ICT 653 Emerging Technologies in IT

Assessment 2

Individual Assessment

A Comprehensive Review of Security and Privacy Issues in IoT Devices

**Name: Ankit**

**Abstract**

Because of the limited functionality of its devices and its widespread implementation, the internet of things (IOT) present serious security risks. To defend against threats in IOT environments, numerous protocols and techniques have been investigated. In order to reduce communication overhead and maintain secure and authenticated connections, a new resource-efficient end to end security scheme has been proposed that assigns computational tasks to fog nodes. In term of bandwidth and resource consumption for Internet of things applications, this method perform better than conventional protocols such as Transport Layer Security(TLS).A strong mitigation strategy is required to safeguard user privacy and data integrity, as the study also identifies vulnerabilities in Bluetooth Low Energy (BLE), which is used in wearable technology and other internet of things systems. Additionally, intrusion detection system may support network security and prevent resource waste, according to research on Secure Shell(ssh) protocol attacks in internet of things edge devices

**Table of Contents**

[Introduction 4](#_Toc174486398)

[Summary of Articles 4](#_Toc174486399)

[Discussion 9](#_Toc174486400)

[Literature-Map 10](#_Toc174486401)

[Concept Matrix 10](#_Toc174486402)

[Conclusions 12](#_Toc174486403)

[References 13](#_Toc174486404)

# Introduction

With the rapid adoption of the Internet of Things in various sectors, such as healthcare, smart homes, and industrial automation, a lot of technological novelties have come along. Besides, it introduces critical security and privacy challenges that should be properly addressed to allow safe and reliable use of these devices. This report dwells on the in-built security vulnerabilities and the privacy threats that IoT devices are breaching users' privacy with and how these problems are affecting user trust and consequently the mass adoption of the IoT technology. This analysis answers the question such as Which security vulnerabilities do most IoT devices have? How do the privacy concerns raised lead to the mistrust of users in and acceptance of IoT technologies? The importance of this research identifies itself by the information that it will ensure, for better practice of security assurance and policymaking on safer IoT, ultimately leading to the overall development and better IoT ecosystems.

# Summary of Articles

***Enhancing Security and Privacy in IoT: Development of a New IoT Model***

Security, privacy, and data protection in the context of the rapidly growing IoT environment are beginning to raise concerns in recent times as discussed in the article presented by Lee & Ahmed, (2021). Despite this technology having multifarious applications that render effective interaction, communication, and transaction amidst its users, it is yet vulnerable to several threats. This study specifically develops a new model for IoT to improve the security and privacy for users. The research methodology is the design and testing of this model, which indicates results that it may be effective for mitigation of security risks. However, further research is encouraged to fine-tune and advance the performance of the model in order to meet the dynamic needs of the IoT user.

***Critical Evaluation***

* Strengths: The article is valuable because it makes an original contribution by proposing an IoT model, looked upon very particularly in raising issues related to serious areas of security and private users although regarded as the most under-researched. The methodology is specific, rigorous, and clear in coming up with practical solutions of problems based on reality. The findings are pertinent in the sense that they can change the course of the IoT landscape in all ramifications, providing a more secure framework for the users likely.
* Weaknesses: On the other hand, its scope is somewhat narrow. Falling mostly into the part where the new model is first developed and tested, with little real-world application and not so much in testing over a long period on performance. Also, the article could have discussed more how the model compares to solutions out there. Besides, the authors are also conscious about the future work as they say that the model may further need refinement so as to altogether cope with all the security and privacy issues that are existing in the IoT.

***Enhancing Privacy and Security in IoT: A Cloud/Edge Supported IoT Layered Model***

The article presented by Tawalbeh et al., (2021) addresses some of the major privacy and security concerns of an IoT system: problems related to updating devices, weak security protocols, and user ignorance. This paper proposes a new cloud/edge-supported IoT layered model for enhancing privacy and security. This model combines AWS-generated IoT nodes at the lower layer, Raspberry Pi 4 at the edge layer, and cloud services at the top layer, with security protocols ensuring data transfer certificates between layers. This model is quite effective at addressing probable lapses in security and hence lays down a strong foundation for combating cybersecurity threats across IoT layers.

***Critical Evaluation***

* **Strengths**: The paper gives us the innovative approach of segregating cloud, edge, and IoT components into layers in one piece with a very effective way of detailing security and privacy issues. Practical implementation using AWS and Raspberry Pi further substantiates the feasibility and strength of the model.
* **Weaknesses**: Few real-life applications in different scenarios need to be further tested. Besides, the performance analysis related to the model's different IoT environments is scant.

***Addressing Security, Privacy, Safety, and Ethics in IoT***

This paper thoroughly highlights Atlam & Wills, (2020), researches the Internet of Things and the key issues entwined within it in terms of security, privacy, safety, and ethics. It starts off by considering the systems, architecture, and related overview of IoT systems and how inexpensive sensors are transforming daily life. While beneficial, IoT has some major challenges in terms of its securities and privacy concerns that it must put into concern to build users' trust. Thus, it is pointed to at the consideration of safety for the IoT and its ethical design, with conclusions summarized later on a smart city case study describing security threats and proposed solutions.

***Critical Evaluation***

* Strengths: The article speaks volumes about the overall approach it carries, which is very comprehensive and does not just focus on the technical area, but also on safety and ethical considerations of IoT. The case of smart cities would give practical insights into keeping high security paradigms.
* Weaknesses: The detailed scope of this paper may make topic details limited in a few areas. More specific data or examples would further enrich the argument in the example of smart city.

***Privacy and Security Risks in Wearable IoT Devices***

A detailed review has been made on the article provided by Ioannidou & Sklavos, (2021), where the article highlights the problems of privacy and security in wearable IoT devices by focusing on sensitive private data gathered by these devices: heart rate, calories burned, and sleep patterns. The work determines the current research into questions of privacy in wearable technology and performs experimentation to see the risks involved in exchanging data through mobile apps. The results indicate that not only is a large amount of personal data being collected and processed, but often shared for advertising purposes, increasing network traffic. Some of the apps required access to messaging, making phone calls, and using cameras without sufficient justification, which raised serious concerns regarding privacy.

***Critical Evaluation***

* Strengths: This paper gives a detailed and practical analysis of problems regarding privacy and security in wearable IoT devices, together with experimental data in support. In the study, a man-in-the-middle attack is simulated to show possible vulnerabilities resulting from the most used fitness tracking applications.
* Weaknesses: However, the research is limited as they only tested only five brands for security and privacy purposes that not cover whole market .The article does present some risks worthwhile, but it gives very short discourse on how to improve data privacy and security or the possible solutions for wearable IoT devices

***Data Privacy Challenges in the Internet of Healthcare Things (IoHT)***

A detailed review has been made on the paper provided by Shahid et al., (2022), the paper discusses IoHT, which represents a subset of IoT targeting healthcare devices for patient monitoring, management, storage, and sharing of personal health information. In the paper, various devices are classified with respect to their functions and deployments, and also brought out are the unique data privacy concerns related to IoHT. This paper reviews, besides compliance challenges in healthcare data protection laws, ways to enhance IoHT systems from the point of view of security and privacy.

***Critical Evaluation***

* Strengths: The paper provides a very nice survey of the domain of IoHT, bringing into the limelight the most critical data privacy concerns and the need for more stringent regulations. It contributes to an understanding of specific challenges in IoHT by grouping healthcare devices into categories and analyzing challenges in compliance.
* Weaknesses: This paper could still be improved with more empirical data or case studies that would further help make its point. Even as it brings out relevant challenges in privacy, some of the recommendations are very general and may miss concrete details for one striving to enhance security within IoHT settings.

***Security Challenges and Mitigation Techniques for IoT Devices***

According to the research paper provided by Aziz Al Kabir, Elmedany & Sharif, (2023), where the article gives insight into some of the major security risks related to devices with an extended usage scope of IoT devices, usually simple designs and low-powered hardware. Convenience-oriented, mass-produced, and cheap, these devices often result in weak security features that make them quite vulnerable to cyber-attacks. This paper considers typical threats and vulnerabilities, such as the potential for IoT devices to create botnets or enable man-in-the-middle attacks. This paper suggests ways through which IoT security can be enhanced by presenting a set of use cases, access controls, secure communication protocols, and regular updates with patches.

***Critical Evaluation***

* Strengths: The following overview article about the security issues associated with IoT devices is a good guide toward fathoming the risks and weaknesses of these technologies, along with this it shows practical ways in which their security could be improved.
* Weaknesses: Also, the wide diversity of subjects exposed in the article might lower its chances of deeply exploring a concrete security problem or method. In addition, the general character of proposed solutions can remain too general to apply to different IoT devices, hence not very effective in highly specialized cases.

***Cybersecurity Threats, Countermeasures, and Mitigation Techniques on the IoT***

In the research paper provided by Altulaihan, Almaiah & Aljughaiman, (2022), it has been highlighted that some of the common cybersecurity threats that particularly target IoT, emphasize unique risks because of the interconnection between physical and digital entities. With the wide spreading of IoT devices across the world, it has become quite an attractive target for cybercriminals aiming to steal sensitive data and invade users' privacy. According to the article, they are classified into three layers of IoT architecture and further discuss the best countermeasures for tackling them. It also discusses the security risks associated with some well-known application-layer protocols in IoT environments. In so doing, it highlights that security features such as confidentiality, authentication, and access control must be provided for both data and services in an IoT environment.

***Critical Evaluation***

* Strengths: The article is extremely useful for researchers and practitioners because the threats to IoT are systemically arranged and countermeasures are discussed. The contribution strengthens the value of the paper, particularly as it focuses on structured analysis of security risks according to a three-layer architecture that mirrors the general structure of most IoT implementations.
* Weaknesses: The article in technical details provided in the paper highlights about the architecture of IoT could prove a bit challenging to readers not very conversant with those. Moreover, general recommendations for countermeasures perhaps cannot help resolve specific security challenges concerning different IoT applications.

***Security Challenges and Solutions in the Internet of Things (IoT)***

As per the research paper provided by Jurcut, Ranaweera & Xu, (2020), where it has been highlighted that in-depth treatment of security challenges in the Internet of Things, considering vulnerabilities and possible attacks and ways to deal with these. If IoT devices are to be pervasive, then it will be important to ensure secure authentication and authorization. These security concerns are reviewed across different IoT technologies and architectures, showing the specific vulnerabilities at each layer. It also speaks to a wider audience of stakeholders, from manufacturers through to users, insisting that they must meet market demand while increasing security awareness. It further goes on to find solutions concerning the risks reduction and management of security breaches, giving an in-depth look into how one should prevent and actually manage such issues.

***Critical Evaluation***

* Strengths: The paper explains an in-depth overview of the weaknesses in IoT security with practical solutions, making it an important text for all practitioners working in the area of IoT technology. As a result of both technology and architecture coverage, it reveals a detailed analysis.
* Weaknesses: However, the broad coverage may result in generalizing some of the security issues and missing some threats unique to a specific setting in the IoT. Moreover, technical details may be complex to understand for readers without specialized knowledge.

# Discussion

The research questions are all related to challenges in IoT applications. This is because the applications, on one hand, have limited resources; on the other hand, there are many security problems common to a variety of communication protocols and devices. The three articles reviewed give different views and solutions to the problems.

One of the similar articles which have been reviewed and related to the articles of research papers is provided by (Diro et al., 2020), which has discussed the addresses a resource-constrained security method tailored for IoT applications. It explains the challenges of legacy security protocols: Transport Layer Security requires too many resources to fit within IoT systems. In this approach, efficiency is achieved by offloading complex tasks on fog nodes and symmetric-key encryption at the endpoint to reduce additional loads and bandwidths for secure communication. This approach provides a very practical way for IoT security hardening while working with limited resources, hence making the systems efficient and secure.

Another article which has been reviewed on the topic is provided by (Barua et al., 2022), where it discusses security and privacy in BLE, one of the most used protocols for communication in IoT and smart devices today. In general, BLE has been considered a rather user-friendly repository of energy efficiency, but it has simplified several major design weaknesses that resulted in serious security problems. This paper classifies these vulnerabilities, explores possible attack scenarios, and proposes ways to mitigate them. This can be an important survey in understanding BLE security threats and guiding the development of robust solutions for them.

The next research article which has been analyzed is provided by (Raikar & Meena, 2021), where it provides information on edge security in IoT devices, specifically the Raspberry Pi. Retrospectively, it talks about how hard it is to prevent zero-day attacks. This article analyses the detection capabilities of an Intrusion Detection System in the identification of SSH brute force attacks for prevention and shows how improvements can be made in saving resources like CPU, power, and memory. The study emphasizes the need for constant monitoring and security policies adapted to IoT, making threat detection and response most challenging with the large amount of data and devices involved.

# Literature-Map

Imaging and radio genomics

Model Performance and Generalizability

Socio-Environmentl factors

Fairness and Bias

challenges

Data privacy and security

Personalized care Delivery

Convergence of iot and ai

Speech and Behavioral Analysis

Genomics based treatment

Resource Allocation

Remote Patient Monitoring

AI -powered IOT and wirless Sensor Networks

Internet of nano things

Blockchain

Big data Analytics

Edge fog Computing

Emerging technologies

Power optimization

Resource constraining

Data privacy and security

Challenges

interoperability

Eldery Care

Early disease detection

Application

Iot in Healthcare System

Smart Cities and health care

Iot in healthcare system

Iot and ai in Personalized healthcare

Emergency Response System

Software-defined Networks (SDNs)

Wearable Devices and Remote Montoring

Personalized Treatment

Remote patient monitoring

This comprehensive literature map breaks down on topics including IOT integration, precise medicine, security, and the advancement of technologies while discussing the importance of IoT to healthcare from a variety of research. Every one of these articles sheds light on the difficulties and advantages of practical implementation as well as other avenues for potentially revolutionary effects. While some of organizations are more wide in their exchange of ideas and proposition, others are more in-depth in their technical depth and methodology.

# Concept Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Paper Criteria** | **Methodology** | **Findings** | **Strengths** | **Weaknesses** |
| ***Lee & Ahmed (2021)*** | New IoT Model Design | Effective risk mitigation | Original contribution, rigorous methodology | Limited real-world application, scope narrow |
| ***Tawalbeh et al. (2021)*** | Cloud/Edge Model | Effective multi-layer security | Practical implementation, innovative model | Few real-life scenarios tested |
| ***Atlam & Wills (2020)*** | Comprehensive Review | Highlights safety, ethics, and security | Broad approach, smart city case study | Limited detailed examples |
| ***Ioannidou & Sklavos (2021)*** | Experimental Analysis | Risks in wearable devices | Detailed analysis, practical experiments | Small sample size, limited solutions |
| ***Shahid et al. (2022)*** | Survey and Review | IoHT data privacy concerns | Good classification, regulatory focus | General recommendations, lack of case studies |
| ***Aziz Al Kabir et al. (2023)*** | Overview and Case Study | General IoT security risks and solutions | Practical risk mitigation approaches | General solutions, broad scope |
| ***Altulaihan et al. (2022)*** | Threat Analysis | Systematic threat classification | Structured analysis, practical countermeasures | Technical details challenging, general recommendations |
| ***Jurcut et al. (2020)*** | In-depth Review | Security challenges across IoT layers | Detailed analysis, practical solutions | Broad coverage, complex details |

The concept matrix has been found to provide a structured comparison of eight important papers regarding IoT security and privacy. Each paper has been evaluated in terms of methodology, findings, strengths and weaknesses. Lee & Ahmed (2021) has proposed a new IoT model that effectively mitigates risks but has limited real-world application. Tawalbeh et al (2021) has been found to present a cloud model that has multi-layer security still it lacks has been found to propose a real-life testing method. Atlam & Wills (2020) provides a review regarding the safety, ethics and security but fails to give specific examples. Ioannidou & Sklavos (2021) has been found to focus on the risks that are associated with wearable devices with practical experiments. Shahid et al. (2022) analyses the data privacy in Internet of Human Things (IoHT) through several recommendations while focusing more on regulatory aspects. Aziz Al Kabir et al.(2023 ) and Altulaihan et al. (2022 ) have given practical solutions for the challenges in the field of IoT security. Jurcut et al. (2020 ) has done a detailed analysis for it.

# Conclusions

This research study explores the significant privacy and security issues with IoT technology, focusing on consumer misunderstanding, vulnerability, as well as adoption. It accomplishes this through reviewing over significant works and highlighting novel models as well as multilayered strategies for improving IoT security, like cloud/edge solutions as well as new frameworks. The research additionally investigates at privacy concerns concerning wearable technology and the Internet of medical things, offering a thorough rundown of current risks and countermeasures. Overall, it underlines the necessity of cutting-edge techniques and solutions to guarantee a dependable and safe Internet of Things environment.

# References

Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 18-33. <https://www.journals.gaftim.com/index.php/ijtim/article/download/12/4>

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. <https://www.mdpi.com/2076-3417/10/12/4102>

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. *Digital twin technologies and smart cities*, 123-149. <https://www.researchgate.net/profile/Hany-Atlam/publication/332859761_IoT_Security_Privacy_Safety_and_Ethics/links/5d45d26992851cd0469f9f62/IoT-Security-Privacy-Safety-and-Ethics.pdf>

Ioannidou, I., & Sklavos, N. (2021). On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. *Cryptography*, *5*(4), 29. <https://www.mdpi.com/2410-387X/5/4/29>

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927. <https://www.mdpi.com/2076-3417/12/4/1927>

Aziz Al Kabir, M., Elmedany, W., & Sharif, M. S. (2023). Securing IOT devices against emerging security threats: Challenges and mitigation techniques. *Journal of Cyber Security Technology*, *7*(4), 199-223. <https://www.tandfonline.com/doi/pdf/10.1080/23742917.2023.2228053>

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics*, *11*(20), 3330. <https://www.mdpi.com/2079-9292/11/20/3330>

Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT security. *IoT security: advances in authentication*, 27-64. <https://www.researchgate.net/profile/Anca-Jurcut/publication/336406296_Introduction_to_IoT_Security/links/5dea257d92851c836465d0af/Introduction-to-IoT-Security.pdf>

Diro, A., Reda, H., Chilamkurti, N., Mahmood, A., Zaman, N., & Nam, Y. (2020). Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication. *IEEE Access*, *8*, 60539-60551. <https://ieeexplore.ieee.org/iel7/6287639/6514899/09045934.pdf>

Barua, A., Al Alamin, M. A., Hossain, M. S., & Hossain, E. (2022). Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *3*, 251-281. <https://ieeexplore.ieee.org/iel7/8782661/8901158/09706334.pdf>

Raikar, M. M., & Meena, S. M. (2021, May). SSH brute force attack mitigation in Internet of Things (IoT) network: An edge device security measure. In *2021 2nd international conference on secure cyber computing and communications (ICSCCC)* (pp. 72-77). IEEE. <https://www.researchgate.net/profile/Meenaxi-Raikar/publication/353378415_SSH_brute_force_attack_mitigation_in_Internet_of_Things_IoT_network_An_edge_device_security_measure/links/60f911492bf3553b2902ba92/SSH-brute-force-attack-mitigation-in-Internet-of-Things-IoT-network-An-edge-device-security-measure.pdf>