2118-9691-1-PB.pdf

Institut Teknologi Dirgantara Adisutjipto

Document Details

Submission ID
trn:oid:::3618:79331768

Submission Date
Jan 16, 2025, 2:42 PM GMT+7

Download Date
Jan 16, 2025, 3:14 PM GMT+7

File Name
2118-9691-1-PB.pdf

File Size
187.7 KB

8 Pages

5,161 Words

31,214 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 10 words)

Exclusions

- 5 Excluded Matches

Match Groups

21 Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
4% Publications
4% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

Hidden Text
9 suspect characters on 1 page
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **21** Not Cited or Quoted 7%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 5% Internet sources
- 4% Publications
- 4% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
derby.openrepository.com		2%
2	Internet	
ejournals.itda.ac.id		<1%
3	Internet	
search.aol.com		<1%
4	Internet	
m.idlk.com.my		<1%
5	Internet	
hdl.handle.net		<1%
6	Submitted works	
Nottingham Trent University on 2023-08-31		<1%
7	Publication	
Ranjit Panigrahi, Victor Hugo C. de Albuquerque, Akash Kumar Bhoi, K.S. Hareesh...		<1%
8	Internet	
www.mdpi.com		<1%
9	Submitted works	
Sheffield Hallam University on 2023-09-04		<1%
10	Submitted works	
University of Huddersfield on 2023-09-07		<1%

11 Internet

ar5iv.labs.arxiv.org <1%

12 Internet

journals.plos.org <1%

13 Submitted works

Liverpool John Moores University on 2025-01-06 <1%

14 Submitted works

University of Sunderland on 2024-04-26 <1%

15 Submitted works

University of Technology, Sydney on 2023-05-19 <1%

16 Submitted works

University of West London on 2024-07-21 <1%

COMPILER
Vol. 13, No. 2, November 2024, pp. 143-150
ISSN: 2252-2403 (Print), ISSN: 2549-2403 (Online)
Aaccredited Fourth Grade by Kemenristekdikti, Decree No:200/M/KPT/2020
DOI: 10.28989/compiler.v13i2.2118

Systematic Literature Review on Cybersecurity Issues in the Smart Home Environment

Rofiq Fauzi[1], Puspa Ira Dewi Candra Wulan[2,*], Danis Putra Perdana[3]
[1,2,3]Cyber Security Engineering, Politeknik Bhakti Semesta, Salatiga, Indonesia

Article Info

Article history:

Received February 12, 2024
Accepted December 5, 2024
Published December 20, 2024

Keywords:

SmartHome
CyberSecurity
Stidy Literature

ABSTRACT

Method A literature study was conducted to examine cyber security in Smart Homes, focusing on vulnerability assessment, privacy, threat mitigation, and policy regulations. Not only smartphones have advanced technology, but smarthomes or smart homes are a technological development that allows users to control functions such as security access, temperature, lighting and home theater remotely. This is the basis for the need for user-friendly cybersecurity measures, considering the rapid adoption of IoT devices in smart homes. This literature review highlights challenges related to inconsistent regulations and varying technology standards. Significant gaps exist in user awareness, device interoperability, data privacy, and security protocols. A multidisciplinary approach that brings together technology, policy, and social science stakeholders is recommended to build a secure, efficient, and privacy-preserving smart home ecosystem.

Corresponding Author:

Puspa Ira Dewi Candra Wulan,
Cyber Security Engineering,
Politeknik Bhakti Semesta,
Email: *puspa@bhaktisemesta.ac.id

1. INTRODUCTION

We live in an era where electronics are an essential aspect of our everyday lives [1]. Housing serves as a fundamental need for society, providing shelter and protection against external elements like heat, storms, and rain. Beyond its basic function, a residence fulfills several crucial roles for its occupants, encompassing security, opportunity, and identity. The concept of security extends beyond physical protection, creating a sense of safety and well-being. Meanwhile, a home acts as a platform for individuals to seize opportunities, contributing to the development of socio-cultural and economic aspects of their lives. Furthermore, a residence serves as a tangible representation of identity and status, reflecting the personality and achievements of its inhabitants.

Today in this century home and offices are equipped with various machinery [2]. There are different types of areas smart home apps like Smart home for security, smart home for the elderly, smart home For healthcare, Smart Home for childcare, smart home for energy efficiency, and smart home for entertainment, music and more [3]. Computer networks today inherit devices commonly known as Internet of Things (IoT) devices. IoT devices are characterized as objects that are connected to the internet [4]. The IoT is fostering innovation across every sector, from smart homes that provide convenience and energy efficiency to industrial settings that optimize operations through predictive maintenance [5]. In the context of our modern era, technological advancements have revolutionized various aspects of daily life. The prevalence of smartphones, equipped with sophisticated technology, has become ubiquitous. Alongside this, the emergence of smart homes, a product of the Internet of Things (IoT) revolution, has significantly impacted the way we experience and interact with our living spaces. The allure of convenience and efficiency associated with IoT has captured the interest of many, as it continues to streamline and enhance daily activities.

ISSN: 2252-3839 (Print)-2549 2403 (Online)

Smart homes leverage devices and networks to automate a myriad of household functions, offering a level of comfort and control that was once unimaginable. This technological paradigm allows appliances and devices within the home to be seamlessly controlled remotely through an internet connection. This includes the management of security features, temperature regulation, lighting systems, and even home theater setups. The integration of automation not only adds a layer of convenience but also contributes to energy efficiency and a more tailored living experience. With the increasing prevalence of burglary and personal threats to home occupants and property damage, it is crucial to have an effective system to keep track of security in the home and environment [6].

While the integration of technology into homes brings undeniable benefits, it is not without its challenges. The increased connectivity inherent in smart homes creates vulnerabilities that can be exploited, leading to significant cybersecurity concerns. The threat of cybercrime, as highlighted by Siddhanti, P et al, cannot be understated, with estimated annual losses reaching £34 billion. These challenges range from potential data breaches and privacy infringements to the compromise of critical home systems.

To mitigate these risks, there is a pressing need for comprehensive cybersecurity measures in Smart Home Environments (SHEs). This involves developing and implementing standardized security protocols across devices, enhancing user awareness regarding potential risks, and fostering collaboration between manufacturers, developers, and users. Additionally, securing remote access and regularly updating software to address vulnerabilities are crucial components of a robust cybersecurity strategy.

As technology continues to advance, the integration of IoT into our homes transforms the way we live, offering unparalleled convenience and efficiency. However, the realization of a truly smart home requires a simultaneous commitment to addressing and overcoming the cybersecurity challenges that accompany this innovation. By prioritizing security measures and staying vigilant against emerging threats, we can ensure that the benefits of smart homes are enjoyed without compromising user privacy and the overall safety of Smart Home Environments. Security strategy has traditionally been defined, implemented, and updated by domain experts [7].

Smart homes use devices and networks to facilitate the automation of various household functions. Rooms that have IoT are used to facilitate human activities. Smart home refers to a comfortable home setup where appliances and devices can be controlled automatically remotely with an internet connection. Smart homes allow users to control functions such as security access to the home, temperature, lighting, and home theater remotely. Over the years, many Smart homes are emerging with distinct technologies. Many systems were proposed based on Arduino and Bluetooth technology [8]. However, this increase in connectivity also opens up opportunities for various cybersecurity challenges that can threaten user privacy and security. Infrastructure-wise, this is also triggered by the development of the Internet of Things (IoT) able to connect smart device to Internet Service [9]. IoT has gained an appeal lately as a term for describing connections between all digital devices such as smartphones, content Telev, refrigerators, lamps, smartwatches, as well as various household appliances, as well as sensors and other devices [10].

Cybercrime poses a significant threat to Smart Home Environments (SHEs), with estimated losses reaching £34 billion each year, explained by Siddhanti, Petal [11]. Common remedies against cyber-attacks include firewalls and intrusion prevention systems [12]. The point of con vergence between electrical engineering and the Internet of Things (IoT) creates an intelligent layer over the current model [13]. Technologies like edge computing are helping in the reduction of cost and improvement computational power of IoT devices [14]. IoT means the Internet of Things. It is very tough to define IoT precisely [15].

A number of studies have been conducted on the security of smart home systems. In the document entitled “CROSS: A framework for optimizing cyber risks in smart homes,” by Zhang, Y et al, describe the vulnerabilities and potential exploits that hackers can use to gain unauthorized access to smart home systems [16].

The aim of this research is to conduct a systematic literature review of cybersecurity issues related to smart home devices and networks. This research aims to identify and analyze various security problems, evaluate existing solutions, and provide recommendations for improving the security of smart home systems [17].

2. RESEARCH METHOD

This research was carried out the application of research methods in obtaining data that necessary so that it can be completed properly and correctly [18]. Literature studies conducted on literature based on Revie's Systematic Literature framework [19]. Phenomenological research is a qualitative approach that aims to explore and understand how individuals subjectively experience a particular phenomenon. In the context of smart home implementation and the evolving landscape of technology, this research delves into the lived experiences of individuals as they navigate the integration of IoT (Internet of Things) into their homes.

Cybersecurity can be defined as technologies and processes that help protecting the integrity, confidentiality and availability of networks and data in computer systems against cyberattacks or unauthorized access [20]. Penetration testing, often referred to as pen testing or ethical hacking, is a proactive approach employed by cybersecurity professionals to assess the security posture of an organization's digital infrastructure [21].

The literature review serves as a foundational aspect of the research, providing insight into the theoretical underpinnings of smart homes and IoT. Drawing from various sources such as academic journals, internet articles, and relevant publications, this phase involves an in-depth exploration of existing knowledge. The researcher engages in collecting, reading, and taking notes on pertinent information, establishing a comprehensive understanding of the phenomena under investigation.

The data collection process involves not only extracting theoretical knowledge but also understanding real-world experiences and perceptions. Through interviews, surveys, or observational methods, the researcher captures the essence of individuals' encounters with smart home technology. These experiences are then subjected to descriptive analysis, a method that involves organizing and summarizing the data to provide a detailed portrayal of the opportunities and challenges associated with smart home implementation.

The initial phase of the literature review involves careful planning. The researcher outlines the scope of the review, defining key research questions and objectives. This includes identifying the relevant theories and concepts related to smart homes and IoT, establishing a framework for analysis, and determining the criteria for selecting literature sources.

Once the planning is complete, the researcher systematically gathers literature from diverse sources. This includes academic databases, journals, reputable websites, and other publications. The goal is to obtain a comprehensive understanding of the theoretical landscape surrounding smart home technology and IoT. As the data is collected, it is organized, categorized, and synthesized to develop a coherent narrative that informs the subsequent phases of the research.

The application of descriptive statistics in this phenomenological research serves to quantify and summarize the findings from the real-world experiences of smart home users. While traditional phenomenological research often emphasizes qualitative analysis, the integration of descriptive statistics can provide additional insights into patterns, frequencies, and relationships within the data. This quantitative approach complements the qualitative richness of the phenomenological exploration, offering a more comprehensive understanding of the impact of smart home implementation.

By employing a phenomenological research approach, this study not only delves into the theoretical foundations of smart homes and IoT but also explores the subjective experiences of individuals navigating this technological landscape. The literature review, data collection, and descriptive analysis collectively contribute to a nuanced understanding of the opportunities and cybersecurity challenges that emerge as smart home technology continues to evolve in our interconnected world. The integration of descriptive statistics adds a quantitative dimension to this qualitative exploration, enriching the overall research findings.

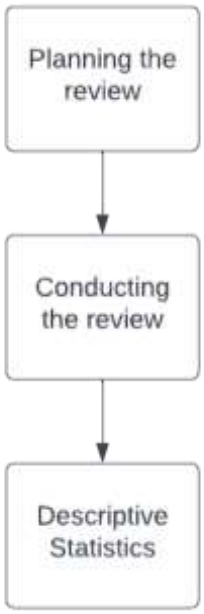

Figure 1. Research Method

The research at hand focuses on delving deep into specific embedded Internet of Things (IoT) security problems within the context of smart home environments. The overarching goal is to address critical questions concerning the cybersecurity landscape, security risks, and measures to enhance the security of smart home devices.

The backdrop for this investigation is the increasing integration of IoT technology into smart home environments. As homes become more connected and automated, the cybersecurity challenges associated with these advancements become more pronounced. Understanding and mitigating these challenges is essential for ensuring the privacy, safety, and functionality of smart homes.

Research Questions:

1. Relevant Cybersecurity Issues:
   The first research question centers around identifying the cybersecurity issues pertinent to smart home environments. This involves a comprehensive examination of potential vulnerabilities, privacy concerns, and emerging threats associated with the deployment of IoT in domestic settings.

2. Security Risks and Threats:
   Building on the identified issues, the research delves into a detailed analysis of the security risks and threats faced by smart home devices. This encompasses potential points of exploitation, such as insecure devices, unencrypted communication, and susceptibility to unauthorized access.

3. Addressing Cybersecurity Issues:
   The third research question seeks to provide insights into effective strategies for addressing cybersecurity challenges in smart home environments. This involves exploring existing security protocols, encryption methods, and risk mitigation measures that can be implemented to enhance the overall security posture of smart homes.

4. Improving Prevention and Detection Efforts:
   Finally, the research aims to contribute to the improvement of prevention and detection efforts in the realm of smart home security. This entails examining existing technologies, methodologies, and best practices for preventing cyber threats and enhancing the detection of anomalous activities within smart home networks.

The anticipated outcomes of this research include a comprehensive understanding of the specific cybersecurity challenges embedded in IoT-based smart home environments. The research is expected to yield actionable insights and recommendations for mitigating risks, enhancing security protocols, and improving prevention and detection mechanisms.

As technology continues to shape the way we live, ensuring the security of smart home environments becomes paramount. This research endeavors to contribute to the body of knowledge surrounding embedded IoT security issues, offering valuable insights that can inform industry practices, regulatory frameworks, and the development of secure smart home technologies. By addressing the identified research questions, the aim is to foster a safer and more resilient ecosystem for the increasingly interconnected smart homes of the future.

3. RESULTS AND ANALYSIS

3.1. Planning the Review

Cybersecurity issues related to the smart home environment include potential unauthorized access to smart devices, data breaches compromising sensitive user information, vulnerability to malware and ransomware attacks, the risk of IoT botnets, and the challenge of securing communication channels between interconnected devices [22]. Internet of things (IoT) refers to various electronic devices and objects that are able to connect, and transfer data through the seamlessly Internet [23]. The use of IoT Smart technology and effective can provide better comfort and security at home, and can optimize the experience of daily life [24].

Smart home devices face several security risks and threats, including the possibility of unauthorized access by hackers, potential data breaches that could compromise personal information, susceptibility to malware and ransomware attacks, the risk of device hijacking for malicious purposes, and the exposure to IoT-based botnet attacks that can exploit vulnerabilities in interconnected devices [25].

Proactive measures should be taken, such as ensuring all smart devices are equipped with the latest security updates and patches, using strong and unique passwords for each device, implementing two-factor

authentication, encrypting data transmissions, regularly monitoring network activity, segregating smart devices from critical systems, and employing network security solutions like firewalls and intrusion detection systems. Additionally, raising awareness among users about potential risks and promoting safe online practices can significantly enhance the overall cybersecurity posture of a smart home environment [26].

Different personal information is collected by a variety of connected devices such as name, date of birth, address, credit card information, etc. several millions of dollars, and could impact the customer-company relationship in terms of customer trust and brand value [27] [28].

In order for the security system to be built more manageable, it requires a microcontroller to control and manage all devices connected to the system [29]. To improve smart home security, prevention and detection efforts should be increased, implementing robust security protocols, such as regular software updates and strong authentication measures, to prevent potential cyber threats. Additionally, investing in advanced intrusion detection systems and artificial intelligence-based monitoring can enhance the detection of suspicious activities, providing timely alerts to users and allowing them to take necessary actions to safeguard their smart home environment [30][31].

3.2. Conducting the Review

The systematic literature review on the topic of cybersecurity issues in Smart Home environments begins with the initial search using the Scopus database. Scopus was chosen because it covers a wide range of peer-reviewed journals from major publishers such as Elsevier, Taylor and Francis, IEEE, Emerald, and Springer. The search was later expanded to include ISI Web of Knowledge, Emerald Insights, and Business Source Premier to identify more comprehensive and relevant works beyond the selected sample of papers. Conference contributions, articles published in trade journals, books, and book contributions were excluded to limit the number of papers for review [32].

The search strategy utilized the following keywords: "Cybersecurity" AND "Smart Home" AND "Literature Review" AND "Vulnerability" AND "Data Privacy" AND "IoT Devices." This resulted in the discovery of a substantial number of publications. However, backward and forward searches were performed to ensure that the selected papers are comprehensive and significant studies in the field of Smart Home cybersecurity [33].

A total of 549 publications were initially found with the specified keywords. To narrow down the selection, the criteria for inclusion were established as follows [34]

1. The paper must be published in a peer-reviewed journal.
2. The study should focus on cybersecurity aspects related to Smart Home systems.
3. The paper should discuss the application of cybersecurity measures, including vulnerability assessment, privacy concerns, threat mitigation strategies, and policy regulations, within the context of Smart Home environments.
4. The paper must be written in English.
5. The paper must pass the reliability test among reviewers.

The identified papers underwent a validation process before the final selection was made for review. Three independent reviewers, two based in India and one from the UK, assigned codes to the papers, and their scores were compared to assess inter-rater reliability. Papers with zero differences in scores were included in the final review process, while papers with discrepancies underwent iterations and discussions. The validation process aimed to ensure that high-quality papers aligned with the study's objectives were selected, rather than relying solely on journal quality rankings [35].

Using the selection criteria mentioned above, a complete sample of 93 papers was chosen for the final review. These papers encompass a substantial portion of the research published in the field of Smart Home cybersecurity [36].

Overall, the systematic literature review employs a rigorous approach to identify and analyze relevant publications concerning the cybersecurity challenges in Smart Home environments. By using a comprehensive search strategy and clear inclusion criteria, the review ensures the inclusion of significant and reliable studies for a well-rounded examination of the topic [36].

3.3. Descriptive Statistics

The research identifies fifteen separate business models mentioned by expert participants for achieving smart home development. These models include energy services provision, data analytics, subscription-based models, and more. The most frequently mentioned business model applications for smart homes were those related to energy services provision or energy monitoring which is presented in Figure 1. It was mentioned by 19 participants.

Figure 1 represents that insurance models and coupling with retrofits was the least frequently mentioned

by 2 expert participants; followed by pay as you go with 3 participants; new advertising channels, electric vehicles, and household data (4 participants); 'prosuming' peer-to-peer trading, capture savings (5 participants); security and safety, demand response (6 participants); convenience and health care (7 participants); subscription and digital platforms, bundling and integration of services (9 participants).

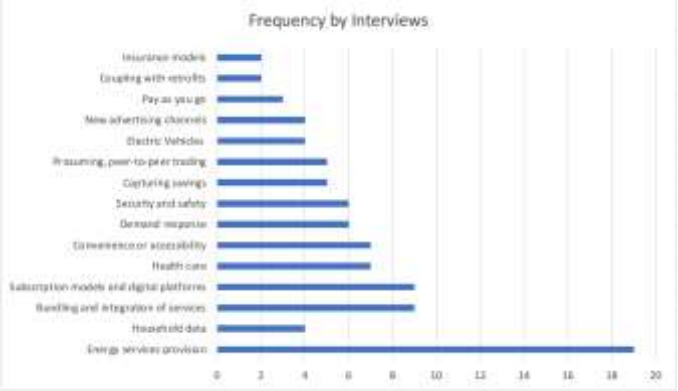

Figure 2. Smart home technology business models

3.4 Review Funding and Discussion

3.4.1 Vulnerabilities in Smart Home Devices

The literature study results indicate a multitude of vulnerabilities in Smart Home devices. This research identifies several common vulnerabilities, such as the use of weak default passwords, non-updatable firmware, a lack of encryption, and inadequate authentication mechanisms. These vulnerabilities can lead to unauthorized access, data breaches, and compromises to the Smart Home system, underscoring the importance of implementing robust security on each Smart Home device and the necessity for routine device updates to mitigate these vulnerabilities.

3.4.2 Threats and Attack Vectors

The reviewed literature identifies various threats and attack vectors that could be exploited by attackers in the Smart Home environment. These threats include unauthorized access by attackers, denial-of-service attacks on the Smart Home network, eavesdropping on communication channels, and manipulation of IoT device functionalities. Additionally, the proliferation of botnets and the use of IoT devices as entry points for large-scale attacks, such as Distributed Denial-of-Service (DDoS) attacks, are also of serious concern. Thus, proactive measures are needed to address potential threats and implement appropriate mitigation strategies to counter these attacks.

3.4.3. Privacy Concerns

The literature study also highlights privacy concerns in the Smart Home environment. Smart Home technology collects a vast amount of personal data, such as daily routines, preferences, and even audio and video recordings. Privacy security has become a major issue in the adoption of Smart Home technology. The research emphasizes the importance of preserving user privacy and the need for transparent practices in data collection and sharing. The potential for data leaks and unauthorized access to personal information poses significant ethical and legal challenges. Therefore, appropriate policies and preventative measures must be taken to protect user privacy in the Smart Home environment.

3.4.4 Security Measures and Mitigation Strategies

To address cybersecurity challenges in the Smart Home environment, various security measures and mitigation strategies have been proposed in the literature. These measures include the implementation of strong authentication mechanisms, regular software updates, the use of encryption protocols, and the segregation of IoT devices from critical systems. Intrusion detection and prevention systems, as well as anomaly detection techniques, have also been proposed as effective ways to detect and respond to potential attacks. By implementing these measures, it can enhance security and reduce the risk of attacks in the Smart

Home environment.

3.4.5 User Awareness and Education

User awareness and education play a crucial role in reducing cybersecurity risks in the Smart Home environment. The literature study emphasizes the importance of educating users about potential threats, safe practices, and the importance of regularly updating device settings and passwords. Enhancing user understanding of cybersecurity can lead to more responsible use of Smart Home technology and reduce the likelihood of successful attacks.

4. CONCLUSION

The literature study on cybersecurity in Smart Home environments underscores the presence of numerous vulnerabilities and potential threats, emphasizing the need for robust security measures, regular device updates, and proactive mitigation strategies. Privacy concerns due to the vast amount of personal data collected necessitate transparent data practices and stringent privacy protections. The study also highlights the importance of user awareness and education in reducing cybersecurity risks. In essence, addressing cybersecurity issues in Smart Home environments requires a comprehensive approach encompassing strong security measures, user education, and appropriate privacy safeguards.

Based on the literature study's conclusions, it is recommended to enhance security measures and ensure regular device updates to address vulnerabilities in Smart Home devices. Proactive mitigation strategies, including the use of intrusion detection and prevention systems, should be employed to counter various threats. Given the significant amount of personal data collected, stringent privacy protections and transparent data practices are necessary. User education about potential threats and safe practices is crucial, and policymakers should consider developing regulations to further protect user privacy and promote cybersecurity in the Smart Home environment. In essence, a comprehensive approach involving technical measures, user education, and policy development is required to address cybersecurity issues in Smart Home environments.

REFERENCES

[1] M. Majchrowicz and P. Duch, “Analysis of tizen security model and ways of bypassing it on smart TV platform,” *Applied Sciences (Switzerland)*, vol. 11, no. 24, Dec. 2021, doi: 10.3390/app112412031.

[2] S. Parashar, M. Zaid, N. Vohra, and S. Kumar, “Advance IOT Based Home Automation,” 2018. [Online]. Available: www.IJARND.com

[3] N. Faizah Rozy, I. Muhamad Malik Matin, T. Informatika, F. Sains dan Teknologi, and U. Syarif Hidayatullah Jakarta, “UJI KERENTANAN SMART HOME MENGGUNAKAN METODE SQUARE UNTUK MENDUKUNG SMART CAMPUS,” 2021.

[4] T. Schiller, B. Caulkins, A. S. Wu, and S. Mondesire, “Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing,” *Information (Switzerland)*, vol. 14, no. 10, Oct. 2023, doi: 10.3390/info14100536.

[5] T. Magara and Y. Zhou, “Internet of Things (IoT) of Smart Homes: Privacy and Security,” *Journal of Electrical and Computer Engineering*, vol. 2024, 2024, doi: 10.1155/2024/7716956.

[6] O. Taiwo and A. E. Ezugwu, “Internet of Things-Based Intelligent Smart Home Control System,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/9928254.

[7] K. Hammar and R. Stadler, “Finding Effective Security Strategies through Reinforcement Learning and Self-Play”, doi: 10.13140/RG.2.2.14128.38405.

[8] U. Pujari, P. Patil, N. Bahadure, and M. Asnodkar, “International Conference on Communication and Information Processing Internet of Things based Integrated Smart Home Automation System,” 2020. [Online]. Available: https://ssrn.com/abstract=3645458

[9] N. Faizah Rozy, I. Muhamad Malik Matin, T. Informatika, F. Sains dan Teknologi, and U. Syarif Hidayatullah Jakarta, “UJI KERENTANAN SMART HOME MENGGUNAKAN METODE SQUARE UNTUK MENDUKUNG SMART CAMPUS,” 2021.

[10] H. Heriadi and G. C. Pamuji, “Cyber Security in IoT communication (Internet of Things) on Smart Home,” in *IOP Conference Series: Materials Science and Engineering*, IOP Publishing Ltd, Aug. 2020. doi: 10.1088/1757-899X/879/1/012043.

[11] P. Siddhanti, P. Asprion, and B. Schneider, “Cybersecurity by Design for Smart Home Environments,” in *Proceedings of the 21st International Conference on Enterprise Information Systems*, SCITEPRESS - Science and Technology Publications, 2019, pp. 587–595. doi: 10.5220/0007709205870595.

[12] M. N. Aman, U. Javaid, and B. Sikdar, “IoT-Proctor: A Secure and Lightweight Device Patching Framework for Mitigating Malware Spread in IoT Networks,” *IEEE Syst J*, 2021, doi: 10.1109/JSYST.2021.3070404.

[13] P. Radoglou-Grammatikis *et al*., “SPEAR SIEM: A Security Information and Event Management system for the Smart Grid,” *Computer Networks*, vol. 193, Jul. 2021, doi: 10.1016/j.comnet.2021.108008.

[14] G. P. Kachare, G. Choudhary, S. K. Shandilya, and V. Sihag, "Sandbox Environment for Real Time Malware Analysis of IoT Devices," in *Communications in Computer and Information Science*, Springer Science and Business Media Deutschland GmbH, 2022, pp. 169–183. doi: 10.1007/978-3-031-10551-7_13.

[15] D. Kundu, Md. E. Khallil, T. K. Das, A. Al Mamun, and A. Musha, "Smart Home Automation System Using on IoT," *Int J Sci Eng Res*, vol. 11, no. 6, pp. 697–701, Jun. 2020, doi: 10.14299/ijser.2020.06.03.

[16] Y. Zhang, P. Malacaria, G. Loukas, and E. Panaousis, "CROSS: A framework for cyber risk optimisation in smart homes," *Comput Secur*, vol. 130, p. 103250, Jul. 2023, doi: 10.1016/j.cose.2023.103250.

[17] D. Buil-Gil *et al.*, "The digital harms of smart home devices: A systematic literature review," *Comput Human Behav*, vol. 145, p. 107770, Aug. 2023, doi: 10.1016/j.chb.2023.107770.

[18] F. T. Atmaja and I. I. Ridho, "SMART HOME SECURITY BERBASIS IOT DENGAN FITUR PUSH NOTIFICATION YANG TERINTEGRASI MELALUI APLIKASI TELEGRAM."

[19] "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan", doi: 10.30743/infotekjar.v5i2.3492.

[20] E. CENGİZ and M. GÖK, "Reinforcement Learning Applications in Cyber Security: A Review," *Sakarya University Journal of Science*, vol. 27, no. 2, pp. 481–503, Apr. 2023, doi: 10.16984/saufenbilder.1237742.

[21] M. Patil, D. Thakare, A. Bhure, S. Kaundanyapure, and Dr. A. Mune, "An AI-Based Approach for Automating Penetration Testing," *Int J Res Appl Sci Eng Technol*, vol. 12, no. 4, pp. 5019–5028, Apr. 2024, doi: 10.22214/ijraset.2024.61113.

[22] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281–292, 2023, doi: 10.1109/OJVT.2023.3234069.

[23] M. Majchrowicz and P. Duch, "Analysis of tizen security model and ways of bypassing it on smart TV platform," *Applied Sciences (Switzerland)*, vol. 11, no. 24, Dec. 2021, doi: 10.3390/app112412031.

[24] S. Supiyandi, C. Rizal, M. Iqbal, M. N. H. Siregar, and M. Eka, "Smart Home Berbasis Internet of Things (IoT) Dalam Mengendalikan dan Monitoring Keamanan Rumah," *Journal of Information System Research (JOSH)*, vol. 4, no. 4, pp. 1302–1307, Jul. 2023, doi: 10.47065/josh.v4i4.3822.

[25] J. E. Klobas, T. McGill, and X. Wang, "How perceived security risk affects intention to use smart home devices: A reasoned action explanation," *Comput Secur*, vol. 87, p. 101571, Nov. 2019, doi: 10.1016/j.cose.2019.101571.

[26] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018, doi: 10.1016/j.dcan.2017.10.006.

[27] "10 IoT Security Concerns to Consider Before App Development." [Online]. Available: https://www.peerbits.com/blog/10-iot-security-concerns-to-keep-in-mind-before-developing-apps.html

[28] A. Arora, A. Kaur, B. Bhushan, and H. Saini, "Security Concerns and Future Trends of Internet of Things," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, IEEE, Jul. 2019, pp. 891–896. doi: 10.1109/ICICICT46008.2019.8993222.

[29] B. Agusti Pramajuri, T. Hadyanto, and M. Ade Cipta Rahmani, "LITERATURE REVIEW : SMART HOME BASED ON IOT FOR SECURITY SYSTEM."

[30] C. Liang, B. Shanmugam, S. Azam, M. Jonkman, F. De Boer, and G. Narayansamy, "Intrusion Detection System for Internet of Things based on a Machine Learning approach," in *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, IEEE, Mar. 2019, pp. 1–6. doi: 10.1109/ViTECoN.2019.8899448.

[31] Y. Kayode Saheed, A. Idris Abiodun, S. Misra, M. Kristiansen Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 9395–9409, Dec. 2022, doi: 10.1016/j.aej.2022.02.063.

[32] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[33] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[34] O. Gkotsopoulou *et al.*, "Data Protection by Design for cybersecurity systems in a Smart Home environment," in *2019 IEEE Conference on Network Softwarization (NetSoft)*, IEEE, Jun. 2019, pp. 101–109. doi: 10.1109/NETSOFT.2019.8806694.

[35] A. Singh and B. Sikdar, "Adversarial Attack for Deep Learning Based IoT Appliance Classification Techniques," in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, IEEE, Jun. 2021, pp. 657–662. doi: 10.1109/WF-IoT51360.2021.9594946.

[36] A. Singh and B. Sikdar, "Adversarial Attack and Defence Strategies for Deep-Learning-Based IoT Device Classification Techniques," *IEEE Internet Things J*, vol. 9, no. 4, pp. 2602–2613, Feb. 2022, doi: 10.1109/JIOT.2021.3138541.

[37] I. Listiawan, Z. Zaidir, S. Winardi, and M. Diqi, "Optimising Bcrypt Parameters: Finding the Optimal Number of Rounds for Enhanced Security and Performance," *Compiler*, vol. 13, no. 1, pp. 1–10, 2024.

[38] S. Piasecki, L. Urquhart, and P. D. McAuley, "Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards," *Computer Law & Security Review*, vol. 42, p. 105542, 2021, doi: https://doi.org/10.1016/j.clsr.2021.105542.