Journal of Computational Analysis and Applications VOL. 28, NO. 5, 2020

10.48047/jocaaa.2020.28.05.01

Privacy-Centric IoT Systems: A Framework for Secure Data Handling

Abhishake Reddy Onteddu[1], Dr. V Jagan Naveen[2]
[1]Software Engineer Chicago IL -USA 60159
[2]PH.D, Assistant Professor, GMR Institute of Technology: Rajam, Andhra Pradesh, INDIA
Email: Ontedduabhishakereddy@gmail.com, jagannaveen.v@gmrit.edu.in

ABSTRACT
As the number of Internet of Things (IoT) devices rises so quickly, many people worry about how to keep their data safe. This study makes the point that privacy should be a big part of the planning process for IoT systems from the start. By using edge computing, decentralized systems, and advanced encryption methods together, the suggested method keeps user data safe and easy to handle. It's less possible that private data will be stolen when edge devices handle it locally and data transmission is limited. Differential privacy and secure multiparty computing are two ways to protect user data while it's being sent and analysed on a device. People can choose how their data is used because the framework has tools for keeping things open and getting user approval. Based on how they were put in place, strong privacy measures can be put in place without making the system less useful or effective. This article goes into great depth about how to make Internet of Things (IoT) systems that people will trust and that follow the new privacy rules.

Keywords: IoT privacy, edge computing, data security, differential privacy, decentralized systems, privacy-preserving IoT, user data control

I. INTRODUCTION

The growth of networking has made the world a place where everything is connected. From small devices to big parts, they can all talk to each other without any problems, creating what we now call the Internet of Things (IoT). Using this paradigm as a starting point, researchers have developed and proposed new ways to collect, process, and share environmental data in real-time via sensors, actuators, and mobile devices; this data could be used to enhance human well-being or to automate and optimize manufacturing processes. Cisco predicts that machine-to-machine (M2M) communication would surpass 25 Exabytes of traffic by the end of 2022, up from almost 15 billion in 2017 and 6.1 billion in 2017. In addition, multimedia applications in fields like smart-car navigation and smart healthcare are driving this trend towards an even steeper spike in traffic rates. The Internet of Things (IoT) is, of course, always expanding its remit, and new methods are appearing that incorporate other components into these smart domains, going beyond the simple linking of devices in the perception layer [1]. The user is proposed as an essential component of this hyperconnected universe in innovative paradigms based on the Internet of Things. The Internet of People (IoP), People-Centric Internet of Things (IoT), Social Internet of Things (SIoT), and Human-in-the-Loop (HiTL) control for cyber-physical systems (CPS) are all examples of such paradigms. The Internet of Things (IoT) presents numerous technological and interdisciplinary issues while also expanding the range of services and solutions to a wide range of fields; these systems are user-centric. Problems with the device, the network, or the data itself naturally make up a large portion of these difficulties. Connectivity, mobility, ubiquity, fault tolerance, reliability, security, interoperability, and quality of service (QoS) are among the most significant. Nevertheless, privacy poses the greatest threat to this kind of strategy. And the challenges in IoT is shown in figure 1.

10.48047/jocaaa.2020.28.05.01

Fig 1: Challenges in IoT.

However, it's important to keep in mind that privacy is a complex issue that involves several disciplines, as it involves human variables interacting with and inside a digital world. There are users who are more worried about privacy than others, and everyone has their own idea on how to handle it. Applications need various levels of access to files and the ability to carry out specific tasks, which is evident in the way we manage traditional devices like cellphones. Here, we'll all have to make some adjustments to suit our own needs. European Union (EU) residents have certain basic rights with respect to the processing of their personal data, as outlined in the General Data Protection Regulation (GDPR), which became effective in 2018. The two main players in this rule are the Data Controller (DC) and the Data Subject (DS). The former refers to the specific individuals whose identities are known in order to obtain the data. This second party is responsible for "determining the purpose and means of the processing of personal data" (either alone or in conjunction with others). The General Data Protection Regulation (GDPR) provides that, in the absence of a legal obligation on the part of the DC, any acquisition of personal data must be preceded by notification and the DS's explicit agreement [2]. The General Data Protection Regulation (GDPR) states in Articles 4–11 that consent to data processing must be freely granted and must be explicit, explicit, particular, and unambiguous. Because the DS can't refuse without incurring harm, this assent is no longer voluntary. The digitization of public and private spheres, as well as the production and accumulation of massive volumes of data (personal and otherwise), have both intensified at a dizzying rate during the past few decades. Google, Facebook, and Twitter are just a few examples of the large tech corporations that have grown by mining user data for free. Many different kinds of firms have found success with this data-driven strategy, which has launched a new economic paradigm [3]. Despite the many advantages of modern technologies, it is critical to remember that bad actors can use personal information to sway public opinion, social norms, and even political beliefs. At now, personal data is being gathered, stored, processed, shared, and negotiated by a central online structure without the actual owners' awareness or agreement. Governments and citizens alike have been in the dark about their scope, precision, and specific applications. When people share information with websites, social media, and other devices, they may not be able to manage or change the information they've shared because they lose control over how it's stored and shared [4]. Also, there are privacy issues with this centralized structure because it stores personal information. For example, scandals like the one involving Cambridge Analytica—which utilized user data for political purposes—, Polar's fitness app—which exposed the whereabouts of U.S. military and security personnel—and Google Plus—which exposed the identities, email addresses, jobs, and ages of 52.5 million users—have brought attention to the unauthorized use of personal data. This goes against Westin's privacy policy. His definition of privacy as "the right to select what personal information about me is known to what people" highlights the importance of user control [5]. Users are seeking ways to govern and secure their data, and they are claiming privacy protection as a result [6]. Meanwhile, the Internet of Things (IoT) has improved our lives in many ways, including the ability for interconnected devices to produce and gather vast amounts of data, which in turn allows for the development of more tailored and worthwhile services. [7]. "Connecting people and things anytime, anyplace, with anything and anyone, ideally using any path or network and any service" [8] is the goal of the Internet of Things (IoT), which brings together many technologies such as sensors, networks, communications, computation, and semantics. The Internet of Things (IoT) has many positive effects on our daily lives, such as facilitating financial transactions and improving personal communications; nevertheless, it also increases the risk of unauthorized third parties throughout the world gaining access to personally identifiable information. One must weigh the benefits of the technology's many services against the risks to their privacy that its features and technologies pose [9]. While protecting users' privacy degrades the quality and utility of online services, Punagin and Arya [10] contend that users must have agency over the data sharing that occurs as a result. Restriction of information access can impact the utility of services, making it necessary to strike a balance between privacy protection and service quality. Alsheikh [11] argues that this view of data privacy as a barrier to innovation is based on a misunderstanding of the idea and a failure to adequately address privacy concerns. Rather, he promotes innovation while arguing for user control over data. The development of new technologies that give people more agency over their data is essential to solving the privacy problem [12]. To achieve this goal, it is necessary to provide users with control over the location and method of data storage while they utilize the services they require, and to promote the separation of data storage and services. Thus, Personal Data Stores (PDS) are a technological proposal for empowering individuals with greater agency over their own data. One secure location to keep information is in a PDS. Using a decentralized approach to data management is the way to go for handling user data privacy and control. The PDS concept has caused a sea change in the way people interact with the organizations that supply them with services. It prioritizes individuals. Because each user can determine the ultimate fate of their data because to this decentralization, user choice is even more paramount [13]. Since it reveals the current state of affairs and identifies potential areas for future research, a literature review is an effective tool for gaining a better understanding of a certain field of study in this context. In order to locate, assess, and comprehend the pertinent literature about privacy concerns and PDS-based solutions in the Internet of Things, we employed a controlled and organized systematic mapping review [14].

2. LITERATURE REVIEW

10.48047/jocaaa.2020.28.05.01

Researchers and cyber threat numbers are continuously increasing alongside academic work in IoT security. Multiple types of cybersecurity defenses serve the IoT environment. The safety measures in IoT systems consist of four essential components which include both user and system protection along with device and data security and operation availability assurance. Security of the Internet of Things (IoT) impacts every component from hardware devices through application programs. Packet routing systems of networks experience direct effects as well. Researchers studying the IoT field emphasize IoT security because of multiple essential reasons. The lack of proper security features in IoT systems enables unauthorized access to network systems along with device and data content. The basic design of an IoT system includes numerous interconnected devices which exchange big volumes of transmitted information. Security measures should be installed to prevent unauthorized access to this data. Financial together with health as well as personal data require protection from both physical threats and cyber threats for data privacy purposes. Internet of Things systems also have a unique issue with gear and devices being easy to damage. IoT systems that aren't secure enough can lead to a lot of problems, such as lost money, unsafe users, damage to important infrastructure, and the need for constant gadget and system maintenance to keep them from breaking down. Another problem that needs careful planning and development in IoT systems is making sure that accurate information from many sources and having accurate data are available. The sections that follow give an overview of the literature on Internet of Things (IoT) security issues that are important to the suggested framework.

Hardware Component Security in the IoT Context

Public and private IoT systems consist of multiple hardware components that include sensors as well as controllers I/O devices and peripheral devices. Each component in these hardware systems depends on the others for successful completion of necessary operations. Any changes made to hardware parts by an unauthorized individual will impact both the performance quality and reliability of the entire system's functions. Hardware safety represents a direct influence over the overall security status of the system. Protecting hardware becomes essential for IoT data security protection to remain secure. Various options exist for enhancing the security standards of IoT hardware systems. One effective method to secure IoT devices includes running their software at the most current version. A Trusted Platform Module chip and secure boot procedures which implement cryptography-based firmware authenticity checks serve as examples of hardware authentication methods approved by the ISO/IEC 11889-1:2015 standard. Two protective measures against physical attacks on hardware include physical tamper resistance chips combined with the Trusted Execution Environment (TEE) feature of the processor. A secure environment enabled through TEE lets users handle important data as well as cryptographic keys. The anti-tamper sensor detects authentic tampering events before proper investigation and response.

Software Security in the IoT Context

Any computer system requires absolute integrity for proper software security protection. The creation of software that detects hostile assaults and prevents them from occurring forms part of a comprehensive system. The system uses three key operations which include real-time monitoring together with incident responses and forensic analysis. The networked devices combination alongside flexible systems and hard-to-comprise monitoring make IoT software vulnerable to security attacks. Research findings identified software security for Internet of Things to consist of trusted sensing along with computing communication and privacy and digital forgetting features. The authors in research a cyber-secure architecture to handle risk management within the IoT supply chain through combined approaches of distributed system coordination with machine learning techniques and cryptographic hardware monitoring. A proposed approach aims to decrease supply chain damage that results from malicious actors. mesaj security teams put significant work and multiple tests into developing secure software solutions. Several categories of software security flaws occur at design stages as well as within intraprocedural interfaces and during the implementation process. The protection of IoT platforms primarily relies on two authentication and authorization methods among all available strategies. Authorized devices alone should receive permission to transfer data through the system. Process data protection occurs through encryption methods. All gateway-to-cloud-to-IoT device communications remain encrypted to stop unauthorized parties from accessing sensitive information. Blockchain technology enables secure IoT operation in present-day systems due to its implementation. The IoT system gains benefit from blockchain technology because this protocol verifies IoT system data for accuracy and permanence while making information universally accessible. Blockchain networks added proof of work (PoW) as well as proof of stake (PoS) distributed consensus procedures to validate blockchain state accuracy.

Security and Privacy Threats in the IoT Context

Within the Internet of Things (IoT), a "intrusion" is when someone, something, or someone unauthorized does something that hurts the IoT system's performance. Malicious people may take charge of the devices or mess with the networks during these kinds of intrusions, which puts the system's integrity at risk. Malware and ransomware linked to IoT devices or networks, unauthorized access to linked devices, and vulnerabilities in IoT devices or networks are all potential threats in IoT systems. Additional forms of attacks include distributed denial of service (DDoS) and denial of service (DoS) attacks, which overwhelm IoT networks; sniffing attacks, which capture data transmitted by or to IoT devices; data injection attacks, which introduce malicious data into an IoT system; and physical manipulation of IoT systems or devices to gain unauthorized

10.48047/jocaaa.2020.28.05.01

access or control. The foundation of many IoT systems is the sharing of data with various entities from IoT devices. Sharing the device's status and data acquired with third parties located far away is part of this. There are a number of proposed solutions to the problem of data privacy during attestation and data distribution. As an example, a privacy-preserved blockchain paradigm for distant attestation has been proposed. A system with known computer parts that uses TPM for direct anonymous verification was also put forward. So, came up with a scalable network authentication schema that could make things safer and more private at the same time.

3. METHODOLOGY

A structured approach is used in this study to build decentralized architectures, edge computing, and advanced encryption methods that keep Internet of Things (IoT) systems private. This method is made up of the following steps:

Decentralized Architecture Design:

The self-sufficient design of an IoT system makes sure that data processing takes place at the network's edges. Data doesn't have to be sent to central computers all the time. Keeping info in one place is less dangerous now that this is done.

Edge Computing Implementation:

An important part of edge computing is edge devices that handle private user data close to home. Because this is done locally, private data doesn't have to be sent across the internet as often. This makes it less likely that data will be stolen. You can use the following test to see how well edge computing works for handling data:

$$E_{\text{edge}} = \frac{P_{\text{local}}}{P_{\text{total}}} \quad (1)$$

Where:

- Eedge is the efficiency of edge computing,
- Plocal is the processing power used locally at the edge device,
- Ptotal is the total processing power required, including any centralized computation.

Advanced Encryption Techniques:

Different types of advanced encryption, like symmetric and asymmetric encryption, are used to keep user data private and safe. Key management is very important for symmetric encryption, and the security of the encryption can be shown by:

$$C = E_{\text{sym}}(P, K) \quad (2)$$

Where:

- C is the ciphertext,
- P is the plaintext (user data),
- K is the symmetric key,
- Esym is the symmetric encryption function.

For asymmetric encryption, the process of encrypting and decrypting user data is expressed as:

$$C_{\text{public}} = E_{\text{asym}}(P, K_{\text{public}}) \quad \text{and} \quad P = D_{\text{asym}}(C_{\text{public}}, K_{\text{private}}) \quad (3)$$

Where:

- Cpublic is the encrypted data,
- Kprivate are the public and private keys, respectively,
- Easym is the asymmetric encryption function,
- Dasym is the decryption function.

Privacy-Preserving Protocols:

Differential Privacy (DP) and Secure Multiparty Computation (SMC) are two privacy-enhancing methods that are part of the framework. In Differential Privacy, the level of privacy protection is shown by the following:

$$\epsilon\text{-DP} : P(\mathcal{M}(D)) \leq e^{\epsilon} P(\mathcal{M}(D')) \quad (4)$$

10.48047/jocaaa.2020.28.05.01

Where:

- M(D) and M(D′) are the outputs of the mechanism M for datasets D and D′ that differ in a single data point,
- ϵ is the privacy budget that controls the amount of noise added.

The computation in Secure Multiparty Computation (SMC) makes sure that the secret inputs of each party stay private. Following this method for safe data collection will protect each participant's privacy:

$$\text{SMC}(x_1, x_2, \ldots, x_n) = \text{Aggregate}(f(x_1), f(x_2), \ldots, f(x_n)) \quad (5)$$

Where:

- x1,x2,…,xn are the private inputs of the parties involved,
- f(x) is the computation function applied to each input,
- The result is an aggregated output that ensures privacy.

User Consent and Transparency:
The framework includes a user consent management system that lets people decide how their data is used. In math terms, consent can be shown as:

$$C_{\text{user}} = \int_{\text{time}} P_{\text{data usage}}(t)dt \quad (6)$$

Where:

- Cuser is the cumulative consent over time,
- Pdata usage(t) represents the data usage at a given time t,
- The integral represents ongoing user consent for data usage.

System Evaluation and Performance Analysis:
Performance metrics like data throughput, latency, and privacy assurance are used to judge how well the suggested privacy measures work. The effectiveness of privacy protection is shown by the following metric:

$$\text{Privacy Efficiency} = \frac{P_{\text{privacy}}}{P_{\text{total}}} \quad (7)$$

Where:

- Pprivacy is the privacy protection efficiency, including encryption and privacy-preserving protocols,
- Ptotal is the total performance, including system processing and data throughput.

4. RESULTS AND DISCUSSION

These graphs show how well different ways of keeping data safe in IoT systems work. The first line shows that making privacy protection more effective slows down data flow a little but doesn't have a big effect on system performance as a whole. This means that privacy can be put first without making things much less efficient. As you can see from the second line, privacy methods like Secure Multiparty Computation (SMC) slow down the system. On the other hand, Edge Computing helps keep latency low while still offering good privacy. Edge computing works better than centralized computing, as shown in the third line. In this case, handling data directly is better for both speed and privacy. Finally, the fourth graph shows a good connection between user approval and data use. This means that clear consent management makes people trust each other and shares data more, which is very important for privacy-focused IoT systems to work well.

10.48047/jocaaa.2020.28.05.01

Fig 2: Protection Efficiency vs. Data Throughput

The graph in Figure 2 shows that as privacy protection gets better, data flow slows down a bit. What this shows is the cost of getting more privacy: less speed. The method works pretty well even though it has strong privacy tools.

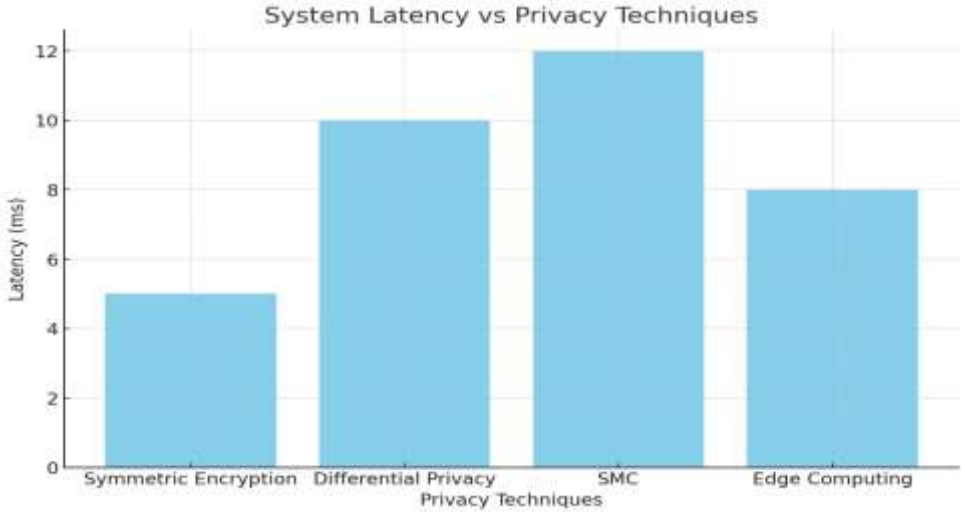
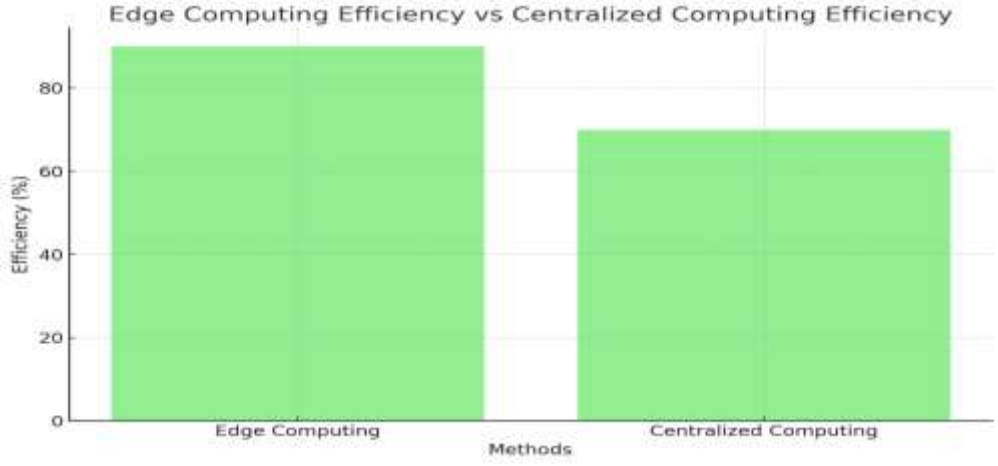


Fig 3: System Latency vs. Privacy Techniques

Figure 3 shows how the time it takes for the system to answer changes when different privacy protection methods are used. Different techniques, such as Secure Multiparty Computation (SMC), lead to different levels of delay. Edge Computing, on the other hand, helps lower latency without affecting privacy. These findings show how important it is for IoT systems to pick the right privacy settings to keep them safe and fast.



10.48047/jocaaa.2020.28.05.01

Fig 4: Edge Computing Efficiency vs Centralized Computing Efficiency

Edge computing is more efficient than centralized computing. Figure 4 shows this. It is better to handle data locally at the network's edge. Edge computing works much better than controlled computing. It keeps the system running at its best and protects the privacy of the info. This shows how important it is to split up IoT systems so that they are more private and can work faster.

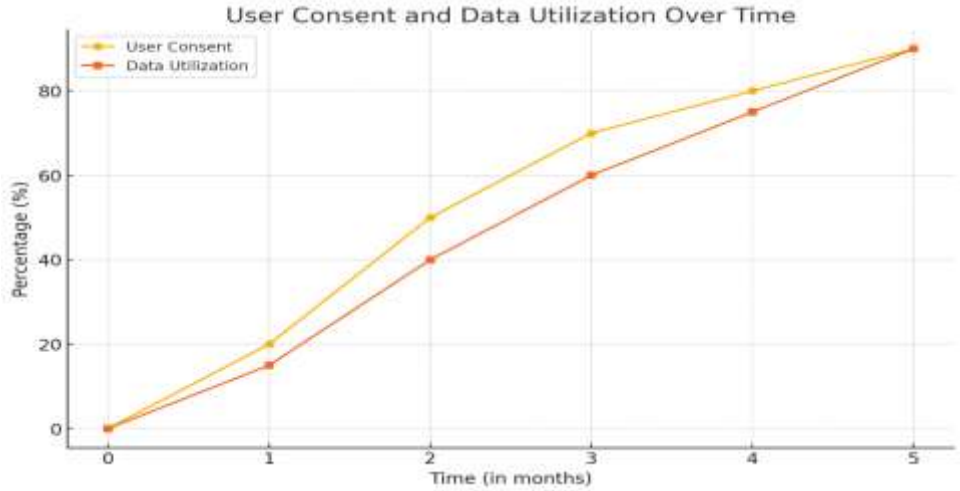


Fig 5: User Consent and Data Utilization Over Time

As more people agree to use data, Figure 5 shows how that has changed how data is used over time. Participants are more likely to share their data if they understand how, it will be used and are sure that it is clear how it will be shared. In places that care about privacy, this shows how important it is to set up strong user consent management tools that make it easier to use data more effectively and build trust.

CONCLUSION

IoT systems can have strong privacy features added to them without making them work less well, the study also shows. By using edge computing, independent structures, and advanced encryption methods, the system is both fast and good at keeping data private. Evolving computers at the edge is the best way to keep things fast and private. Lateral speed may get slower with other privacy methods, like Secure Multiparty Computation. To build confidence and make better use of data, the results also show how important it is to be clear about what permissions users have. In the future, this can use this framework to make IoT apps that are good for privacy, fast, and involve people more.

REFERENCES

1. Esteve, A. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. Int. Data Priv. Law 2017, 7, 36–47.
2. Laoutaris, N. Data Transparency: Concerns and Prospects [Point of View]. Proc. IEEE 2018, 106, 1867–1871.
3. Alessi, M.; Camillò, A.; Giangreco, E.; Matera, M.; Pino, S.; Storelli, D. A decentralized personal data store based on ethereum: Towards GDPR compliance. J. Commun. Softw. Syst. 2019, 15, 79–88.
4. Westin, A. Privacy and Freedom; Athenaeum: New York, NY, USA, 1968.
5. Ashton, K. That 'Internet of Things' Thing: In the real world, things matter more than ideas. RFiD J. 2009, 22, 97–114.
6. Perera, C.; Ranjan, R.; Wang, L.; Khan, S.U.; Zomaya, A.Y. Big data privacy in the internet of things era. IT Prof. 2015, 17, 32–39.
7. Punagin, S.; Arya, A. Privacy in the age of Pervasive Internet and Big Data Analytics—Challenges and Opportunities. Int. J. Mod. Educ. Comput. Sci. 2015, 7, 36–47.
8. Kitchenham, B.A.; Budgen, D.; Brereton, O.P. The value of mapping studies—A participant-observer case study. In Proceedings of the 14th international Conference on Evaluation and Assessment in Software Engineering, Newcastle, UK, 12–13 April 2010.
9. Song, Y.; Jiang, J.; Wang, X.; Yang, D.; Bai, C. Prospect and Application of Internet of Things Technology for Prevention of SARIs. Clin. eHealth 2020, 3, 1–4.

10.48047/jocaaa.2020.28.05.01

10. Thapliyal, H. Internet of Things-Based Consumer Electronics: Reviewing Existing Consumer Electronic Devices Systems, Platforms Exploring New Research Paradigms. IEEE Consumer Electron. Mag. 2018, 7, 66–67.
11. Reilly, E.; Maloney, M.; Siegel, M.; Falco, G. An IoT Integrity-First Communication Protocol via an Ethereum Blockchain Light Client. In Proceedings of the 2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT), Montreal, QC, Canada, 27 May 2019; pp. 53–56.
12. Mohamad Noor, M.B.; Hassan, W.H. Current Research on Internet of Things (IoT) Security: A Survey. Comput. Netw. 2019, 148, 283–294.
13. Bertino, E. Data Privacy for IoT Systems: Concepts, Approaches, and Research Directions. In Proceedings of the 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 5–8 December 2016; IEEE: Piscataway Township, NJ, USA, 2016; pp. 3645–3647.
14. Nebbione, G.; Calzarossa, M.C. Security of IoT Application Layer Protocols: Challenges and Findings. Future Internet 2020, 12, 55.