Scientific Research Publishing

Journal of Information Security, 2022, 13, 181-209
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Meta-Review of Recent and Landmark Honeypot Research and Surveys

Gbenga Ikuomenisan*, Yasser Morgan

Faculty of Engineering & Applied Science, University of Regina, Regina, Canada
Email: *gti002@uregina.ca, Yasser.Morgan@uregina.ca

How to cite this paper: Ikuomenisan, G. and Morgan, Y. (2022) Meta-Review of Recent and Landmark Honeypot Research and Surveys. *Journal of Information Security*, **13**, 181-209.
https://doi.org/10.4236/jis.2022.134011

Received: May 3, 2022
Accepted: August 20, 2022
Published: August 23, 2022

Abstract

The growing interest in Honeypots has resulted in increased research, and consequently, a large number of research surveys and/or reviews. Most Honeypot surveys and/or reviews focus on specific and narrow Honeypot research areas. This study aims at exploring and presenting advances and trends in Honeypot's research and development areas. To this end, a systematic methodology and meta-review analysis were applied to the selection, evaluation, and qualitative examination of the most influential Honeypot surveys and/or reviews available in scientific bibliographic databases. A total of 188 papers have been evaluated and 22 research papers are found by this study to have a higher impact. The findings of the study suggest that the Honeypot survey and/or review papers of considerable relevance to the research community were mostly published in 2018, by IEEE, in conferences organized in India, and included in the IEEE Xplore database. Also, there have been few qualities Honeypot surveys and/or reviews published after 2018. Furthermore, the study identified 10 classes of vital and emerging themes and/or key topics in Honeypot research. This work contributes to research efforts employing established systematic review and reporting methods in Honeypot research. We have included our meta-review methodology, in order to allow further work in this area aiming at a better understanding of the progression of Honeypot research and advances.

Keywords

Honeypot, Network Security, Intrusion Detection, Systematic Review, Meta-Review

1. Introduction

According to a recent Deloitte article [1], there has been increased in new types of

malware and attacks from 20% to 35% during the pandemic period of 2020-2021. The 2021 Data Breach Investigation Report [2] establishes the main motive behind most security incidents as financial. To provide an effective risk mitigation strategy in preparation for and in response to intrusive attacks, organizations typically review their overall security policies, and most importantly, reinforce network security by implementing multiple defense mechanisms one of which is Honeypot.

As defined by Lane Spitzner [3], a Honeypot system is a decoy security resource and/or facility which generate value only when it has been successfully probed, attacked, and compromised. It is typically deployed by network security analysts for monitoring and detecting new and zero-day attacks and vulnerabilities. It operates as a deception technique designed to lure and engage only attackers for the purpose of trapping and collecting information about intrusive attacks. Logged attack data collected by Honeypot systems can be comprehensively analyzed and lessons learned are further implemented in network security policies to improve network security.

Numerous empirical studies advancing Honeypot research have been conducted, and consequently, summarized, synthesized, and presented in reviews and/or survey papers for the benefit of network security researchers. In 2012, Bringer *et al.* [4] surveyed Honeypot systems, and various key Honeypot research studies were identified in terms of: 1) types of Honeypots; 2) types of deployments and configurations; 3) detection, anti-detection, and security threats; 4) data analysis metrics and methods; and 5) ethical/legal issues. However, to the best of our knowledge, most surveys and/or reviews focus only on specific Honeypot research areas. Also, given the pandemic and the realities of current security attacks, we argue that Honeypot research areas (going back to 2012) require a fresh look. Hence, we aim to develop a holistic view of Honeypot's research areas and trends.

This paper examines studies in Honeypot research and shows how it evolves and in which direction. It summarizes, synthesizes, and quantitatively analyzes selected quality Honeypot survey and/or review articles published since 2010 to develop an overview of the breadth and depth of studies common in Honeypot research. It additionally identifies, classifies, and maps key Honeypot research study themes, revealing current research opportunities and directions, and also relationships between main research topics and sub-topics. We hope this work serves as a reference to current Honeypot research topics, and quality survey and/or review papers, and also directs and guides the work of researchers in the field.

The rest of the paper is laid out as follows: Section 2 reviews common Honeypot technologies and classifications; Section 3 presents the methodology adopted by this study followed by a summary of selected articles in Section 4. The research results and discussion of the findings are given in Section 5, and Section 6 presents the conclusion.

2. Background

Traditional security defense mechanisms, such as firewalls and Network Intrusion Detection Systems (NIDSs), have been used by organizations for many years to avert and mitigate intrusive attacks. In operation, these security outfits block, log, and alert unwanted malicious sources and network traffic patterns for effective network monitoring and security. However, they have known deficiencies, in that they typically generate a significant number of false positives and/or negatives, making them unfit to be used alone in mitigating sophisticated attacks.

In today's networks, Honeypots are commonly deployed in addition to the aforementioned defense mechanisms to reinforce organizations' overall security. Honeypots are surreptitious security decoys designed by default to lure and engage only attackers. They are capable of logging relatively more attack and attacker activities with low levels of false positives, thus addressing the deficiencies of traditional firewalls and NIDSs.

2.1. Honeypot Types

The notion of Honeypots has been in use in the network and information security field since the 1990s [5], and as such is not new. According to Lane Spitzner [3], Fred Cohen's Deception Toolkit was regarded as the first instance of a Honeypot. It was used to deploy fake services which could be attacked by adversaries. However, the field of Honeypot has experienced consistent evolution particularly in areas such as architecture, deployment, and use [6] [7], and several Honeypot technologies have been proposed and developed since inception [7]:

- Shadow Honeypots are Honeypot deployments typically in cooperation with NIDS.
- Honeynet are Honeypots typically deployed in a distributed cooperative fashion.
- Honeytoken are typically fake digital resources such as data, files, and emails which can be deployed on the network and monitored for attacks.
- Honeywall is a type of Honeypot deployed for monitoring, controlling and analyzing attacks.
- Honeypot frameworks such as T-POT, Community Honey Network, and Modern Honey Network [8] employ docker technology for centralized deployment and management of different Honeypot types, thus enabling ease of deployment, use, and maintenance.

2.2. Honeypot Classifications

Honeypots can be classified based on 1) field of deployment—production and research Honeypots, and 2) the physicality of deployment—physical and virtual Honeypots [9]:

- Production Honeypots are deployed inside an organization's production network (with other production servers) for improved network monitoring and

security. They are easy to deploy and use, and can only capture limited attack information.

- Research Honeypots are deployed in organizations typically for researching vulnerabilities, threats, and attacks. They are complex to deploy and maintain, and can capture extensive attack and attacker information.
- Physical Honeypots are commonly deployed on bear-metal (*i.e.* physical computer systems).
- Virtual Honeypots, on the other hand, are deployed in virtualized environments with virtual compute resources.

Other common classifications are based on: 1) Honeypot'S level of interaction relating to the amount of attack information that can be gathered—low-interaction and high-interaction Honeypots, and 2) the direction of interaction relating to how attack traffic is initiated—client and server Honeypots [9]:

- Low-interaction Honeypots typically simulate only a set of operating system's services and resources. They can be easily deployed and maintained, and are easily detected by attackers. Consequently, the amount of attack information that can be collected is limited as they are not capable of deceptively engaging attackers for so long. Collected data are mostly traffic flows from which valuable attack information (such as attack level, type, and source) can be statistically extracted.
- High-interaction Honeypots, on the other hand, are deployed as real operating systems resources, and as such are not easily detected by attackers. Their purpose is to get attackers to interact with fake operating systems data, applications, and/or services for longer time periods in order to collect, extract, and evaluate a wider scope of attacks and attacker information such as the attacker's intentions, behavior, malware, commands, keystrokes, and tools. Additionally, high-interaction Honeypots are useful for detecting zero-day attacks and vulnerabilities, and consequently, are more resource-intensive, and difficult to deploy, maintain, and monitor.
- Server Honeypots are passive in that they wait to be probed, attacked, and/or compromised by adversaries.
- Client Honeypots, on the other hand, actively seek possible malicious internet-connected systems to initiate communication with.

Honeypots can also be classified based on the threat type being investigated or the application service being addressed [5]. Examples are, email, data, and malware:

- Email Honeypots are fake hidden email addresses deployed as decoys to be harvested by spammers and to trap, investigate, and block illicit spams emails in organizations.
- Decoy data Honeypots are fake data or databases deployed typically for monitoring attackers' exploits on insecure computer systems architecture and software vulnerabilities such as SQL services exploitation and file systems privilege abuse.

- Malware is malicious computer software. Malware Honeypots typically run vulnerable remote connection (e.g. telnet, secure shell) and file system (e.g. server message block, application programming interface) application services, thus inviting malware attacks, and enabling trapping and storing of downloaded malware samples for further analysis.

3. Materials and Methods

The Preferred Reporting Items of Systematic Reviews and Meta-Analysis (PRISMA) methodology [10] [11] is a framework for the systematic selection, evaluation, review, and reporting of research articles. It ensures that planning and execution of review and meta-analysis work is repeatable and bias-free. Furthermore, meta-analysis is a statistical analysis method that can be used for developing a holistic view of multiple related secondary studies to identify common themes and overall trends [12] [13]. The procedure basically involves searching and identification of key documents, followed by screening, reviewing, data extraction, and in-depth statistical analysis and reporting.

In this work, we conduct a meta-analysis of developments in Honeypot systems research (using Honeypot survey and/or review papers) following the PRISMA methodology. We include both traditional and systematic (published and unpublished) Honeypot-related review and/or survey articles based on pre-defined inclusion and exclusion criteria. We also evaluate both paper and study characteristics, and present results and findings.

3.1. Eligibility Criteria

Survey and/or review papers, in English language, relating to Honeypot research, from 2003 to 2021 were considered. Articles not relevant to our study were excluded, in particular, empirical studies, white papers, posters, and other survey and/or review papers that were not related to Honeypot technology.

To be selected, survey and/or review articles needed to present topics directly related to Honeypot technology and its variants such as shadow Honeypot, honeynet, and honeytoken. To be included in this study, selected papers needed to be qualitative and as such must meet one or more of the following requirements: 1) have been at least moderately cited; 2) is published by a reputable research-oriented organization with strong peer review process; 3) is published in a high impact peer-reviewed conference proceeding or journal.

3.2. Information Sources and Search Strategy

To identify possible Honeypot survey and/or review papers, on the 30th of September, 2021 we first conducted a manual search of Honeypot-related articles using the Google Scholar web search interface to understand what key combinations to use as search strings. We used "*Honeypot*" as the search keyword and selected the "*Review articles*" option to view only survey and/or review-related papers. After quickly traversing 50 pages of the search results, we observed that

most plausible Honeypot-related review and/or survey papers have the "survey" keyword used in their titles. Consequently, we conducted a second Google Scholar search using an automated python script [14] executed with default parameters through the Google Colaboratory web interface. The automated python script was configured to rank publications by the number of citations (per year) with the aim of revealing the most relevant survey papers in the field. For this search, the authors combined only two keywords—"*Honeypot*" and "*survey*"—as a search string.

- "Honeypot AND survey"

On the 11th of November 2021, a third search was conducted with to identify and update the search database with possibly missed and/or new records. Manual searches were performed directly from the Google Scholar web search interface up to the 20th page and after the "*Review articles*" option was selected to view only survey and/or review-related papers. The search database was saved as a single CSV file and uploaded to Google Docs as a spreadsheet for further processing. For this search, specific keywords and phrases found in a number of Honeypot literature retrieved from the second search were combined into a complex search string (**Table 1**) in order to increase the scope of the search to include papers having other key terms, such as "honeynet", "honeytoken", "review", "current state", "trend" and "systematic literature review".

- "(Honeypot OR honeynet OR honeytoken) AND ('systematic literature review' OR 'literature review' OR 'survey' OR 'review' OR 'current state' OR 'trend')"

Records of articles in the search database were found to have been indexed (by the Google Scholar search engine) from several online bibliographic databases. Most notable and of concern are: SpringerLink [15], ScienceDirect [16], IEEE Xplore [17], and ACM Digital Library [18]. **Table 1** shows the attributes that characterizes the search operation such as: search engine type, search tool/interface type, date of coverage, search keyword and string, and source name.

3.3. Selection of Sources

This study follows a four-step process (data cleaning, first screening, second

Table 1. Characteristics of the paper search process: This table displays the search engine used, the search tool/interface, the date of coverage for each search, the search strings used, and the number of returned articles by database. Google Scholar searches were conducted using different search interfaces and strings, and the results were collated.

Search Engine	Search Interface	Coverage	Search String	Sources	# of Records
Google Scholar	1) Google Colab; 2) Web search	2003-2021	1) Honeypot AND survey; 2) (Honeypot OR honeynet OR honeytoken) AND ("systematic literature review" OR "literature review" OR "survey" OR "review" OR "current state" OR "trend")	SpringerLink [15]	25
				ScienceDirect [16]	15
				IEEE Xplore [17]	38
				ACMDigitalLibrary [18]	9
				arXiv [19]	13
				CiteSeer [20]	4
				Others	84

screening, and article rating) for selection of sources based in the aforementioned inclusion and exclusion requirements.

3.3.1. Data Cleaning

The search database was first preprocessed as follows: records were sorted by paper title and author; records with no author(s) and/or title were identified and deleted; duplicates records were removed; and direct web URL to articles were retrieved (*i.e.* for records without links).

3.3.2. First Screening

In this step, the title and abstract of each article were independently studied and papers with the following characteristics were excluded: papers not presented in English language; papers that do not represent reviews or surveys (e.g. case studies, white papers, original research, etc.); papers not related to Honeypot, honeynet, and/or honeytoken.

3.3.3. Second Screening

After the first screening, the full literature content of each article retained were independently reviewed and analyzed. Authors discussed the results of the screening process and agreed on the most relevant survey and/or review articles to be selected. In this step, papers not related to Honeypot, honeynet, and/or honeytoken were further identified and excluded.

3.3.4. Article Rating

In an attempt to include only quality Honeypot survey and/or review papers in this study, a non-traditional article ranking scheme was developed and applied for the purpose of classifying individual article. The ranking guidelines are as follows: 1) the number of citations per year must be higher than 1; 2) articles must be published by a well-recognized organization that follows stringent re-view process; and 3) articles must be published in a prestigious conference proceedings or journal. The reasoning is that articles satisfying one or more guidelines of the ranking scheme may be regarded as having high relevance and/or importance to the re-search community and low relevance and/or importance if otherwise.

To achieve guideline (3) above, we used the Scimago Journal Ranking version 2020 (SJR2020) online database [21]. The SJR is a publicly available portal that computes the prestige of publications based on information obtained from the Scopus database. We assume that publications are of considerable impact if at the least are included (and not as discontinued) in the SJR2020 and ranked at levels Q1 or Q2. If otherwise, items 1) and/or 2) must apply.

In this step, qualitative and quantitative data were collected for the selected articles and each paper was appropriately grouped into two based on the ranking scheme: group 1 (high-relevance) and group 2 (low-relevance). We regarded papers in group 1 as the final list and included the list in this study for review and further analysis. On the other hand, papers in group 2 are only retained for

statistical analysis, reference, and potential future re-evaluation.

3.4. Data Collection Process

In order to categorize, synthesize, and analyze each paper included in the final list, we collected data on the paper (Table 2), the study areas, and possible research openings.

3.4.1. Data on the Paper

- Paper—name(s) of the authors and reference to as stated in our search database.

Table 2. Paper characteristics: This table shows the Honeypot survey/review papers included in this work and their physical features. The number of citations/year, helps to show the relevance of paper irrespective of the publication year. SJR2020 shows if publications are included in the Scimago Journal Ranking 2020 database [21] (x) and their associated rankings (Q1 - Q4). Location shows the country of conference or journal.

Paper	# of Citations	# of Citations/Yr.	Year	Publisher	Venue	SJR2020	Location
Mairh [22]	95	9	2011	ACM	Conference		India
Bringer [4]	101	10	2012	MEC Press	Journal	x	China
Zanoramy [23]	24	3	2013	SST under Royal Patronage	Journal	x, Q3	Thailand
Baykara [24]	27	4	2015	EverScience Publications	Journal		India
Campbell [25]	42	6	2015	IEEE	Conference	x	UK
Fan [26]	9	1	2015	IEEE	Conference	x	France
Nawrocki [5]	116	19	2016		Preprint		
Jogdand [27]	7	1	2016	IEEE	Conference	x	India
Pothumani [28]	172	34	2017	Academic Publications Ltd.	Journal	x	Bulgaria
Uitto [29]	20	5	2017	Springer	Conference	x	Portugal
Fan [9]	49	12	2018	IEEE	Journal	x, Q1	US
Oza [30]	5	1	2018	IEEE	Conference	x	India
Veni [31]	6	2	2018	American Scientific Publishers	Journal	x, Q4	US
Fraunholz [32]	28	7	2018		Preprint		
Lu [33]	1	0	2018	Springer	Conference	x	Malaysia
Razali [34]	7	2	2018	IEEE	Conference	x	Malaysia
Sharma [35]	95	24	2018	Elsevier	Journal	x, Q1	US
Zobal [7]	7	2	2019	IEEE	Conference		Ireland
Bhagat [36]	1	0	2019	Springer	Conference		India
Lee [37]	6	3	2020	The SAI Organization	Journal	x, Q3	UK
Matin [38]	1	1	2020	IEEE	Conference	x	Indonesia
Franco [39]	1	1	2021	IEEE	Journal	x, Q1	US

- # of Citations—this is the number of citations as stated in our search database.
- # of Citations/Year—this is the number of citations divided by duration of coverage.
- Year—this is the year of publication as stated in our search database.
- Venue—this is the publication type as stated in our search database; we considered only journals, conferences, book series, and preprints.
- Location—this is the country of conference or journal.
- Publication and Publisher.
- SJR2020—this indicates the ranking status of the publication in the SJR 2020 database.

3.4.2. Data on the Study

We studied the selected review papers independently to identify and extract commons topics (mapping keywords). We merged similar and/or closely related topics to form a 10-class categorization scheme which closely follows key Honeypot research study areas as identified by Bringer *et al.* [4]. We finally extracted the following additional data items:

- Study area—the specific Honeypot themes/subjects/topics presented in the paper.
- Future work—research opportunities (if any) discussed in the publication.

3.5. Synthesis of Results

First, we present a summary of each survey paper in the final list (by year) to give an overview of the breath of study and research direction. Then, we tabulate and chart the characteristics of the survey papers to give insights into the inter-relationships. We finally synthesized and discussed our findings based on the categorized Honeypot study areas and future research opportunities.

4. Survey Review

Many surveys and/or reviews have been carried out in the various fields of Honeypot technologies, including shadow Honeypot, honeynet and honeytokens, as information and network security decoys. In this section we present an overview of included Honeypot-related survey and/or review papers based on the year of publication.

In 2011, Mairh *et al.* [22] conducted a survey on Honeypots and reviewed concepts and applications especially in teaching and research.

In 2012, Bringer *et al.* [4] presented a survey on Honeypot software tools, configuration, detection and anti-detection techniques, and an overview of Honeypot related legal and ethical issues as it applies especially in the US were discussed.

In 2013, Zanoramy *et al.* [23] presented an overview of Honeypot concepts, classifications, and deployment challenges. In addition, Zanoramy discussed the difference between static and dynamic Honeypot types and also summarized

notable works in dynamic and intelligent Honeypots proposed in literature. The authors [23] acknowledge that very little research work was done in applying Artificial Intelligence (AI) techniques for development of dynamic and intelligent Honeypot systems, and farther proposed the use of already existing AI techniques such as Expert Systems (ES) [40], Fuzzy Logic (FL) [41], and Swarm Intelligence (SI) [42].

In 2015, Baykara *et al.* [24] presented an overview of Honeypot systems, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The Baykara suggested and discussed possible architectures and deployments of the aforementioned technologies. In addition, Campbell *et al.* [25] presented their survey work where they reviewed emergent trends in Honeypot research. The authors synthesized and discussed their findings according to the following: 1) the year of publication; 2) the type of publication; 3) the country of origin of the publication; and 4) the identified subject themes from selected sources relevant to their study.

An emerging field in Honeypot research concerns the development and standardization of common (technology independent) honeynet descriptive language for parallel operation of different honeynet platforms. In 2015, Fan *et al.* [26] presented an overview of existing common descriptive languages and proposed one that could be used in the configuration and management of disparate honeynet deployments, included in a flexible configuration tool—HoneyGen [43]. The authors [26] suggested, most importantly: 1) extending the HoneyGen [43] tool for compatibility with more honeynet platforms; and 2) studying of the automatic translation between the proposed technology independent language and the proprietary deployment languages of honeynet platforms.

In 2016, Nawrocki *et al.* [5] presented a detail survey on Honeypot technology in which they discussed Honeypot concepts, software, related tools, long-term projects, data analysis methods and metrics, and general legal and ethical reasonings and considerations. Further, Jogdand *et al.* [27] presented an overview of cybersecurity mitigation solutions (such as Firewalls and IDS) integrating honeypots as well as honeytoken (with encrypted pointers) generation techniques for the purpose of improving detection and mitigation of intrusive attacks. They described different techniques used in trapping attackers such as using query-based honeytokens and honeytokens created using the HoneyGen [43] tool.

One of the current challenges relating to Honeypot deployment concerns the ability to successfully engage adversaries undetected [7]. Also, malwares submitted by attackers are known to have built-in intelligence for detecting and avoiding unwanted execution environments [29] using detection vectors (such as Honeypot operating system type, virtualize machine type, etc.) which characterizes the execution environment. In 2017, Pothumani *et al.* [28] presented a survey on all classes of decoys used in various domains such as document, traffic, system or even network which can be used as honeytokens or Honeypots. Similarly, Uitto *et al.* [29] surveyed Honeypot detection techniques by malware. Uitto *et al.*

investigated and discussed existing anti-Honeypot and anti-introspection approaches typically used by malwares to detect Honeypot signatures by means of detection vectors at the network, systems, application, service, and operational levels. As the black hat community continues to improve the sophistication of malwares for effective (execution environment) fingerprinting, authors [29] proposed future research direction as: 1) the development of new ways to identify and classify malware detection vectors; and 2) the development of inexpensive, and more robust and adaptive Honeypot solutions with better and advanced deception.

In 2018, Fan *et al.* [9] presented a comprehensive survey on Honeypot systems. The authors reviewed Honeypot concepts, classifications, architectural elements (decoy and captor) and deployments (centralized and distributed), software tools and features, virtualization techniques and configuration, and emergent trends. In the work of Oza *et al.* [30] different Honeypot and honeynet deployment architectures in an IoT network (typically for collecting threat intelligence data necessary for analysis and mitigation of cyberattacks) were discussed. Also, Veni *et al.* [31] presented a concise overview of cloud-based Honeypot and honeynet concepts, architectural deployments and models.

Just as in [28], a detailed survey of deception technologies (e.g. Honeypot and honeynet) was presented by Fraunholz *et al.* [32]. In their work, the fundamental concepts and typical software tools, architectural implementations, and ethics and legal aspects of deception technologies were discussed. Lu *et al.* [33] presented an overview of information monitoring system of Industrial Control System (ICS) called Supervisory Control and Data Acquisition (SCADA) and also Honeypot-based SCADA while the survey work presented by Razali *et al.* [34] reviewed different concepts, functionality, software, architecture of Internet-of-Things (IoT) Honeypot. In addition, the application of Honeypot technology in Industrial Control Systems was surveyed. The authors [34] suggested: 1) further review of attacks on IoT devices based on security metrics (such as source IP, source ports, malware login/password, type and distribution of attack source, etc.) characterizing the attacker; 2) design of an intelligent IoT Honeypot which can adapt to attacker's interaction level.

Sharma *et al.* [35] presented an overview of IDS and Honeypot systems in VANET and VANET Cloud networks. They suggested future research works in relating to: 1) how to effectively position a Honeypot in VANET to aid detection capability and overall performance; 2) detection of novel and previously unknown vulnerabilities and attacks; 3) collection of up-to-date attack dataset that truly represents the attack process; 4) investigating benefits and disadvantages of existing Honeypot deployment methods and attack detection techniques; 5) to improve and use of some generalized validation strategies; 6) development of Honeypot auto detection and response system; 7) development of intelligent and predictive Honeypot systems.

In 2019, Zobal [7] presented a review of existing Honeypot technologies. In their work, an overview of definitions, concepts, classifications, software tools,

benefits, legal and ethical issues, and challenges were discussed. In addition, Bhagat *et al.* [36] presented a concise overview of Honeypots concepts, classifications and typical architectural deployments and operations within a network. They [36] suggested further study is needed in Honeypot deployments against internal and external attacks and its applications in various networks.

In 2020, Lee *et al.* [37] presented a review on botnet, botnet attacks, and Honeypot used in capturing such attacks. For future research directions, authors suggested further studies into the applications of Honeypot in smart factory IoT networks is needed, especially for improved attack detection and response time. Also, Matin *et al.* [38] reviewed Honeypot-based malware detection and collection systems in which Machine Learning was used. They investigated the application of Honeypots in malware detection using machine learning techniques and models. Due to the availability of different training malware datasets collected at different times using Honeypot platforms, authors suggested concern of selecting qualitative dataset for development of machine learning models. Hence as future work, the authors [38] suggested further Honeypot development which establishes a fit-for-use of malware data.

In 2021, Franco *et al.* [39] presented a survey on Honeypot and honeynet systems in use in IoT and Cyber Physical System (CPS) application areas. They developed a novel taxonomy for classification purposes, and further discussed Honeypot and honeynet concepts, and lessons learned from various deployments. The authors [39] suggested: development of Honeypot systems for effective insider attack detection and mitigation; investigating technologies, platforms, and domains recently becoming prominent; investigating established but yet unexplored protocols; investigating effective deployment locations and remote management; and also, effective anti-Honeypot and ant-detection approaches.

5. Results and Discussions

In this section, we present and discuss the results of our findings by the characteristics of selected papers, characteristics of the research study areas, and the identified possible research openings.

5.1. Research Paper Characteristics

A total of 188 survey and/or review papers were initially retrieved as follows: 25 from SpringerLink [15]; 15 from ScienceDirect [16]; 38 from IEEE Xplore [17]; 9 from the ACM Digital Library [18]; and 101 from remaining sources. Before the screening phase, 38 duplicates and 10 records without authors and/or titles were removed remaining 140 records. After the title and abstract screening, 102 articles were excluded: 2 were white papers, 1 was poster, 1 was not in English, 53 were not survey and/or review papers, and 45 were not directly related to Honeypot technology. Thus, we retained 38 papers for further investigation. After the full-text screening, we further excluded 4 papers which were not Honeypot survey and/or review papers and as such were not relevant to this study. Thus,

we selected 34 related Honeypot surveys and/or review papers and rated them based on our qualitative selection scheme as previously highlighted: 22 papers were identified as high-impact and thus were included in this study; 12 papers were identified as low-impact and were only added for statistical analysis. The PRISMA flow diagram of the source selection process is shown in Figure 1. It illustrates how the most relevant Honeypot related papers were identified, screened, and selected from our search database.

5.1.1. Research Material by Source

Analysis of the publication source reveals that about 27% of the identified papers were selected as related and relevant for this study. Figure 2 shows the contributions of major online bibliographic sources such as SpringerLink [15]; ScienceDirect [16]; IEEE Xplore [17]; and ACM Digital Library [18]. Each database shows two bars: the left blue bar and the right orange bar shows the number of identified papers (through searches) and the number of relevant papers (*i.e.* papers

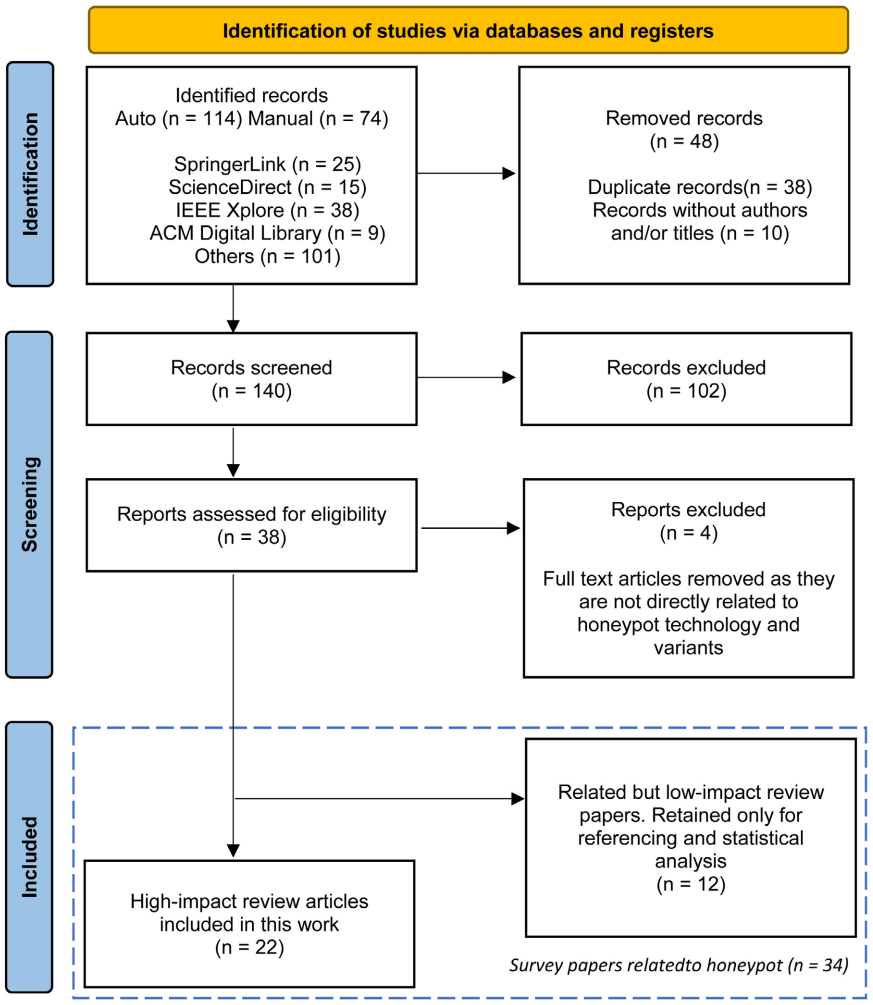

Figure 1. The PRISMA flow diagram showing the process of meta-analysis in this research. Papers were identified through searches of bibliographic databases, screened for eligibility, and finally selected and included in this study.

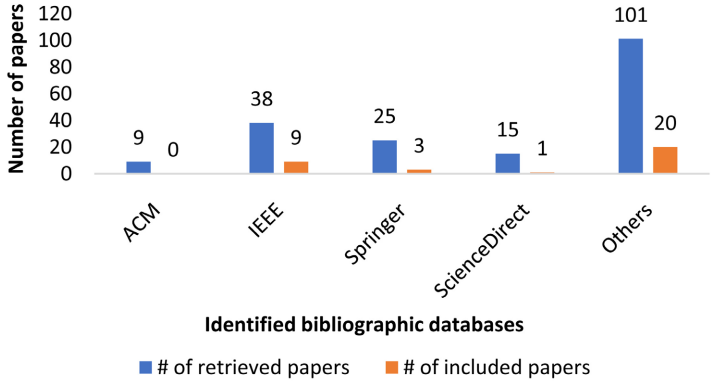

Figure 2. The proportion in number of papers contributed from four major bibliographic databases (and others). Each database shows two bars: the left blue bar and the right orange bar shows the number of identified papers (through searches) and the number of relevant papers (*i.e.* papers included and retained) respectively.

included and retained) respectively. Comparatively analyzing these sources (as shown in **Figure 2**), it can be observed that IEEE Xplore [17] has the highest contributions in terms of the number of retrieved (38) and included (9) papers respectively. On the other hand, the number of articles retrieved (9) from the ACM Digital Library [18] was the lowest and no articles were eventually selected from it. Furthermore, 101 and 20 papers were retrieved and selected respectively from other online databases accounting for about 54% and 59% of total retrieved and selected papers respectively.

5.1.2. Research Material by Publication Type

Further analysis of the type of publication of the selected 34 papers reveal that 50% were published in journals (17 articles); 44% in conference proceedings (15 articles); and 6% (2 articles) are preprints retrieved from arXiv [19] (an online bibliographic archive) as shown in **Figure 3**. Honeypot related survey and/or review papers published in conference proceedings have almost half of the papers (47%) published by IEEE alone and 20% (3 articles) published by Springer as shown in **Figure 4**. The (detailed) characteristics of the 22 included articles are shown in **Table 2**. These survey and/or review papers are regarded as high-impact and of immense importance to the research community. In total, 11 were published in conferences; 9 in journals and 2 were not published articles but preprints. We included the preprints due to the relatively high rate of citations and the assumed relevance to this study.

5.1.3. Research Material by Publication and Publisher

Selected articles (excluding preprints) were found to be published by 21 distinct publishers in a total of 31 distinct publication titles—16 conference proceedings and 15 journal titles. **Figure 5** shows the distribution of selected papers according to publishers. Only IEEE (2 articles) and Engg Journals Publications (2 articles) were observed to have published in two journals with only IEEE publishing in two different journals. Also, selected articles (excluding preprints) were

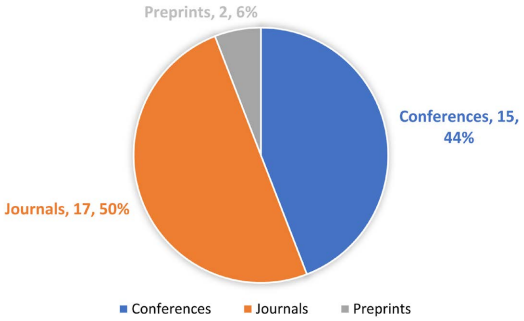

Figure 3. This pie chart shows the distribution of the 34 selected survey and/or review papers relevant to Honeypot from different publication types—Conferences, Journals, and Preprints. Preprints are not published articles, and are only used here for analysis.

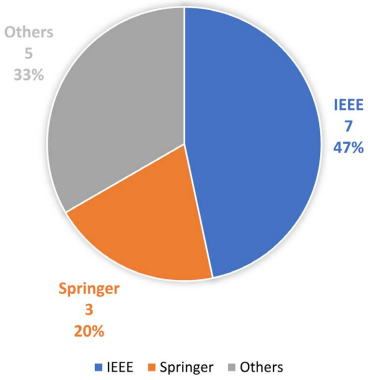

Figure 4. This pie chart shows the distribution of survey and/or review papers published in conference proceedings only, relevant to Honeypot technology. About half of the papers (47%) were published by IEEE alone and 20% (3 articles) by Springer.

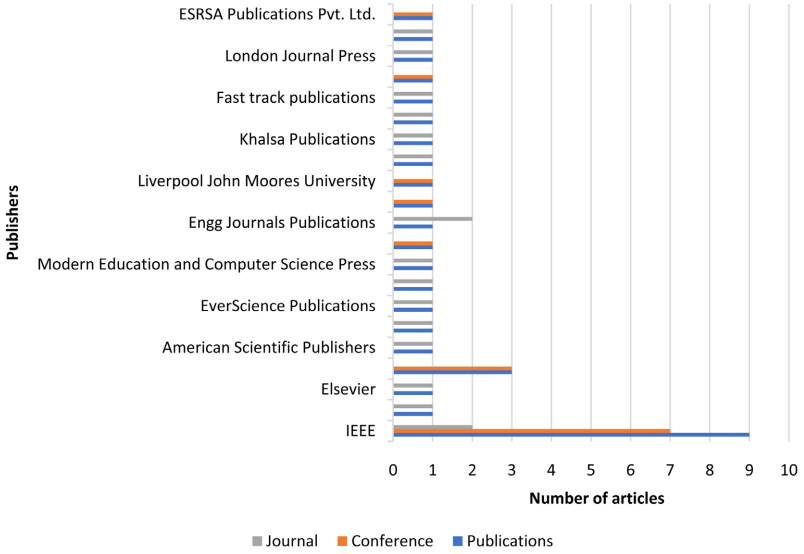

Figure 5. Distribution of selected survey and/or review papers relevant to Honeypot technology according to different publishers. For each publisher, the grey and orange bar(s) show the number of papers published in journals and/or conference proceedings respectively, while the blue bar shows the total number of publications in which the articles were published.

found to have been mostly evenly distributed across publications journal titles and conference proceedings such that no two articles originated from the same publication: IEEE published in 9 publications (2 in different conferences and 7 in different journals); Springer published in 3 publications (3 in different conferences); Engg Journals Publications published in one publication (2 articles in the same journal); the remaining publishers published only one article in either a conference proceeding or a journal. Hence, most publishers (about 86%) were found to have published only one article either in a conference or journal. Table 3 shows the characteristic features of each publisher including references and the period of publication.

Table 3. Characteristics of publishers, with respect to the number and period of publications. It shows the distribution of relevant to papers and references.

Publishers	# of Publications	# in Conference	# in Journal	Year of Coverage	Selected Papers
IEEE	9	7	2	2015-2021	[7] [9] [25] [26] [27] [30] [34] [38] [39]
Science and Information Organization	1	0	1	2020	[37]
Elsevier	1	0	1	2018	[35]
Springer	3	3	0	2017-2019	[29] [33] [36]
American Scientific Publishers	1	0	1	2018	[31]
Academic Publications Ltd.	1	0	1	2017	[28]
EverScience Publications	1	0	1	2015	[24]
Science Society of Thailand under Royal Patronage	1	0	1	2013	[23]
Modern Education and Computer Science Press	1	0	1	2012	[4]
Association for Computing Machinery (ACM)	1	1	0	2011	[22]
Engg Journals Publications	1	0	2	2012-2019	[44] [45]
SciTePress	1	1	0	2021	[46]
Liverpool John Moores University	1	1	0	2012	[47]
Technical University of Aachen (RWTH)	1	0	1	2017	[48]
Khalsa Publications	1	0	1	2013	[49]
National Chung Hsing University	1	0	1	2013	[50]
Fast track publications	1	0	1	2020	[51]
SSRN	1	1	0	2020	[52]
London Journal Press	1	0	1	2020	[53]
Auricle Technologies Pvt. Ltd.	1	0	1	2018	[54]
ESRSA Publications Pvt. Ltd.	1	1	0	2021	[55]
arXiv.org	2	2	0	2016-2018	[5] [32]

5.1.4. Research Material by Publication Country

In this section, we present our findings on the country of publication (*i.e.* the location of the conference proceedings and journals). The selected papers (excluding preprints) have been found to originate from 13 different countries as shown in Figure 6: India (12), UK (4), Taiwan (1), Russia (1), Portugal (2), US (4), Indonesia (1), Bulgaria (1), France (1), China (1), Thailand (1), Ireland (1), and Malaysia (2). India (38%), followed by the US (13%) and UK (13%) has been found to produce most of the papers.

A possible reason may be that these countries experience more cyberattacks compared to others and as such are more active in security research and in investigation of novel attack mitigation methods.

5.1.5. Research Material by Publication Year

To the best of our knowledge (based on our source inclusion and exclusion criteria), we noticed that there were little or no survey and/or review papers published between 2003 and 2011. This may be because survey and/or review papers before this period were really detailed and comprehensive enough and as such were sufficient for guiding the works of researchers. Another possible reason could be that there were no significant contributions both in Honeypot research and/or practice worth noting. There is also the possibility of the issue of adoption were Honeypot technology was still considered to be in the infancy stage coupled with the legal and ethical issues relating to deployment. Hence, significant (or landmark) deployments and research data may have been limited and research may not have been taken seriously during this period. Notwithstanding, as illustrated in Figure 7, survey and/or review contributions were found to have increased steadily from 2011 to 2017, and sharply to 2018. However, a general decline in the number of Honeypot survey and/or review papers has been observed in recent times.

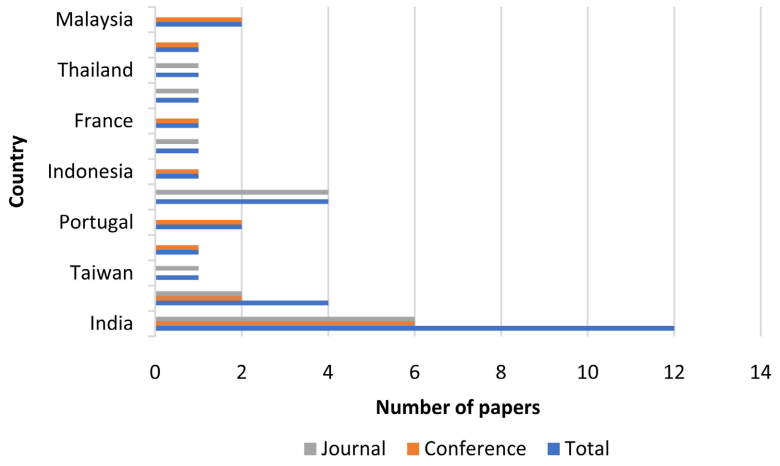

Figure 6. Distribution of selected survey and/or review papers relevant to Honeypot technology according to different countries. Each country has three bars: the grey and orange bar(s) depicts the number of survey papers published in journals and conference proceedings respectively; the blue bar shows the total number of publications.

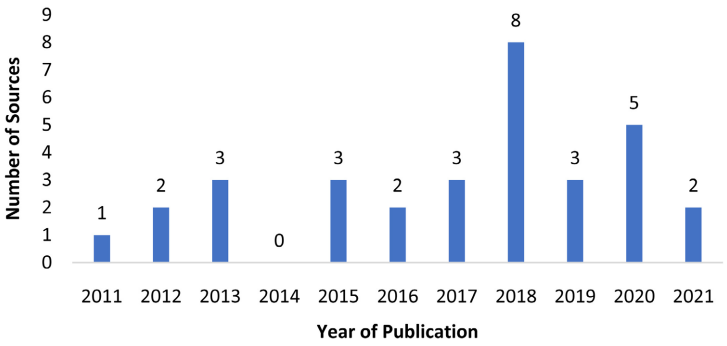

Figure 7. Distribution of selected survey and/or review papers relevant to Honeypot technology according to year of publication. Year 2018 experience a sharp increase in survey publications and this may be related to the severity of attacks at that time.

Out of the 32 selected survey and/or review papers about 25% (8 papers) were published in 2018, which accounts for the highest publications so far within the period of study. This sharp increase may be attributed to the major cybersecurity incidents of 2018 such as: 1) the Facebook's Cambridge Analytica scandal; 2) the Magecart malware affecting Ticketmaster and British Airways; and 3) the Meltdown and Spectre CPU vulnerabilities affecting Intel, Advanced Micro Devices, and ARM [56]. It is possible that due to the severity and high impact of these attack incidents, researchers started investigating advancements in Honeypot research and how Honeypot could be used to for effective mitigation. Also, no survey and/or review paper was published in 2014, and on the average, about 2 survey and/or review papers were published each year between 2011 and 2021.

5.2. Research Study Characteristics

Several Honeypot related keywords and topics were identified and extracted during the screening and full-text reviews of the 34 selected papers. Based on these data, we created a 10-category classification scheme as shown in **Table 4** In addition, we developed a visual representation of the classification scheme (**Figure 8**) showing the relationship between Honeypot technology, the main topics (key study areas) and the subtopics (keywords).

- Category C1—survey and/or review papers in this category discuss concepts, terminologies, definitions, classifications, and taxonomies in one or more of Honeypots, honeynets and honeytokens technologies [4] [5] [9] [22]-[39].
- Category C2—papers in this category present trends in Honeypot (and related) software, technologies, and tools [4] [5] [7] [9] [31] [32] [34].
- Category C3—papers in this category present trends in Honeypot (and related) deployments, architectures, designs, models, and configurations [4] [9] [22] [24] [26] [27] [30]-[38].
- Category C4—log collection, storage, collation, and data analysis tools, techniques, and methods were discussed [4] [5] [39].
- Category C5—papers in this category present discussions relating to Honeypot visualization tools, techniques, methods, and frameworks [5].

Table 4. A 10-category classification scheme developed from keywords and topics identified from Honeypot related articles during screening and full-text review process.

Category	Honeypot related research study areas
C1	Concepts, Terminologies, Definitions, Classifications, and Taxonomies. References: [4] [5] [9] [22]-[39].
C2	Software technologies and Honeypot related tools. References: [4] [5] [7] [9] [31] [32] [34].
C3	Configurations, Deployments, Architectures, Designs, Models, and Frameworks. References: [4] [9] [22] [24] [26] [27] [30]-[38].
C4	Security Metrics, Stream/Log Analysis tools, techniques, and methods. References: [4] [5] [39].
C5	Data Visualization tools, techniques, and methods. Reference: [5].
C6	Detection, Anti-detection, Anti-introspection, Adaptive/Deceptive techniques and approaches. References: [4] [23] [28] [29] [32].
C7	Legal/Ethical issues. References: [4] [5] [7] [32] [37].
C8	Cloud, Mobile, Wireless, ML, Blockchain, Internet-of-Things (IoT), Industrial Control Systems (ICS), Botnet, Robotics, Crypto, Vehicular ad-hoc Network (VANET), etc. References: [22] [30] [33] [34] [35] [37] [38] [39].
C9	Honeypot use cases, advantages, disadvantages, other emerging trends, challenges, open issues, and future research directions. References: [7] [9] [23] [25] [26] [29] [31] [34] [35] [36] [37] [38] [39].
C10	Other uncategorized/distinct/novel/emerging study areas. For example, Technology Independent Honeynet Description Language (TIHDL) and Honeytoken generation with Encrypted Pointers. References: [26] [27].

- Category C6—presents overviews on Honeypot detection, anti-detection, anti-introspection and adaptive concepts, techniques and approaches such as Game Theoretic Modelling (GTM) [4] [23] [28] [29] [32].
- Category C7—papers in this category, present discussions about legal and ethical concerns relating to Honeypot use and user privacy [4] [5] [7] [32] [37].
- Category C8—discuss Honeypot specialized applications areas such as in Teaching and Research, Cloud, Mobile, Wireless deployments, ML, Blockchain, Internet-of-Things (IoT), Industrial Control Systems (ICS), etc.), Botnet, Robotics, Crypto, Vehicular ad-hoc Network (VANET), and Smart Factory [22] [30] [33] [34] [35] [37] [38] [39].
- Category C9—present discussion on Honeypot use cases, advantages, disadvantages, other emerging trends, challenges, open issues, and future research directions [7] [9] [23] [25] [26] [29] [31] [34] [35] [36] [37] [38] [39].

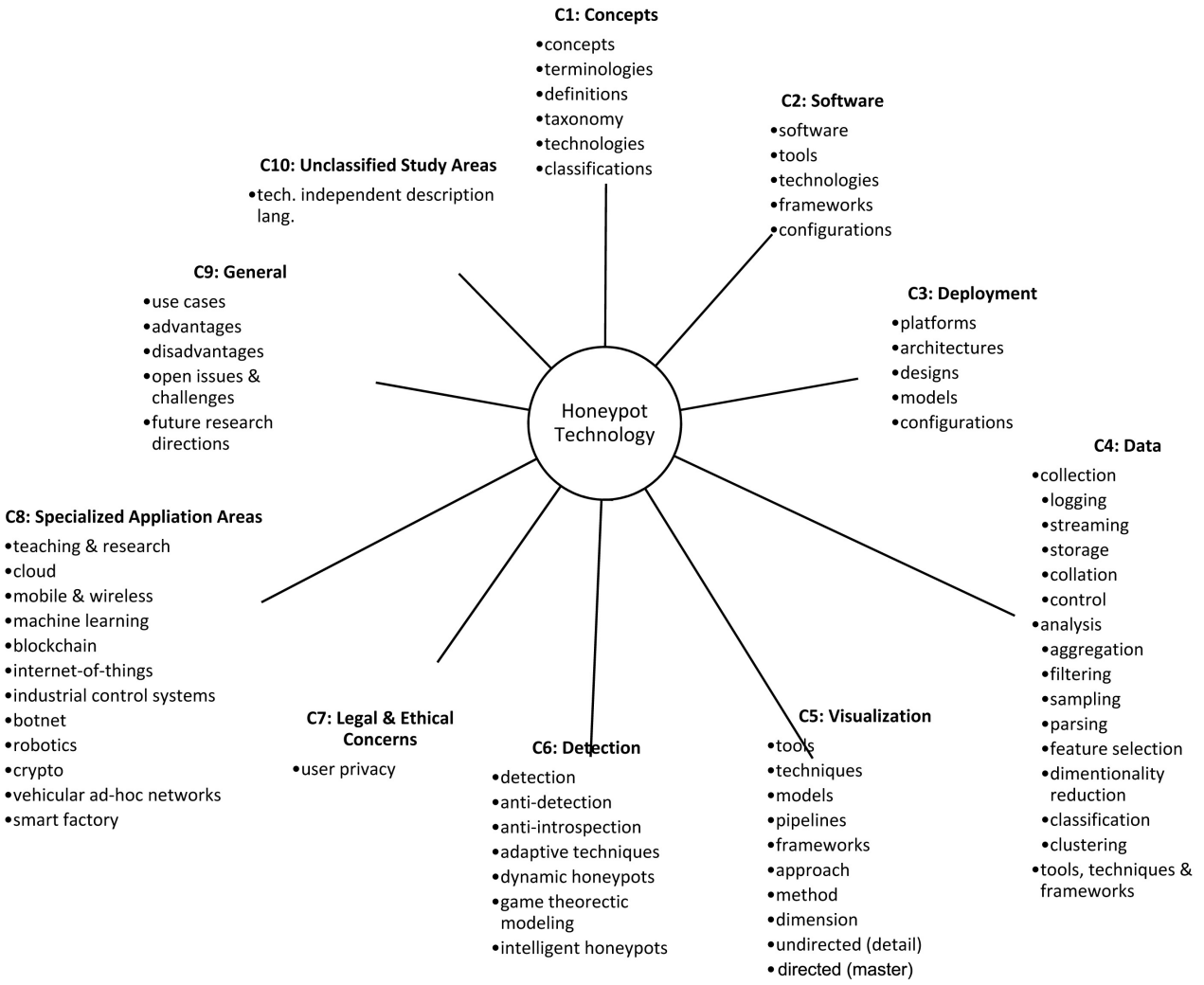

Figure 8. Mind map representation of the 10-category classification scheme based on keywords and titles extracted from survey and/or articles during screening and full-text review.

- Category C10—present other study areas which are novel, emerging, or distinct and are not classifiable under any previously motioned categories. As an example, Technology Independent Honeynet Description Language (TIHDL) [26].

Selected papers cover key Honeypot study areas as identified by Bringer *et al.* [4].

As shown in **Table 5**, all the articles (published and preprints) presented a form of background in Honeypot technology as explained in C1 above. About 35% (12 articles) presented Honeypot types; 62% (21 articles) topics relating to types of Honeypot deployments; 24% (8 articles) Honeypot detection; and 21% (7 articles) topics relating to Honeypot ethical/legal issues. We found data analysis (3 papers) and visualization (1 paper) study areas to have little survey and/or review contributions (C4 and C5). In addition, about 35% (12 articles) addressed specialized Honeypot applications and about 38% (13 articles) presented topics in Category C9. Only one (1) article was intentionally classified as Category C10.

Table 5. Study characteristics of selected articles showing the category of keywords and/or topics presented in each of the papers. This table shows how individual paper was categorized.

Author	Year	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	Type
Mairh [22]	2011	x		x					x			Conference
Bringer [4]	2012	x	x	x	x		x	x				Journal
Zanoramy [23]	2013	x					x			x		Journal
Baykara [24]	2015	x		x								Journal
Campbell [25]	2015	x								x		Conference
Fan [26]	2015	x		x						x	x	Conference
Nawrocki [5]	2016	x	x		x	x		x				Preprint
Jogdand [27]	2016	x		x							x	Conference
Pothumani [28]	2017	x					x					Journal
Uitto [29]	2017	x					x			x		Book series
Fan [9]	2018	x	x	x						x		Journal
Oza [30]	2018	x		x					x			Conference
Veni [31]	2018	x	x	x						x		Journal
Fraunholz [32]	2018	x	x	x			x	x				Preprint
Lu [33]	2018	x		x					x			Book series
Razali [34]	2018	x	x	x					x	x		Conference
Sharma [35]	2018	x		x					x	x		Journal
Zobal [7]	2019	x	x					x		x		Conference
Bhagat [36]	2019	x		x						x		Conference
Lee [37]	2020	x		x				x	x	x		Journal
Matin [38]	2020	x		x					x	x		Conference
Franco [39]	2021	x	x		x				x	x		Journal

We consider Technology Independent Honeynet Description Language (TIHDL) [26] a novel, distinct, and emerging honey field.

Furthermore, discussions on Honeypot topics in categories C1 (concepts), C3 (deployment) and C9 (general) have been found to be mostly prevalent in the selected survey and/or review papers as shown in **Figure 9**. This may be a clear indication that these topics typically receive more attention from within the research community. Similarly, study areas in categories C2 (software), C6 (detection), C7 (legal/ethical) and C8 (special applications) have also received considerable share of attention—again, with the exception of topics in categories C4 and C5.

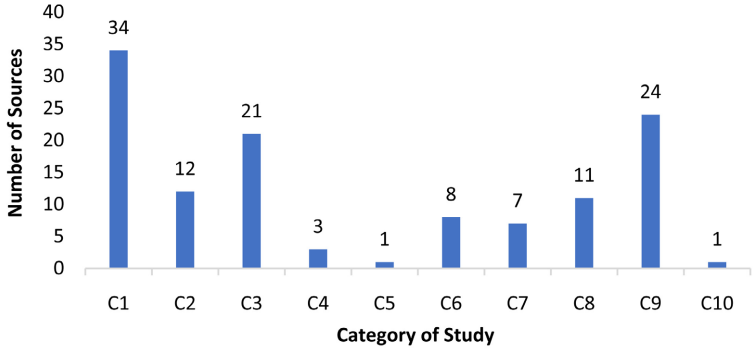

Figure 9. Distribution of selected survey and/or review papers relevant to Honeypot technology according to the Honeypot study 10-category classification scheme.

5.3. Honeypot Research Directions

We identified a number of open research questions and future research opportunities from the selected survey and/or review papers [23] [26] [29] [34] [35] [36] [38] [39]. As show in **Table 6**, these have been grouped by application or domain areas—particularly, in categories C6, C2, C3, and C10. This section provides researchers an overview of possible research directions.

The authors [26] presented an overview of existing common descriptive languages and proposed one that could be used in the configuration and management of disparate honeynet deployments, included in a flexible configuration tool—HoneyGen [43]. They [26] suggested, most importantly: 1) extending the HoneyGen [43] tool for compatibility with more honeynet platforms; and 2) studying of the automatic translation between the proposed technology independent language and the proprietary deployment languages of honeynet platforms. Similarly, the authors [36] suggested further study is needed in Honeypot deployments against internal and external attacks and its applications in various networks.

As the black hat community continues to improve the sophistication of malwares for effective (execution environment) fingerprinting, authors [29] proposed future research direction as: 1) the development of new ways to identify and classify malware detection vectors; and 2) the development of inexpensive, and more robust and adaptive Honeypot solutions with better and advanced deception. Additionally, the authors [23] acknowledge that very little research work was done in applying Artificial Intelligence (AI) techniques for development of dynamic and intelligent Honeypot systems, and farther proposed the use of already existing AI techniques such as Expert Systems (ES) [40], Fuzzy Logic (FL) [41], and Swarm Intelligence (SI) [42]. In a similar direction, the authors [38] presented the concern of selecting qualitative dataset for development of machine learning models, due to the availability of different training malware datasets collected at different times using Honeypot platforms.

Hence, they [38] suggested further Honeypot development which establishes a fit-for-use of malware data.

Table 6. Research opportunities identified from selected survey and/or review papers relevant to Honeypot technology.

Category	Domain	Research opportunities
C6	Detection, Anti-detection	1) Use of AI techniques in the development of dynamic and intelligent Honeypot systems [23]. 2) The development of new ways to identify and classify malware detection vectors and consequently the development of inexpensive, more robust, adaptive, solution with better advanced deception [29]. 3) Detection of novel and previously unknown vulnerabilities and attacks; Investigating benefits and disadvantages of existing Honeypot attack detection techniques [35].
C2, C3, C4, C10	Software, Tools, ML, Deployment	1) Extending the HoneyGen tool for compatibility with other platforms and automatic translation between the common technology independent and proprietary language [26]. 2) Development of Honeypot software for collecting fit-for-use malware data for efficient ML model development [38]. 3) Honeypot deployments against internal and external attacks in various application areas [36]. 4) Collection of up-to-date attack dataset that truly represents the attack process; 5) Investigating benefits and disadvantages of existing Honeypot deployment methods; 6) Development of Honeypot auto detection and response systems; 7) Development of intelligent and predictive Honeypot systems [35].
C8	IoT, VANET, CPS	1) Farther investigation of malware attacks on IoT devices based on security metrics [34]. 2) How to effectively position a Honeypot in VANET to aid detection capability and overall performance [35]. 3) IoT and Cyber Physical System (CPS) [39].

Vehicular ad-hoc network (VANET) [57] and Internet-of-Things [58] are some of the rising specialized application areas benefiting from Honeypot research. VANET involves a spontaneous creation of wirelessly connected vehicles in a network in which vehicles can join or leave at will. The authors [35] presented an overview of IDS and Honeypot systems in VANET and VANET Cloud networks. They [35] suggested future research works relating to: 1) how to effectively position a Honeypot in VANET to aid detection capability and overall performance; 2) detection of novel and previously unknown vulnerabilities and attacks; 3) collection of up-to-date attack dataset that truly represents the attack process; 4) investigating benefits and disadvantages of existing Honeypot deployment methods and attack detection techniques; 5) to improve and use of some generalized validation strategies; 6) development of Honeypot auto detec-

tion and response system; 7) development of intelligent and predictive Honeypot systems.

Internet-of-Things (IoT), on the other hand, involves the networking of physical sensor-embedded objects for the purpose of inter-communication over the internet. The authors [34] presented an overview of IoT and Industrial Control Systems. They [34] suggested: 1) further review of attacks on IoT devices based on security metrics (such as source IP, source ports, malware login/password, type and distribution of attack source, etc.) characterizing the attacker; 2) design of an intelligent IoT Honeypot which can adapt to attacker's interaction level. Similarly, the authors [39] presented a survey on Honeypot and honeynet systems in use in IoT and Cyber Physical System (CPS) application areas. They [39] suggested as future research works (broadly categorized): 1) development of Honeypot systems for effective insider attack detection and mitigation; 2) investigating technologies, platforms, and domains recently becoming prominent; 3) investigating established but yet unexplored protocols; 4) investigating effective deployment locations and remote management; 5) investigating effective anti-Honeypot and ant-detection approaches.

6. Conclusions

To researchers and professionals alike, the Honeypot technology presents a perfect tool for studying and evaluating cyberattacks. It is uniquely positioned to collect data on novel vulnerabilities and attacks, and hence, can facilitate better and newer ways to protect organizations' networks. In this paper, we systematically conducted a meta-analysis of Honeypot systems research areas to develop an overview of and identify trends in Honeypot research. We selected, synthesized, and quantitatively analyzed quality Honeypot survey and/or review papers. We identified and classified key Honeypot research study areas and examined how Honeypot research has evolved over time. Hence, this study contributes to the pool of research efforts by systematically conducting and reporting reviews in Honeypot research.

The study finds that most Honeypot survey and/or review papers of high relevance to the research community are published in 2018, by IEEE, in conferences, organized in India, and included in the IEEE Xplore database. Also, there have been only a few quality Honeypot reviews published after 2018, and survey and/or review contributions have been low, particularly in the areas of data analysis and visualization. This means that there are opportunities for the research community to investigate scientific contributions in these areas. In addition, research in new Honeypot areas is emerging, for example, the development of highly intelligent, dynamic, and evasive Honeypot systems, and the development of platform-independent honeynet management language and framework. Although there could be other critical review papers that missed our selection criteria, it is worth noting that the important content of the articles has been carefully organized in tables to help researchers with quick navigation and insights. We

have grouped Honeypot study areas into ten categories based on key Honeypot research topics found in literature, and have observed overlapping study areas.

Furthermore, the search strategy in the study may have missed other critical papers, hence other emerging Honeypot areas. We, therefore, recommend a further in-depth investigation into developments and trends in Honeypot research by: 1) including other paper types (e.g. empirical, books, etc.); and 2) searching across premier bibliographic databases using search interfaces peculiar to individual databases (to increase search scope); and 3) developing finer-grained research-area classifications of identified Honeypot topics. Additionally, there have been few systematic reviews in Honeypot research, hence we recommend more systematic future Honeypot surveys and/or reviews using established methods and/or frameworks to foster research that is repeatable and free of bias.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Nabe, C. (2020) Impact of COVID-19 on Cybersecurity. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[2] Verizon (2021) DBIR 2021 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdfx

[3] Spitzner, L. (2002) Honeypots: Tracking Hackers. Addison-Wesley, Boston.

[4] Bringer, M.L., Chelmecki, C.A. and Fujinoki, H. (2012) A Survey: Recent Advances and Future Trends in Honeypot Research. *International Journal of Computer Network and Information Security*, **4**, 63-75. https://www.proquest.com/scholarly-journals/survey-recent-advances-future-trends-honeypot/docview/1624271912/se-2 https://doi.org/10.5815/ijcnis.2012.10.07

[5] Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C. and Schönfelder, J. (2016) A Survey on Honeypot Software and Data Analysis. Cornell University Library, Ithaca. https://www.proquest.com/working-papers/survey-on-honeypot-software-data-analysis/docview/2079608235/se-2

[6] Silva, D. and Rodriguez, G. (2017) A Review of the Current State of Honeynet Architectures and Tools. *International Journal of Security and Networks*, **12**, 255-272. https://doi.org/10.1504/IJSN.2017.088133

[7] Zobal, L., Kolář, D. and Fujdiak, R. (2019) Current State of Honeypots and Deception Strategies in Cybersecurity. 2019 11*th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (*ICUMT*), Dublin, 28-30 October 2019, 1-9. https://doi.org/10.1109/ICUMT48472.2019.8970921

[8] Moore, C. and Al-Nemrat, A. (2015) An Analysis of Honeypot Programs and the Attack Data Collected. *Global Security*, *Safety and Sustainability*: *Tomorrow's Challenges of Cyber Security*, London, September 2015, 228-238.

https://doi.org/10.1007/978-3-319-23276-8_20

[9] Fan, W., Du, Z., Fernández, D. and Villagrá, V.A. (2018) Enabling an Anatomic View to Investigate Honeypot Systems: A Survey. *IEEE Systems Journal*, **12**, 3906-3919. https://doi.org/10.1109/JSYST.2017.2762161

[10] Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. and Group, T.P. (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLOS Medicine*, **6**, e1000097. https://doi.org/10.1371/journal.pmed.1000097

[11] Page, M.J., *et al*. (2021) The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Systematic Reviews*, **10**, Article No. 89. https://doi.org/10.1186/s13643-021-01626-4

[12] Rosenthal, R. and Dimatteo, M.R. (2001) Meta-Analysis: Recent Developments in Quantitative Methods for Literature Reviews. *Annual Review of Psychology*, **52**, 59-82. https://doi.org/10.1146/annurev.psych.52.1.59

[13] Jayadi, K., Abduh, A. and Basri, M. (2022) A Meta-Analysis of Multicultural Education Paradigm in Indonesia. *Heliyon*, **8**, e08828. https://doi.org/10.1016/j.heliyon.2022.e08828

[14] Wittmann, F.M. (2017) Sort Google Scholar by the Number of Citations V2.0b. https://github.com/WittmannF/sort-google-scholar

[15] SpringerLink, Springer Nature Switzerland AG (2021). http://link.springer.com

[16] Science Director, Elsevier B.V. (2021). https://www.sciencedirect.com

[17] IEEE Xplore, Institute of Electrical and Electronics Engineers (2021). https://ieeexplore.ieee.org

[18] ACM Digital Library, Association for Computing Machinery (2021). https://dl.acm.org

[19] arXiv (2021). https://arxiv.org

[20] CiteSeer^{x} (2021). https://citeseerx.ist.psu.edu

[21] SCImago. SJR-SCImago Journal & Country Rank Portal (2021). http://www.scimagojr.com

[22] Mairh, A., Barik, D., Verma, K. and Jena, D. (2011) Honeypot in Network Security. *Proceedings of the* 2011 *International Conference on Communication, Computing & Security*, Odisha, 12-14 February 2011, 600-605. https://doi.org/10.1145/1947940.1948065

[23] Zakaria, W.Z.A. and Kiah, M.L.M. (2013) A Review of Dynamic and Intelligent Honeypots. *ScienceAsia*, **39S**, 1-5. https://doi.org/10.2306/scienceasia1513-1874.2013.39S.001

[24] Baykara, M. and Das, R. (2015) A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. *International Journal of Computer Networks and Applications*, **2**, 203-211.

[25] Campbell, R.M., Padayachee, K. and Masombuka, T. (2015) A Survey of Honeypot Research: Trends and Opportunities. 2015 10*th International Conference for Internet Technology and Secured Transactions* (*ICITST*), London, 14-16 December 2015, 208-212. https://doi.org/10.1109/ICITST.2015.7412090

[26] Fan, W., Fernández, D. and Villagrá, V.A. (2015) Technology Independent Honeynet Description Language. 2015 3*rd International Conference on Model-Driven Engineering and Software Development* (*MODELSWARD*), Angers, 9-11 February 2015, 303-311.

[27] Jogdand, P. and Padiya, P. (2016) Survey of Different IDS Using Honeytoken Based

Techniques to Mitigate Cyber Threats. 2016 *International Conference on Electrical, Electronics, and Optimization Techniques* (*ICEEOT*), Chennai, 3-5 March 2016, 802-807. https://doi.org/10.1109/ICEEOT.2016.7754797

[28] Pothumani, S. and Anuradha, C. (2017) Decoy Method on Various Environments—A Survey. *International Journal of Pure and Applied Mathematics*, **116**, 197-200.

[29] Uitto, J., Rauti, S., Laurén, S. and Leppänen, V. (2017) A Survey on Anti-Honeypot and Anti-Introspection Methods. *Recent Advances in Information Systems and Technologies*, Madeira, 11-13 April 2017, 125-134. https://doi.org/10.1007/978-3-319-56538-5_13

[30] Oza, A.D., Kumar, G.N. and Khorajiya, M. (2018) Survey of Snaring Cyber Attacks on IoT Devices with Honeypots and Honeynets. 2018 3*rd International Conference for Convergence in Technology* (*I2CT*), Pune, 6-8 April 2018, 1-6. https://doi.org/10.1109/I2CT.2018.8529510

[31] Veni, K., Prabakaran, S. and Sivamohan, S. (2018) A Survey on Honeypot and Honeynet Systems for Intrusion Detection in Cloud Environment. *Journal of Computational and Theoretical Nanoscience*, **15**, 2949-2953. https://doi.org/10.1166/jctn.2018.7572

[32] Fraunholz, D., *et al.* (2018) Demystifying Deception Technology: A Survey. https://arxiv.org/pdf/1804.06196.pdf

[33] Lu, K.-C., Liu, I.-H., Sun, M.-W. and Li, J.-S. (2018) A Survey on SCADA Security and Honeypot in Industrial Control System. In: *Recent Trends in Data Science and Soft Computing*, Springer International Publishing, Cham, 598-604. https://doi.org/10.1007/978-3-319-99007-1_56

[34] Razali, M.F., Razali, M.N., Mansor, F.Z., Muruti, G. and Jamil, N. (2018) IoT Honeypot: A Review from Researcher's Perspective. 2018 *IEEE Conference on Application, Information and Network Security* (*AINS*), Langkawi, 21-22 November 2018, 93-98. https://doi.org/10.1109/AINS.2018.8631494

[35] Sharma, S. and Kaul, A. (2018) A Survey on Intrusion Detection Systems and Honeypot Based Proactive Security Mechanisms in VANETs and VANET Cloud. *Vehicular Communications*, **12**, 138-164. https://doi.org/10.1016/j.vehcom.2018.04.005

[36] Bhagat, N. and Arora, B. (2019) Honeypots and Its Deployment: A Review. In: Rathore, V.S., *et al.*, Eds., *Emerging Trends in Expert Applications and Security*, Springer, Berlin, 505-512. https://doi.org/10.1007/978-981-13-2285-3_59

[37] Lee, S., Abdullah, A. and Zaman, N. (2020) A Review on Honeypot-Based Botnet Detection Models for Smart Factory. *International Journal of Advanced Computer Science and Applications*, **11**, 418-435. https://doi.org/10.14569/IJACSA.2020.0110654

[38] Matin, I.M.M. and Rahardjo, B. (2020) The Use of Honeypot in Machine Learning Based on Malware Detection: A Review. 2020 8*th International Conference on Cyber and IT Service Management* (*CITSM*), Pangkal Pinang, 23-24 October 2020, 1-6. https://doi.org/10.1109/CITSM50537.2020.9268794

[39] Franco, J., Aris, A., Canberk, B. and Uluagac, A.S. (2021) A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. *IEEE Communications Surveys & Tutorials*, **23**, 2351-2383. https://doi.org/10.1109/COMST.2021.3106669

[40] Wikipedia Contributors (2021) Expert System. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Expert_system&oldid=1068448586

[41] Wikipedia Contributors (2021) Fuzzy Logic. Wikipedia, the Free Encyclopedia.

https://en.wikipedia.org/w/index.php?title=Fuzzy_logic&oldid=1089130200

[42] Wikipedia Contributors (2021) Swarm Intelligence. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Swarm_intelligence&oldid=1084731709

[43] Bercovitch, M., Renford, M., Hasson, L., Shabtai, A., Rokach, L. and Elovici, Y. (2011) HoneyGen: An Automated Honeytokens Generator. *Proceedings of* 2011 *IEEE International Conference on Intelligence and Security Informatics*, Beijing, 10-12 July 2011, 131-136. https://doi.org/10.1109/ISI.2011.5984063

[44] Srivastava, N. and Prakash, V. (2012) A Survey on the Approaches in Honeypot for Implementing Network Security. *International Journal on Computer Science and Engineering*, **4**, 1691-1694.

[45] Titarmare, N., Hargule, N. and Gupta, A. (2019) An Overview of Honeypot Systems. *International Journal of Computer Sciences and Engineering*, **7**, 394-397. https://doi.org/10.26438/ijcse/v7i2.394397

[46] Lackner, P. (2021) How to Mock a Bear: Honeypot, Honeynet, Honeywall & Honeytoken: A Survey. *Proceedings of the* 23*rd International Conference on Enterprise Information Systems*, Prague, 26-28 April 2021, 181-188. https://doi.org/10.5220/0010400001810188

[47] Almutairi, A., Parish, D. and Phan, R. (2012) Survey of High Interaction Honeypot Tools: Merits and Shortcomings. *Proceedings of the* 13*th Annual Post-Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, Liverpool, 25-26 June 2012. https://www.academia.edu/2670489/Survey_of_High_Interaction_Honeypot_Tools_Merits_and_Shortcomings

[48] Vishnevsky, A. and Klyucharev, P. (2018) A Survey of Game-Theoretic Approaches to Modeling Honeypots. http://ceur-ws.org/Vol-2081/paper29.pdf

[49] Ahmed Salman, H., Hassan, N. and Fahad, A. (2013) A Survey on Smartphone Honeypot. *International Journal of Computers & Technology*, **11**, 2476-2480. https://doi.org/10.24297/ijct.v11i4.3131

[50] Goel, R., Sardana, A. and Joshi, R.C. (2013) Wireless Honeypot: Framework, Architectures and Tools. *International Journal of Network Security*, **15**, 373-383.

[51] Baker, B., Kelsey, Q. and Jason, P. (2020) Machine Learning Classifiers in Honeynets: A Critical Review. *International Research Journal of Engineering and Technology*, **7**, 6850-6853. https://www.irjet.net/archives/V7/i5/IRJET-V7I51289.pdf

[52] Tiwari, A. and Kumar, D. (2020) Comparitive Study of Various Honeypot Tools on the Basis of Their Classification & Features. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3565078

[53] Verma, A.S. and Anubha, D. (2020) A Review on Honeypot Deployment. *London Journal of Research in Computer Science and Technology*, **20**, 1-10. https://journalspress.com/a-review-on-honeypot-deployment

[54] Manchekar, S., Makarand, K. and Krantee, J. (2018) Application of Honeypot in Cloud Security: A Review. *International Journal on Future Revolution in Computer Science & Communication Engineering*, **4**, 63-65. http://www.ijfrcsce.org/index.php/ijfrcsce/article/view/1688/1688

[55] Shirsath, V. (2021) A Survey on Current States of Honeypots and Deception Techniques for Attack Capture. *International Journal of Engineering Research & Technology*, **9**, 438-443.

[56] Kerner, S.M. (2018, December 31) Looking Back at the Top Cyber-Security Incidents of 2018. https://www.eweek.com/security/looking-back-at-the-top-cyber-security-incidents-

of-2018

[57] Sheikh, M.S., Liang, J.and Wang, W. (2019) A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs). *Sensors*, **19**, Article 3589. https://doi.org/10.3390/s19163589

[58] Wang, B., Dou, Y., Sang, Y., Zhang, Y. and Huang, J. (2020) IoTCMal: Towards A Hybrid IoT Honeypot for Capturing and Analyzing Malware. *ICC* 2020 *IEEE International Conference on Communications* (*ICC*), Dublin, 7-11 June 2020, 1-7. https://doi.org/10.1109/ICC40277.2020.9149314