TEKNOKOM : Jurnal Teknologi dan Rekayasa Sistem Komputer
Vol. 4, No. 1, March 2021, pp. 16 - 20
ISSN: 2686-3219, DOI: 10.31943/teknokom.v4i1.54

A SYSTEMATIC REVIEW METHOD FOR SECURITY ANALYSIS OF INTERNET OF THINGS ON HONEYPOT DETECTION

Andrie Yuswanto[1], Budi Wibowo[2*]
[1,2]Departement of Informatic Engineering, Institut Teknologi Budi Utomo, Indonesia

ARTICLE INFO

History of the article:
Received April 3, 2021
Revised May 22, 2021
Accepted May 22, 2021
Published May 24, 2021

Keywords:
Honeypot
Malware
Systematic Review
Internet of Things

ABSTRACT

A very significant increase in the spread of malware has resulted in malware analysis. A recent approach to using the internet of things has been put forward by many researchers. Iot tool learning approaches as a more effective and efficient approach to dealing with malware compared to conventional approaches. At the same time, the researchers transformed the honeypot as a device capable of gathering malware information. The honeypot is designed as a malware trap and is stored on the provided system. Then log the managed events and gather information about the activity and identity of the attacker. This paper aims to use a honeypot in machine learning to deal with malware The Systematic Literature Review (SLR) method was used to identify 207 papers in the IEEE Xplore database, digital science library direct and tandfonlin based on automatic search and predefined strings. Then 12 papers were selected to be investigated based on inclusion and exclusion criteria. From the literature study, it can be concluded that the trend of honeypot use in malware detection-based learning has increased from 2016 to 2020. The technique used by most researchers is to utilize the available honeypot dataset. Meanwhile, based on the type of malware being analyzed, honeypot in machine learning is mostly used to collect IoT-based malware.

Correspondece:
Budi Wibowo
Department of Informatic Engineering,
Institut Teknologi Budi Utomo Jakarta,
Email : budi.wibowo@ieee.org

INTRODUCTION

The main model of the Internet of Things (IoT) is based on intelligence and configures itself an interconnected object in a dynamic and global network infrastructure. In conducting a study required an understanding in research which is an important and major requirement that must be met as a researcher. The development of IoT technology has an effect on the need for convenience and a technological evolution that represents the future of computing and communications, and its development depends on dynamic technical innovation in the number of important areas, from wireless sensors to nanotechnology [1]. The need for security makes many people look for ways to protect their properties [2].

There is now a growing awareness that this trend will continue as the number of simpler and more restricted devices (sensors, actuators, home appliances, personal medical devices) connected to the Internet. The term "embedded Internet" is often used to refer to parts of the Internet that are not visible and closely interwoven into our daily lives [3].

There is now a growing awareness that this trend will continue as the number of simpler and more restricted devices (sensors, actuators, home appliances, personal medical devices) connected to the Internet. The term "embedded Internet" is often used to refer to parts of the Internet that are not visible and closely interwoven into our daily lives [4]. In general the IoT definition as a network allows the identification of digital entities and physical objects. Every day has a tendency to see a shift in the conception of the internet about the "network of intelligent" networking things all over the world that might be known as the "internet of things" (IoT). There is now a growing awareness that this progress can continue as more and more numbers are easier, many devices are tense (sensors, actuators, household appliances, personal medical equipment) connected to the net internet. The term "embedded internet" is generally accustomed to visiting parts of the internet that are not visible and knitted firmly into everyday life [5]. IoT is growing rapidly for almost 10 years now, where different physical items will be interconnected with the utilization of various existing innovations, such as Sensors and Wireless technologies such as GSM, UMTS, Wi-Fi, Bluetooth and ZigBee, which is said through Cisco. IoT related security requirements are very limited in terms of technological security [6]. Many problems provide guidance in further Research and useful references for researchers, many of the focus of surveys published on IoT security. Kamble, et al [7]. Malware is one of the threats to information security that continues to increase. In 2014 nearly six million [8] presents promising research challenges and solutions based on different security mechanisms including authentication, access control, confidentiality and privacy. A recent survey published by Yang et al [9]. Summarizes the main points of the previous survey and presents the classification of IoT attacks. Although this survey presents most aspects of IoT open security, threat, and open-ended research, and suggests some guidance for future research, some of them reveal the causes of research difficulties and security threats, and clearly identify what new challenges arise from IoT. So illegal activities can be reduced by analyzing log data on the snort server it detects possible intruders in the network around IoT devices and assists in the process of digital forensic investigation [10].

Therefore, the importance of research do systematic review related to Internet of Things Security based on mechanism of activity done to answer the problem and give solution of problem related to IoT security [11]. Table 1 describes previous studies on IoT Security.

SLR is used to find better methods that can be used for the security of the internet of things in assisting forensic information. From studying past studies. From table 1, there are lots of research regarding Table 1 is also some results of SLR process for this paper. All those papers are then used to formulate main question [12]. The main question is how to find a method that can be used to formulate main question. The main question is how to find a method that can be used to have better analyze security on the internet of things.

Table 1. Previous Studies on Not Security

Paper	Year	Issue
[1]	2016	Establish the current state of security in IoT device
[2]	2018	Illustrates the developing trend of IoT security research and reveals how IoT features affect existing security
[3]	2016	IoT to gather knowledge technology and to document its current degree of integrity, anonymity and adaptability
[4]	2020	Consideration of the IoT Security has increased dramatically
[5]	2018	The potential forensic information that can be gathered, derived, or inferred from IoT- collected data.
[6]	2018	Certain vulnerabilities to device IoT devices
[7]	2017	To secure the IoT devices
[8]	2019	Detect malware by classifying its class
[9]	2020	Identifies IoT benefits and risks.
[10]	2020	The potential for DDoS attacks using IoT devices is growing rapidly
[11]	2020	Security challenges and problems of IoT devices are identified
[12]	2020	State-of-the-art of IoT security threats and vulnerabilities by conducting a classification
[13]	2021	Ransomware evolution, prevention and mitigation in the context of IoT

The paper will contain 4 sections. First section discusses literature review. Second section tells research method. Third section constitutes result and analysis. Last section concludes the result of the study and recommends future research.

RESEARCH METHODS

To ensure the quality of the literature review, this study also uses guidelines for citation and evaluation procedures to complement the original SLR approach. SLR approach has been applied in distinct stages. In the process of reviewing the article the author uses a method that is clearly described in Figure 1. The method used consists of five stages including; select a topic, determine the scope of the review, choose which online library to be visited to operate to search for documents / articles / literature, search and find literature, and review the vast literature.

In this study, the topic selection process begins by looking for questions related to the topic to be used as research or what is the background related to this topic. There are two basic questions that are used as a reference in this study, namely; what is the basis of security against IoT and ways of analyzing IoT security.

In the process of selecting a database to search for topics that occur at this stage is to choose a database search that will be used to get data that matches the phrases that have been determined in the previous stage. The databases used in the search for related topics were taken from ScienceDirect, Tandfonline and Ieeexplore. Database search on the three sources consists of two methods, namely without using quotes and using quotes.

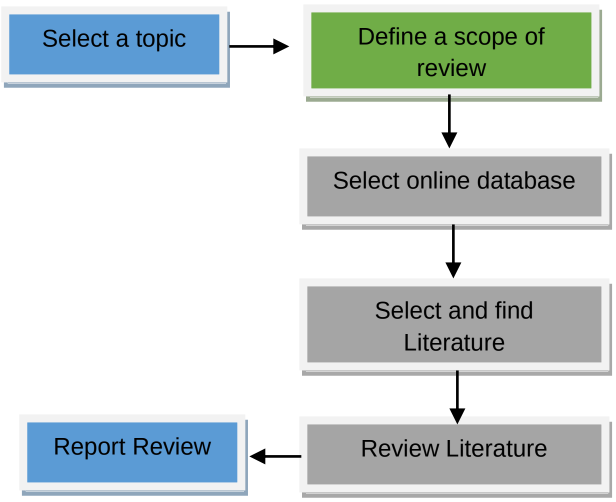

Figure 1. Stages for systematic review

From the results of the search process that has been done before, the writer can carry out the mapping stage of the results obtained using the Mendeley tool. This tool makes it easy to categorize search results by source and extract data from each selected article. This stage is called searching and finding literature. The last stage is reviewing the literature. At this stage, a discussion is carried out regarding the data that has been obtained based on the title and year of each article.Sistematic Review is a formal review and only translates the research questions. This study uses the SLR method because there is a need to study previous papers for better IoT device security. The same rationale applies to research on science education and network load balancing. There are 5 steps in SLR, namely: making research questions, selecting libraries, extracting the required data, synthesizing data and discussing the results [11]. The table below describes the questions for this paper.

Table 2. Research Question IoT Security

Question	Target Archievment
Whats is IoT ?	establish the current state of security in IoT device
What is the research contribution?	Identification of contributions that can be applied to facilitate the identification of malware threats

To answer the questions specified in table 2, there are 3 trusted digital library databases as a reference for this study named IEEE Xplore, ScienceDirect and Tandfonline are used. Libraries have been trusted for research. Table 3 describes the digital library used to solve this problem.

Table 3. Digital Library Journal

Digital Library Online	Link Website
ScienceDirect	www.sciencedirect.com
IEEE Xplore	ieeexplore.ieee.org
Tandfonline	www.tandfonline.com

In this trusted digital library database, a search was carried out for related papers on March 25, 2021 during 2016 to 2020. Research questions in table 2 were then translated into keywords. Keywords for search were "Internet of Things", "Internet of Things Security" and "Security Analysis Internet of Things". All keywords use lowercase with spaces and without quotation marks. Therefore, these keywords are searched in 3 trusted digital library databases. This study also describes the criteria used in finding related papers to answer research questions. The following table illustrates the selection of paper criteria defined for the study. Using the definition of the paper selection criteria and Keywords, some reliable and related papers were taken by following the picture below. Figure 1 shows the SLR process that will be generated. The result of paper selection is shown in table 4.

Table 4. Paper Research Result

Digital Library	Keyword	Result
Science Direct	Internet of Things	87815
	Internet of Things Security	15934
	Security Analysis of Internet of Things on honeypot	179
IEEE Explore	Internet of Things	9352
	Internet of Things Security	2458
	Security Analysis of Internet of Things on honeypot	3
Tandfonline	Internet of Things	25887
	Internet of Things Security	11301
	Security Analysis of Internet of Things on honeypot raspbery	25

From the results mentioned above, it can be used as a basis for obtaining data synthesis and presentation data in the results and discussion sections.

RESULT AND DISCUSSION

All questions from research related to systematic review of internet of things security analysis on honeypot are in the research methods section. The question that needs to be answered is the threat of threats to the Internet. The second question that must be addressed is to develop internet of things threat detection with a honeypot. The last question is the contribution to the internet tools from the things that are in the attack of intruders quickly. From table 4, it can be changed graphic. This will present paper search result in order to ease reading process. Below figure explains the result.

SLR Result of Reported Articles

From table 4, it can be changed graphic. This will present paper search result in order to ease reading process. Below figure explains the result.

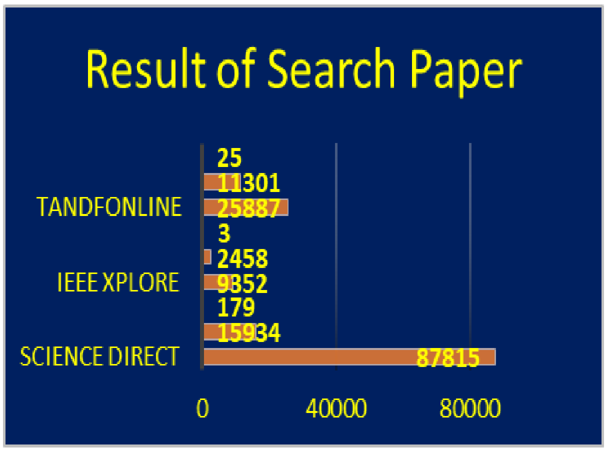

Figure 2. Result of paper search by keywords

From Figure 2, the results obtained from a digital database include: 3 related papers in IEEE, 179 related papers on ScienceDirect and 25 related papers on Tandfonline. All papers do not discuss the SLR method.

Journal Review

Of the many papers received from 3 trusted digital databases of libraries, researchers took several papers that were potential to be discussed in this case related to internet security of things with honeypot to answer research questions. 10 papers were taken as samples and extracted to get the results. Table 5 describes each definition, such as:

Table 5. Describes Each Definition

Paper	Topic		Quantity Measurement
	IoT Security	Honeypot	
[13]	√	×	×
[14]	√	×	√
[10]	√	×	√
[3]	√	×	√
[15]	√	×	×
[5]	√	×	√
[6]	√	×	√
[2]	√	×	×
[13]	√	×	×
[16]	√	×	√
[17]	√	√	√
[18]	×	√	√
Author	√	√	√

From the table above, the extracted results are obtained from the 12 papers. 12 papers discussing matters related to Safety In addition, 6 papers describe the measurement of quantity. Based on these results, the research contribution is to develop IoT in analyzing malware threats by measuring it through a honeypot. From the results of malware or ransomware threat information, it is necessary to consider choosing a honeypot as a dataset with different techniques to improve performance

CONCLUSSION

The honeypot is designed as a malware trap and is stored on the provided system. Then log the managed events and gather information about the activity and identity of the attacker. This paper aims to use a honeypot in machine learning to deal with malware The Systematic Literature Review (SLR) method was used to identify 207 papers in the IEEE Xplore database, digital science library direct and signature based on automatic search and predefined strings. Then 12 papers were selected to be investigated based on inclusion and exclusion criteria. The technique used by most researchers is to utilize the available honeypot dataset. Meanwhile, based on the type of malware being analyzed, honeypot in machine learning is mostly used to collect IoT-based malware.

ACKNOLEDGEMENT

The authors thank the Department of Informatic Engineering Institut Teknologi Budi Utomo Jakarta for providing support to authors in terms of research.

REFERENCES

[1] M. R. Bashir and A. Q. Gill, “IoT Enabled Smart Buildings : A Systematic Review,” *Intell. Syst. Conf.*, no. September, pp. 151–159, 2017.

[2] J. Martinez, J. Mejia, and M. Munoz, “Security analysis of the Internet of Things: A systematic literature review,” *2016 Int. Conf. Softw. Process Improv.*, pp. 1–6, 2016.

[3] W. Zhou, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” *IEEE Internet Things J.*, vol. PP, no. c, p. 1, 2018.

[4] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” *2016 IEEE/ACS 13th Int. Conf. Comput. Syst. Appl.*, pp. 1–6, 2016.

[5] A. M. Awadelkarim Mohamed and Y. Abdallah M. Hamad, “IoT Security: Review and Future Directions for Protection Models,” *2020 Int. Conf. Comput. Inf. Technol. ICCIT 2020*, pp. 166–169, 2020.

[6] C. Shin, P. Chandok, R. Liu, S. J. Nielson, and T. R. Leschke, “Potential forensic analysis of IoT data: An overview of the state-of-the-art and future possibilities,” *Proc. - 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, vol. 2018-Janua, pp. 705–710, 2018.

[7] A. Kamble and S. Bhutad, “SURVEY ON INTERNET OF THINGS (IOT),” *2018 2nd Int. Conf. Inven. Syst. Control*, no. Icisc, pp. 307–312, 2018.

[8] H. Artail, H. Safa, M. Sraj, I. Kuwatly, and Z. Al-Masri, “A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks,” *Comput. Secur.*, vol. 25, no. 4, pp. 274–288, 2006.

[9] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017.

[10] B. Wibowo, “Smart Home Security Analysis Using Arduino Based Virtual Private Network.” 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1-4, 2019.

[11] T. Hidayat, “Internet of Things Smart Agriculture on ZigBee: A Systematic Review,” *J. Telekomun. dan Komput.*, vol. 8, no. 1, p. 75, 2017.

[12] T. Hidayat, “Encryption Security Sharing Data Cloud Computing By Using Aes Algorithm: a Systematic Review,” *Teknokom*, vol. 2, no. 2, pp. 11–16, 2019.

[13] T. Hidayat, R. Mahardiko, and S. T. D. Franky, “Method of Systematic Literature Review for Internet of Things in ZigBee Smart Agriculture,” *2020 8th Int. Conf. Inf. Commun. Technol. ICoICT 2020*, pp. 7–10, 2020.

[14] I. Idrissi, M. Azizi, and O. Moussaoui, “IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review,” *4th Int. Conf. Intell. Comput. Data Sci. ICDS 2020*, 2020.

[15] Y. Liao, E. de F. R. Loures, and F. Deschamps, “Industrial Internet of Things: A Systematic Literature Review and Insights,” *IEEE Internet Things J.*, vol. 4662, no. c, 2018.

[16] H. C. Sihombing, A. N. Fajar, and D. N. Utama, “Instant Messaging as Information Goldmines to Digital Forensic: A Systematic Review,” *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 235–240, 2018.

[17] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, “Internet of things and ransomware: Evolution, mitigation and prevention,” *Egypt. Informatics J.*, vol. 22, no. 1, pp. 105–117, 2021.

[18] I. M. M. Matin and B. Rahardjo, “Malware Detection Using Honeypot and Machine Learning,” *2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019*, no. January, pp. 1–5, 2019.