IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

AN ANALYSIS ON DIFFERENT IOT BASED SECURITY APPROACHES.

[1]Prof. Sonam Dubey, [2]Prof. Anjali Vishwakarma, [3]Dr. Ritu Shrivastava,[4]Prof. Amit Dubey
[1]Asst. Professor,[2] Asst. Professor, [3] Professor, [4]Assoc. Professor
[1]Computer Science and Engineering Department,
[1]Sagar Institute of Research and Technology, Bhopal, India

Abstract:

The paper investigates various security measures within the realm of the Internet of Things (IoT). It is expected to cover strategies aimed at enhancing the security of IoT systems, with a primary focus on protecting devices, networks, and data from potential threats and vulnerabilities. The content likely includes discussions on encryption methods, authentication approaches, secure communication protocols, and other pertinent security measures specific to IoT. Through a comprehensive survey and analysis of these security strategies, the paper aims to offer valuable insights into effective approaches for addressing security challenges associated with IoT.

Index Terms - *Internet of Things (IoT), cloud computing, RFID research, Ad Hoc Network, hybrid wireless networks.*

I. INTRODUCTION

The Internet of Things (IoT) represents a transformative paradigm in the realm of technology, signaling the convergence of physical devices, sensors, and network connectivity to enable seamless communication and data exchange. In this interconnected landscape, everyday objects are embedded with smart capabilities, allowing them to collect, transmit, and receive data in real-time. The essence of IoT lies in its ability to create an intricate web of interconnected devices, ranging from household appliances and industrial machinery to wearable gadgets and smart infrastructure. This interconnected ecosystem facilitates the generation of vast amounts of data, providing valuable insights and enabling more informed decision-making processes. As IoT continues to evolve, it promises to revolutionize diverse sectors, including healthcare, transportation, agriculture, and urban planning, ushering in an era of unprecedented efficiency, automation, and connectivity.

The introduction of IoT has not only redefined the way we interact with technology but has also opened up new possibilities for innovation, ushering in a future where our surroundings are seamlessly integrated into the digital life. The integration of the Internet of Things (IoT) and cloud computing represents a powerful synergy that has significantly transformed the landscape of modern technology. IoT devices, embedded with sensors and communication capabilities, generate vast amounts of data, and cloud computing provides the ideal infrastructure for processing, storing, and analyzing this data.

IoT devices can offload resource-intensive tasks, such as data storage and complex analytics, to powerful cloud servers. This not only enhances the efficiency of IoT devices but also allows for scalable and cost-effective solutions .Cloud platforms offer the necessary computational power, storage Security and privacy are critical considerations in IoT, and cloud computing plays a pivotal role in addressing these concerns. Cloud providers implement robust security measures, including encryption and authentication protocols, helping safeguard the sensitive data transmitted and stored by IoT devices. Additionally, centralizing security management in the cloud enables consistent monitoring and updates, reducing vulnerabilities across the IoT ecosystem. Furthermore, the cloud facilitates seamless communication and collaboration between different IoT devices and applications. It acts as a centralized hub where data from various sources can be aggregated, processed, and made available for real-time decision-making. This interconnectedness enhances the overall functionality and utility of IoT solutions.

II. Literature Survey

I.Integration of cloud computing and internet of things: A survey.

Botta, A.; de Donato, W.; Persico, V.; Pescapé [1] have presented , the paper addresses the integration of Cloud Computing and the Internet of Things (IoT), referred to as the Cloud IoT paradigm. While existing literature has separately explored Cloud and IoT, examining their individual properties, features, technologies, and challenges, there is a notable absence of a comprehensive analysis of the emerging CloudIoT paradigm. The paper aims to fill this gap by conducting a literature survey that delves into the integration of Cloud and IoT. The analysis begins by examining the fundamentals of both IoT and Cloud Computing, with a focus on uncovering new applications, challenges, and research issues arising from the integration of these two technologies.

II. On the interplay of Internet of Things and Cloud Computing: A systematic mapping study.

Cavalcante, E.; Pereira, J.; Alves, M.P.; Maia, P.; Moura, address the integration of Internet of Things (IoT) and Cloud Computing, focusing on identifying open issues for future research and development. The paper aims to fill a gap in the existing literature by systematically collecting and analyzing studies related to the integration of IoT and Cloud Computing. The specific goals include obtaining a comprehensive understanding of integration providing an overview of the current state of research, and identifying gaps and potential research directions. The methodology involves a systematic mapping study that covers recently published papers in journals, conferences, and workshops related to the topic.

III. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing

Cavalcante, E.; Pereira, J.; Alves, M.P.; Maia, P.; Moura, R.;Batista,T,Delicato,F.C.;Pires,P.F.[3]provides a comprehensive survey of integration components in the context of the Internet of Things (IoT) and cloud computing. It focuses on three key elements: Cloud platforms, Cloud infrastructures, and IoT Middleware. Additionally, the survey covers integration proposals and data analytics techniques relevant to this integration. The paper not only explores the existing landscape but also highlights various challenges and open research issues associated with the integration of Cloud platforms, Cloud infrastructures, and IoT Middleware. By addressing these components and associated challenges, the paper contributes to a better understanding of the current state of integration in IoT and cloud computing, providing insights into potential areas for further research and development.

IV. Data mining for internet of things: A survey.

Tsai, C.-W.; Lai, C.-F.; Chiang, M.-C.; Yang, L.T.[4] it provides a concise review of the features associated with "data from IoT" and "data mining for IoT." The paper concludes by addressing changes, potentials, open issues, and future trends within this field. The aim is to offer insights into the current state and potential developments in the realm of IoT data and data mining, setting the stage for understanding the evolving landscape of this technology.

V.Internet of things: Vision, applications and research challenges. Ad Hoc Network.

Miorandi,D.;Sicari,S.;dePellegrini,F.;Chlamtac[5] This article discusses the concept of the "Internet of Things" (IoT), which refers to the extension of the Internet and the Web into the physical world through the deployment of devices with embedded identification, sensing, and actuation capabilities. The IoT aims to connect digital and physical entities using information and communication technologies, paving the way for new applications and services. The article provides a survey of IoT technologies, applications, and research challenges, offering insights into the current state and potential future developments in this rapidly evolving field.

*VI. **Internet of things in industries: A survey.***

Da-Xu, L.; He, W.; Li, S. [6] This paper provides a comprehensive review of the current research landscape in the field of the Internet of Things (IoT). It covers key enabling technologies, major applications of IoT in various industries, and highlights ongoing research trends and challenges. The main contribution of the paper lies in systematically summarizing the state-of-the-art of IoT in industries, offering a valuable resource for understanding the current advancements and directions in this rapidly evolving domain.

*VII. **RFID technology and its applications in Internet of Things (IoT).***

Jia, X.; Feng, Q.; Fan, T.; Lei, Q.[7] This paper explores The Radio Frequency Identification System (RFID),an automatic technology that facilitates the identification metadata recording, and control of objects through radio waves. By connecting RFID readers to the Internet, these devices can globally identify, track, and monitor objects in real-time, forming the basis for the Internet of Things (IoT). The paper introduces RFID and IoT technologies, delves into the applications of RFID within the IoT framework, and discusses the associated challenges in implementing RFID technology in IoT systems.

VIII. RFID research: An academic literature review (1995 - 2005) and future research directions.

Ngai, E.; Moon, K. Int. J. Prod. Econ. 2008[8]The analysis of various papers on Radio Frequency Identification (RFID) literature yields valuable insights into the structure of this domain, serving as a beneficial resource for knowledge creation and accumulation. The review includes a comprehensive list of references, making it a valuable tool for individuals interested in RFID research. The paper aims to stimulate further interest in the field and provides implications for both RFID researchers and practitioners. Additionally, suggestions for future research areas are discussed, contributing to the ongoing development and exploration of RFID technology.

IX. Security Framework for Internet of Things (IoT)

Sherif El-Gendy; Marianne. A. Azer[9] In our approach to IoT security, we concentrate on securing IoT devices, applications, and networks. This includes addressing potential attack vectors and meeting essential security requirements for IoT systems. Additionally, we emphasize the organizational perspective on IoT security, advocating for training, incident response planning, and compliance. Our proposed security architecture aims to enable secure IoT services, establishing a baseline for effective security deployment. The comprehensive strategy encompasses authentication, encryption, network segmentation, and continuous monitoring to create a robust defense against potential threats and vulnerabilities in the dynamic IoT landscape.

X. Security Issues and Architecture of IOT.

Kushagra Jha; Sitara Anumotu; Pronika; Kritika Soni[10]This research work focuses on IoT-based applications and their vulnerabilities, examining the challenges and issues faced by IoT devices. The paper discusses specific security requirements in IoT applications and concludes proposing solutions to address these challenges. The goal is to provide insights that contribute to steering the development of IoT applications in a more secure direction.

XI. An Architectural Approach towards the Future Internet of Things;

Uckelmann,D.;Harrison, M.; Michahelles, F 50. [11] This Paper endeavors to outline a conceptual framework for the future architecture of the Internet of Things (IoT). It encompasses a definition of IoT, a review of ongoing developments, a compilation of key requirements, and a technical design proposal for potential implementation. The chapter addresses open issues such as evaluating usability in both user-centric and business-centric scenarios, as well as emphasizing the importance of quantifying costs and benefits for various stakeholders, including businesses, consumers, society, and the environment. The conclusion offers guidelines derived for the benefit of researchers and practitioners in the field of IoT.

XII. Integration of hybrid wireless networks in cloud services oriented enterprise information systems.

Li,S.; Xu, L.;Wang, X.;Wang, J. [12] The proposed approach involves the integration of access control functionalities into a hybrid framework, offering users filtered views of available cloud services based on both service access requirements and user security credentials. The future plan includes implementing this framework on the SwanMesh platform, with an additional integration of the UPnP standard into an enterprise information system. This development aims to enhance user access to cloud services while ensuring security and compatibility within the enterprise environment.

XIV. Data cleaning for RFID and WSN integration.

Wang, L.; Da-Xu, L.; Bi, Z.; Xu, Y[13]. This paper addresses key challenges in integrating Wireless Sensor Networks (WSN) and Radio-Frequency Identification (RFID) technologies. It introduces a five-layer system architecture aimed at achieving synergistic performance. The communication efficiency issue, arising from redundant data leading to increased energy consumption and time delays in WSN and RFID integration, is highlighted. The paper proposes an improved data cleaning algorithm to tackle this challenge, demonstrating its feasibility and effectiveness through simulations and comparisons with existing algorithms. Furthermore, the application of the developed architecture and data cleaning algorithm in relief supplies storage management is discussed to illustrate their practical capacity.

*XV. **Internet of things (IoT) security: Current status, challenges and prospective measures** .*

Rwan Mahmoud; Tasneem Yousuf; Fadi Aloul; Imran Zualkernan[14] the authors proposed an overview encompassing security principles, technological and security challenges, proposed countermeasures, and outlines future directions for enhancing IoT security.

XVI. IoT Security: Ongoing Challenges and Research Opportunities

Zhi-KaiZhang; MichaelChengYiCho; Chia-Wei Wang;Hsu; Chong-Kuan Chen; Shiuhpyn[15],This paper initiates with a general overview of the information security background in the context of the Internet of Things (IoT). It then delves into the information security challenges that IoT is likely to face. Finally, the paper highlights potential research directions that could serve as future endeavors for devising solutions to address the security challenges confronting IoT. The objective is to provide a comprehensive understanding of the information security landscape within the realm of IoT and guide future research initiatives for enhancing its security.

XVII. The Current Research of IoT Security

Jian Zhang; Huaijian Chen; Liangyi Gong; Jing Cao; Zhaojun Gu [16] This paper provides a comprehensive review of the threat challenges and security models associated with each level of the Internet of Things (IoT) in recent years. It delves into the various IoT security threats, systematically examining them from the perspectives of physics, network, and data. The paper introduces mainstream IoT security models and subsequently discusses solutions to address these threats. Three key perspectives are explored: IoT access control, intrusion detection, and distribution methods. The paper concludes by highlighting the absence of a unified standard in the current IoT security models and expresses expectations for the development of a cohesive and standardized future security model.

XVII. IOT BASED ALL IN ONE SECURITY SYSTEM.

ItishaVarshney; Anushka Chowdhury; Afaq Ahmad; Hriday Banerjee [17] The project is designed to enhance security by detecting various environmental hazards, including gas leaks (using MQ6 and MQ135 sensors), temperature changes (via LM-35 sensor), fire, smoke, and unwanted movement (using a motion sensor). When any of these hazards are detected, the system alerts the user by sending a message and activating a buzzer. The GSM modem plays a crucial role in transmitting sensor readings to an IoT website, facilitated by AT commands. A 16 x 2 alphanumeric display provides a visual representation of the data. The buzzer serves as an audible indicator when sensor readings surpass predefined threshold levels. This integrated system provides a comprehensive solution for monitoring and alerting users about potential safety risks.

CONCLUSION

The Internet of Things (IoT) refers to the network of interconnected devices, objects, and systems that communicate and share data with each other through the internet. In this paper I have surveyed different IoT based papers (2008-2023).In this there is the exploration of various security measures within the IoT context. It may emphasize the importance of strategies aimed at safeguarding devices, networks, and data in the face of potential threats and vulnerabilities. The paper could highlight the significance of encryption techniques, authentication methods, secure communication protocols, and other security measures specific to IoT.By synthesizing insights gained from the survey and analysis of different security strategies, the paper aims to contribute to the development of effective approaches for addressing the unique security challenges associated with IoT systems. It might call for ongoing research, collaboration, and innovation in the field to stay ahead of emerging threats and ensure the continued growth and adoption of IoT technologies with a strong focus on security.

REFERENCES

[1] Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. Integration of cloud computing and internet of things: A survey. Future
Gener. Comput. Syst. 2016, 56, 684–700.

[2]Cavalcante, E.; Pereira, J.; Alves, M.P.; Maia, P.; Moura, R.; Batista, T.; Delicato, F.C.; Pires, P.F. On the interplay of
Internet of Things and Cloud Computing: A systematic mapping study. Comput. Commun. 2016, 89–90, 17–33.

[3] Díaz, M.; Martín, C.; Rubio, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud
computing. J. Netw. Comput. Appl. 2016, 67, 99–117.

[4] Tsai, C.-W.; Lai, C.-F.; Chiang, M.-C.; Yang, L.T. Data mining for internet of things: A survey. Commun. Surv. Tutor.
IEEE 2014, 16, 77–97.

[5] Miorandi, D.; Sicari, S.; de Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research Challenges.
Ad Hoc Netw. 2012, 10, 1497–1516.M

[6]. Da-Xu, L.; He, W.; Li, S. Internet of things in industries: survey. Ind. Inform. IEEE Trans. 2014, 10,2233–2243.

[7]. Jia, X.; Feng, Q.; Fan, T.; Lei, Q. RFID technology and applications in Internet of Things (IoT).In Proceedings of the 2nd
International Conference on Consumer Electronics,Communications and Networks (CECNet), Yichang, China,
21–23 April 2012; pp. 1282–1285.

[8] . Ngai, E.; Moon, K. RFID research: An academic literature review (1995–2005) and future research directions.Int. J. Prod.
Econ. 2008, 112, 510–520.

[9]. Sherif El-Gendy; Marianne. A. Azer .Security Framework for Internet of Things (IoT) 2020 15th International
Conference on Computer Engineering and Systems (ICCES) Cairo, EgyptDecember 2020.

[10]. Kushagra Jha; Sitara Anumotu; Pronika Security Issues and Architecture of IOT 2021 International Conference on Artificial Intelligence and Smart Systems(ICAIS) march 2021 Coimbatore, India.

[11]. Uckelmann, D.; Harrison, M.; Michahelles, F. An Architectural Approach towards the Future Internet of Things ;Springer: Berlin, Germany, 2011.

[12]. Li, S.; Xu, L.;Wang, X.;Wang, J. Integration of hybrid wireless networks in cloud services oriented enterprise information systems. Enterp. Inf. Syst. 2012, 6, 165–187.

[13] Wang, L.; Da-Xu, L.; Bi, Z.; Xu, Y. Data cleaning for RFID and WSN integration. Ind. Inform. IEEE Trans. 2014,10, 408–418.

[14]. Rwan Mahmoud; Tasneem Yousuf; Fadi Aloul; Internet of things (IoT) security: Current status, challenges and prospective measures 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) London, UK June 2019.

[15].Zhi-Kai Zhang; Michael Cheng Yi Cho; Chia-Wei Wang; Chia-Wei Hsu; Chong-Kuan Chen; Shiuhpyn IoT Security: Ongoing Challenges and Research Opportunities 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications Matsue, Japan.

[16]. Jian Zhang; Huaijian Chen; Liangyi Gong; Jing Cao; Zhaojun Gu :The Current Research of IoT Security. 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC) Hangzhou, China.

[17]. Itisha Varshney; Anushka Chowdhury; Afaq Ahmad; Hriday Banerjee : IoT based all in one Security System,2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks(IEMECON) Jaipur, India.