms, and the potential risks associated with IoT devices necessitate a proactive approach to user education else, the efforts put into

manufacturing these devices and the comfort they come with will be all for nothing [49]. Academic discourse emphasizes the need for users to comprehend the implications of their interactions with IoT technologies, fostering a sense of agency in managing their privacy. Proposing strategies for educating users involves multifaceted approaches, including user-friendly guides, interactive platforms, and awareness campaigns tailored to diverse user demographics [50]. Such strategies aim to empower users with knowledge, enabling them to make informed decisions regarding the adoption and usage of IoT devices [51]. Fig. 3 below expatiates the importance of user awareness and education as it has effects on continuous use. For users to be intentional about continuously using any IoT device, they must first be aware of the functions of the device, know the privacy details and how securely the communication channels are, gain trust in the device, and finally intend to make use of it continuously [52].

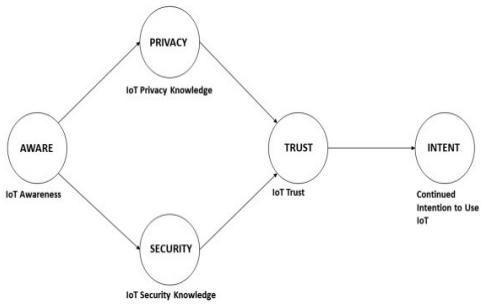

Figure 3: IoT user education

B. Building a Privacy-Conscious Culture

Building a Privacy-Conscious Culture is an important aspect of addressing the ethical and societal factors of IoT applications. Establishing a privacy-conscious culture involves fostering awareness and understanding of privacy considerations not only among end-users but also within the broader ecosystem of developers, manufacturers, and policymakers [6]. It emphasizes the responsibility of manufacturers to prioritize privacy features and provides users with transparent controls over data sharing. This cultural shift involves instilling a proactive mindset where privacy is not an afterthought but an inherent part of the IoT development process [52].

IX. IMPLEMENTING PRIVACY IN DESIGN

A. Privacy by Design Principles

1. Reiterating the Importance of Incorporating Privacy from the Outset

Reference [54] encourages the use of Privacy by Design (PbD), a foundational concept that surpasses mere compliance with privacy laws, right from the onset of IoT device design. At its core, PbD advocates for the proactive infusion of privacy considerations throughout the entire lifecycle of IoT device development [54]. This principle posits that privacy should not be treated as an addendum but as an integral component woven into the fabric of every design decision. The PbD framework is about ensuring that privacy is entrenched in the design specifications of the technology. As shown in Fig. 4 below, this framework involves seven steps which include imbibing a user-centric approach, avoiding to unnecessary dichotomies, being transparent with users, deploying full-scale or full lifecycle protection, prioritising privacy as a default setting, being proactive to prevent a breach as opposed to having mechanisms to react after a breach, and imbedding privacy into the design of the device itself [56].

The importance of incorporating privacy from the onset cannot be overstated.

2. Practical Guidelines for Implementation in IoT Projects

Implementing PbD principles in IoT projects involves translating theoretical concepts into actionable steps [56]. Practical guidelines encompass strategies for anonymization, data minimization, and secure data transmission [57].

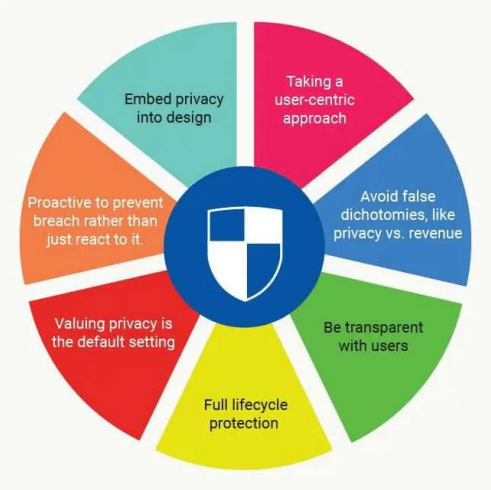

Figure 4: The Privacy by Design (PbD) Framework

- Anonymization Techniques: Are used to ensure that user identities are adequately protected through robust encryption methods, in a bid to avoid the correlation of data with specific individuals [58].
- Data Minimization Strategies: Advocate for the collection and retention of only vital data, reducing the potential for misuse or unauthorized access [59] [60].
- Secure Data Transmission Protocols: Prioritize the use of encryption and secure communication channels to safeguard data during transmission [58].

B. Collaborative Industry Efforts

Collaborative industry efforts are instrumental in establishing unified standards for privacy in IoT. This involves alliances, consortia, and standard-setting bodies working collectively to define and promote best practices [45][46]. Through the collaboration of diverse stakeholders, including technology companies, policymakers, researchers, and standard-setting bodies, with the shared objective of addressing privacy challenges inherent in IoT ecosystems, privacy by design and the practical implementation of guidelines can be easily achieved [56]. Standard-setting bodies contribute by developing and disseminating guidelines that help manufacturers and developers align their practices with universally recognized privacy principles [11]. This collaborative approach not only facilitates knowledge exchange but also accelerates the establishment of comprehensive and adaptive standards that can keep pace with the rapid evolution of IoT technologies [2]. By developing a sense of shared responsibility, collaborative industry efforts augment the credibility and effectiveness of privacy measures, ultimately contributing to the creation of a more trustworthy and secure IoT environment for end-users [61].

X. FUTURE TRENDS AND CHALLENGES IN IOT PRIVACY

The trajectory of IoT in the future presents a range of challenges and evolving privacy concerns that demand anticipatory analysis and flexible adaptive solutions. As the IoT industry continues to expand and rapidly so, having a grasp of the potential impacts of emerging technologies on privacy considerations is paramount.

A. Evolving Privacy Concerns

The rapid growth of the IoT industry as a whole introduces new privacy risks, further escalating security concerns for all new technologies. One of the most popular fears is the large amounts of data that is constantly being generated by IoT devices [2]. This enormous data collected from the wide spectrum of

IoT devices (smart home appliances, wearables, smart vehicles, etc) has the potential to constitute widespread surveillance and the exploitation of data [6].

Furthermore, cutting-edge technologies such as artificial intelligence (AI) and machine learning (ML) are being incorporated into IoT systems, thereby adding a new layer of complexity, as privacy concerns increases [66]. Also, the autonomous decision-making capabilities of AI-powered algorithms are likely to constitute another threat to user privacy [67].

B. Continuous Improvement in Privacy Measures

To successfully mitigate these constantly evolving threats, continuous improvement in privacy measures become imperative. The stakeholders involved in the privacy and data security must implement strategies that are adaptive and flexible, capable of staying ahead of new challenges [4]. The adoption of several factors is important in achieving this. Firstly, the requirement of nurturing collaboration between stakeholders such as technology developers, privacy advocates and policymakers, is crucial [45]. The facilitation of such collaboration promotes the exchange of insights, developing the best practice guidelines, and observe emerging threats, which further prompts the need to launch robust regulatory frameworks that are flexible enough to adapt to the constant changes of IoT technologies [46]. Furthermore, motivating the development and implementation of privacy-enhancing technologies (PETs) is a strategy that can be utilized in the achievement of continuous improvement [68]. PET ranges from advanced encryption methods to decentralized identity solutions, providing users with extra control over their data and devices [69].

XI. INFORMED CONSENT

The basis of ethical data privacy practices and informed consent plays a major role in providing security to IoT devices [6]. Comprehending the fundamental principles of informed consent as well as the implementation of robust consent management mechanisms within the IoT are crucial factors that factors in the legal, technological and ethical considerations.

A. Consent in IoT

One of the fundamental principles of data privacy is informed consent. This emphasizes the right and authority users have over their personal information either generated or stored on their devices [63]. The advantage of this concept is in ensuring that every user is fully informed about the purpose, scope, and potential consequences of the data collected from their device, because the IoT industry usually receives data seamlessly and ubiquitously, however, the challenge is in upholding the principle of user consent despite the complexity and enormity of interconnected devices [3].

There ought to be an incorporation of privacy-preserving consent management as an essential factor in the implementation of informed consent within the IoT ecosystem [13]. Mechanisms that ensures explicit user agreement as well as guarantee data practices align with the expectations and preferences of the user are some of the inculcation, otherwise, are not acted upon [70]. One common obstacle in achieving this feat is in reconciling seamless functionality of IoT devices with explicit and contextually relevant consent mechanisms [71].

B. Consent Management Mechanism

Helen Nissenbaum [72] proposed the theory of contextual integrity which provides a vigorous conceptual lens through which devices analyze and evaluate informed consent. This theory suggests that privacy norms are inherently context-dependent, which implies that the suitability of data practices is dependent on the specific environment in which they occur [73]. With diverse applications ranging from healthcare to smart homes, the IoT domain needs to acknowledge the existence of varying contextual norms. For instance, the sensitivity of health-related data might necessitate more strict consent mechanisms compared to data generated within a smart home or Industrial Internet of Things environment.

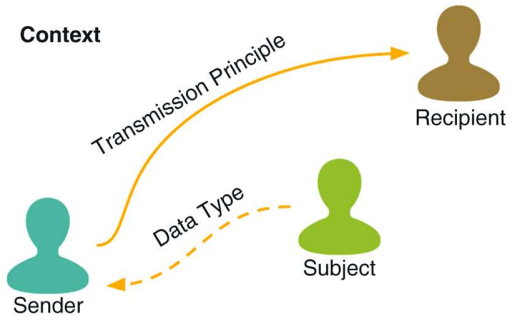

Figure 5: Illustrating the Theory of Contextual Integrity

The User-Managed Access (UMA) protocol is a practical-based framework which provides a technical dimension to the theoretical foundations of informed consent within the IoT. The UMA framework is designed to empower individuals with control over access to their digital resources [74]. In the IoT ecosystem, where devices continuously exchange data, UMA offers a standardized and interoperable mechanism for initiating requests and granting permissions [20]. This aligns with the predominant goal of this research, which is to explore practical consent management mechanisms in the IoT. By incorporating UMA into the discussion, we bridge the gap between theory and implementation, providing an emphasis for the importance of not just theoretical understanding but also the development of tangible, privacy-preserving solutions within the IoT landscape.

These models/theories contribute not only to a balanced understanding of the contextual difference of privacy but also to the practical application of consent management mechanisms within IoT devices. This integration enhances the professionalism and research-oriented tone of the essay, aligning with the main goal of comprehensively addressing privacy implications in the IoT landscape.

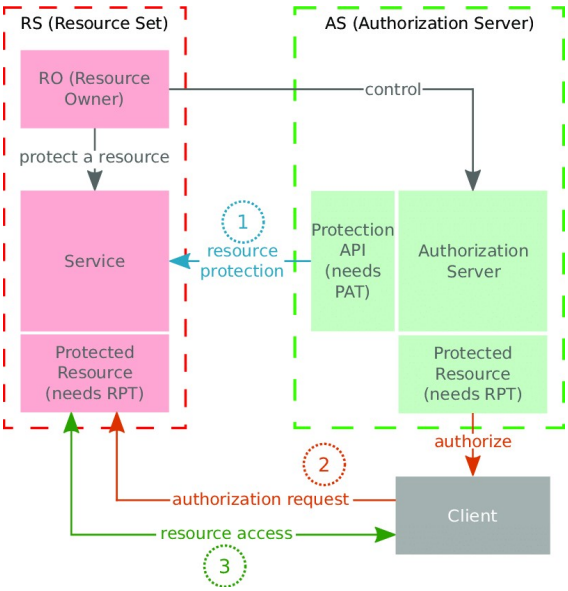

Figure 6: The User-Managed Access (UMA) Protocol

Proposing mechanisms for establishing new consent procedures in the evolving landscape of the Internet of Things (IoT) involves considering innovative approaches that balance technological advancements with ethical and legal considerations. As the IoT ecosystem continues to expand, new consent

procedures must be designed to address the complexity of data interactions across interconnected devices.

C. Dynamic Consent Frameworks

The implementation of dynamic consent framework is one of the innovative mechanisms for establishing new consent procedures. As opposed to traditional static consent models, dynamic consent allows users to exert real-time control over their data preferences [75]. In IoT, data flows non-stop and are multi-layered, enabling users to adapt their preferences based on evolving circumstances [76]. This framework leverages technology to provide users with granular control, allowing them to specify the duration, scope, and context of data usage. For example, a healthcare IoT device could prompt users for consent before sharing sensitive data for research purposes, and the user could dynamically adjust this consent based on changing privacy preferences.

D. Blockchain-Based Consent Management

The integration of blockchain technology offers another mechanism for establishing new consent procedures in the IoT landscape [77]. The decentralized and tamper-resistant nature of blockchain can enhance transparency and trust in consent management. Smart contracts, self-executing agreements on the blockchain, can be employed to automate and enforce consent agreements [78]. When an IoT device seeks access to user data, a smart contract could execute the predefined consent conditions, providing an immutable record of the user's agreement [79]. This mechanism not only ensures the integrity of consent records but also allows users to maintain sovereignty over their data across diverse IoT platforms. To augment the academic discourse, connections can be drawn to relevant blockchain models such as the consensus algorithms and cryptographic principles that underpin secure and transparent transactions.

XII. CONCLUSION AND FUTURE WORK

IoT privacy is a complex topic, with challenges such as data breaches, security risks, and intricate consent management. Key findings emphasize the necessity of a holistic approach, wherein cutting-edge technologies, regulatory frameworks, and user-centric measures harmoniously coexist. The complex nature of this approach involves implementing privacy by design principles, secure data transmission protocols, and informed consent mechanisms. Looking forward, future research directions highlight the ethical implications of advanced technologies within IoT, the development of standardized frameworks for device authentication, and the socio-technical aspects of user awareness. Encouraging ongoing collaboration among researchers, policymakers, and industry stakeholders is deemed essential to navigate the evolving landscape of IoT privacy effectively. As the interconnected world of the Internet of Things continues to evolve, a comprehensive and collaborative effort is imperative to address privacy concerns and shape a future where innovation and ethical considerations coalesce seamlessly.

References

[1] C. L. Ng and S. Y. L. Wakenshaw, “The Internet-of-Things: Review and research directions,” *International Journal of Research in Marketing*, vol. 34, no. 1, pp. 3–21, Mar. 2017.

[2] B. D. Weinberg, G. R. Milne, Y. Andonova, and F. Hajjat, “Internet of Things: Convenience vs. privacy and secrecy,” *Business Horizons*, vol. 58, no. 6, pp. 615–624, Nov. 2015.

[3] Y. Shen, “Intelligent infrastructure, ubiquitous mobility, and smart libraries –

innovate for the future," *Data Science Journal*, vol. 18, Jan. 2019.
[4] S. Nižetić, P. Šolić, D. López-De-Ipiña, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *Journal of Cleaner Production*, vol. 274, p. 122877, Nov. 2020.
[5] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, Sep. 2021.
[6] "Grammatical evolution for detecting cyberattacks in internet of things environments," *IEEE Conference Publication | IEEE Xplore*, Jul. 01, 2021.
[7] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, Aug. 2021.
[8] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. Singh, and W. Hong, "Internet of Things: evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, p. 1809, Mar. 2021.
[9] B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, Sep. 2018.
[10] M. Di Martino, "Personal information leakage by abusing the {GDPR} 'Right of Access,'" 2019.
[11] A. D. Kounoudes and G. M. Kapitsaki, "A mapping of IoT user-centric privacy preserving approaches to the GDPR," *Internet of Things*, vol. 11, p. 100179, Sep. 2020.
[12] A. Crabtree *et al.*, "Building accountability into the Internet of Things: the IoT Databox model," *Journal of Reliable Intelligent Environments*, vol. 4, no. 1, pp. 39–55, Jan. 2018.
[13] Aljeraisy, M. Barati, O. Rana, and C. Perera, "Privacy laws and privacy by design schemes for the internet of things," *ACM Computing Surveys*, vol. 54, no. 5, pp. 1–38, May. 2021.
[14] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," *Proceedings of the ACM on Human-computer Interaction*, vol. 2, no. CSCW, pp. 1–20, Nov. 2018.
[15] E. Carolan, "The continuing problems with online consent under the EU's emerging data protection principles," *Computer Law & Security Review*, vol. 32, no. 3, pp. 462–473, Jun. 2016.
[16] X. Su *et al.*, "Privacy as a service: Protecting the individual in healthcare data processing," *IEEE Computer*, vol. 49, no. 11, pp. 49–59, Nov. 2016.
[17] P. Muralidhara, "IoT applications in cloud computing for smart devices," Mar. 08, 2017.
[18] K. Echenim, "Ensuring Privacy Policy Compliance of Wearables with IoT Regulations," Nov. 01, 2023.
[19] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jul. 2018.
[20] P. Macnaghten, S. R. Davies, and M. Kearnes, "Understanding Public Responses to Emerging Technologies: A Narrative approach," *Journal of Environmental Policy & Planning*, vol. 21, no. 5, pp. 504–518, Jun. 2015.
[21] K. Sharif and B. Tenbergen, "Smart Home Voice Assistants: A literature survey of user privacy and security Vulnerabilities," *Complex Systems Informatics and Modeling Quarterly*, no. 24, pp. 15–30, Oct. 2020.
[22] P. Certified and P. Certified, "New PSA Certified Report Shows that Consumers are Concerned about Device Security," *PSA Certified - Created to Improve the Security and Trust of Internet of Things Devices and Their Data*, Oct. 11, 2023.
[23] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, "Biometrics for Internet-of-Things Security: A review," *Sensors*, vol. 21, no. 18, p. 6163, Sep. 2021.
[24] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, p. 100312, Nov. 2020.
[25] J. Bugeja, A. Jacobsson, and P. Davidsson, "PRASH: A Framework for Privacy Risk Analysis of Smart Homes," *Sensors*, vol. 21, no. 19, p. 6399, Sep. 2021.
[26] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things*, vol. 14, p. 100075, Jun. 2021.
[27] Amorim and I. Costa, "Leveraging Searchable Encryption through Homomorphic Encryption: A Comprehensive Analysis," *Mathematics*, vol. 11, no. 13, p. 2948, Jul. 2023.
[28] P. Pronika, "Performance analysis of encryption and decryption algorithm," 2021.

https://www.semanticscholar.org/paper/Performance-analysis-of-encryption-and-decryption-Pronika-Tyagi/440cab3f46d5d2f8765702a77ef1773c4a05ba16?p2df (Accessed: 25 November 2023).

[29] P. S. F. Sheron, K. Sridhar, S. Baskar, and P. M. Shakeel, "A decentralized scalable security framework for end-to-end authentication of future IoT communication," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, Nov. 2019.

[30] Höglund, S. T. Lindemer, M. Furuhed, and S. Raza, "PKI4IoT: Towards public key infrastructure for the Internet of Things," *Computers & Security*, vol. 89, p. 101658, Feb. 2020.

[31] "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things era: An Artificial Intelligence perspective," *IEEE Journals & Magazine | IEEE Xplore*, Sep. 01, 2020.

[32] "Proposing encryption selection model for IoT devices based on IoT device design," *IEEE Conference Publication | IEEE Xplore*, Feb. 13, 2022.

[33] "A review of security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Journals & Magazine | IEEE Xplore*, 2021. https://ieeexplore.ieee.org/abstract/document/9528421 (Accessed: 28 November 2023).

[34] BCS, The Chartered Institute for IT, "The internet of things," *O'Reilly Online Learning*. https://learning.oreilly.com/library/view/the-internet-of/9781780173337/10_Chapter06.xhtml (Accessed: 28 November 2023).

[35] S. Velliangiri, "Internet of things," *O'Reilly Online Learning*. https://learning.oreilly.com/library/view/internet-of-things/9781000291674/xhtml/cover.xhtml (Accessed: 27 November 2023).

[36] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive survey," *Electronics*, vol. 11, no. 1, p. 16, Dec. 2021.

[37] "Privacy and security in Internet-Connected Cameras," *IEEE Conference Publication | IEEE Xplore*, Jul. 01, 2019.

[38] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of IP-Based video surveillance systems," *Sensors*, vol. 20, no. 17, p. 4806, Aug. 2020.

[39] M. Schukat *et al.*, "Unintended consequences of wearable sensor use in healthcare," *Yearbook of Medical Informatics*, vol. 25, no. 01, pp. 73–86, Aug. 2016.

[40] Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444–458, Dec. 2017.

[41] M. Fisher, V. Mascardi, K. Y. Rozier, B.-H. Schlingloff, M. Winikoff, and N. Yorke-Smith, "Towards a framework for certification of reliable autonomous systems," *Autonomous Agents and Multi-Agent Systems*, vol. 35, no. 1, Dec. 2020.

[42] H. Allioui and Y. Mourdi, "Exploring the full potentials of IoT for better financial growth and stability: a comprehensive survey," *Sensors*, vol. 23, no. 19, p. 8015, Sep. 2023.

[43] HeinOnline, "About | HeinOnline," *HeinOnline*, Mar. 08, 2021. https://heinonline.org/HOL/LandingPage?handle=hein.journals/nylr94&div=28&id=&page= (Accesed: 19 November 2023).

[44] M. T. Nguyen, "Balancing Security and Privacy in the Digital Age: An In-Depth Analysis of legal and Regulatory Frameworks impacting Cybersecurity practices," Sep. 12, 2023.

[45] Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, "Agent-based Internet of Things: State-of-the-art and research challenges," *Future Generation Computer Systems*, vol. 102, pp. 1038–1053, Jan. 2020.

[46] Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and Security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, Jun. 2020.

[47] P. Mugariri, H. Abdullah, M. García-Torres, B. D. Parameshachari, and K. N. A. Sattar, "Promoting information privacy protection awareness for internet of things (IoT)," *Mobile Information Systems*, vol. 2022, pp. 1–11, Sep. 2022.

[48] Savaglio, M. Ganzha, M. Paprzycki, C. Bădică, M. Ivanović, and G. Fortino, "Agent-based Internet of Things: State-of-the-art and research challenges," *Future Generation Computer Systems*, vol. 102, pp. 1038–1053, Jan. 2020.

[49] X. Page, P. Bahirat, M. I. Safi, B. P. Knijnenburg, and P. Wiśniewski, "The internet of what?," *Proceedings of the ACM on Interactive, Mobile, Wearable and*

Ubiquitous Technologies, vol. 2, no. 4, pp. 1–22, Dec. 2018.

[50] P. Menard and G. J. Bott, "Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment," *Computers & Security*, vol. 95, p. 101856, Aug. 2020.

[51] A. Koohang, C. S. Sargent, J. H. Nord, and J. Paliszkiewicz, "Internet of Things (IoT): From awareness to continued use," *International Journal of Information Management*, vol. 62, p. 102442, Feb. 2022.

[52] H. C. Van Rest, D. Boonstra, M. H. Everts, M. Van Rijn, and R. J. G. Van Paassen, "Designing Privacy-by-Design," *Lecture Notes in Computer Science*, pp. 55–72, Jan. 2014.

[53] Malina, G. Srivastava, P. Dzurenda, J. Hajný, and S. Ricci, "A Privacy-Enhancing framework for internet of things services," in *Lecture Notes in Computer Science*, 2019, pp. 77–97.

[54] P. Ninja, "7 Key principles of Privacy by design for businesses," *Privacy Ninja*, Jun. 25, 2020. https://www.privacy.com.sg/resources/7-key-principles-of-privacy-by-design/ (Accessed: 30 November 2023)

[55] H. F. Atlam and G. Wills, "IoT Security, Privacy, Safety and Ethics," in *Internet of things*, 2019, pp. 123–149.

[56] Ni, S. C. Li, P. Gope, and G. Min, "Data anonymization evaluation for big data and IoT environment," *Information Sciences*, vol. 605, pp. 381–392, Aug. 2022.

[57] "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Journals & Magazine | IEEE Xplore*, Jan. 01, 2020.

[58] "A critical analysis of privacy design strategies," *IEEE Conference Publication | IEEE Xplore*, May 01, 2016.

[59] S. Sicari, S. Sicari, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015.

[60] A. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law & Security Review*, vol. 34, no. 1, pp. 134–153, Feb. 2018.

[61] A. Kaplan, "PHI Protection under HIPAA: An Overall Analysis," *Social Science Research Network*, Jan. 2020.

[62] B. C. Drolet, J. S. Marwaha, B. T. Hyatt, P. E. Blazar, and S. D. Lifchez, "Electronic communication of protected health information: privacy, security, and HIPAA compliance," *The Journal of Hand Surgery*, vol. 42, no. 6, pp. 411–416, Jun. 2017.

[63] HazraAbhishek, AdhikariMainak, AmgothTarachand, and S. Narayana, "A Comprehensive Survey on Interoperability for IIOT: Taxonomy, standards, and future directions," *ACM Computing Surveys*, vol. 55, no. 1, pp. 1–35, Nov. 2021.

[64] A. Mourtzis, N. Panopoulos, and J. Angelopoulos, "Production management guided by industrial internet of things and adaptive scheduling in smart factories," in *Elsevier eBooks*, 2022, pp. 117–152.

[65] P. Kearney, "IoT security: Experience is an expensive teacher," *The Internet of Things*, pp. 107–120, Mar. 2020.

[66] B. Chander, S. Pal, D. De, and R. Buyya, "Artificial intelligence-based Internet of Things for Industry 5.0," in *Internet of things*, 2022, pp. 3–45.

[67] V. Bjørlo, Ø. Moen, and M. Pasquine, "The Role of Consumer Autonomy in Developing Sustainable AI: A Conceptual framework," *Sustainability*, vol. 13, no. 4, p. 2332, Feb. 2021.

[68] Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey," *Journal of Network and Computer Applications*, vol. 171, p. 102807, Dec. 2020.

[69] B. S Kely, "Mitigating the Privacy Risks of AI through Privacy-Enhancing Technologies," *Questa Soft*, 2022. https://www.ceeol.com/search/article-detail?id=1098183 (Accessed: 27 November 2023)

[70] E.-M. Schomakers, C. Lidynia, and M. Ziefle, "All of me? Users' preferences for privacy-preserving data markets and the importance of anonymity," *Electronic Markets*, vol. 30, no. 3, pp. 649–665, Feb. 2020.

[71] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, Oct. 2019.

[72] , D. Reisman, and N. Feamster, "Discovering smart home internet of things privacy norms using contextual integrity," *Proceedings of the ACM on Interactive, Mobile, Wearable*

and Ubiquitous Technologies, vol. 2, no. 2, pp. 1–23, Jul. 2018.

[73] Nissim and A. Wood, "Is privacy privacy ?," *Philosophical Transactions of the Royal Society A*, vol. 376, no. 2128, p. 20170358, Aug. 2018.

[74] P. Machulak, "User-controlled access management to resources on the Web," 2014. https://theses.ncl.ac.uk/jspui/handle/10443/2715 (Accessed: 30 November 2023)

[75] C. Schraefel, R. Gomer, A. T. Alan, E. H. Gerding, and C. Maple, "The internet of things," *Interactions*, vol. 24, no. 6, pp. 26–33, Oct. 2017.

[76] S. H. A. Muller, G. J. Van Thiel, M. Mostert, and J. J. M. Van Delden, "Dynamic consent, communication and return of results in large-scale health data reuse: Survey of public preferences," *DIGITAL HEALTH*, vol. 9, Jan. 2023.

[77] "Blockchain Technology for Applications in Internet of Things—Mapping from System Design Perspective," *IEEE Journals & Magazine | IEEE Xplore*, Oct. 01, 2019. https://ieeexplore.ieee.org/abstract/document/8752029/ (Accessed: 04 December 2023)

[78] H. H. Pajooh, S. Demidenko, S. Aslam, and M. Harris, "Blockchain and 6G-Enabled IoT," *Inventions*, vol. 7, no. 4, p. 109, Nov. 2022.

[79] M. M. Merlec, Y. K. Lee, S.-P. Hong, and H. P. In, "A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR," *Sensors*, vol. 21, no. 23, p. 7994, Nov. 2021.