

# Attack graph-based security metrics: concept, taxonomy, challenges and open issues

Zaid. J. Al-Araji<sup>1\*</sup>, Sharifah Sakinah Syed Ahmad<sup>2</sup>, Hussein M. Farhood<sup>3,4</sup>, Ammar Awad Mutlag<sup>5</sup> and Mahmood S. Al-Khaldee<sup>6</sup>

<sup>1</sup>Technical Computer Engineering Department, Al-Hadba University College, Mosul, Iraq

<sup>2</sup>Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

<sup>3</sup>Department of Communication and Engineering, School of Electrical Engineering, College of Engineering, University Teknologi MARA, Shah Alam, Selangor, Malaysia

<sup>4</sup>Department of Computer Engineering, College of Engineering, Mustansiriyah University, 10047 Baghdad, Iraq

<sup>5</sup>Ministry of Education/General Directorate of Curricula, Pure Science Department, Baghdad 10065, Iraq

<sup>6</sup>Ministry of Education, Mosul, Iraq

**ABSTRACT** Context: Security issues have increased recently because of the increased use of networking. The researchers have proposed many models, approaches, and models, for example, attack graphs. The attack graph model is a valuable tool for vulnerability analysis as well as for displaying all network paths. In general, attack graphs can be utilized for a variety of purposes, including the calculation of security metrics. Nonetheless, in order to sufficiently safeguard networks, a technique for gauging the security degree provided by these activities is required, as "you cannot improve what you cannot measure." The security level of a system or network is typically represented by network security metrics in qualitative and quantitative ways. The network security metrics are typically employed to evaluate a system's security level and meet security objectives. Aim: This study aims to present a review of attack graph-based security metrics and analyse the previous work. Provides the limitations and issues the researchers faced to improve this important research area. Methodology: The attack graph security metrics field was thoroughly investigated in all research, and four databases—ScienceDirect, Web of Science (WoS), Scopus, and IEEE—were used to collect data between 2001 and 2022. Results: 46 papers were founded on attack graph security metrics with different methods and techniques based on the exclusion and inclusion criteria. The results of the taxonomy created three significant categories: proposed, implemented, reviewed, and surveyed. We believe this study will aid in highlighting research ability, which will subsequently broaden and establish new research topics.

## 1 Introduction

The use of network technology has grown in recent years [1], [2], [3], [4]. However, despite the network's benefits for human life, it also has security issues that must not be disregarded [2]. Security is a serious challenge that has been and will continue to be in numerous important computer applications and systems. A comprehensive cyberattack has the potential to cause significant harm to both the target system and the businesses or organizations that utilize it. An attacker might use such assaults to impede network performance, obtain authorization to access sensitive data, and ultimately take complete control of a targeted machine. The researchers have employed a variety of techniques to either detect or protect the network from threats [5]. Attack graph (AG) is one of the important models that has been used to either detect or protect the attacks.

---

\*Corresponding Author: [zaid.jm@hcu.edu.iq](mailto:zaid.jm@hcu.edu.iq)

The AG was proposed by Philips and Swiler [6], [7]. Since then, scholars have proposed various techniques for creating AGs. For instance, [8] developed a generation approach based on monotonicity, whereas AG ranking using a neural network graph was proposed by [9]. In addition, [10] presented an AG construction approach based on a Kohonen neural network supervised, whereas [11] presented an approach for finding forward full AG construction that relies on hypergraph partitioning. The network vulnerability assessment approach based on the database graph was also introduced by [12], who elaborated on its effectiveness in resolving state explosions and many other issues.

An AG can be used for several aspects, in negative or positive ways [13], [14]. Researchers frequently employ AG to strengthen network security. The security metrics calculation is one of these applications. Additionally, security metrics can be developed and assessed, as well as the overall security of the network, using AGs. The danger in the network can also be assessed using these measures. According to the National Institute of Standards and Technology (NIST), security metrics are methods for obtaining, evaluating, and disseminating pertinent performance-related data to facilitate decision-making and improve network performance [15].

Generally, security metrics are classified into two classes: primary-based and secondary-based [16]. The primary-based metrics contain architectural and performance metrics. The architecture has many metrics; the AG-based security metrics are one of these types. AG-based security metrics result from monitoring a network's internal characteristics that impact the security of the information technology and operational security. The values are obtained by creating an AG and then applying analytics.

Many AG-based security measures have been suggested and launched in the last few years, and these metrics have been used to quantify security levels in numerous published studies. Nevertheless, to the best of our knowledge and inquiry, no comprehensive article exists that explains every AG-based statistic. This study examines the subject of AG-based security metrics and examines earlier studies that mostly concentrated on developing or utilizing AG-based metrics. An SLR can determine, categorize, and synthesize a comparative analysis of state-of-the-art studies. It enables knowledge transfer within the scientific field [17], [18]. The SLR was conducted to identify, perform taxonomic classification, and systematically compare existing studies on planning, executing, and validating AG-based metrics by performing a methodological review of the existing studies, we aim to provide answers to the following questions:

What are the main practical motivations for AG-based security metrics?

What are some of the most well-known AG-based security metrics?

Which type of classification in research approaches can be applied for AG-based security metrics?

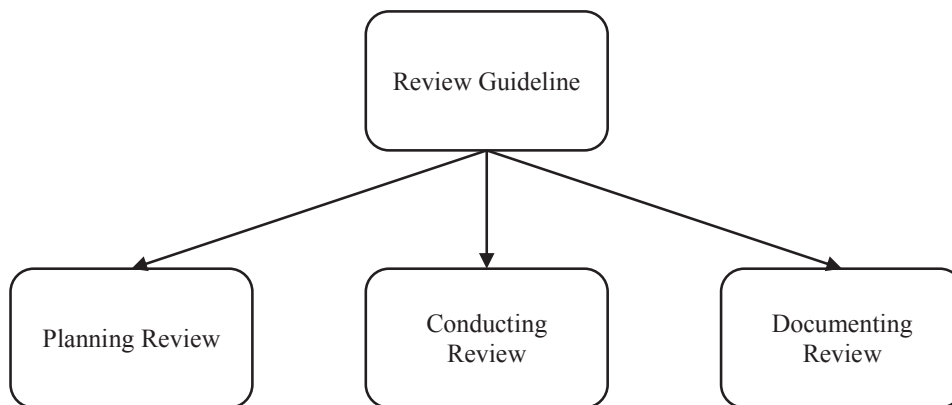
What are the open issues and future trends of AG-based security metrics?

The guidelines in [19]–[22] were followed in this study. The criteria and factors taken into account for deepening comprehension of various pertinent components of this topic in the literature included motivations, challenges faced by researchers, and recommendations made to analyze for advancing this crucial study area. Therefore, 46 studies were selected, classified, and compared by applying characterization taxonomy. The characterization taxonomy based on these fields comprises three groups: host, network, and composite-based metrics. Furthermore, open issues and future directions related to AG-based security metrics are also presented.

This article is organized as follows: Section 2 explains the research methodology; the security metrics overview is explained in detail in Section 3. Section 4 presents the related work. Section 5 represents the research analysis. Section 6 presents the limitations and challenges, and section 7 represents the research conclusion.

## 2 Research Methodology

The processes listed below are used in the planning and review process for AG-based metrics as shown in Figure 1: (1) Identify the need and necessity for an exhaustive analysis of the available AG security-based metrics. (2) Identify and study the research gap, concerns, and issues the prior studies raise. (3) Improve/assess the process for conducting a systematic literature review on the AG-based security metrics.



**Fig 1.** Guideline of research methodology

The following phases lead to the systematic literature review of AG-based security metrics: (1) Identify the AG-based metrics research. (2) Articles selection technique. (3) Extraction of the information. The implementation of the findings of the comprehensive literature review of AG-based security metrics is done in the documenting review phase, which also looks at how to choose the research.

### 2.1 Planning the Review

Review planning begins with gaining insights into the motivations for systematic work and the results of a review protocol as follows:

#### 1. Motivation of the Review

A systematic review results from identifying, categorizing, and comparing current evidence on AG-based security metrics. It focuses on categorizing and contrasting security metrics in the AG. Concerning the importance of deriving security metrics in AG, it is necessary to consolidate the existing evidence on AG-based security metrics. This section answers the RQ1 which is "What are the main practical motivations for AG-based security metrics".

#### 2. Information Source

The studies were methodically carried out using the following four databases, ScienceDirect, Scopus, WoS, and IEEE. The study was chosen based on an index, demonstrating a simple and complicated query in numerous publications and conference articles on network security. Technical studies were therefore taken into account throughout the selection process, offering a wider perspective on research projects taking into account many scientific domains, as shown in Table 1.

**Table 1.** The exclusion and inclusion criteria for the papers

Criteria	Type	Prenominal
Inclusion	Research articles (technical, survey, and review) that are related to AG-based metrics	Scientific reports that derive the security metrics using an AG
Exclusion	<ul style="list-style-type: none"> <li>• Books, Book Chapters, and Thesis.</li> <li>• Not English papers.</li> <li>• Unrelated papers.</li> </ul>	Not English, Books, Theses, and unrelated papers are excluded

### 3. Research Selection

The selection technique of the studies for effective review is complicated, considering different research fields. It is the most important and perhaps neglected perspective while examining a certain issue. First, duplicated and unrelated publications had to be omitted while considering the abstracts and titles of each paper. Second, full articles will be read off the remaining papers to find the related articles.

### 4. The SLR Search

We produced the query using particular keywords in IEEE, Web of Science (WoS), ScienceDirect, and Scopus databases. The search queries were ("attack graph" AND ("security metric" OR "vulnerabilities metric" OR "path metric" OR "host metric") OR ("attack graph security metrics")). We chose journals and conferences as the only advanced search choices in each database, excluding additional alternatives like chapters, books, or other publications.

#### 4.1 Article Search Results

From 2001 to 2022, the query resulted in 804 papers, 223 from IEEE Xplore, 26 from WoS, 137 from Scopus, and 418 from ScienceDirect, as shown in Figure 2. 365 duplicate articles were found in all databases, and 393 papers are unrelated.

, most of the papers were published in ScienceDirect and IEEE databases. Figure 2 illustrates the overtime classification of the articles in every category, including IEEE, ScienceDirect, Scopus, and Web of Science, through the years.

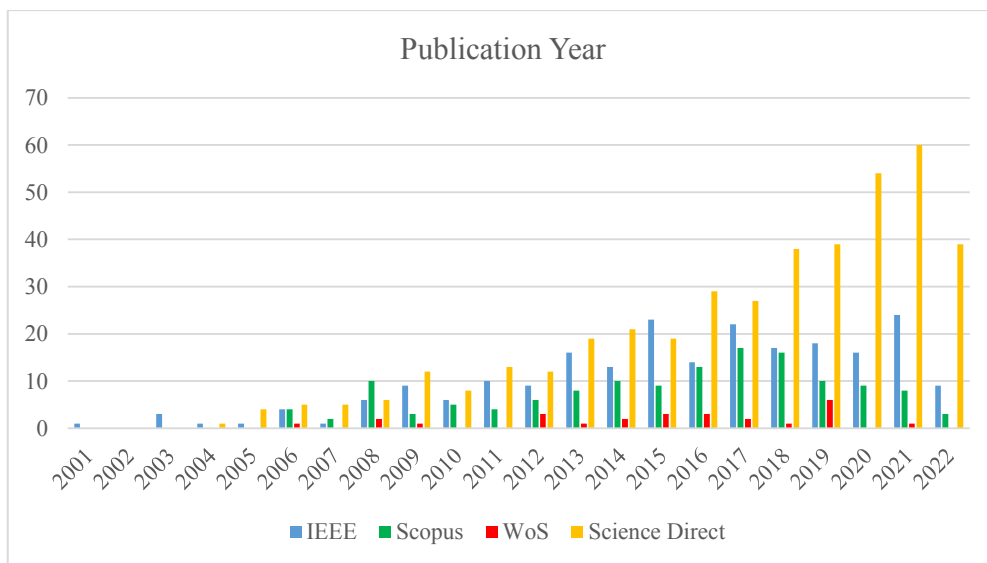


Fig2. The distribution of articles over time

### 4.2 Security Metrics Overview

According to the NIST, metrics are tools that collect, evaluate, and present relevant performance related to the data to help in decision-making, and enhance transparency and performance[25]. Security metrics are required for CSA management and comprehensive network security [15].

The security metrics can be classified into two categories. According to Nwokedi C. Idika [16], There are two basic categories of security metrics: primary and secondary, as shown in Figure 3. Architectural and performance-based metrics are the two primary categories of security metrics. The variety of characteristics that each class measures account for the differences between them. Architectural-based metrics measure internal characteristics. External qualities are measured through performance-based metrics. Complexity and time-based metrics are the secondary security metric classes. These metrics can be used to analyze both a network's internal and exterior properties.

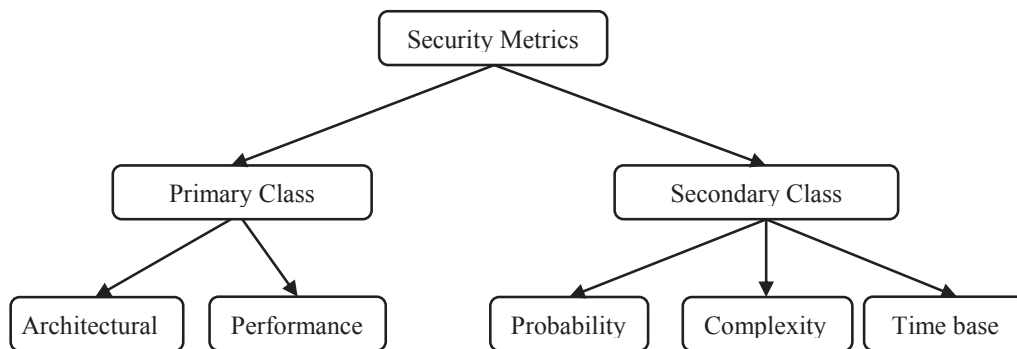


Fig 3. Security metrics classification [16]

AG-based security metrics and architecture-based metrics [16]. It results from calculating the internal network characteristics that impact IT or operational security. The parameters were obtained by constructing an AG and then applying analytics. The measurement used to create the AG-based metric is this analysis [16].

Based on [26], AG-based metrics could be classified into three main classes based on the reachability of the network: network-based, Host-based, and Composite metrics, as shown in Figure 4.

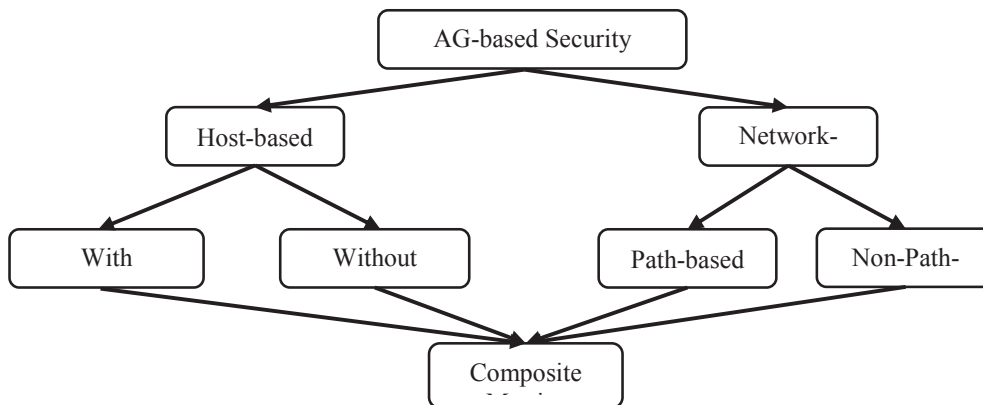


Fig 4. AG security metrics classification [26]

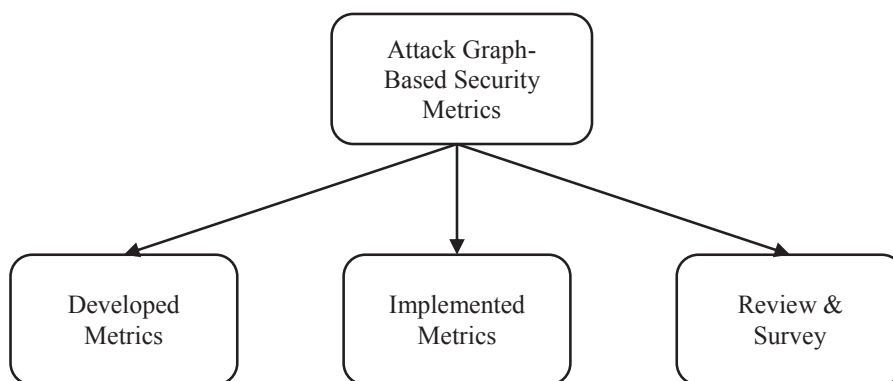
The security level of each host in the network is measured using host-based metrics. Security metrics without and with probabilities are the two categories of host-based metrics [27]. The classification was carried out since, in some cases, determining a probability value for an assault is not practicable. Several analyses and optimizations could be carried out without or with probability assignments [13].

The network-based metrics utilize the structure of a network to aggregate the network's security characteristics. Network-based security could be divided into two types: path and non-path-based metrics. Path-based metrics calculate the network's security level using reachability information. While in non-path-based metrics, a network's characteristics and structure are not taken into account [16].

The composite metrics combine individual metrics to enhance network security [26]. This metric depends on combining host- and network-based metrics to design a new set of metrics. The following section will review the recent articles based on these types.

## 5 Related Work

This section represents the related papers that used AG-based metrics. Based on the taxonomy, the research can be classified into three primary parts, as shown in Figure 5 developed metrics which focus on the articles that proposed metrics; implemented metrics which focus on the articles that used previous metrics; and the last part focuses on review and survey about AG-based security metrics.



**Fig5.** AG security metrics taxonomy

### 5.1 Developed Metric

This section is focused on the articles that proposed new AG security metrics, this section will answer the RQ2 which is What are some of the most well-known AG-based security metrics. According to Figure 4, the AG security metrics are categorized into three main classes as the following:

#### 1. Host-Based Metrics

This section is focused on host-based metrics. Researchers have recently proposed many metrics based on host resources.

[28] proposed several host metrics, which are Host Address Variability (HAV), Compromise Success Probability (CSP), Exploit Success Probability (ESP), Scan Success Probability (SSP), Attack Impact (AI), and Risk. The HAV metric monitors changing the IP address assigned to every host over time. CSP metric that represents the possibilities of an attacker successfully compromising the system. This metric depends on SSP and EPS metrics. SSP is a metric to discover the information in the host ( $h_i$ ) like vulnerabilities, IP, protocol, and services. The researchers estimated the SSP in terms of MTD interval time and scan duration for the attacker to learn about a host's security information. ESP metric is used to scan host vulnerabilities whether they are exploitable or not. AI metric A successful breach of a host or component would result in a loss of confidentiality, integrity, and availability measured by AI metrics. To determine whether the MTD shuffling procedure had a positive or negative influence or had no impact, the authors recorded changes in attack impact for every host in a network during each MTD shuffling interval. The last metric is Risk. Every

MTD interval time, the risk metric calculates the probability of compromise of a host (or component) in a network. The authors record the change in risk at each MTD interval so that it might be utilized to measure how effectively the MTD shuffling process worked.

The Probabilistic Security Metric (PSM) was proposed by [29]. Considering some prerequisites, this measure calculates the likelihood that the attacker can breach the security policy by fulfilling the objective condition. Probabilities,  $p(e)$  and  $p(c)$ , are assigned for each exploit  $e$  and condition  $c$ , indicating the unique score for each. Attack Success Probability (ASP) is a metric utilized to determine the likelihood that the attacker will succeed in achieving a target during an attack [30]. This metric can be used at both the host and network levels. At the host level, the metric measures the possibility that an attacker may compromise a node. Attack cost (AC) is utilized to determine the amount of cost an attacker must spend to achieve their attack goal [30]. This metric also can be used in both host and network-based. At the host level, the cost incurred by the attacker to a node serves as the metric [31]. Attack impact (AI) estimates the possible damage an attacker could inflict to accomplish their attack target [30]. Loss of availability, integrity, and confidentiality are potential losses. The loss the attacker causes to compromise a node is the metric at the node level.

Mean-time-to-compromise (MTTC) is applied to calculate the average time it takes for the attacker to reach their target [30]. The host level measures the mean time it takes the attacker to compromise a node. If the host has one vulnerability only, it means the AG or attack tree includes just a node with a compromise rate  $cr_{root}$ . The Factor of Security (FoS) and Probabilistic Factor of Security (PFoS) metrics were proposed by [32]. When PFoS metrics are assigned to vulnerabilities, they are understood as the probabilities that the relevant vulnerabilities' exploits can be used if all the prerequisites are already achieved. FoS metrics define the factor of security metrics based on the redundant AG model. While [33] proposed the Attack Cost Exploitation (ACE) metric. This metric could be calculated by accounting for all potential attack paths. The authors presumptively do not reduce attack efforts by leveraging the same variant (such as an application, operating system, and others). The exploitability of every attack path is then calculated as the sum of all necessary vulnerabilities. However, these metrics cannot be worked alone to evaluate the network security because they are not enough to secure the network or to show the weaknesses. These metrics must be combined with network metrics to create a better metric to evaluate the network security.

## 5.2 Network Based

This section is focused on network-based metrics. In recent years, researchers have proposed many metrics based on network resources and paths. As we mentioned above, ASP, AC, AI, MTTC, and ANC can be used in both network and host-based, so the network-based, the probability that the attacker might compromise the goal node through the attack paths is known as the ASP metric. The AC metric can measure the amount an attacker must compensate for breaching the target using the attack paths [31]. The AI metric can measure the maximum loss the attacker may do to breach the goal node out of all possible routes. MTTC Metric measures how quickly the attacker may compromise the goal node out of all possible attack paths. At the same time, ANC represents the average local node connection across all network node pairs [30].

The shortest Path (SP) Metric was proposed by Phillips and Swiler [6]. The attack path with the smallest steps between the attacker's initial point and the target node is known as the shortest attack path. The administrator who analyses the AG chooses the length function that is utilized to calculate the distance. These statistics, however, do not reflect the quantity of shortest pathways in the network, and there is no guarantee that the shortest path is the optimal path utilized by the attackers [6]. The weakest Adversary (WA) metric was proposed by [34]. The WA metric and the SP metric aim to explain network security in terms of various permutations of the network's weak points. The metric's underlying assumption is that no network is stronger than its weakest adversary. Initial characteristics of the AG are associated with an opponent's weakness. At the same time, Shortest Attack Path Variability (SAPV), Shortest Attack Path Variability with IP Shuffling (SAPVIS), Attack Path Variability (APV), and Attack Path Variability with IP Shuffling (APVIS) were proposed by [28]. The length of the shortest attack path from the attackers' starting point to the target node is represented by the SAPV security metric, which is frequently displayed graphically; the SAPVIS metric refers to the shortest attack path with IP-shuffling; the effect of deploying MTD is measured using the APV metric

by changes on attack paths. Additionally, the APVIS metric was developed to measure network shuffle dynamics' effect on attack pathways. However, these metrics depend on the paths and measuring the changes on the paths, not the network's resources; this might mislead the results of the optimal path the attackers might use.

The number of Paths metric (NAP) was suggested by Ortalo (1999) [35]. It describes the number of attack paths in a particular graph. It determines how weak the network is to be hacked or attacked. A higher NAP metric reflects a more exposed network. Besides the NAP metric, three metrics are proposed by [36], which are the percentage of severe systems (PSS), the number of severe systems (NSS), and the total number of network hosts (TNH) metrics. Besides the Variability of the Number of Attack Paths (VNAP) metric proposed by [28]. VNAP represents an attacker's various attack paths to access a goal host. This metric calculates the change in the number of attack paths by time. These metrics, however, do not consider the attack's effort, suggesting that two networks with the same number of paths have an equal level of security [35]. To solve the issue, [37] proposed the Weighted Number of Paths (WNAP) metric. WNAP considers each path's weight by calculating the path's vulnerabilities score. However, this metric only calculates the number of weighted attack paths without considering the weakest ones.

[33] proposed Attack Path Exposure (APE) metric. This metric aims to calculate the duration of every attack path exposed. If an attack path is exposed for a sufficient time, the attacker will likely prepare and start an attack effectively. Therefore, to improve security, the length of an attack vector should be kept to a minimum. Determining how long an attacker will take to plan and start an attack can be challenging. Therefore, the ideal scenario is to reduce the time an attack channel is exposed.

The Mean of Path Length (MPL) metric was proposed by [38] as an average length of the paths. It computes the mean of the path length to represent the average path length. It also calculates the amount of effort an attacker would impose to circumvent network security policy. It is crucial because the attacker might not have a similar understanding of the vulnerabilities as the administrator. As a result of the lack of knowledge, an attacker might choose a route that is not the quickest. The attacker may also decide to use the alternative route if they think the security engineer employs the analysis of the shortest path. However, because it depends on the NP metric, this metric cannot be used alone [39]. Besides, it does not consider the resources in the calculation.

The Median of Path Lengths (MePL) metric was proposed [39] It determines the path's length that appears in the center of all the path length amounts. This number is helpful because the MePL measure could not accurately reflect the typical path lengths in the AG due to the possibility of skewed path lengths. The Mode of Path Length (MoPL) metric proposed by [39], reveals the attack path's length that usually occurs. It demonstrates a different interpretation of "typical." The word "typical" here means "most often." The administrator might use the principle of insufficient reason to give each attack path an equal probability if they are unable to identify the chance of an attacker traveling any particular attack path.

Attack Resistance (AR) Metric was proposed by [40] to assess a network configuration's defense against a coordinated attack as the sum of its exploits. The AG assigns a unique resistance value  $r(e)$  to each exploit  $e$ . This number intuitively indicates how challenging it is to use an exploit. At the same time, the Network Compromise Percentage (NCP) metric was proposed by [41]. It shows the proportion of network resources that the attacker can take over. While the term "compromise" might be interpreted differently depending on the context, the authors defined it as the attacker gaining user- or administrator-level access to a host. The NCP value increases as more hacked machines are discovered. However, these metrics do not calculate the weakest path and do not recommend the optimal paths the attacker might use.

Return-On-Attack (ROA) metric was proposed by [42]. The metric calculates the benefits the attackers might gain when they already exploit vulnerabilities. It measures the advantages of the attacker from the viewpoint of the defender. The ROA measures security from the viewpoint of an attacker. Organizations use this security metric to assess how well a countermeasure works to deter a particular kind of intrusion attempt. At the same time, the explicit recognition of steps in the plans drawn from the plan library makes the Percent Complete (PC) statistic relevant to plan-based representation [43]. The PC metric calculates the assault goal's completion rate, given the data. The Minimum Remaining Path Length (MRPL) metric indicates a lower bound on how advanced an attack has progressed [43]. Checkpoint (CP) ranking of the AG steps depends on the number of plans that should use them; this metric can help the administrators to secure the network; this is meant to be used as a technique for a network administrator to stop an attack before it happens [43]. However,

these metrics focus only on the resources without considering the path and steps, which may give misleading results.

Spectral graph robustness metrics were investigated by [44], which are algebraic connectivity used to enhance network resilience against centrality attacks, Spectral gap, which demonstrates the graph's resistance to targeted attacks, to forecast robustness against node and link removals, natural connectivity has been compared to Algebraic Connectivity using a collection of structural and random graphs. To examine Internet topology, a Weighted Spectrum has been developed, and network criticality is a graph metric that assesses how resilient a network is to topological changes. However, these metrics are focused on the specific type of attack.

The diversity metric was proposed by [45] tested network. The metric provides each path with a numerical score and ranks them according to the degree of diversification. While [46] develops a software diversity metric to reduce security vulnerabilities against epidemic attacks (such as malware/virus propagation), it measures for assessing network topology. This will be done while maintaining a high enough level of network connectivity to ensure continuous service availability. However, these metrics are based on the path steps only without considering the resources or weaknesses in the network.

Attack Difficulty metric were proposed by [47] to evaluate the attack difficulty of a certain exploit about the location of that exploit in the attack path. While [48] modified on mean time-to-compromise metric and adopted considering the known and zero-day vulnerabilities on the cyber components, and the frequency of incursions through different channels is estimated. However, these metrics focus on the network's weaknesses without considering the path or path's steps.

In our previous work, we proposed the Number of Vulnerabilities metric (NV) [25]. The NV represents the vulnerability number in each network node that attackers could exploit to violate privilege boundaries. This metric tries to comprehend the number of network vulnerabilities, enable the administrator to correct them, and compare the two networks' security of various sizes and topologies.

### 5.3 Composite Metrics

This section is focused on Composite metrics. In recent years, researchers have proposed many metrics based on network resource paths and host resources. [50] proposed several composite metrics, which are Min-Cost Target Node Security Index (MTSI), Target Node Security Index (TNSI), Intermediate Node Min-Cost Betweenness Security Index (MBSI), Intermediate Node Betweenness Security Index (BSI), Min-Cost Source Node Security Index (MSSI), and Source Node Security Index

TNSI assists in determining crucial nodes with a big impact and low access for an attacker, but it does not give the whole picture. Similar to TNSI, the BSI metric measures the significance of intermediary nodes along all attack pathways. This metric takes into account all potential attack routes from all sources to all targets. The MTSI metric takes into account the impact of the breach as well as the least expensive attack vector to compromise a target node. It is similar to the Security Index metric proposed in [51]. The betweenness centrality-inspired MBSI metric emphasizes the significance of intermediary nodes as enablers of low-cost attack pathways between source and destination nodes. While the SSI metric measures the importance of source nodes by taking into account all minimum cost attack paths emanating from this node, MSSI measures the relevance of source nodes by taking into account the target nodes in the system for whom they operate as the source of a minimum cost attack; however, the author combines the attack impact on the network and the attack cost to of the host, which does not consider to calculate the weakest path in the network. Besides, it is very difficult to calculate the cost of each node individually, and it is time-consuming.

[52] proposes a method for calculating the target node's cumulative reachable probability using a simplified AG. The authors proposed an attack probability (AP) metric for internal attacks. Basically, the metric depends on the host's weight ( $H$ ), which can be calculated based on location in the network, and ( $V$ ), which indicates the probability of being used vulnerability. However, the metrics do not calculate the weight of the vulnerability.

In our previous work, we proposed two metrics which are Mean Vulnerabilities on Path (MVoP) and Weakest Path (WP) metrics, to overcome the limitation of previous metrics [25]. The MVoP metric represents the average vulnerabilities on the network's paths. This metric presents how much effort the attacker needed

to break the network policy. It provides a full view for the administrator to predict the attacker's next step. At the same time, the WP metric is like the SAP metric, but it focuses on another term, which is the path weaknesses. The path's weaknesses do not depend only on the NV but also on the vulnerability score itself. The vulnerability score uses the CVSS that NIST had invented. After calculating the path vulnerability score, the score results are compared between all paths in the network to represent the WP metric.

#### 5.4 Implemented Metrics

This section is focused on the articles that implemented and used AG security metrics. [30] presented a paradigm for graphically assessing and modeling security for the Internet of Things. The framework is divided into five stages: (1) data pre-processing, (2) model generation, (3) model visualization, (4) model analysis, and (5) model update. The authors used security decision-making to select the security metrics that will be used as input for security analysis. The security metrics that have been used are ASP, AC, AI, MTTC, and ANC in both host and network-based. [53] presented a framework for IoT security modeling and evaluation. An examination of two sample IoT networks is used to demonstrate the framework's advantages. The authors used ASP, AC, Risk, and MTTC metrics for security evaluation, which are used in both host and network-based.

[36] use a Temporal Hierarchical Attack Representation Model, which can record and analyze changes in the security of network systems, to conduct an extensive analysis to assess the efficacy of security metrics. Investigate the various consequences of security metrics in more detail when changes in dynamic networks are noticed. The authors tested a few metrics: AC, Risk, ASP, and AI in both hosts and network-based with SAP, NAP, MAPL, SDPL, MoPL, NMPL, PSS, NSS, and TNH metrics. [33] have classified attack and defense attempts to capture the efficacy of MTD approaches and have implemented MTD techniques into a T-HARM to model changes in the security of the dynamic networks. The authors developed some new metrics besides using other metrics like APV and VNAP to provide comprehensive evaluation methodologies to compare different MTD techniques.

[54] investigate the effect of change in the network on different security metrics. The authors used Risk, AC, ASP, SDPL, MAPL, NAP, MoPL, SAP, and NMPL metrics in five different scenarios which are with the following changes: (i) New vulnerabilities appear without being patched (ii) Vulnerabilities are patched as they appear (iii) Introducing new hosts (i.e., hosts having vulnerabilities) (iv) Removal of existing hosts and (v) Change the firewall rules. By taking into account both the skill level of an attacker and the causal connection that exists between all of the vulnerabilities in the network, [55] presents a unified framework for calculating a network's MTTC. The Continuous Time Markov (CTMC)-based model is a more comprehensive risk analysis method component. The MTTC metric depends on both an attacker's skill level and recognized security flaws in an organization. The NVD CVSS dataset was used to estimate the skill level coefficients for the three types of attackers, which were then utilized to calculate the Markov model's transition rates from one state to another.

To enhance the ability to assess the security strength of a particular network, [56] has provided a comparative analysis of the available security metrics. They used ten different metrics to test the network security level: SAP, NAP MPL, NMPL, SDPL, MoPL, MePL, PSM, AR, and WA. However, the case study used presented only one configuration for a given network. A novel method of evaluating network security under exploit attacks was proposed by [57]. The author used the CVSS metric's impact and exploitability to measure the network's security. To analyze the security risk for platform virtualized infrastructures that are used to create cloud services, [58] offers a unique model using Bayesian Attack Graphs (BAG). Using the model, they evaluate different security metrics: SAP, NMPL, and SDPL.

[59] presented a novel stochastic model to measure cyber security by fusing time and probability. The AGs and Markov Chain metrics inspired the suggested approach. The AGs and Markov Chain metrics inspired the suggested approach. A complementary set of quantitative indicators was offered to help the security engineer assess the current state and forecast the system's future security. [60] implement the address space layout randomization (ASLR) technique for the node, denoted as  $Defense_{ASLR}$ . The ASLR approach increases security by expanding the search space and is predicated on the low probability that an attacker will guess the locations of randomly allocated sections. The authors used ASP, AC, and AI metrics to test and evaluate the model. The model focuses on the defense against the attacker; however, the author sets the

metrics to value statically. [61] introduced the automated defense, defense enforcement, and security assessment for network infrastructures, which dynamically implement defenses and evaluate the network defense capabilities before and after. They performed experiments to represent the framework's abilities and uses on various networks. The authors measure the security level of the network before and after defense evaluation using different metrics: Risk, NP, and ROA.

[62] introduced a graphical security model (GSM) called the Time-independent Hierarchical Attack Representation Model (TI-HARM), which analyzes the security of several network states combined considering the duration time of all network states and the visibility of the network components (for example, edges). The authors implemented a few security metrics to analyze the dynamic network security. They selected Risk and NAP metrics to analyze the security of the network. While [63] developed a GSM called Temporal-HARM (T-HARM) to capture the network changes and investigate the network changes' effect on the current security metrics depending on the suggested model. The authors tested several metrics: ROA, SDPL, AC, SAP, NAP, MPL, NMPL, and MoPL.

## 5.5 Review and Survey

In this section, review and survey articles were included in this category to describe AG-based metrics.

[64] provide a review of the generation and analysis of the AG. The authors consider the security metrics as an AG analysis; also, [13] provided a review paper on AG generation phases. The authors considered the security metrics as one of the AGs used. However, the authors only reviewed a few metrics and did not provide a classification for the metrics.

A review of general security metrics is presented by [1]. The state-of-the-art of model-based quantitative NSMs has been thoroughly reviewed. First, a classification system and an overview of the security metrics field have been presented. The CVSS structure was then described, providing the input for several security metric models. It has also been shown how security metrics differ from other closely connected fields. Then, a comprehensive and in-depth analysis of the key metric recommendations has been provided, focusing on model-based quantitative NSMs. While [65] presents a systematic literature review of life cycle security metrics. The study classified the metrics into eight categories and 22 sub-categories. In this paper, the authors found 324 security metrics in general in 71 papers; however, the paper did not focus on AG-based security metrics.

To enhance the attacking effort, [66] suggested changing the IoT network's attack surface. They create two proactive protection mechanisms that change the topology of the IoT network using software-defined networking (SDN). Additionally, they use a GSM and numerous simulation metrics to examine how the security and performance change when the suggested remedies are implemented.

[67] present a comprehensive review of the quantitative network security metrics. The paper contains categories of software, network, economic, and effective security metrics. To begin with, the authors provide a hierarchical taxonomy for categorizing the metrics surveyed. Then a brief description of each metric follows. The authors also discuss model-based quantitative network security metrics, which should be noticed. Supervisory Control and Data Acquisition (SCADA) systems' security metrics and risk assessment techniques are covered in detail in [68]. The authors discuss certain quantitative model-based measures as well as some qualitative metrics. [69] discuss the security metrics that can be derived using HARMs to evaluate the security of enterprise networks, Cloud, SDN, IoT, and the effectiveness of defense mechanisms.

## 6 Analysis of Results

This section analyzes the results of the systematic review. In response to the RQs, we review the chosen articles in Section 5.1 before introducing a comparison of the articles in Section 5.2.

### 6.1 Overview of Selected Study

As we can see in Figure 6, 52% of the articles were found in ScienceDirect, 28% in IEEE, 17% in Scopus and 3% in WoS. There were 804 papers in all databases. A total of 365 papers were discovered to be replicated across the databases after applying the first filter, which involved removing duplicates. In the

second filter, unrelated papers were disregarded by scanning titles and abstracts. Of the 439 papers, 393 papers were not related, whereas 64 papers used AG-based security metrics.

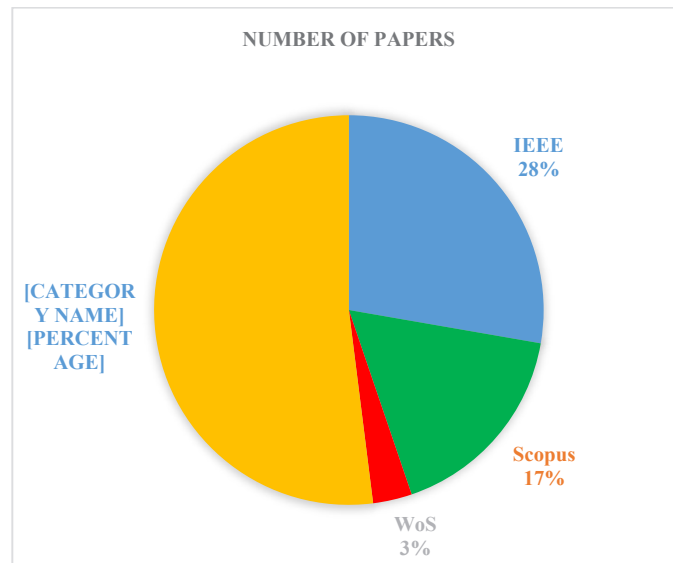


Fig 6. The percentage of articles based on the databases

## 6.2 Research Objective

The review process of the selected articles on AG-based security metrics is covered in Section 4 within three main categories proposed, implemented, and review articles. The analytical and statistical reports of the research questions are presented based on the plan in Section 2.1, as follows:

**RQ3:** Which type of classification in research can be applied for AG-based security metrics?

The AG-based security metrics fell into three categories which are Host, Network, and Composite-based security metrics as shown in Figure 7. The number of metrics found is (60) AG-based metrics, where (13) metrics in host-based, (38) metrics are network-based, and (9) are composite-based metrics.

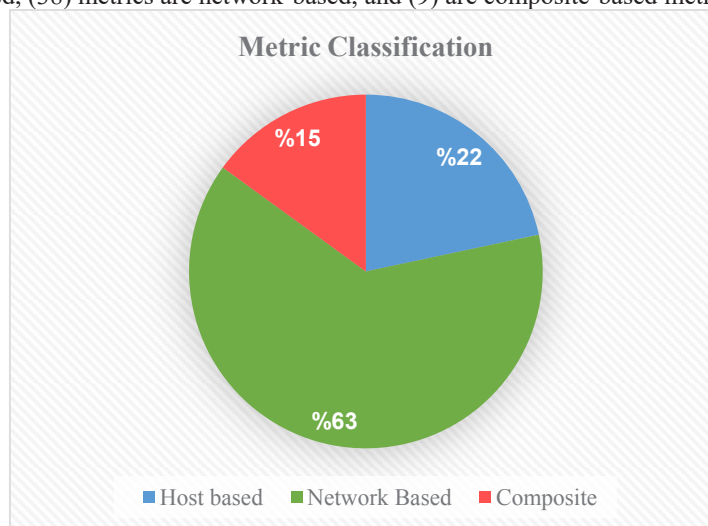
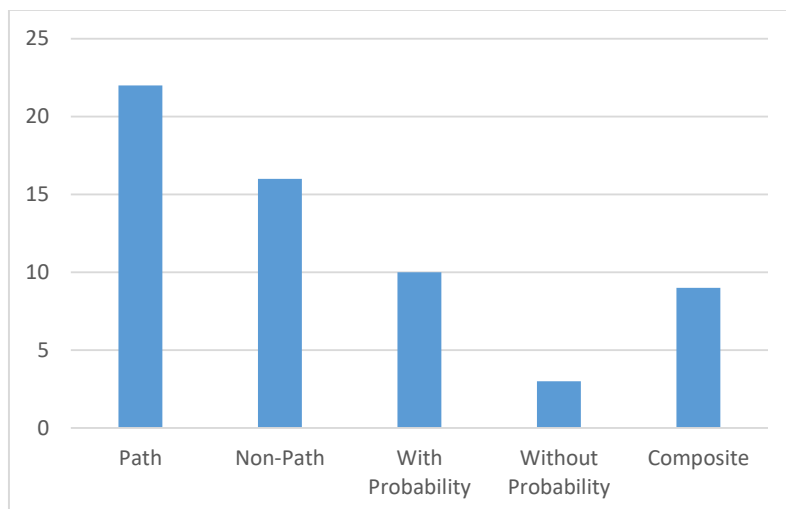


Fig 7. Metrics classifications

The host-based metrics are divided into two types which are without and with probability-based metrics, as mentioned in Figure 3. For those without probability-based metrics, we found (3) metrics while for those with probability-based metrics, we found (10) metrics. At the same time, the network-based metrics are divided into two types as well which are path-based metrics and non-path-based metrics. For path-based metrics, we found (22) metrics, while for non-path-based metrics, we found (16) metrics. For the last category, which is composite-based metrics, we found only (9) metrics, as shown in Figure 8.



**Fig 8.** Number of metrics based on each category

### 6.3 Limitation

Despite many advantages of AG security metrics, they also have several major limitations. All these limitations can be used as a new direction for a new study to enhance the AG-based metrics, which will lead to the improved measuring of the security level. This section provides answers to RQ 3.

**RQ5:** What are the open issues and future trends of AG-based security metrics?

These limitations will be demonstrated in the following:

- **Misleading Results**

Most of the path metrics provide misleading results [1]. For example, two networks have the same number of paths; according to NAP, both networks have the same level of security, which is inaccurate because they did not consider the efforts of the attacks. Besides, most metrics depend on the arithmetic mean; it might not record some changes in the network's security level [1]. Also, the metrics did not consider the relationships between the system components, vulnerabilities, and configurations [64].

- **The difficulty of applying the metrics**

Many approaches are proposed and use the metrics in the literature; however, it might be difficult to determine whether they are applicable in a particular situation and how to use them. Future research should presumably concentrate on creating a strong theoretical framework, empirical research, and systematically enhancing current methods [70]. Besides, the metrics did not provide solutions or recommendations for improvements [25]. Also, it is difficult to apply the metrics with different network characteristics; the network may have a variety of topologies or a combination of topologies, making it complex.

- **Scalability**

To apply the metrics, I require a long time to calculate the metrics. For example, to calculate the SAP in the network, the researchers need to identify all paths in the network before calculating the shortest path based on the steps needed to reach the target, which requires a long time to identify large networks. Another

example is calculating the change in the IP shift; the researchers need to collect the network information and then calculate the changes; this procedure requires a long time to finish.

## 7 Conclusion

Security metrics are one of the important research directions for measuring and improving network security levels. Research efforts in this field are continuously growing. However, important representations and limitations are still thought to be ambiguous. Developing knowledge and insights in this field is considered in this study. This study intends to add to such understanding and knowledge by reviewing and arranging applicable research exertions. This paper's previous articles are divided into three parts; proposed metrics, implemented metrics, and review. In this study, we discovered difficulties, and problems and provided various recommendations to identify existing and possible limitations in current AG security metrics. Furthermore, this work has examined the current metrics' weaknesses, which can be used for future research studies.

## References

1. A. Ramos, M. Lazar, R. Holanda Filho, J. J. P. C. P. C. Rodrigues, R. H. Filho, and J. J. P. C. P. C. Rodrigues, "Model-based quantitative network security metrics: A survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2704–2734, 2017, doi: 10.1109/COMST.2017.2745505.
2. Z. J. Al-araji, S. S. A. Syed, M. W. Al-salihi, H. A. Al-lamy, M. Ahmed, and W. Raad, "Network Traffic Classification for Attack Detection Using Big Data Tools : A Review," *Intelligent and Interactive Computing, Lecture Notes in Networks and Systems* 67, vol. 67, pp. 355–363, 2019, doi: DOI: 10.1007/978-981-13-6031-2\_37.
3. A. A. Mutlag, M. K. A. Ghani, and M. A. Mohammed, "A Healthcare Resource Management Optimization Framework for ECG Biomedical Sensors," in *Efficient Data Handling for Massive Internet of Medical Things*, Springer, Cham, 2021, pp. 229–244.
4. Zaid. J. Al-Araji, S. S. Syed Ahmad, and R. S. Abdullah, "Attack Prediction to Enhance Attack Path Discovery Using Improved Attack Graph," *Karbala International Journal of Modern Science*, vol. 8, no. 3, pp. 313–329, Aug. 2022, doi: 10.33640/2405-609X.3235.
5. M. A. Mohammed et al., "A comprehensive investigation of machine learning feature extraction and classification methods for automated diagnosis of covid-19 based on x-ray images," *Computers, Materials and Continua*, vol. 66, no. 3, 2020.
6. C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 Workshop on New Security Paradigms*, 1998, pp. 71–79. doi: 10.1145/310889.310919.
7. L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-attack graph generation tool," *Proceedings - DARPA Information Survivability Conference and Exposition II, DISCEX 2001*, vol. 2, pp. 307–321, 2001, doi: 10.1109/DISCEX.2001.932182.
8. P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2002, no. June, pp. 217–224. doi: 10.1145/586110.586140.
9. V. Mehta, C. Bartzis, H. Zhu, E. Clarke, and J. Wing, "Ranking attack graphs," in *International Workshop on Recent Advances in Intrusion Detection*, 2006, pp. 127–144.
10. Chen, Y., Lv, K., & Hu, C., "Optimal Attack Path Generation Based on Supervised Kohonen Neural Network," in *11th International Conference, NSS 2017 Helsinki, Finland, August 21–23, 2017 Proceedings*, 2017, vol. 32, no. 2, pp. 399–412. doi: 10.1016/j.jnca.2008.06.001.

11. H. Li, Y. Wang, and Y. Cao, "Searching Forward Complete Attack Graph Generation Algorithm Based on Hypergraph Partitioning," *Procedia Comput Sci*, vol. 107, no. Icict, pp. 27–38, 2017, doi: 10.1016/j.procs.2017.03.052.
12. B. Yuan, Z. Pan, F. Shi, and Z. Li, "An Attack Path Generation Methods Based on Graph Database," in *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2020, vol. 1, no. Itnec, pp. 1905–1910.
13. K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *Journal of Information Security and Applications*, vol. 29, no. August, pp. 27–56, 2016, doi: 10.1016/j.jisa.2016.02.001.
14. Z. J. Al-Araji, S. S. S. Ahmed, R. S. Abdullah, A. A. Mutlag, H. A. A. Raheem, and S. R. H. Basri, "Attack graph reachability: concept, analysis, challenges and issues," *Network Security*, vol. 2021, no. 6, pp. 13–19, 2021, doi: 10.1016/S1353-4858(21)00065-9.
15. Y. Cheng, J. Deng, J. Li, S. A. Deloach, and A. Singhal, *Metrics of Security*, vol. 62. Springer International Publishing Switzerland 2014, 2014. doi: 10.1007/978-3-319-11391-3.
16. N. C. Idika, "Characterizing and Aggregating Attack Graph-Based Security Metrics," Purdue University, 2010.
17. P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud Migration Research: A Systematic Review," *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 142–157, Jul. 2013, doi: 10.1109/TCC.2013.10.
18. P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, Apr. 2007, doi: 10.1016/j.jss.2006.07.009.
19. M. Haghi Kashani and E. Mahdipour, "Load Balancing Algorithms in Fog Computing: A Systematic Review," *IEEE Trans Serv Comput*, 2022, doi: 10.1109/TSC.2022.3174475.
20. A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, Jan. 2019, doi: 10.1016/j.future.2018.07.049.
21. S. Bansal, H. Aggarwal, and M. Aggarwal, "A systematic review of task scheduling approaches in fog computing," *Transactions on Emerging Telecommunications Technologies*, p. e4523, May 2022, doi: 10.1002/ett.4523.
22. Z. J. Al-Araji, S. S. S. Ahmad, N. Kausar, A. Farhani, E. Ozbilgekahveci, and T. Cagin, "Fuzzy Theory in Fog Computing: Review, Taxonomy, and Open Issues," *IEEE Access*, vol. 10, pp. 126931–126956, 2022, doi: 10.1109/ACCESS.2022.3225462.
23. M. A. Mohammed, M. K. Abd Ghani, R. I. Hamed, and D. A. Ibrahim, "Review on Nasopharyngeal Carcinoma: Concepts, methods of analysis, segmentation, classification, prediction and impact: A review of the research literature," *J Comput Sci*, vol. 21, pp. 283–298, 2017.
24. A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62–78, 2019, doi: 10.1016/j.future.2018.07.049.
25. Zaid. J. Al-Araji, S. S. S. Ahmad, and R. S. Abdullah, "Propose Vulnerability Metrics to Measure Network Secure using Attack Graph," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 51–58, 2021, doi: 10.14569/IJACSA.2021.0120508.
26. S. Y. Enoch, J. B. Hong, M. Ge, and D. S. Kim, "Composite metrics for network security analysis," *Software Networking*, vol. 2017, no. 1, pp. 137–160, 2017.
27. A. Roy, D. S. Kim, and K. S. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, 2012, pp. 1–12.

28. D. P. Sharma et al., "Dynamic Security Metrics for Software-Defined Network-based Moving Target Defense," *Journal of Network and Computer Applications*, vol. 170, no. November, p. 102805, 2020, doi: 10.1016/j.jnca.2020.102805.
29. L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5094, no. 2008, pp. 283–296, 2008, doi: 10.1007/978-3-540-70567-3\_22.
30. M. Ge, J. B. Hong, W. Guttman, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, no. January, pp. 12–27, 2017, doi: 10.1016/j.jnca.2017.01.033.
31. A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees," *Security and Communication Networks*, vol. 5, no. 8, pp. 929–943, 2012.
32. O. Duman, M. Zhang, L. Wang, M. Debbabi, R. Atallah, and B. Lebel, "Factor of Security (FoS): Quantifying the Security Effectiveness of Redundant Smart Grid Subsystems," *IEEE Trans Dependable Secure Comput*, vol. 19, no. 2, pp. 1018–1035, 2020, doi: 10.1109/tdsc.2020.3009931.
33. J. B. Hong, S. Y. Enoch, D. S. Kim, A. Nhlabatsi, N. Fetais, and K. M. Khan, "Dynamic security metrics for measuring the effectiveness of moving target defense techniques," *Comput Secur*, vol. 79, pp. 33–52, 2018, doi: 10.1016/j.cose.2018.08.003.
34. J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," in *Proceedings of the 2nd ACM workshop on Quality of protection*, 2006, pp. 31–38.
35. R. Ortalo, Y. Deswarte, and M. Kaâniche, "Experimenting with quantitative evaluation tools for monitoring operational security," *IEEE Transactions on Software Engineering*, vol. 25, no. 5, pp. 633–650, 1999, doi: 10.1109/32.815323.
36. S. Y. Enoch, M. Ge, J. B. Hong, H. Alzaid, and D. S. Kim, "A systematic evaluation of cybersecurity metrics for dynamic networks," *Computer Networks*, vol. 144, no. October, pp. 216–229, 2018, doi: 10.1016/j.comnet.2018.07.028.
37. M. Keramati and M. Keramati, "Novel security metrics for ranking vulnerabilities in computer networks," in *2014 7th International Symposium on Telecommunications, IST 2014, Dec. 2014*, pp. 883–888. doi: 10.1109/ISTEL.2014.7000828.
38. W. Li and R. B. Vaughn, "Cluster security research involving the modeling of network exploitations using exploitation graphs," in *Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGRID'06)*, 2006, vol. 2, no. July, p. 26. doi: 10.1109/ccgrid.2006.1630921.
39. N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Trans Dependable Secure Comput*, vol. 9, no. 1, pp. 75–85, 2010, doi: 10.1109/TDSC.2010.61.
40. L. Wang, A. Singhal, and S. Jajodia, "Measuring the overall security of network configurations using attack graphs," in *IFIP Annual Conference on Data and Applications Security and Privacy*, 2007, pp. 98–112. doi: 10.1007/978-3-540-73538-0\_9.
41. R. Lippmann et al., "Validating and Restoring Defense in Depth Using Attack Graphs," in *MILCOM 2006 - 2006 IEEE Military Communications conference*, 2006, pp. 1–10.
42. M. Cremonini and P. Martini, "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)," in *4th Workshop on the Economics of Information Security*, 2005, no. January, p. 4.
43. A. Amos-Binks, J. Clark, K. Weston, M. Winters, and K. Harfoush, "Efficient Attack Plan Recognition using Automated Planning," in *2017 IEEE Symposium on Computers and Communications (ISCC)*, 2017, pp. 1–6.

44. M. J. F. Alenazi and J. P. G. Sterbenz, "Evaluation and Improvement of Network Resilience against Attacks using Graph Spectral Metrics," in *Proceedings - 2015 Resilience Week, RSW 2015*, 2015, pp. 206–211. doi: 10.1109/RWEEK.2015.7287447.
45. G. S. Bopche and B. M. Mehtre, "Exploiting curse of diversity for improved network security," in *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*, 2015, pp. 1975–1981. doi: 10.1109/ICACCI.2015.7275907.
46. Q. Zhang, J. H. Cho, T. J. Moore, and I. R. Chen, "Vulnerability-Aware Resilient Networks: Software Diversity-based Network Adaptation," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3154–3169, 2020, doi: 10.1109/TNSM.2020.3047649.
47. P. Mukherjee and C. Mazumdar, "Attack difficulty metric for assessment of network security," in *ACM International Conference Proceeding Series*, 2018, pp. 1–10. doi: 10.1145/3230833.3232817.
48. Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Transactions on ...*, pp. 1–15, 2015.
49. G. S. Bopche and B. M. Mehtre, "Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks," *Comput Secur*, vol. 64, no. January, pp. 16–43, 2017, doi: 10.1016/j.cose.2016.09.010.
50. P. S. Patapanchala, C. Huo, R. B. Bobba, and E. Cotilla-Sanchez, "Exploring security metrics for electric grid infrastructures leveraging attack graphs," in *2016 IEEE Conference on Technologies for Sustainability, SusTech 2016*, 2017, pp. 89–95. doi: 10.1109/SusTech.2016.7897148.
51. S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "SOCCA: A security-oriented cyber-physical contingency analysis in power infrastructures," *IEEE Trans Smart Grid*, vol. 5, no. 1, pp. 3–13, 2013.
52. C. Shan, B. Jiang, J. Xue, F. Guan, and N. Xiao, "An Approach for Internal Network Security Metric Based on Attack Probability," *Security and Communication Networks*, vol. 2018, Apr. 2018, doi: 10.1155/2018/3652170.
53. M. Ge and D. S. Kim, "A framework for modeling and assessing security of the internet of things," in *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, 2015, pp. 776–781.
54. S. E. Yusuf, M. Ge, J. B. Hong, H. Alzaid, and D. S. Kim, "Evaluating the effectiveness of security metrics for dynamic networks," in *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, 2017, pp. 277–284. doi: 10.1109/Trustcom/BigDataSE/ICISS.2017.248.
55. S. M. Abraham, "Estimating Mean Time to Compromise Using Non-homogenous Continuous-Time Markov Models," *Proceedings - International Computer Software and Applications Conference*, vol. 2, pp. 467–472, 2016, doi: 10.1109/COMPSAC.2016.11.
56. A. Kundu, N. Ghosh, I. Chokshi, and S. K. Ghosh, "Analysis of attack graph-based metrics for quantification of network security," in *2012 Annual IEEE India Conference, INDICON 2012*, 2012, pp. 530–535. doi: 10.1109/INDCON.2012.6420675.
57. F. Dai, K. Zheng, S. Luo, and B. Wu, "Towards a multiobjective framework for evaluating network security under exploit attacks," in *IEEE International Conference on Communications*, Sep. 2015, vol. 2015-September, pp. 7186–7191. doi: 10.1109/ICC.2015.7249473.
58. B. Asvija, R. Eswari, and M. B. Bijoy, "Bayesian attack graphs for platform virtualized infrastructures in clouds," *Journal of Information Security and Applications*, vol. 51, p. 102455, 2020.
59. A. Ben Aissa, I. Abdalla, L. F. Hussein, and A. Elhadad, "A novel stochastic model for cybersecurity metric inspired by markov chain model and attack graphs," *International Journal of Scientific and Technology Research*, vol. 9, no. 3, pp. 6329–6335, 2020.

60. M. Ge, J. B. Hong, W. Guttman, and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, no. April 2016, pp. 12–27, 2017, doi: 10.1016/j.jnca.2017.01.033.
61. S. Y. Enoch, C. Y. Moon, D. Lee, M. K. Ahn, and D. S. Kim, "A practical framework for cyber defense generation, enforcement and evaluation," *Computer Networks*, vol. 208, no. November 2021, p. 108878, 2022, doi: 10.1016/j.comnet.2022.108878.
62. S. Y. Enoch, J. B. Hong, and D. S. Kim, "Security modelling and assessment of modern networks using time independent Graphical Security Models," *Journal of Network and Computer Applications*, vol. 148, no. May, p. 102448, 2019, doi: 10.1016/j.jnca.2019.102448.
63. S. E. Yusuf, M. Ge, J. B. Hong, H. K. Kim, P. Kim, and D. S. Kim, "Security Modelling and Analysis of Dynamic Enterprise Networks," in *2016 IEEE International Conference on Computer and Information Technology (CIT)*, 2016, pp. 249–256.
64. M. S. Barik, A. Sengupta, and C. Mazumdar, "Attack Graph Generation and Analysis Techniques," *Def Sci J*, vol. 66, no. 6, pp. 559–567, 2016, doi: 10.14429/dsj.66.10795.
65. P. Morrison, D. Moye, R. Pandita, and L. Williams, "Mapping the field of software life cycle security metrics," *Inf Softw Technol*, vol. 102, no. May, pp. 146–159, 2018, doi: 10.1016/j.infsof.2018.05.011.
66. M. Ge, J. B. Hong, S. E. Yusuf, and D. S. Kim, "Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities," *Future Generation Computer Systems*, vol. 78, pp. 568–582, 2018, doi: 10.1016/j.future.2017.07.008.
67. M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys (CSUR)*, vol. 49, no. 4, pp. 1–35, 2016.
68. Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," *Comput Secur*, vol. 56, pp. 1–27, 2016, doi: 10.1016/j.cose.2015.09.009.
69. S. Y. Enoch, M. Ge, J. B. Hong, and D. Seong Kim, "Model-based Cybersecurity Analysis: Past Work and Future Directions," in *Proceedings - Annual Reliability and Maintainability Symposium*, 2021, vol. 2021-May, doi: 10.1109/RAMS48097.2021.9605784.
70. A. Longueira-Romerc, R. Iglesias, D. Gonzalez, and I. Garitano, "How to Quantify the Security Level of Embedded Systems? A Taxonomy of Security Metrics," *IEEE International Conference on Industrial Informatics (INDIN)*, vol. 2020-July, pp. 153–158, 2020, doi: 10.1109/INDIN45582.2020.9442219.