A personalized privacy protocols for different interconnected smart devices

By

Student

Instructor

Date

Table of Contents

Project Aims

The following are the ultimate goals of our proposed work:

Aim 1: Review the current status of privacy protection methods for smart devices.

Aim 2: Proposing an Internet of Things-specific protocol for negotiating privacy contracts.

Aim 3: Create an accurate and reliable smart privacy preservation protocol that protects users' personal information.

Aim 4: To create a reliable personalized privacy model for smart devices.

Statement of the research problems and significance

The potential privacy issues with utilizing smart gadgets are well-known. Remember, these gadgets are always keeping track of what we do and where we go. However, not everyone is aware of the entire scope of the issue. The privacy risks posed by smart gadgets are indeed bigger than most people realize [5].

The proliferation of data-gathering devices across the IoT ecosystem has given rise to previously unanticipated privacy concerns. One of these issues is getting people's permission before collecting their data, as well as giving them control over what information they provide and how it's used, and making sure it's only used for what it was intended. Worsening matters is the fact that there is a growing threat of misuse of personal information in the IoT realm. This is because of the pervasive monitoring of individuals' behaviors and locations over extended periods. The advent of IoT technology has resulted in hitherto unseen risks to people's security [2]. The Internet of Things (IoT) has improved communication, information exchange, and collection, while the rise of digital computers has permitted the advancement of particular sectors like statistics.

There has been a considerable slowdown in the adoption of IoT devices due to privacy fears. These worries about personal data security are predicated on the fact that data collecting, mining, and provisioning in the IoT will be carried out differently than is now the case. The privacy policy for Samsung Smart TVs, for instance, has been criticized for advising users to avoid having private discussions near the screens [3]. Many scenarios will need the collection of personal information, making it nearly difficult for individuals to exercise independent control over the dissemination of this data. The issue of privacy in the IoT affects everyone, not just those who utilize IoT services, which is in stark contrast to the old internet.

Research Background

There is a lot of discussion about data privacy and security these days [6]. With all of the high-profile data breaches that have occurred, it's no wonder that people are concerned about their privacy. While there are many steps you can take to protect your privacy, one of the most important is to choose a privacy preservation scheme that is both accurate and reliable [7].

There are several different privacy preservation schemes available, and it can be difficult to know which one to choose [8]. You want to make sure that the scheme you choose will be effective in preserving your privacy. Here are a few things to look for when choosing a privacy preservation scheme [9]:

Accuracy: The scheme should be able to accurately preserve the privacy of the data.

Reliability: The scheme should be reliable and not susceptible to data breaches.

Effectiveness: The scheme should be effective in preserving the privacy of the data.

Related Work

Privacy in the IoT

Consumers benefit greatly from IoT's automation and management of routine activities because of the pervasive presence of smart objects in their immediate surroundings [45]. Smart objects in the Internet of Things refer to a wide variety of non-standard computer devices, such as microcontrollers, sensors, and actuators that may broadcast and share data to facilitate better interactions and promote informed decision-making [7]. Sensors called "things" are already being built into everything from consumer electronics to industrial machines. Things may be controlled locally or through the Internet to effect a variety of physical changes in their settings [6].

Privacy-Preserving Approaches In IoT

Several cryptographic and anonymization methods can prevent a privacy breach in an IoT system. Protecting users' anonymity while still allowing them access to their IoT-generated data is illustrated in the following figure [11]. To protect individuals' privacy while still making data available for study and investigation [8].

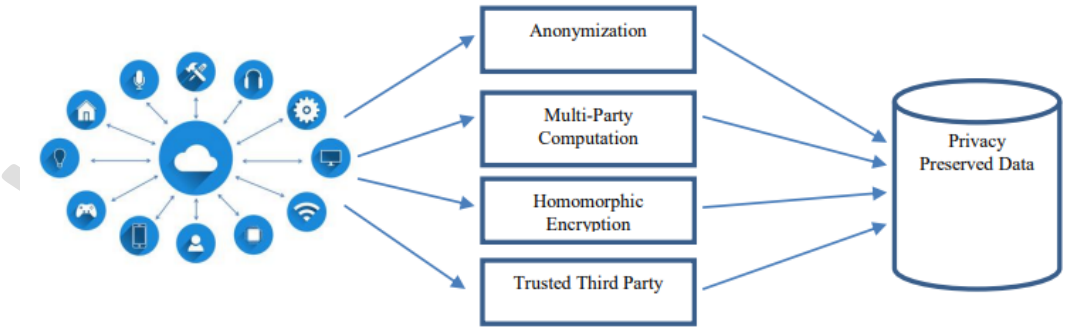

Figure 1: Approaches of Privacy Preserving in IoT [11]

1) IoT Anonymization Techniques

By pooling together data from multiple IoT nodes, private information can be kept safe. As a result, problems such as slow computation, inaccurate results, software defects,

etc., arise. [12] Proposes a technique for publicly verifiable aggregation. Using this method, data from untrustworthy nodes can be combined into a single, more trustworthy whole [2]. Public verification of the data's accuracy is made possible by the suggested tuple algorithms [9]. However, there are still some data owners who aren't participating in the plan [31].

2) IoT Secure Multi-Party Computation

OppNet maintains a database of the past locations of each node in the network [32]. It keeps track of previous transmissions to determine the most efficient path for delivering messages from the source node to the destination node. Privacy-sensitive data may be exposed due to the vulnerability of the history table. In [13], authors offer a history-based routing technique that protects users' anonymity. The secrecy of the OppNets' identities and whereabouts is a primary concern. The message is sent and received anonymously through a multiparty computation mechanism. It guarantees confidentiality and privacy at the cost of certain additional computational burdens. Several techniques are explored in reference [14] that aim to alleviate privacy problems in smart grids. Smart meters use IoT to gather information about individual consumers [3].

3) IoT Homomorphic Encryption

To address the reaction time and service delivery problem caused by IoT security approaches, a fog orchestration idea is developed [15]. The network, including any appropriate privacy and security measures, may be optimized for the service being supplied with the help of fog orchestration. This method maintains data privacy using attribute-based encryption (ABE) and homomorphic encryption (HE) while having a negligible impact on the latency and energy consumption of IoT devices. In [16], authors offer a strategy for keeping private information private in a fog-enhanced IoT system by use of anonymous data aggregation. To provide both privacy and credibility, the pseudonym approach was used in this strategy [33].

4) IoT Trusted Third Party

In [17], the authors offer a technique to protect users' anonymity while yet allowing their mobile IoT devices to follow a predetermined path. Due to the scheme's ability to provide spatial k-anonymity for snapshot queries made by a group of users, their location privacy is safeguarded. In [18], the authors propose an attribute-based encryption method for multi-authority access control that may be outsourced.

Data privacy and granular authorization are both benefits of the ciphertext-policy [21] attribute-based encryption technique. To make the characteristics anonymous and safely authenticable, the suggested strategy employs this technique to develop a privacy-preserving algorithm [23]. By moving the decryption work to a third party, we have lessened the computational load [22].

Research Question

Q: How to create accurate and reliable privacy preservation protocols for different interconnected smart devices by taking into consideration personalized communication privacy demands?

Sub Questions

Q1: What are the particular protocols for negotiating privacy contracts that pertain to the Internet of Things?

Q2: How to create a smart privacy preservation strategy that is both accurate and reliable and that safeguards the personal information of users.

Q3: How to Conduct a Critical Analysis of the Present State of Methods for the Protection of Individual Privacy in Connection with Smart Devices?

Q4: How to construct a privacy framework that can be relied upon for smart devices?

Research Methodology

Several different research methods can be used for this research, and the most appropriate method will vary depending on the topic and area of research. We will use the waterfall methodology to complete this research project. Because the research will design a smart privacy preservation protocol.

Moreover, the questionnaire and interview will be used to find out the current privacy issues of interment of things. Questionnaires and interview is a very convenient ways of collecting information from a large number of people within a period of time. Hence, the questionnaire design is of utmost importance to ensure accurate data is collected so that the results are interpretable and generalizable.

The following are the steps used in the waterfall methodology:

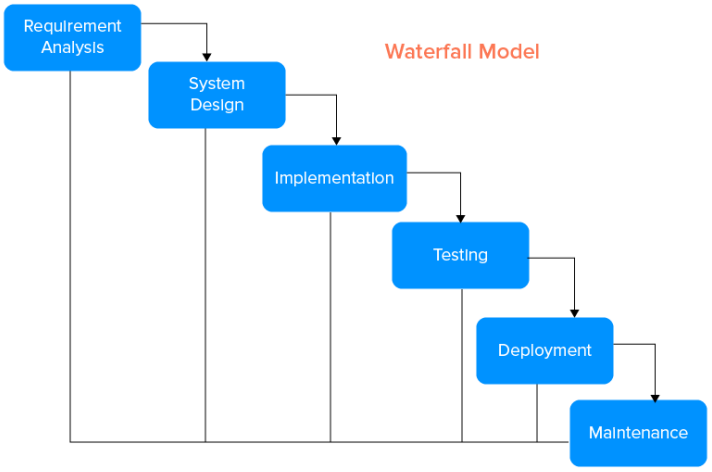

Figure 2: Stages of Waterfall Model

Conceptual Framework

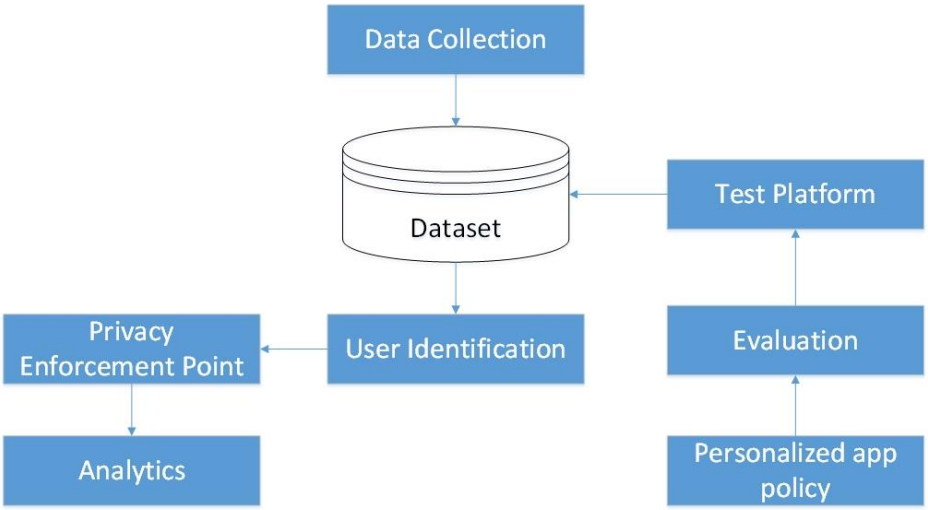

Figure 3: Conceptual Framework

This conceptual model of the proposed work under the environment of 5G-enabled IoT infrastructure is shown above. Users in a privacy-protecting smart environment are afforded various levels of transparency, control, and agency over the data collected about them. When a user enters an Internet of Things (IoT) environment, they will be given advance notice of any data-collecting IoT devices in the vicinity. They will be educated on how IoT devices collect data and how that data is typically used. By giving people a say in what data about them is collected, choice and consent help people protect their privacy. Depending on the IoT device's privacy policy [31], users can choose whether or not to participate in data collection or set preferences for the level of detail to which data is collected. To strike a middle ground between the two competing interests of data collection and privacy protection, a protocol for negotiating privacy contracts will soon be implemented [34].

References

[1] Sarrab, M., & Alshohoumi, F. (2020). Privacy concerns in IoT a deeper insight into privacy concerns in IoT based healthcare. International Journal of Computing and Digital Systems, 9(03).

[2] Bashir, A., & Mir, A. H. (2017). Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol. EAI Endorsed Transactions on internet of things, 3(12), e1-e1.

[3] Matyszczyk, C. (2015). Samsung changes smart tv privacy policy in wake of spying fears.

[4] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54 (15), 2787–2805.

[5] Wright, D. (2012). The state of the art in privacy impact assessment. Computer law and security review, 28(1), 54–61.

[6] Lu, R., Liang, X., Li, X., Lin, X., & Shen, X. (2012). EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Transactions on Parallel and Distributed Systems, 23(9), 1621-1631.

[7] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Federated learning for data privacy preservation in vehicular cyber-physical systems. IEEE Network, 34(3), 50-56.

[8] Nasr Esfahani, M., Shahgholi Ghahfarokhi, B., & Etemadi Borujeni, S. (2021). End-to-end privacy preserving scheme for IoT-based healthcare systems. Wireless Networks, 27(6), 4009-4037.

[9] Huo, Y., Meng, C., Li, R., & Jing, T. (2020). An overview of privacy preserving schemes for industrial internet of things. China Communications, 17(10), 1-18.

[10] Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 6(5), 8770-8781.

[11] Andrew, J., & Karthikeyan, J. (2019). Privacy-preserving internet of things: techniques and applications. International Journal of Engineering and Advanced Technology, 8(6), 3229-3234.

[12] Li, T., Gao, C., Jiang, L., Pedrycz, W., & Shen, J. (2019). Publicly verifiable privacy-preserving aggregation and its application in IoT. Journal of Network and Computer Applications, 126, 39-44.

[13] Rashidibajgan, S., & Doss, R. (2019). Privacy-preserving history-based routing in Opportunistic Networks. Computers & Security, 84, 244-255.

[14] Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A. S., & Nojoumian, M. (2018). Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Future Generation Computer Systems, 78, 547-557.

[15] Viejo, A., & Sánchez, D. (2019). Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services. Ad Hoc Networks, 82, 113-125.

[16] Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., & Hu, J. (2019). APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. Journal of Network and Computer Applications, 125, 82-92.

[17] Zhang, L., Jin, C., Huang, H. P., Fu, X., & Wang, R. C. (2019). A trajectory privacy preserving scheme in the CANNQ service for IoT. Sensors, 19(9), 2190.

[18] Fan, K., Xu, H., Gao, L., Li, H., & Yang, Y. (2019). Efficient and privacy preserving access control scheme for fog-enabled IoT. Future Generation Computer Systems, 99, 134-142.

[19] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for Internet of Things (IoT) services and applications. Journal of Network and Computer Applications, 89, 3-13.
[20] Tedeschi, P., Bakiras, S., & Di Pietro, R. (2021). IoTrace: a flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing. IEEE Communications Magazine, 59(6), 82-88.
[21] Emura, K., Miyaji, A., Nomura, A., Omote, K., & Soshi, M. (2009, April). A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In International Conference on Information Security Practice and Experience (pp. 13-23). Springer, Berlin, Heidelberg.
[22] Waters, B. (2011, March). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In International workshop on public key cryptography (pp. 53-70). Springer, Berlin, Heidelberg.
[23] Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an {IoT} world. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) (pp. 399-412).
[24] Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized privacy assistants for the internet of things: Providing users with notice and choice. IEEE Pervasive Computing, 17(3), 35-46.
[25] Mikusz, M., Houben, S., Davies, N., Moessner, K., & Langheinrich, M. (2018). Raising awareness of IoT sensor deployments.
[26] De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer law & security review, 28(2), 130-142.
[27] Guessoum, D., Miraoui, M., Zaguia, A., & Tadj, C. (2016). A measure of semantic similarity between a reference context and a current context. Journal of Ambient Intelligence and Smart Environments, 8(6), 697-707.
[28] Gagnon, Y. C. (2010). The case study as research method: A practical handbook. PUQ.
[29] Milian, E. Z., Spinola, M. D. M., & de Carvalho, M. M. (2019). Fintechs: A literature review and research agenda. Electronic Commerce Research and Applications, 34, 100833.
[30] Bell, E., Bryman, A., & Harley, B. (2022). Business research methods. Oxford university press.
[31] Karjoth, G., & Schunter, M. (2002, June). A privacy policy model for enterprises. In Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15 (pp. 271-281). IEEE.
[32] Perez, A. J., Zeadally, S., & Cochran, J. (2018). A review and an empirical analysis of privacy policy and notices for consumer Internet of things. Security and Privacy, 1(3), e15.
[33] Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in human behavior, 28(3), 889-897.
[34] Kuznetsov, M., Novikova, E., Kotenko, I., & Doynikova, E. (2022). Privacy Policies of IoT Devices: Collection and Analysis. Sensors, 22(5), 1838.
[35] Hu, Y. J., Guo, H. Y., & Lin, G. D. (2008, June). Semantic enforcement of privacy protection policies via the combination of ontologies and rules. In 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008) (pp. 400-407). IEEE.

[36] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 471-478).
[37] Peisert, S. (2019). Some Experiences in Developing Security Technology That Actually Gets Used. IEEE Security and Privacy, 17(2), 4-7.
[38] Xu, X., Fu, S., Qi, L., Zhang, X., Liu, Q., He, Q., & Li, S. (2018). An IoT-oriented data placement method with privacy preservation in cloud environment. Journal of Network and Computer Applications, 124, 148-157.
[39] Notare, M. S., Monteiro, E., & Kantarci, B. (2016). Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks.
[40] Gheisari, M., Wang, G., Khan, W. Z., & Fernández-Campusano, C. (2019). A context-aware privacy-preserving method for IoT-based smart city using software defined networking. Computers & Security, 87, 101470.
[41] Mutimukwe, C., Kolkowska, E., & Grönlund, Å. (2020). Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. Government Information Quarterly, 37(1), 101413.
[42] Mugariri, P., Abdullah, H., García-Torres, M., Parameshchari, B. D., & Abdul Sattar, K. N. (2022). Promoting Information Privacy Protection Awareness for Internet of Things (IoT). Mobile Information Systems.
[43] Lee, H., & Kobsa, A. (2017, March). Privacy preference modeling and prediction in a simulated campuswide IoT environment. In 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom) (pp. 276-285). IEEE.
[44] Castelluccia, C., Cunche, M., Le Métayer, D., & Morel, V. (2018, April). Enhancing transparency and consent in the IoT. In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 116-119). IEEE.
[45] Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards privacy preserving iot environments: a survey. Wireless Communications and Mobile Computing, 2018.

Appendix

Literature Review

S.N	Year	Paper Title	Main Work	Paragraph Used	Line number used
1	2018 [45]	Towards privacy preserving IoT environments: a survey	This study is mainly concerned with privacy issues and covers a wide variety of privacy-related concerns in open IoT environments to better inform the design concepts and development of privacy preserving IoT settings.	2nd of page 3	9-19
				3rd of page 3230	1-4
				4th of page 3230	1-4
				9th of page 3230	1-6
				2nd of page 3231	1-5
3	2019 [12]	A verifiable and privacy-preserving multidimensional data aggregation scheme in mobile crowd sensing	They propose a verifiable privacy-preserving data aggregation scheme.	1st of page 1	8-10
4	2019 [13]	Privacy-preserving history-based routing in Opportunistic Networks	A new Privacy-Preserving History-Based (PPHB) routing mechanism is proposed based on historical location tracking.	1st of page 1	11-12
5	2019 [17]	A trajectory privacy preserving scheme in the CANNQ service for IoT	This paper focuses on the 'sum' function because it properly takes into account the distance traveled by everyone in the group.	2nd of page 1	17-19
6	2009 [21]	A ciphertext-policy attribute-based encryption scheme with constant ciphertext length	They propose a novel attribute-based encryption scheme in this work called Ciphertext-Policy Attribute-Based Encryption (CP-ABE) that uses a constant-length ciphertext. And the number of pairing	1st of page 1	3-5

			calculations is likewise fixed.		
7	2017 [2]	Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol	This paper proposes a security algorithm for the Internet of Things (IoT) using simple lightweight cryptographic operations. The main advantage of the proposed algorithm is the simplicity, energy efficiency, and the speed of algorithm such that it can be computed quickly using a low-power microcontroller.	1st of page 1	1-2
8	2015 [3]	Samsung changes smart TV privacy policy in wake of spying fears	Samsung insists that it uses industry standard encryption to secure the data. The updated privacy wording was, of course, written by lawyers. So it should be held with an outstretched arm in just two fingers for examination.	6th, 7th, and 9th	
9	2012 [5]	The state of the art in privacy impact assessment	The paper provides some background on privacy impact assessment, identifies some of its benefits and discusses elements that can be used in construction of a state-of-the-art PIA methodology.	1st of page 1	14-17
10	2019 [18]	Efficient and privacy-preserving access control scheme for fog-enabled IoT	They propose an efficient and privacy preserving outsourced multi-authority access control scheme, named PPO-MACS.	1st of page 1	8-10
11	2018 [14]	Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems	Fully homomorphic encryption (FHE) and secure multiparty computation (secure MPC) are the systems that enable performing multiple operations on concealed data.	1st of page 1	8-10
12	2019 [15]	Secure and privacy-preserving orchestration and delivery of fog-	In this paper, they tackle this issue by relying on the novel concept of fog orchestration. Through	1st of page 1	9-13

		enabled IoT services	orchestration, the network is self-tailored to the service to be delivered, and we use this possibility to enable a secure and efficient service delivery.		
13	2019 [16]	APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT	They compare thier scheme with existing schemes to demonstrate the effectiveness and efficiency of our proposed scheme in terms of low computational complexity and communication overhead.	1st of page 2	20-22
14	2011 [22]	Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization.	They present a new methodology for realizing Ciphertext-Policy Attribute Encryption (CPABE) under concrete and noninteractive cryptographic assumptions in the standard model.	1st of page 3	1-2
15	2020 [1]	Privacy concerns in IoT a deeper insight into privacy concerns in IoT-based healthcare	This study conducts a deeper investigation into IoT data privacy. It discusses the IoT privacy concerns in healthcare and provides a complete scenario of the IoT data flow with privacy concerns.	1st of page 5	5-6
16	2010 [4]	The internet of things: A survey	This survey paper addresses the Internet of Things. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development.	1st of page 1	1 10-12
17	2012 [6]	EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications	This paper propose an efficient and privacy-preserving aggregation scheme, named EPPA, for smart grid communications.	1st of page 1	1-2
18	2020 [7]	Federated learning for data privacy preservation in vehicular cyber-physical systems	They first propose a secure and intelligent architecture for enhancing data privacy. Then present their new privacy-preserving federated learning	1st of page 1	9-12

			mechanism and design a two-phase mitigating scheme consisting of intelligent data transformation and collaborative data leakage detection.		
19	2021 [8]	End-to-end privacy-preserving scheme for IoT-based healthcare systems	The proposed scheme preserves end-to-end privacy against insider threats as well as external attacks concerning the resource restrictions of the sensors.	1st of page 1	5-6
20	2020 [9]	An overview of privacy preserving schemes for industrial internet of things	They summarize privacy issues in a cloud- or an edge-based industrial IoT system.	2nd of page 3	8-9
21	2019 [10]	Health chain: A blockchain-based privacy preserving scheme for large-scale health data	They propose Healthchain, a large-scale health data privacy preserving scheme based on blockchain technology, where health data are encrypted to conduct fine-grained access control.	1st of page 1	4-5
22	2017 [19]	Efficient location privacy algorithm for Internet of Things (IoT) services and applications	They proposed DLP algorithm has clear advantages over the DLS algorithm in term of lower probability of revealing the user's real location and improved computational cost and efficiency (i.e., time, speed, accuracy, and complexity) while preserve the same privacy level as DLS algorithm.	1st of page 1	10-12
23	2021 [20]	IoTrace: a flexible, efficient, and privacy-preserving IoT-enabled architecture for contact tracing	They propose an IoT-enabled architecture for contact tracing that relaxes the smartphone-centric assumption, and provide a solution.	1st of page 1	3-4
24	2017 [23]	Privacy expectations and preferences in an {IoT} world	Their study suggests that after observing individual decisions in just three data-collection scenarios, it is possible to predict their	2nd of page 2	1-4

			preferences for the remaining scenarios, with our model achieving an average accuracy of up to 86%.		
25	2018 [24]	Personalized privacy assistants for the internet of things: Providing users with notice and choice	They summarizes ongoing research to develop and field privacy assistants designed to empower people to regain control over their privacy in the Internet of Things (IoT).	1st of page 1	4-5
26	2018 [25]	Raising awareness of IoT sensor deployments		1st of page 1	1-6
27	2012 [26]	The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals		1st of page 1	5-6
28	2016 [27]	A measure of semantic similarity between a reference context and a current context		1st of page 1	3
29	2010 [28]	The case study as a research method: A practical handbook		1st of page 1	4
30	2019 [29]	Fintechs: A literature review and research agenda		1st of page 1	6-7
31	2022 [30]	Business research methods		1st of page 1	5-6
32	2002 [31]	A privacy policy model for enterprises		1st of page 1	5-6
33	2018 [32]	A review and an empirical analysis of privacy policy and notices for consumer Internet		1st of page 1	3

		of things			
34	2012 [33]	The effect of online privacy policy on consumer privacy concern and trust		1st of page 1	6
35	2020 [41]	Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior		1st of page 1	8-10
36	2022 [42]	Promoting Information Privacy Protection Awareness for Internet of Things (IoT)		1st of page 1	9-13
37	2017 [43]	Privacy preference modeling and prediction in a simulated campuswide IoT environment		1st of page 1	8-10
38	2018 [44]	Enhancing transparency and consent in the IoT		1st of page 1	9-13
39	2022 [34]	Privacy Policies of IoT Devices: Collection and Analysis		1st of page 1	8-10
40	2008 [35]	Semantic enforcement of privacy protection policies via the combination of ontologies and rules		1st of page 1	9-13
41	2004 [36]	Privacy policies as decision-making tools: an evaluation of online privacy		1st of page 1	8-10

		notices			
42	2019 [37]	Some Experiences in Developing Security Technology That Actually Gets Used		1st of page 1	9-13
43	2018 [38]	An IoT-oriented data placement method with privacy preservation in cloud environment		1st of page 1	9-13
44	2016 [39]	Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks		1st of page 1	8-10
45	2019 [40]	A context-aware privacy-preserving method for IoT-based smart city using software defined networking		1st of page 1	9-13