Bit-Tech (Binary Digital - Technology)

Vol.7, No.1, August 2024
Available online at: http://jurnal.kdi.or.id/index.php/bt

IoT Security Attacks on the Public Sector: Systematic Literature Review

Fandan Dwi Nugroho Wicaksono[1], Winny Purbaratri[2]*, Moch Fajar Purnomo Alam[3], Agnes Novita Ida Safitri[4]

[1)2)4)]Perbanas Institute,[3)]Universitas Kristen Satya Wacana
[1)2)4)]Jl.Kuningan, Jakarta, Indonesia, [3)]Jl.Salatiga, Jawa Tengah, Indonesia

[1)]fandan.dwi@perbanas.id

[2)]winny.purbaratri@perbanas.id

[3)]9802022025@student.uksw.edu

[4)]agnes.novita@perbanas.id

Article history:

Received 19 August 2024;
Revised 20 August 2024;
Accepted 20 August 2024;
Available online 20 August 2024

Keywords:

Attack
e-Government
IoT
Public Sector
Security

Abstract

The primary objective of this study is to examine security threats that specifically target the Internet of Things (IoT) used in the Public Sector. This sector is widely acknowledged as a crucial element of the fourth industrial revolution. The high volume of intelligent devices employed in the public sector, which are linked in the Internet of Things (IoT), and each of them transmits sensitive data in numerous instances, makes security of utmost importance. The objective of this study is to categorize various forms of security attacks and propose strategies to mitigate security breaches through many approaches. This study employed a systematic review, which is a methodical examination of current literature. The data synthesis methodology in this study consisted of comparing 15 literature sources that had been evaluated for quality and satisfied the specified criteria for inclusion and exclusion. The utilized database sources include renowned platforms such as Scopus, ACM, and IEEE. The present study employs a qualitative methodology, specifically utilizing the perspectives of two information security specialists to examine the existing literature. The findings of this study have made a meaningful contribution to the field of public sector. This study categorizes four types of assaults against Public Sector IoT: 37% Denial-of-Service (DoS) attacks, 31% Malware attacks, and 19% Phishing attacks. System attacks account for 13% of all system attacks. By contrast, 50% of the security attack mitigation strategies rely on authentication, 36% on Secure Communication, and 14% on Application Security.

I. Introduction

The Internet of Things (IoT) is a widely adopted technology throughout the globe that facilitates the connection of various objects, including sensors, automobiles, hospital devices, industries, and domestic appliances, over the internet [1]. The Internet of Things (IoT) is a progressive development of the Internet concept, which establishes a worldwide framework for linking devices and humans [2]. The Internet of Things (IoT) has garnered significant attention from both academic and industrial sectors. A multitude of information carriers, including radio frequency identification (RFID), sensors, smart devices, the Internet, smart networks, cloud computing, and vehicle networks, are integrated into the Internet of Things (IoT). The Internet of Things (IoT) refers to a concept of a global ecosystem where b*illions of things equipped with intelligence, communication, and sensing and actuation capabilities will be interconnected over IP (Internet Protocol) networks [3]. Internet connectivity ensures constant availability of data and devices. The Internet of Things (IoT) is formed by the linking of properly identifiable entities (objects) and diverse networks. An alternative definition of the Internet of Things (IoT) explicitly excludes it from being classified as a device or technology. More precisely, it is a theoretical structure, motivated by the concept of combining connectivity and intelligence among gadgets [4].

The integration of Internet of Things (IoT) technology in the public sector has extended to and affected many facets of services and infrastructure, encompassing, The implementation of closed-circuit television (CCTV) cameras linked to the internet network facilitates the real-time monitoring of security and coordination of urban traffic [5]. Public transit management, smart parking systems, and vehicle tracking are all applications

[*] Corresponding author

ISSN 2622-2728 (online) 2622-271X (print) © 2018 The Authors. Published by Komunitas Dosen Indonesia.
This is an open access article under the CC BY-SA 4.0 license (http://creativecommons.org/licenses/by/4.0/)
doi: 10.32877/bt.v7i1.1627

of the Internet of Things (IoT) [6][7][8]. Within the healthcare industry, the Internet of Things (IoT) enables communication between patients and healthcare professionals, as well as immediate monitoring of patient well-being, thereby potentially decreasing hospital transfers and expediting medical interventions[9]. The adoption of IoT in villages provides enhancements in quality of life by using technology that facilitates activities such as water resource management, security, and related public services [10]. This include the provision of transportation information and the implementation of automatic water level recording (AWLR), which facilitates improved management of natural resources and urban planning [11].

This study is significant because the Internet of Things (IoT) is extensively employed in vital government infrastructure, ranging from traffic control to public security applications. Malicious attacks on these systems can result in significant disruption and financial damage [12]. Security assaults have the potential to cause data breaches, compromise the privacy of residents, and reduce public confidence in government [13]. The IoT is confronted with intricate security risks including unauthorized access, man-in-the-middle attacks, DDoS breaches, and viruses. An analysis of strategies to mitigate these risks is crucial for preserving the integrity and dependability of e-government systems [14]. As the number of Internet of Things (IoT) linked devices increases, the complexity and security issues they encounter also escalate. Research can facilitate the development of efficient security solutions to mitigate the threats linked to these interconnected devices. The threat posed by IoT-based attacks on the public sector to national security necessitates additional research to enhance the development of more resilient and proactive defense mechanisms.

The methodologies employed in comparable studies include literature reviews and article surveys. The current research findings encompass a wider range of objects, specifically the Internet of Things (IoT), which have application within the public sector.

The current body of research on the many forms of IoT hazards employed in the public sector remains limited. Through the identification and classification of various types of attacks such as Denial of Service (DoS), Man-in-the-Middle (MitM), and data injection attacks, this research makes a substantial contribution to enhancing IoT security in the public sector.

Furthermore, the study suggests several defensive strategies such as sophisticated encryption methods, integration of blockchain technology, and application of machine learning algorithms to mitigate the vulnerability to security breaches. Through thorough examination and suggested pragmatic remedies, this study not only enhances the security of IoT systems but also contributes to the formulation of more efficient and all-encompassing security frameworks, so fostering public confidence and safeguarding vital government infrastructure.

II. RELATED WORKS/LITERATURE REVIEW

Research conducted to identify security threats to IoT in the public sector encompasses several methodologies, including systematic reviews, bibliometric analyses, and standard literature reviews.

This paper highlights the susceptibility of IoT systems to a range of attacks, encompassing however not restricted to Denial of Service (DoS)[15], Man-in-the-Middle (MitM), Furthermore, data injection attacks. As an illustration, within the healthcare industry [16], Internet of Things (IoT) devices used for patient monitoring are extremely susceptible to data breaches and illegal manipulation. Similarly, in the execution of intelligent urban networks [17] , failure to implement robust security measures while integrating numerous IoT devices can result in substantial hazards, including the potential disruption of vital infrastructure functions. The paper suggests many defensive strategies, such as utilization of sophisticated encryption methods, integration of blockchain technology for secure data administration, and application of machine learning algorithms to promptly identify and address security risks. The development of standard security standards and the regular execution of security audits are emphasized as crucial measures to enhance the resilience of IoT systems against rising cyber threats.

III. METHODS

An often-employed approach is to carry out a research literature review or a written literature review. With the growing use of research reviews in shaping policy and practice decisions, the significance of the credibility of these reviews becomes more pronounced [18]. Prior scholars have conducted numerous such investigations dispersed over different scientific literature, thereby necessitating a methodical approach to compilation. A comprehensive analysis was carried out using the Kitchenham criteria as outlined in prior study publications. [19]. To address the two research inquiries listed in Table 1. Publications sourced from global scholarly journals and conferences. Aggregated from the digital repositories of three renowned publishers, specifically ACM, IEEE, and Scopus Digital Library. The research conducted to categorize the collection into four tiers is depicted in Figure 1. A first level of filtering was conducted, followed by a subsequent stage of filtering the literature and synthesising the various forms of literature.

A. Strategy for Data Search

IoT Security Attack and Public Sector are the designated areas of focus inside this electronic database. Keywords exert a significant impact on the quality of search results, so its influence extends to the search process as well. During the paper search, several often used or broad terms were included, as they were widely utilized in the majority of the research.

B. Information Source

Collected from the electronic databases of three well-known publishers, namely ACM, IEEE and Scopus Digital Library.

C. Eligibility Criteria

The study's eligibility criteria encompass both inclusion and exclusion criteria. TABLE 2outlines the inclusion criteria for this research, which include 1) Literature in the form of scientific publications and/or proceedings. 2) Scientific journals and /or proceedings sources include ACM, IEEE, and Scopus Digital Library. 3) Scientific journals and/or proceedings are publicly accessible and privately restricted. 4) Articles must be available in their complete text. 5) Scientific journals and/or proceedings are written in English. 6) Scientific journals and/or proceedings are published typically between the years 2020 and 2024. Discussions in scientific publications and proceedings encompass IoT security breaches targeting the public sector.

D. Quality Assessment

Literature selection using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-analyses) method[20]. The PRISMA Flow Diagram in this research is shown in Fig. 1.

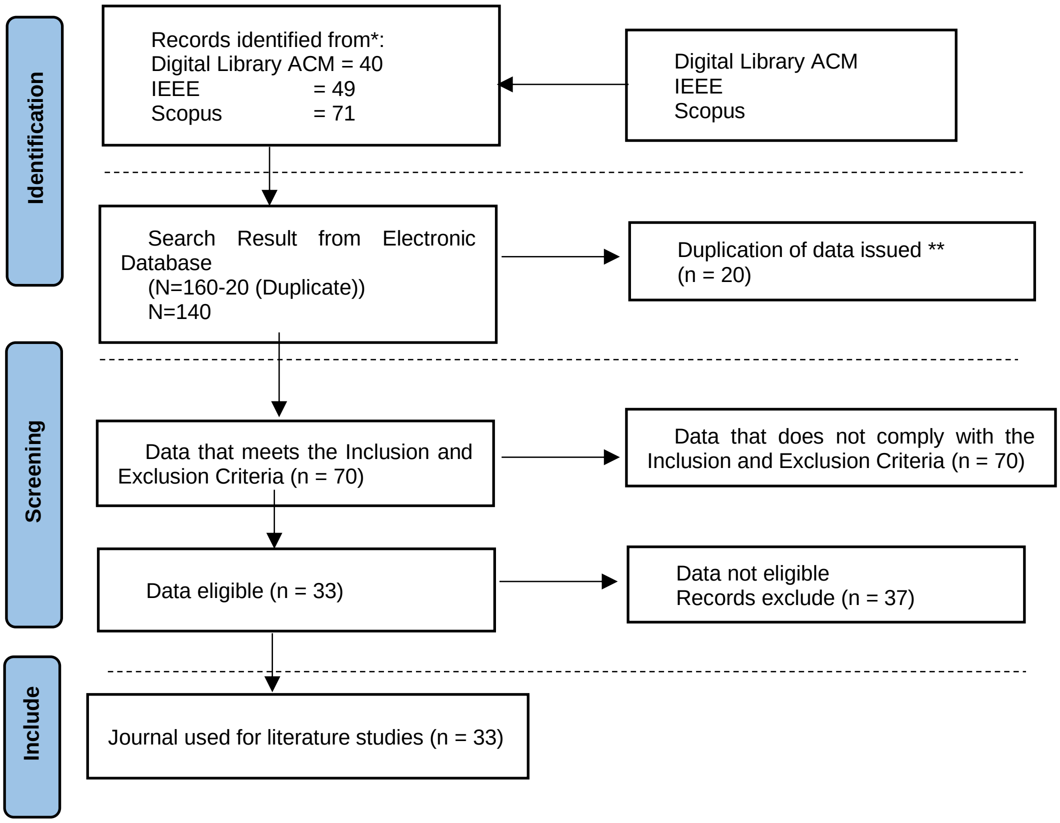
Identification
Records identified from*:
Digital Library ACM = 40
IEEE = 49
Scopus = 71
Digital Library ACM
IEEE
Scopus
Search Result from Electronic Database
(N=160-20 (Duplicate))
N=140
Duplication of data issued **
(n = 20)
Screening
Data that meets the Inclusion and Exclusion Criteria (n = 70)
Data that does not comply with the Inclusion and Exclusion Criteria (n = 70)
Data eligible (n = 33)
Data not eligible
Records exclude (n = 37)
Include
Journal used for literature studies (n = 33)

Fig. 1 Prisma Flow Diagram

The PRISMA approach yielded results indicating that out of 160 journal articles and sessions evaluated, 20 were eliminated due to data duplication, while another 107 did not satisfy the inclusion and exclusion criteria. Merely 33 scholarly articles were included in the literature analysis.

E. Data Synthesis

The data synthesis procedure in this study involved comparing literature that satisfied the quality evaluation and the chosen criteria for inclusion and exclusion. Synthetic data pertains to the scientific endeavor of detecting and analyzing the prevalent forms of attacks on IoT in the public sector, with the aim of devising strategies to mitigate these risks.

F. Data Extraction

A tabular representation of the data extraction result includes the researcher's name, publication year, research title, research object, research design, prevalent types of assaults against IoT in the public sector, and proposed solutions to mitigate these risks.

G. Article Quality Assessment

A questionnaire was administered to each literary work included in this study in order to obtain a literature evaluation. TABLE 3 presents a concise overview of the questions and criteria used to evaluate the quality of each piece of literature examined. In order to mitigate the impact of subjective viewpoints, the reliability of the evaluation literature is established by the degree to which the instrument has undergone previous validation. The validation technique was improved by the evaluation of two specialists by analyzing a set of probing questions. Subject matter experts are chosen based on their specialized knowledge and professional experience in the field of information security and the Internet of Things (IoT).

TABLE 1
RESEARCH QUESTIONS

Research Questions	Description
Q1 : This study aims to investigate the prevailing forms of cyber threats against IoT infrastructure in the public sector and propose effective mitigations?	The aim is to identify and analyze the types of attacks that often occur on IoT in the public sector and find solutions to reduce these risks.
Q2 : Which strategies have been adopted to mitigate the vulnerability to security breaches?	The objective is to tackle the distinct security vulnerabilities encountered by IoT in public settings.

TABLE 2
ELIGIBILITY CRITERIA

Inclusion	• Publication Year 2020-2024 • Sources: Esteemed International Journals and International Seminars • Obtained from electronic publisher databases • Focuses of IoT security threats • Exclusively available online version • Articles with unrestricted access
Exclusion	• Only a brief summary of the article/abstract • The article writing language is not English.

TABLE 3
ARTICLE QUALITY ASSESSMENT

Quality Assessment		Sum	%
Does the research focus on information security attacks and their solutions?		33	100 %
All	The article describes information security attacks and solutions against IoT in the Public Sector	30	90%
Half	The article partly describes information security attacks against IoT in the Public Sector	2	7%
None	The article does not describe information security attacks against IoT in the Public Sector	1	3%

IV. RESULTS

The final results yielded 33 papers that align with the study topics, as shown in TABLE 4. To address the initial research inquiry, what are the many categories of security assaults targeting IoT in the public sector? Meanwhile, TABLE 5 provides a response to the second research question, specifically addressing the measures that have been adopted to mitigate the vulnerability to security assaults.

TABLE 4
SECURITY ATTACK SYNTHESIS ARTICLE RESULTS

No	Code	Author	Attack Type	Ref
1	C1	(Shayma, A and Wael, E)	Denial-of-Service (DoS)	[21]
2	C2	(Parvathy, K and Nataraj, B)		[22]
3	C3	(A, Gupta, A, Kapoor et.al)		[23]
4	C4	(Westerlund,O and Asif, R)		[24]
5	J1	(Meng, W et al)		[25]
6	J2	(Abbas, S et al)		[26]
7	C5	(Krishna,ODS et al)	Malware	[27]
8	C6	(Kala,M.K and Priya,M)		[28]
9	C7	(Ramzan, T and Zafar, M)		[16]
10	C8	(Singh,J et al)		[29]
11	C9	(Bajpai,P and Enbody,R)		[30]
12	J3	(Pegorini, et al)	Phishing	[31]
13	C10	(Matey, AH et al)		[32]
14	C11	(Iacovazzi, A et al)		[33]
15	C12	(Chavis, JS and Syed DP)	Attacks on System	[34]
16	J4	(Kumari, S et al)		[35]

Code: J= Journal; C= Conference

TABLE 5
RESULTS OF THE SOLUTION SYNTHESIS ARTICLE CARRIED OUT

No	Code	Author	Solution	Ref
1	C13	(Lama,R and Karmakar, S)	Authentication	[36]
2	C14	(Liu et al.)	Secure Communication Solutions	[37]
3	C15	(Almulhim, M and Zaman,N)		[38]
4	C16	(Shakeel, M et al.)		[39]
5	C17	(Jaison, F et al.)		[40]
6	C18	(Pahlevi, RR et al.)		[41]
7	C19	(Mishra, AK et al.)		[42]
8	J5	(Hussein, SM et al.)		[43]
9	C20	(Altayran, S et al.)		[44]
10	C21	(An,Y et al.)		[45]
11	C22	(Vangala, A et al.)		[46]
12	C23	(Lourens, M et al.)		[47]
13	J6	(Gutfleisch, M et al)	Application Security	[48]
14	J7	(Dang, LM et al)		[49]

Code: J= Journal; C= Conference

V. DISCUSSION

A. Security Attacks on Public Sector IoT

The security threats targeting Public Sector IoT encompass Denial-of-Service (DoS), Malware, Phishing, and System Attacks. This information was acquired from a comprehensive review of 16 scholarly articles. The overall distribution of research subjects on security assaults on Government IoT from 2020 to 2024 is depicted in Fig. 2. Approximately 37% of research studies pertain to the subject of Denial-of-Service (DoS) assaults, with 31% specifically addressing Malware attacks and 19% focusing on Phishing. Various subjects address exploitations of the system (System Attacks). In conclusion, the predominant security threats targeting government IoT are Denial-of-Service (DoS) and Malware. Similar to other IoT devices, security is frequently disregarded, resulting in many drones being susceptible to potential cyber attacks [24]. Internet of Things (IoT) network infrastructure is highly susceptible to attackers/hackers due to the open accessibility of supplementary functionalities [26]. The proliferation of intelligent and interconnected gadgets has led to an expansion of the threat surface, therefore increasing the likelihood of being exposed to Internet-based threats, including ransomware [30]. The primary focus of this research is on IoT security, privacy concerns, and measures adopted in the public health sector to safeguard sensitive data [28].

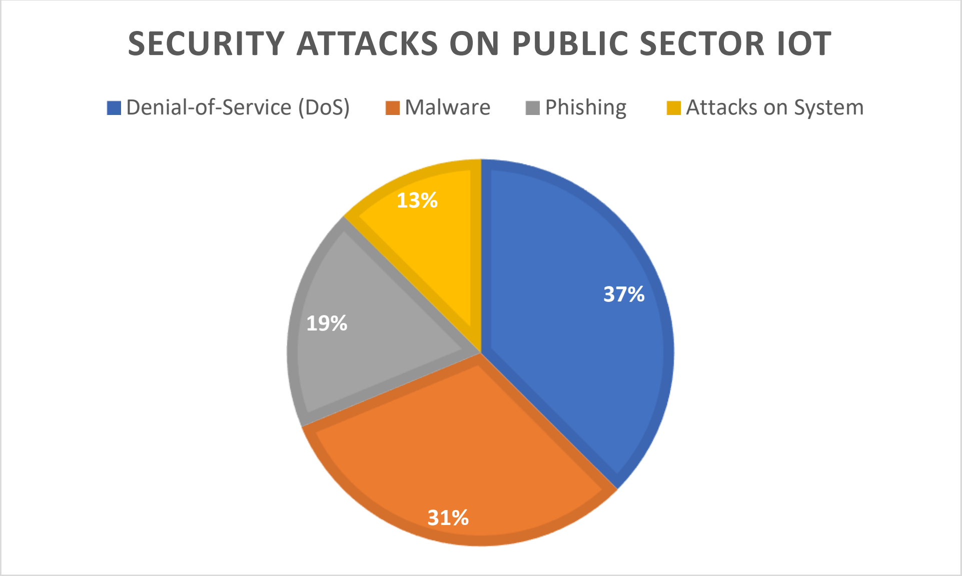

Fig. 2 Security Attacks on Public Sector IoT

B. *Solutions to overcome security attacks*

This study defines the various security risks encountered by IoT devices in the public sector, encompassing DDoS attacks, malware, and physical incursions. Potential remedies to counter these attacks encompass several strategic methodologies. Based on the findings of the literature search, a total of 14 publications were identified. The overall distribution of research topics on strategies to mitigate security threats on Government IoT from 2020 to 2024 is depicted in Figure 3. 50% of the research papers pertaining to vulnerabilities in assaults focus on authentication methods, while 36% employ Secure Communication methods. Only 14% of the studies propose solutions for Application Security. It can be inferred that the advancement of IoT devices is not accompanied by advancements in information security. Cyberattacks can use IoT devices as a novel entry point. Brute force and sniffer attacks are two types of attacks known to target IoT devices. Appropriate measures are required to prevent cyber-attacks. In order to prevent assaults, authentication measures might be employed. In addition to authentication mechanisms, alternative approaches to ensure secure network communication on IoT devices can also be considered. In the Smart Argo sector, novel scalable group distribution key management techniques and protocols are employed to facilitate secure communications in IoT systems [41]. Employing elliptic curve cryptography, the objective is to guarantee that the transmission of information between levels of the IoT architecture remains unaffected by sensor faults or deliberate attacks[43].

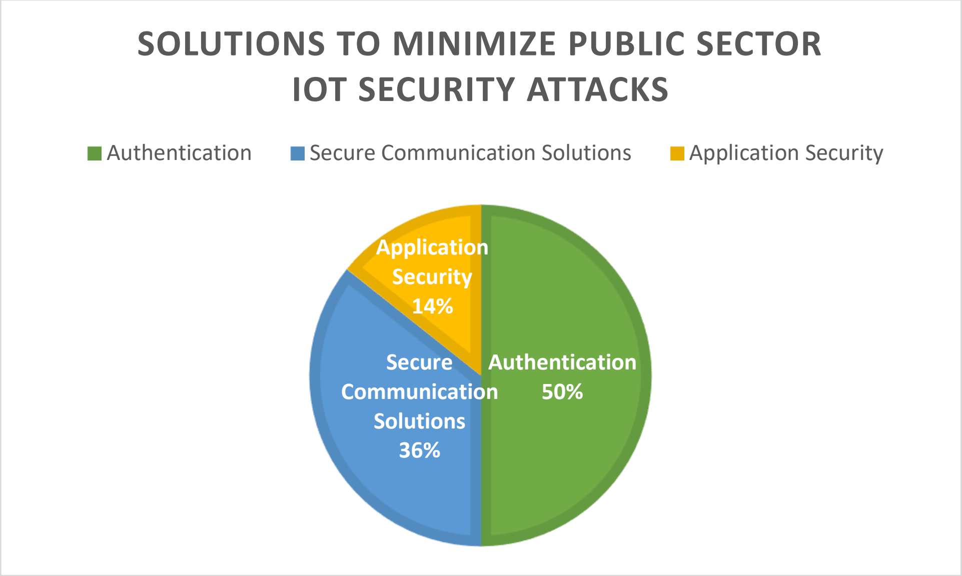

Fig. 3 Solutions to minimize public sector IoT security attacks

VI. CONCLUSIONS

A large percentage of IoT devices suffer from inadequate security as a result of compromised default configurations or infrequent updates. Consequently, this facilitates the access and exploitation of these devices by hackers. An Internet of Things (IoT) network has numerous interconnected devices, each of which might serve as a potential vulnerability for cyber attacks. The proliferation of devices amplifies the potential for hackers to exploit vulnerabilities in security systems. An assault known as Distributed Denial of Service (DDoS) involves the deliberate transmission of fraudulent traffic to a system or server, therefore rendering it unattainable for authorized users. The proliferation and inadequate security of IoT devices make them readily exploitable as "zombies" within the network, thereby making them a common target in such assaults. Internet of Things (IoT) devices frequently gather personal information from consumers. Insufficient security of these devices may result in the theft of this information by hackers, who can then exploit it for subsequent assaults.Future research should prioritize the development and application of advanced attack detection and mitigation techniques utilizing technologies like as machine learning and artificial intelligence.

Furthermore, it is necessary to conduct further investigation on the implementation of blockchain technology to enhance data security on Internet of Things (IoT) devices. Extensive study on the impact of worldwide security legislation and policies on the deployment of IoT in the public sector is critical to establish a comprehensive and effective framework for addressing changing security risks.

REFERENCES

[1] W. Najib, S. Sulistyo, and Widyawan, “Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 9, no. 4, pp. 375–384, 2020, doi: 10.22146/jnteti.v9i4.539.

[2] D. Serpanos and M. Wolf, *Internet-of-Things (IoT) Systems*. 2018. doi: 10.1007/978-3-319-69715-4.

[3] Q. F. Hassan, A. ur R. Khan, and S. A. Madani, *Internet of things*, vol. 44, no. 3. 2017. doi: 10.4018/ijssoe.2017070103.

[4] Peter Yeung, *Hong Kong Science Park*. 2017. [Online]. Available: http://hdl.handle.net/10722/28381

[5] V. N. Fathya *et al.*, “Pemanfaatan Teknologi Dalam Pelayanan Publik (E-Government)”, [Online]. Available: www.freepik.com

[6] L. Hidayat, E. Kurniawan, and M. Ramdhani, “Perancangan Sistem Palang Parkir Otomatis Dan Pendeteksi Slot Parkir Berbasis Iot,” *e-Proceeeding Eng.*, vol. 9, no. 2, pp. 174–180, 2022.

[7] G. R. Koten *et al.*, “Penerapan internet of things pada smart parking system untuk kebutuhan pengembangan smart city,” *J. Tek. Ind. dan Manaj. Rekayasa*, vol. 1, no. 1, pp. 49–59, 2023, doi: 10.24002/jtimr.v1i1.7204.

[8] Sumarno, H. S. Setiawan, V. H. Valentino, and A. S. Putra, “Penerapan Internet of Think (IoT) Pada Transportasi Cerdas,” *Semin. Nas. Pengaplikasian Telemat.*, vol. 1, no. 1, pp. 94–98, 2021.

[9] H. I. Adauwiyah, M. R. Kamaluddin, R. F. Al Kautsar, and F. Fitroh, “Systematic Literature Review terhadap Pemanfaatan Internet of Things (IoT) dalam Bidang Kesehatan,” *Appl. Inf. Syst. Manag.*, vol. 5, no. 2, pp. 67–74, 2022, doi: 10.15408/aism.v5i2.21187.

[10] L. A. Maulana, D. A. Saputra, A. K. Putra, and J. P. Surya, “PENERAPAN IOT DAN MEDIA INFORMASI PADA DESA KERTOSARI,” *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 1, no. April, pp. 873–887, 2015.

[11] Bunyamin, S. Wahjusaputri, and Johan, *Penerapan Model SMK Membangun Desa - IoT*, no. 0. 2016.

[12] P. Papadopoulou, K. Kolomvatsos, and S. Hadjiefthymiades, “Internet of Things in E-Government,” *Int. J. Artif. Intell. Mach. Learn.*, vol. 10, no. 2, pp. 99–118, 2020, doi: 10.4018/ijaiml.2020070106.

[13] B. A. Iswandari, “Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance,” *J. Huk. Ius Quia Iustum*, vol. 28, no. 1, pp. 115–138, 2021, doi: 10.20885/iustum.vol28.iss1.art6.

[14] M. amin Hariyadi and J. E. W. Prakasa, *Sistem Informasi Manajemen – Keamanan Sistem Informasi*, no. January. 2014. [Online]. Available: https://datakata.wordpress.com/2014/03/31/sistem-informasi-manajemen-keamanan-sistem-informasi/

[15] N. Saxena, D. S. Chakravarthi, A. N. Venkatesh, N. Soni, and S. Kant, “The Future of Blockchain Technology and the Internet of Things in Healthcare,” *Proc. 2022 Int. Conf. Innov. Comput. Intell. Commun. Smart Electr. Syst. ICSES 2022*, pp. 1–9, 2022, doi: 10.1109/ICSES55317.2022.9914080.

[16] T. Ramzan and S. Zafar, “Blockchain-based Security for Internet of Medical Things Application,” *2022 Int. Conf. Cyber Warf. Secur. ICCWS 2022 - Proc.*, pp. 69–74, 2022, doi: 10.1109/ICCWS56285.2022.9998443.

[17] G. Ganapathy, S. J. Anand, M. Jayaprakash, S. Lakshmi, V. B. Priya, and S. Pandi V, “A blockchain based federated deep learning model for secured data transmission in healthcare Iot networks,” *Meas. Sensors*, vol. 33, no. January, p. 101176, 2024, doi: 10.1016/j.measen.2024.101176.

[18] D. Gough, S. Oliver, and J. Thomas, *An introduction to systematic reviews / David Gough, Sandy Oliver, James Thomas*. 2012. [Online]. Available: https://b-ok.asia/book/2718381/a08a63

[19] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[20] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, “Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector: A Systematic Analysis,” *IEEE Access*, vol. 11, no. July, pp. 80181–80198, 2023, doi: 10.1109/ACCESS.2023.3298824.

[21] S. Altayaran and W. Elmedany, “Security Threats of Application Programming Interface (API's) in Internet of Things (IoT) Communications,” *IET Conf. Proc.*, vol. 2021, no. 11, pp. 552–557, 2021, doi: 10.1049/icp.2022.0399.

[22] K. Parvathy and B. Nataraj, “Certain Investigation of Attacks in the Field of Internet of Things and Blockchain Technology,” in *Proceedings - 2nd International Conference on Smart Technologies, Communication and Robotics 2022, STCR 2022*, IEEE, 2022, pp. 1–6. doi: 10.1109/STCR55312.2022.10009205.

[23] A. Gupta, A. Kapoor, G. Gupta, and Di. Wanchoo, “Perils and Applications of IoT Security in Military Operations,” in *Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021*, IEEE, 2021, pp. 690–697. doi: 10.1109/ICESC51422.2021.9532996.

[24] O. Westerlund and R. Asif, “Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things,” in *2019 1st International Conference on Unmanned Vehicle Systems-Oman, UVS 2019*, IEEE, 2019, pp. 1–10. doi: 10.1109/UVS.2019.8658279.

[25] W. Meng, W. Li, and L. Zhu, “Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management against Insider Attacks,” *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1377–1386, 2020, doi: 10.1109/TEM.2019.2921736.

[26] S. Abbas *et al.*, “Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks,” *PeerJ*

Comput. Sci., vol. 10, pp. 1–23, 2024, doi: 10.7717/peerj-cs.1793.

[27] O. D. Sai Krishna, M. Dhinesh, U. S. Ram, P. D. S. V. R. Raju, G. Bindu, and S. Srithar, "A Survey of Key Challenges in Integrating IoT and Cloud Security," *Proc. - 2023 3rd Int. Conf. Pervasive Comput. Soc. Networking, ICPCSN 2023*, pp. 1439–1442, 2023, doi: 10.1109/ICPCSN58827.2023.00240.

[28] M. K. Kala and M. Priya, "A Comprehensive Survey on the IoT-Based Electronic Healthcare Records Security, Privacy Issues, and Countermeasures Using Blockchain Technology," *Proc. - 2023 Int. Conf. Innov. Eng. Technol. ICIET 2023*, pp. 1–8, 2023, doi: 10.1109/ICIET57285.2023.10220624.

[29] J. Singh, G. Singh, and S. Negi, "Evaluating Security Principals and Technologies to Overcome Security Threats in IoT World," *Proc. 2nd Int. Conf. Appl. Artif. Intell. Comput. ICAAIC 2023*, no. Icaaic, pp. 1405–1410, 2023, doi: 10.1109/ICAAIC56838.2023.10141083.

[30] P. Bajpai and R. Enbody, "Preparing smart cities for ransomware attacks," *Proc. - 2020 3rd Int. Conf. Data Intell. Secur. ICDIS 2020*, no. Section III, pp. 127–133, 2020, doi: 10.1109/ICDIS50059.2020.00023.

[31] J. I. Pegorini, A. C. C. Souza, A. R. Ortoncelli, R. T. Pagno, and N. C. Will, "Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Tests," *ACM Int. Conf. Proceeding Ser.*, pp. 157–164, 2021, doi: 10.1145/3494193.3494301.

[32] A. H. Matey, P. Danquah, and G. Y. Koi-Akrofi, "Predicting Cyber-Attack using Cyber Situational Awareness: The Case of Independent Power Producers (IPPs)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 1, pp. 700–709, 2022, doi: 10.14569/IJACSA.2022.0130181.

[33] A. Iacovazzi, H. Wang, I. Butun, and S. Raza, "Towards Cyber Threat Intelligence for the IoT," *Proc. - 19th Int. Conf. Distrib. Comput. Smart Syst. Internet Things, DCOSS-IoT 2023*, pp. 483–490, 2023, doi: 10.1109/DCOSS-IoT58021.2023.00081.

[34] J. S. Chavis and D. P. Syed, "Envisioning Cybersecurity Analytics for the Internet of Things," *2020 IEEE 3rd 5G World Forum, 5GWF 2020 - Conf. Proc.*, pp. 193–198, 2020, doi: 10.1109/5GWF49715.2020.9221018.

[35] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, 2018, doi: 10.1007/s11227-017-2048-0.

[36] R. Lama and S. Karmakar, "3-way Authentication Approach for Agricultural IOT using IFTTT application," *2021 12th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2021*, pp. 1–7, 2021, doi: 10.1109/ICCCNT51525.2021.9579958.

[37] J. Liu, A. Ren, L. Zhang, R. Sun, X. Du, and M. Guizani, "A Novel Secure Authentication Scheme for Heterogeneous Internet of Things," *IEEE Int. Conf. Commun.*, vol. 2019-May, pp. 1–6, 2019, doi: 10.1109/ICC.2019.8761951.

[38] M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018-Febru, pp. 481–487, 2018, doi: 10.23919/ICACT.2018.8323802.

[39] M. Shakeel, C. Lakshmana Rao, T. Shyam Prasad, T. Alam, N. Rawat, and R. Kavitha, "An Examination of Cybersecurity Threats and Authentication Systems," *2023 3rd Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2023*, pp. 2727–2731, 2023, doi: 10.1109/ICACITE57410.2023.10182687.

[40] F. Jaison, C. Chaudhary, and R. Manaswini, "Blockchain and Edge Computing for IoT Advancements," *3rd IEEE Int. Conf. ICT Bus. Ind. Gov. ICTBIG 2023*, pp. 1–6, 2023, doi: 10.1109/ICTBIG59752.2023.10456203.

[41] R. R. Pahlevi, V. Suryani, H. H. Nuha, and R. Yasirandi, "Secure Two-Factor Authentication for IoT Device," *2022 10th Int. Conf. Inf. Commun. Technol. ICoICT 2022*, pp. 407–412, 2022, doi: 10.1109/ICoICT55009.2022.9914866.

[42] A. K. Mishra, M. Wazid, D. P. Singh, A. K. Das, and M. Guizani, "Securing Fog Computing-based Industry 4.0 Communication Using Authenticated Key Agreement Scheme," *2023 Int. Wirel. Commun. Mob. Comput. IWCMC 2023*, vol. 0, pp. 1448–1453, 2023, doi: 10.1109/IWCMC58020.2023.10183021.

[43] S. Mawlood Hussein, J. A. López Ramos, and J. A. Álvarez Bermejo, "Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro," *Sensors (Basel).*, vol. 20, no. 8, pp. 1–13, 2020, doi: 10.3390/s20082242.

[44] S. Altayran, T. Homeed, and W. Elmedany, "APIs in Internet of Things Communications Security Threats and Solutions," *IET Conf. Proc.*, vol. 2022, no. 26, pp. 458–463, 2022, doi: 10.1049/icp.2023.0646.

[45] Y. An, F. R. Yu, J. Li, J. Chen, and V. C. M. Leung, "Edge Intelligence (EI)-Enabled HTTP Anomaly Detection Framework for the Internet of Things (IoT)," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3554–3566, 2021, doi: 10.1109/JIOT.2020.3024645.

[46] A. Vangala, R. Maheshwari, A. K. Das, and S. Pal, "Cloud-Assisted Security Framework for Drone-Enabled Offshore Communications," *IEEE INFOCOM 2023 - Conf. Comput. Commun. Work. INFOCOM WKSHPS 2023*, pp. 1–6, 2023, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225952.

[47] M. Lourens, D. Gangodkar, M. Tiwari, D. Buddhi, D. Dharamvir, and S. Kuchhal, "IoT Implementation in Various Applications: A Detailed Review of Cyber Security Issues and Challenges," *2023 3rd Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2023*, pp. 1543–1547, 2023, doi: 10.1109/ICACITE57410.2023.10183094.

[48] M. Gutfleisch *et al.*, "Caring About IoT-Security-An Interview Study in the Healthcare Sector," *ACM Int. Conf. Proceeding Ser.*, pp. 202–215, 2022, doi: 10.1145/3549015.3554209.

[49] L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electron.*, vol. 8, no. 7, pp. 1–49, 2019, doi: 10.3390/electronics8070768.