Scientific Research Publishing

Journal of Information Security, 2021, 12, 250-269
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey

Onyekware U. Oluoha[1], Terungwa S. Yange[2], George E. Okereke[1], Francis S. Bakpo[1]

[1]Department of Computer Science, University of Nigeria, Nsukka, Nigeria
[2]Department of Computer Science, Joseph Sarwuan Tarka University, Makurdi, Nigeria
Email: d_blackdiamond@ymail.com

How to cite this paper: Oluoha, O.U., Yange, T.S., Okereke, G.E. and Bakpo, F.S. (2021) Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey. *Journal of Information Security*, **12**, 250-269.
https://doi.org/10.4236/jis.2021.124014

Received: August 16, 2021
Accepted: September 27, 2021
Published: September 30, 2021

Abstract

Cyber criminals have become a formidable treat in today's world. This present reality has placed cloud computing platforms under constant treats of cyber-attacks at all levels, with an ever-evolving treat landscape. It has been observed that the number of threats faced in cloud computing is rising exponentially mainly due to its widespread adoption, rapid expansion and a vast attack surface. One of the front-line tools employed in defense against cyber-attacks is the Intrusion Detection Systems (IDSs). In recent times, an increasing number of researchers and cyber security practitioners alike have advocated the use of deception-based techniques in IDS and other cyber security defenses as against the use of traditional methods. This paper presents an extensive overview of the deception technology environment, as well as a review of current trends and implementation models in deception-based Intrusion Detection Systems. Issues mitigating the implementation of deception based cyber security defenses are also investigated.

Keywords

Cloud Computing, Intrusion Detection System, Cyber Security, Cyber Deception, Deception Technology

1. Introduction

The cloud computing treat landscape is ever evolving and security concerns persist and still remain a top priority in cloud computing today. Such treats include insecure interfaces and APIs, system and application vulnerabilities, abuse of cloud services, network threats and Advanced Persistent Threats (APTs). The main aim of most information security defenses is to deny and isolate all unauthorized access, execution or manipulations in a given information system, the-

reby creating a boundary which acts to isolate the information system from the outside world. Such controls for denying access may include a firewall, access controls and end-point protection such as anti-virus. Other such controls may include the use of Network Address Translation (NAT), Virtual Private Networks (VPN), encryption and steganography, which aid in isolating and hiding parts of our information systems.

If the use of security controls to deny and isolate intruders fails, then the next steps would be to slow down the would-be attackers (such as to slow down the response of system calls when anomalies are detected), prevent (or in the least significantly reduce the likelihood) that an intruder will gain sensitive data by:

1) Creating electronic noise around the valuable information thereby reducing its utility.

2) Obfuscating the nature or value of the information systems and data within it.

One of the major tools in the arsenal of a network/system administrator in the fight against attackers is the intrusion detection/prevention system. IDS are very versatile and can be deployed at numerous levels of our information system (such as at the network level, application level or host level).

While IDS affords great protection to information systems, traditional IDS models come with several inherent flaws and can easily be defeated by the share sophistication (such as zero-day attacks and advanced persistent treats) and attack volume of modern treats. Several techniques have been put forward to help strengthen the capability and resilience of IDS against modern attacks. One of such techniques is the use of deception technologies in IDS design. A major difference between traditional cyber-security methods and deception-based techniques is that while traditional methods focus on attacker's actions and take appropriate actions, deception mechanisms go a step further, focusing on attacker's perceptions thereby anticipating such attacks even before they happen.

1.1. Intrusion Detection System (IDS)

In our context of study, intrusion could be described as any given set of actions which attempts to compromise the integrity, confidentiality or availability of any given system [1]. Intrusion detection Systems (IDS) are therefore systems involved in monitoring and analyzing events triggered by intrusion activities aimed at undermining the integrity, confidentiality or availability of the system. The ultimate aim of the IDS is to ascertain intruders and aid in triggering counter-measures against such identified attacks.

An IDS needs to be designed with multiple performance specifications [2] [3]. It should be able to collect data from the network related to suspected attack-like behaviors, store the data locally or on the network, analyze the data, and raise alerts and alarms [3]. The performance of an IDS in carrying out these tasks is characterized by its hardware capacity (CPU, Memory, Storage, and Network bandwidth), accuracy of detection of attacks, coverage of attacks (content, aspect, and

form of attacks), ability to resist techniques of evading detection, speed of detection and reporting, overheads, and capacity to process the workloads assigned in a network [2].

The detection approach may be signature-based (knowledge-based), anomaly-based (behavioral detection), or a hybrid of both the techniques [4]. **Figure 1** gives a detailed taxonomy of Intrusion Detection Systems (IDS).

The traditional IDS processes of signature or anomaly detection becomes even more cumbersome on cloud computing [5]. Anomaly-based IDS while showing great prospects in identifying new and evolving threats, are notorious in misidentifying legitimate traffic patterns as malicious, while possibly allowing malicious traffic as legitimate traffic. In a similar vein, while signature-based IDS are very effective in stopping all attacks documented in its signature database, they are grossly ineffective in identifying new evolving attacks and day-0 attacks. Also, building and maintaining a meaningful, dynamic and relevant signature database remains a major challenge. **Figure 2** gives a general architecture of Intrusion Detection Systems.

In recent times, it has become quite common to find IDS being complimented by incorporating appropriate Machine Learning (ML) algorithms in their design [6]. Machine Learning has the ability to detect patterns of similarities between two data sets with definitive distance measures [7]. In NIDS, the patterns of attacks in the data flows passing through a network port can be detected by employing an appropriate Machine Learning Algorithm (MLA) [7] [8] [9] [10]. The accuracy and effectiveness of MLA depends upon the quality, relevance, and accuracy of the training data set used to train the MLA. Based on the quality, relevance, and accuracy of learning, MLAs can recognize highly complex data patterns in massive voluminous data flows. In this quest, MLAs can be used to detect

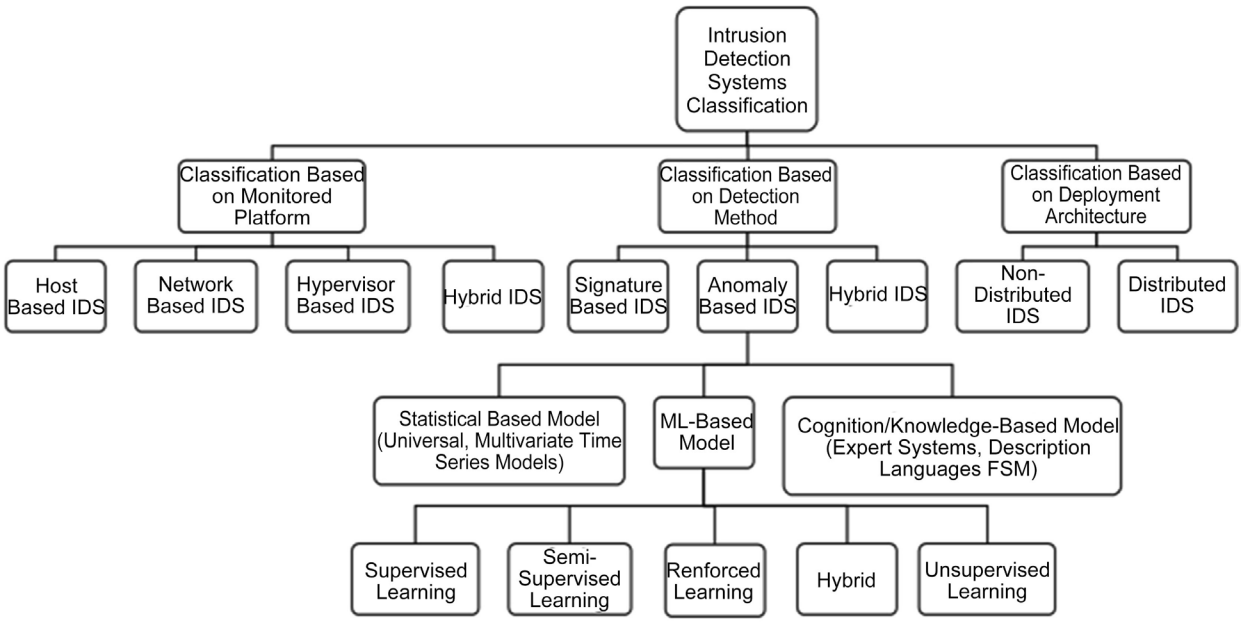

Figure 1. Taxonomy of intrusion detection systems (IDS).

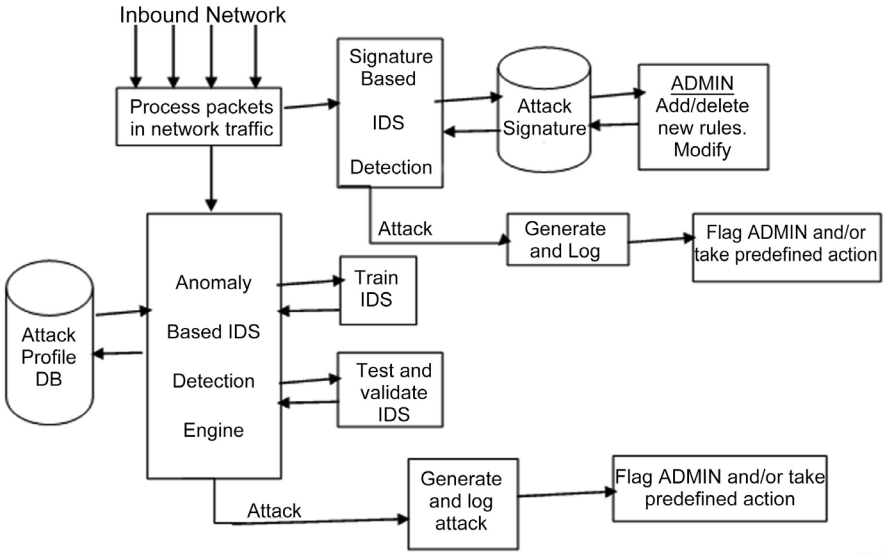

Figure 2. General architecture of traditional ID.

new forms of attacks if they have any similarities of patterns with the prior known attacks.

1.2. Deception Technology

Deception based techniques are a very powerful tool in the right hands [11]. Deception could be described as an untrue perception, which is induced intellectually by the actions or inactions of other entities. Deceptive mechanism has been used by mankind since the beginning of recorded history. In the field of computing, deception techniques have been advanced as a means of information security as far back as the 1980s [12]. A generally accepted definition of deception-based computer security is given by [13] as the deliberate actions taken to mislead attackers, which is aimed to ultimately cause them to take (or not take) specific actions that will benefit computer-security defenses. However, the use of deceptive techniques in computer-security was adopted and became more widespread in the 2000s [14] [15]. Several authors have advanced different taxonomy for deception technologies (see **Figure 3**). [16] argues that all deception involves one or both of two distinct phases including dissimulation and simulation. Dissimulation involves the act of hiding the real, including masking (hiding the real data/information so it cannot be discovered), repackaging (hiding data/information by making it look like something else), and dazzling (involves confusing the targeted objects with other objects, thereby making it much more difficult to distinguish truth from deceit). Simulation on the other hand involves showing the false, including: mimicking, inventing and decoying (turning attacker's attention away from the valuable data/information to less valuable information). He further posits that both phases are actually interdependent and that a comprehensive deception technique must incorporate both phases (implicitly or explicitly) in its design. They go on to assert that dissimulation and simulation can be applied at three levels including:

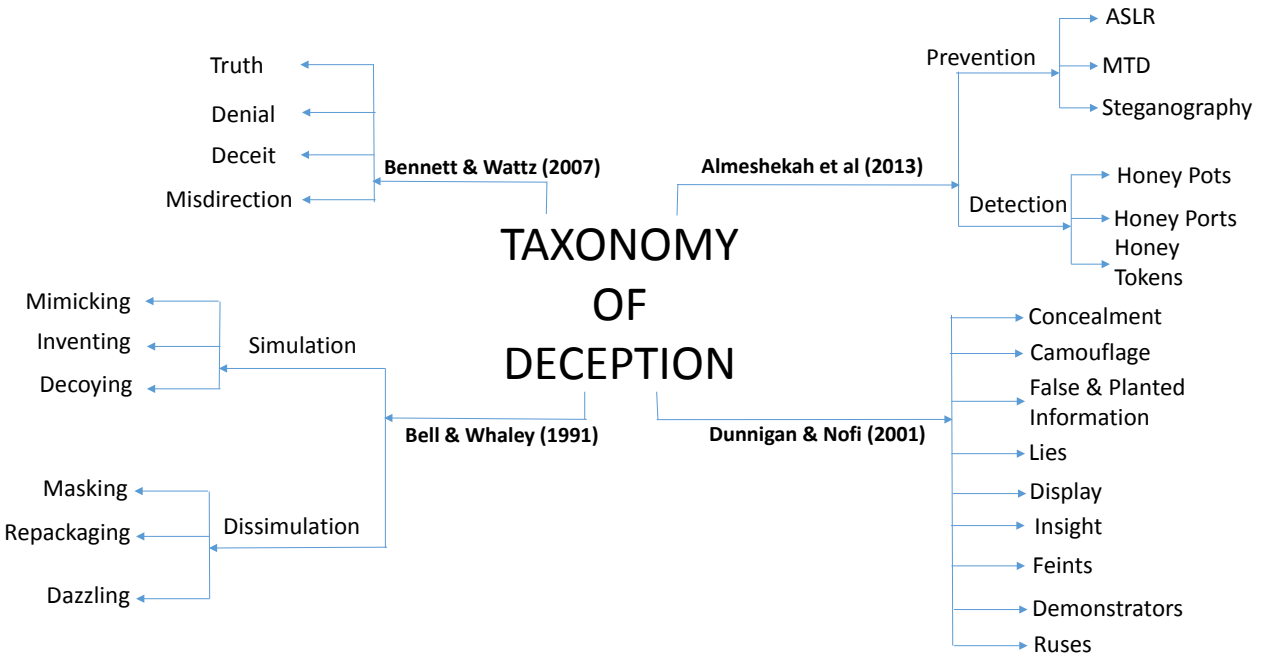

Figure 3. Taxonomy of deception techniques.

1) On the existence of the targeted information

2) On the nature of the targeted information

3) On the value of the targeted information

On the other hand, [17] proposed that deception techniques be divided into ten major groupings including camouflage, concealment, demonstrations, displays, feints, insights, lies, false/planted information and ruses. [18], however, divides deception techniques into four groups, including truth, deceit, misdirection and denial.

Finally, [19] categorizes deception techniques into two broad groups, including Prevention techniques (such as steganography) and detection techniques (such as honeypots).

In cybersecurity, the general aim of deception and decoy-based techniques include:

1) Aid in leading would-be attackers astray.

2) Aid in adding doubts and/or risk to data obtained by would be attackers.

3) Detecting data intrusions or leakages by adding decoys to the system.

Some of the major advantages of deception-based techniques include:

1) It is more of a proactive approach to cyber-security than the traditional reactive approach.

2) Aids in understudying and understanding the ever-changing dynamics of attackers, thereby increasing information gotten from such compromise attempts.

3) With deception-based techniques, attackers can be actively fed with false information, thereby causing the attackers to ultimately make wrong decisions.

4) Since deceptive techniques help in giving a deeper understanding of attack-

er's modus operandi, it ultimately gives you an edge over them thus greatly increases defense response time.

This paper explores the backgrounds of intrusion detection systems and deception-based technologies. It further considers the novel application of deception and decoy-based techniques in intrusion detection systems, the limitations of such IDS models and challenges to the use of deception technologies in cyber-security.

2. Related Works

Cyber-attack footprints are ever evolving [20]. In their research work, [21] reviewed approaches to detecting DDoS attack in cloud computing, considering both the application-bug and infrastructure levels. In the same vein, [22] carried out a survey on current Intrusion Detection System techniques in cloud-based platforms. He further presented a comprehensive comparative study on iCloud, Dropbox and Google Drive and how they go about securing their various cloud infrastructure. Similarly, [23] [24] [25] and [26] all carried out extensive surveys on IDS deployment in cloud-based environment. However, all these authors failed to address the use of deception-based techniques for intrusion detection in cloud-based platforms. In recent times, the use of deception techniques in cyber security has expanded greatly, with numerous authors advocating the use of deception-based technologies in protecting information systems and to react against would be attackers [15] [27]. [28] highlighted some key technology- and business-related challenges in designing and deploying honey pot systems on cloud computing. Likewise, [26] presents an extensive survey on intrusion detection, including methods used for obtain feature selection, computation of high dimensional data, and choice of learning algorithm. [29] stresses the importance of web-based applications and extensively outlines the possible use scenarios of deception techniques which can be incorporated into application-layer traffic of web applications for detecting various web-based application attacks. [30] went further in his research to give an extensive game-theoretical taxonomy for deception-based techniques. [31] presents a comprehensive survey of deception-based security mechanisms in Vehicular ad-hoc Network (VANETs) and VANET clouds, highlighting major trends, challenges and future research directions in the use of deception-based Intrusion Detection Systems in VANET, while reviewing current research works being carried out in the novel field of VANET clouds.

In their paper, [32] gives an all-encompassing overview of deception-based technology including in-depth discussions on taxonomies, psychological concepts of deception, implementation of deception based, legal and ethics issues. Similarly, [33] presented a survey of technological trends in cyber deception research. They identified several gaps with presented techniques, extensively surveyed current research works in novel fields of deception-based techniques in cyber security defense. In their paper, [34] gives a comprehensive classification

and survey current application of deception techniques in cyber security including limitations of current solutions, deployment of deception in complex systems, novel techniques and experiments for evaluating effectiveness of deception-based techniques and current research directions. [35] presented a comprehensive introduction to deception technology and the use of detection in cyber security. The authors also stressed that approach to overall cyber security architecture must be comprehensive, thus proposing a security model referred to as the conceptual Hybrid Threats Model.

3. Novel Deception Technologies and Limitations

The landscape of cloud computing is constantly evolving in an astronomical scale [36], and so are the treats associated with the cloud platform. It is therefore imperative that security measures in cloud computing should not lag behind in innovation and efficacy. Outlined below are current trends and innovations in deception-based Intrusion Detection Systems for cloud computing platforms:

In recent times, Honey pots have gained significant research attention in the field of cyber deception. [37] used the KDD 99 data set as the baseline and upgraded it with NSL KDD and Gure KDD data sets collected in a honey pot configured using Honey package in Linux. The authors used a Gini index for classification and reduction of attack patterns, and trained a multi-class SVM to obtain better results than the KDD 99 existing database used as a trainer. [38] used Raspberry P1 honey pot on Ubuntu 14.04 to collect data from the university's lab network through port 22 forwarding of SSH traffic from Internet. The SSH sensor used was Kippo SSH Python script that emulates the POSIX file system with some customisations needed to keep the attackers engaged for long periods. The attack data was collected on Apache Spark server running Hadoop File System (HDFS). A Naive Bayes classifier was used to categorise the traffic patterns as good and bad, and behaviour training module of the Raspberry P1 honey pot was used to generate and store alarms. In their experiment, the top 20 attacker Ids tried 1.21 million attack events on the honey pot using some of the top commands in Python attack scripting. These were all real attackers indicating the seriousness of network attacks ongoing on the Internet. In a similar experiment, [39] used a Puppet Enterprise Server with four agents used as honey pot sensors and HonSSH for redirecting traffic to the honey pots. [39] detected about half a million attacks during the data collection phase.

[7] presented an extensive classification framework based on bots collected from botnet-based honey pots. [7] also presented a framework for collaborative analysis of attack traces from multiple traces on an attack network. Here, multiple MLAs need to be used on the cloud computing to arrive at a final comprehensive classification of attack patterns. As presented by [40], mobile honey pots can be used to collect distributed attack patterns throughout the cloud network that can dynamically roam on the cloud and position themselves intelligently on the propagation paths of ongoing attacks. This research is similar to the dynamic

Markov chain formation using intelligent dynamic honey pot agents presented by [41]. The data collected by dynamically distributed mobile honey pot agents need to be collaborated at the analysis engine to create new forms of attack classifiers prevailing on the cloud computing networks. In another study involving mobile intelligent honey pots, [28] designed DNS honey tokens, web server honey tokens, and fake social network avatars to create network and application layer deception models such that attackers believe the victims as real social network users.

[42] presented a multi-paradigm modeling approach that stipulated the incorporation of deception tactics in system components during software development stages. This is in order to more quickly identify and mitigate potential conflicts and risks in initial phases of software development that could compromise cyber security, ultimately reducing costs of ill-planned decisions.

Dynamic networking techniques could be used in protecting hosts from internal and external attacks. [43] demonstrated this deception model, which employed dazzling techniques by mimicking transitory or false network configurations. Here, host address randomization was implemented by creating an interconnection of subnet switches and a central network. This model was successfully built by taking advantage of improvements in software-defined networking, which are not available in traditional physical infrastructure. The use of decoy routing is a unique tool in deception based cyber security and has earlier been proposed by authors such [44]. [45] proposed a unique approach in the use of decoy routing in deception based cyber defense. Simply put, decoy routing is essentially designed to circumvent IP address-based network filtering by leveraging a decoy destination. A decoy router that supports a secret channel is implemented on the path between the decoy destination and the user. Thus, the user is able to access filtered content through the hidden channel.

[46] presented a technique based on the innovative deception-based defense mechanism referred to as the moving target defense (MTD) technique. This novel defense mechanism is based on the frequent migration of VMs follows a signaling game technique. While the claims in this novel theoretical research looks plausible, the finding were not validated with data, nor was the proposed system analyzed with experimentations and real scenarios. Furthermore, the signal gamming mode was not evaluated with numeric analysis in other to truly picture its workings and effectiveness. It is also imperative that the bevaiour of the system for live and non-live migration defense of VMs be properly evaluated with the use of appropriate real-life case studies. Similarly, [30] presented a novel dynamic host mutation (DHM) architecture based on moving target defense (MTD) which actively deals with a variety of complex insider threats. The proposed dynamic host mutation (DHM) architecture is targeted to break the cyber kill chain, while expanding attack surface in order to increase the attacker's target analysis cost. Finally, it disrupts the attacker's fingerprinting, effectively disabling the server trace.

[47] presented a novel real-time threat monitoring system centred on the Cloudera platform. A Flume module was designed and implemented, which helped to reduce and distribute real time data streams from numerous sources into the data analysis mode. Apache Spark 2015 (an implementation of MapReduce) was used to further design the analysis mode. In order to detect abnormalities in network activities and alert the network administrators, the fuzzy *c*-means algorithm and *k*-means were used. The system could also incorporate and combine the use of Artificial Neural Networks (ANN) and Support Vector Machines (SVM). This threat monitoring system was further trained and evaluated using the relatively new CAIDA Dataset from Chicago Equinix data centre (CAIDA Data 2015), with promising results. However, this study only considered types of attacks namely traffic flooding attacks DDoS attacks. Also, a preconfigured dataset is used to build this system with its attendant disadvantages [47].

In [48], the researchers presented a deception-based approach to security in a campus network. Here, a honeypot server was combined with an Intrusion detection and prevention system, which carried out real-time analysis of network traffic. The honeypot was a hybrid deployment, with both high interaction and low interaction honeypots, which were virtually segregated from the intrusion detection and prevention system. The proposed system was setup and tested in a simulated campus network environment. This real-time simulation may prove beneficial on enterprise campus networks; however, it was not tested on an enterprise cloud infrastructure and its benefits in such a terrain are yet to be proven. [35] presented a novel hybrid threat model for deploying deception based cyber defenses.

The authors in [49] presented a cloud IDS based on the novel Spiking Neural Network (SNN) architecture (also termed the NeuCube algorithm). The NeuCube algorithm with SNN (core processing module) can easily manage huge data traffic thereby improving performance in classification and identification of various malicious attacks. It also used two machine learning algorithms including; classification and clustering algorithms. This security architecture was trained and tested using the NSL-KDD dataset. It was shown that the proposed system would exhibit high performance in high-speed real-world networks. An identified shortcoming of this research is the fact that it relied on existing datasets for training/testing the model, with research showing that such an approach has its inherent flows for Intrusion Detection Systems. [50] presented an IDS design which leveraged on Support Vector Machine (SVM) for classification, while using firefly algorithm for optimization. The firefly algorithm is a meta-heuristic method derived from the behavioural patterns of fireflies. It helps in identifying the best features in a given feature set. The Support Vector Machine (SVM) is trained using the features extracted with the optimized firefly algorithm. This security model was tested in CLOUDSIM virtualized environment. While this research work was quite novel, it was mainly focused on maximizing the effectiveness of IDS operations on scarce cloud resources, while minimizing its nega-

tive impact.

[51] proposed a novel IDS model which featured a mixture of Artificial Bee Colony (ABC) algorithm, Multilayer Perceptron (MLP) network and fuzzy clustering algorithm. In this model, while the fuzzy clustering algorithm is used to create numerous training subsets, the ABC algorithm is used to train the multilayer perceptron network by ensuring the optimization of biases values and linkage weight values. The Multilayer Perceptron (MLP) network on the other hand aids in identifying normal and abnormal network traffic patterns in network traffic flow. The unique combination of ABC, ANN and fuzzy clustering algorithm gives the proposed IDS very great capabilities. The proposed model was simulated using the CloudSim simulator, while the NSL-KDD dataset is used in training, testing and evaluation of the said model, with attacks grouped into four major categories. Also, [52] proposed a fuzzy logic approach. In their research, they presented a network intrusion detection module, which leveraged on the fuzzy c mean algorithm. The proposed model proved very capable, with observed high attack detection rates and a low false positive rate.

[53] proposed a hypervisor-based cloud IDS, where an IDS was deployed at hypervisor level and leverages on data and communications at the hypervisor level, which it uses for anomaly detection. This system employs a mixture of the gradient descent algorithm and the E-Div algorithm to identify anomalous cloud behaviour by observing and noting statistical changes and multivariate sequential change discovery. In other to address the paucity of publicly available datasets, the researchers in conjunction with a cloud service provider (CSP) generated a new cloud intrusion dataset which comprised of a large assortment of attack types. This new dataset was used in the training, testing and evaluation of the model. However, proposed IDS was deployed at hypervisor level and therefore cannot give universal cloud protection. Also, this novel approach needs further investigations in other to conclusively ascertain its advantages. Furthermore, [54] proposed an attack detection method, leveraging on Virtual Machine (VM) memory snapshot analysis. Here, an algorithm using snapshots is used to model an IDS which effectively detects malware and also has the capability to self-heal after an attack. The authors assert that the self-healing approach with machine learning algorithms is capable of effectively detecting novel threats.

[55] demonstrated a novel and complex deception-based security architecture which relied on a proxy system for misery digraphs in cloud-based virtual networks. Misery digraphs are systems which have been developed to evolve and change their fundamental structures over a period of time, thereby increasing the entropy in the cloud platform for would be attackers. These misery digraphs (which were developed based on Apache's reverse proxy module) acted by greatly obfuscating and complicating the attack paths of would-be malicious intruders. This it achieves by introducing endlessly repositioning decoys, while enlarging the pathway to the attacker's target. The misery digraphs as proposed by [55] were composed of two major parts: 1) Several identical and bloated paths to a given attack target, 2) a timetable of relocating/resetting hosts on arbitrarily

chosen paths to attack target. While this was a novel contribution towards improving security on cloud platforms, a major identified challenge is to ensure the misery digraphs do not unfairly compete (for computing resources) with legitimate network requests. Further, the presented security architecture failed to address the issue of insider-attacks. Also, it could not be conclusively demonstrated that misery digraphs could give protection against distributed attacks.

[56] proposed an attack detection model which introduced intrusion detection for layers of the IOS model (such as the network and application layers). The presented model is divided into two zones; Host IDS (HIDS)/VM-IDS and Network IDS (NIDS) are located in the first zone and are used as signature-based detectors, while Web-IDS (WIDS)/Application IDS presented as anomaly-based detectors are used in the second zone. However, this model still possesses the inherent weakness of signature-based IDS which are rather ineffective against new and custom-made attacks. Further, the performance of the anomaly detection section/zone was not remarkable. [57] in their part, presented a novel security framework for an innovative system defense based on dynamic location of honeypots. Here, a distributed honeypot network scheme is configured so as to periodically and randomly change its services. An active attacker can therefore not differentiate between honeypot services and real services, thereby making the malicious network flow more readily recognizable. In other to validate their proposed system and illustrate its effectiveness, the authors used game theoretic reasoning (Bayesian system game model) and conducted gambit simulations using MATLAB. The service allocation algorithm introduces uncertainty into the system by periodically changing services and keeping the occurrence of honeypots in high probability. Due to the uncertainty introduced to the security system, intending attackers are inevitably forced to abandon lunching any attacks. However, research as primarily geared towards protecting and ensuring the security of honeypots and ML was not explored to improve performance. Further, the cost on cloud infrastructure and resources needs to be closely studied. [58] and [59] also demonstrated the use of adaptive deployment strategies to effectively create deception based cyber defenses against would be attackers.

Several authors have also proposed the use of game theory in cyber deception. While [60] presented an extensive experimental analysis of a novel game-theoretic model, [61] went further to illustrate the attack graph game in an actual case study. Similarly, [62] published a game which allows to model probes within the game. An attacker as well as a defender is able to choose the effort, they want to invest in the obfuscation of the deception systems or the examination of systems of unknown nature. After the strategy is chosen, the attacker decides whether to attack, probe or ignore the system. Also, [63] presented a unique game-theory model for deception. In their model, a defender can deploy two deception defenses; 1) make a honeypot look like a legitimate server or 2) conceal a legitimate server as a honeypot [63] went further to model a similar approach, using game theory, that offers to disguise a real system as a honeypot (or vice versa) in an attempt to mitigate Denial of Service (DoS) attacks. Similarly, [64] proposed a

game theory deception-based security approach for smart grid applications. The security benefits of deception against distributed denial of service attacks were demonstrated in their proposed model. Finally, [65] in their research presented a game-theoretical framework that modeled the attacker's belief while deception is deployed in a three-layer network.

4. Challenges to Adoption of Deception Techniques

While the use of deception-based techniques in cyber defenses have been shown to have numerous advantages and have proven to have great prospects in real world applications, yet implementation of deception-based techniques is beset by several issues which need to be carefully considered while deploying them. Enumerated below are some of the major challenges faced while opting for the use of deception-based approaches in cyber security (see **Figure 4**).

4.1. Difficulties in Attribution and Counter Operations

It is a widely known fact that the better the enemies are known, the easier it becomes to contain the enemy. Attribution plays a major role in this regard. The main aims of attribution and counter-operations include; attributing the adversaries in other to gain a deeper insight into their operations and identify them, causing damage to attackers where possible, and ultimately increase overall risk associated with carrying out an attack on protected systems. Generally speaking, the attacker may respond in three different ways namely: 1) The attacker may believe the presented deception and fall for it 2) The attacker might suspect the presented deception and tread more cautiously. Here, we may decide to increase the level of deception presented or terminate presented deception in other to avoid exposure, or 3) The attacker may disbelieve the deception and take evasive steps or terminate attack, in which case, we fail to obtain needed information

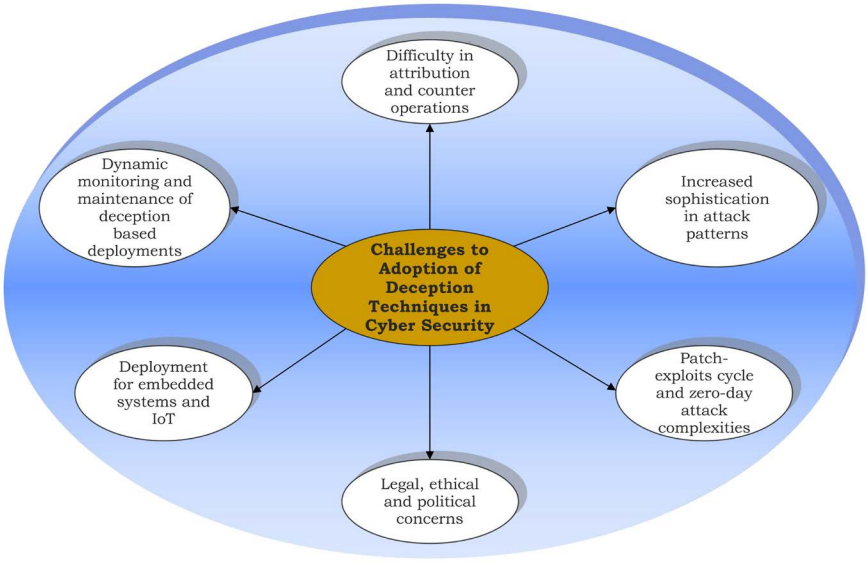

Figure 4. Challenges to deception based approaches in cyber security.

form the attacker. It has been argued that ultimately, the attacker always has the upper hand. This position could be traced to the difficulty in adversary attribution. [19] points out that the major challenge deterring the adaptation of mechanisms intended for attributing adversaries can be traced to mixing attribution mechanisms with counter-attacking ("hacking back") mechanisms. This could also lead to legal, ethical and political entanglements.

4.2. Increased Sophistication in Attack Patterns

The attack landscape is ever evolving and off-the-shelf tools for carrying out complex attacks are increasing steadily and is now readily available to the general public and upcoming cyber criminals. This has created a major dilemma for cybersecurity experts. Not only are they trying to ward off expert attackers and APTs, but upstarts and "rookie" cyber criminals have become a formidable treat in today's world. Cyber security experts must therefore evolve, innovate and device novel means of defense.

4.3. Patch-Exploits Cycles and Zero-Day Attack Complexities

Exploitation of vulnerabilities in software patches are one of the most common and deadly attacks. Here the attacker exploits defects in the target's software components and exploits these to the attacker's benefits. This kind of attack is extremely dicey, since the cybersecurity expert remains oblivious of the fact that a "back door" has been exploited by an assailant. Such vulnerabilities are used successfully to stage complex zero-day attacks. One of the major ways to check such attacks is to constantly probe patch releases to ascertain if they present any vulnerabilities to the system. Here, many organizations opt to invite "white hat" hackers to probe their systems and pay them if they discover any major vulnerabilities. This is commonly referred to as "bug hunting".

4.4. Legal, Ethical and Political Concerns

Several legal issues arise with the extensive use of deception-based techniques in cyber security. For instance, what kind of data can be legally collected and what are the set legal conditions for data collection and rendition [66]? Such issue of privacy creates webs of legal considerations, which vary from one geographic region to the other (such as the EU Directive on the security of network and information systems: 2016/1148/EU and EU Regulation No. 2016/679) and can greatly limit the effective deployment and use of deception-based techniques [67] [68] [69] and [70]. Furthermore, ethical and political considerations may arise when using deception-based techniques, especially in offensive mode. Is it justifiable to stage a counter-attack on an adversary? What level of counter-attack is morally justifiable in such cases and how do you handle the possible political fallout occasioned by such attacks? These are questions which must be carefully considered while deploying deception-based techniques in cyber security.

4.5. Deployment for Embedded Systems and IoT

Internet of Things (IoT) and embedded systems are a field of computing which have experienced massive proliferation and extensive use in recent years. It is expected that their widespread use in the future will continue to increase as we make the transition to smart homes and cities [71], driverless cars and the full implementation of 5G and 6G mobile standards. However, IoTs and embedded devices have inherent security concerns, which can easily be exploited by would be attackers to devastating degrees [72]. Unfortunately, due to resource constraints, implementation of deception-based techniques for defense is very difficult and, in many cases, impracticable. Research is currently ongoing to address these challenges and various innovations have been proposed in this regard such as in [31].

4.6. Dynamic Monitoring and Maintenance of Deception-Based Deployments

Unlike traditional cyber security techniques, deception based cyber security deployments should not be considered as a single one-time defensive measure. It is imperative that such defenses be dynamically monitored and the impact it has on would be adversaries' perceptions/actions be carefully measured. The honey pots with honey accounts, honey tokens, and honey files need to be deployed in relevant areas such that they appear valuable and realistic to attackers. For example, there should be no differences between the deception indicators and real platform specifications (example, services with open ports, versions in the operating system, and file sizes). If a Linux honey pot is discovered in a Windows network, the attacker will quickly recognize and ignore it. Further, honey pot networks should be deployed and managed by expert security administrators and not by regular IT administrators. Errors in handling the system can highlight it as a honey pot and ignored by attackers. Further, honey pots will need very specialised and deceptive designs to detect insider attackers.

5. Conclusion

Deception based techniques are very powerful tools which can be deployed in cyber based defenses to effectively protect Information Technology infrastructure against a vast variety of cyber threats and attacks. They not only delay and confuse attackers, but also create a false belief system in the attacker, which can be greatly exploited for extended periods of time. The use of deception techniques in cyber defenses has been proven to be very effective in various situations where traditional cyber security approaches have not performed as per expectations. The use of deception can help the cyber security expert to continuously learn about what would be attackers at various levels of the cyber kill-chain, thus enhancing defense capabilities, effectively detecting and attributing such cyber-attacks. Cyber security practitioners must however recognize and appreciate the myriads of issues and potential pitfalls associated with the use

of deception-based techniques in cyber security defenses. It should also be noted that the use of deception in cyber security defenses may also introduce real risks, which must be carefully considered, analyzed and accounted for before they are deployed. It is therefore imperative that planning and deception-based model designs must be meticulously approached, the deception-based system carefully monitored, and continuously evaluated post deployment.

Conflicts of Interest

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

References

[1] Yange, S.T., Oluoha, O. and Abdulmuminu, M.Y. (2020) A Data Analytics System for Network Intrusion Detection Using Decision Tree. *Journal of Computer Sciences and Applications*, **8**, 21-29.

[2] Milenkoski, A., Viera, M., Kounev, S., Avritzer, A. and Payne, B.D. (2015) Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. *ACM Computing Surveys*, **48**, Article No. 12. https://doi.org/10.1145/2808691

[3] Mitchell, R. and Chen, I. (2014) A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Computing Surveys*, **46**, Article No. 55. https://doi.org/10.1145/2542049

[4] Brindha, P. and Senthilkumar, A. (2016) High Speed and Low Power Architecture for Network Intrusion Detection System. *Circuits and Systems*, **7**, 1324-1333. https://doi.org/10.4236/cs.2016.78115

[5] Kumar, R.S.S., Wicker, A. and Swann, M. (2017) Practical Machine Learning for Cloud Intrusion Detection: Challenges and the Way Forward. *AISec*'17: *Proceedings of the* 10*th ACM Workshop on Artificial Intelligence and Security*, Dallas, TX, 3 November 2017, 81-90. https://doi.org/10.1145/3128572.3140445

[6] Emmah, V.T., Ejiofor C.I. and Onyejegbu, L.N. (2017) Review of Malware and Techniques for Combating Zero Day Attacks. *International Journal of Engineering Research & Technology* (*IJERT*), **6**, 267-275.

[7] Stevanovic, M. (2016) Machine Learning for Network-Based Malware Detection. PhD Thesis, Aalborg University, Aalborg, 1-90.

[8] Buczak, A.L. and Guven, E. (2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, **18**, 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[9] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C. and Atkinson, R. (2017) Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey. Department of Electronic & Electrical Engineering, University of Strathclyde, Glasgow, 1-43.

[10] Salem, M. (2014) Adaptive Real-Time Anomaly-Based Intrusion Detection Using Data Mining and Machine Learning Techniques. PhD Thesis, Faculty of Electrical Engineering/Computer Science, University of Kassel, Kassel, 1-195.

[11] Almeshekah, M.H. and Spafford, E.H. (2016) Cyber Security Deception. In: Jajodia, S., Subrahmanian, V., Swarup, V. and Wang, C., Eds., *Cyber Deception*, Springer, Cham, 23-50. https://doi.org/10.1007/978-3-319-32699-3_2

[12] Stoll, C. (2005) The Cuckoo's Egg: Tracing a Spy through the Maze of Computer Espionage. Gallery Books. (First published 1989).

[13] Yuill, J.J. (2006) Defensive Computer-Security Deception Operations: Processes, Principles and Techniques. http://www.lib.ncsu.edu/resolver/1840.16/5648

[14] Spitzner, L. (2003) Honeypots: Tracking Hackers, Volume 1. Addison-Wesley, Reading.

[15] Almeshekah, M.H. and Spafford, E.H. (2014) The Case of Using Negative (Deceiving) Information in Data Protection. *International Conference on Cyber Warfare and Security*, 237-246.

[16] Bell, J.B. and Whaley, B. (1991) Cheating and Deception. Transaction Publishers, New Brunswick.

[17] Dunnigan, J. F. and Nofi, A.A. (2001) Victory and Deceit: Deception and Trickery at War. Writers Club Press.

[18] Bennett, M. and Waltz, E. (2007) Counter-Deception Principles and Applications for National Security. Artech House, Norwood, MA.

[19] Almeshekah, M., Spafford, E.H. and Atallah, M.J. (2013) Improving Security Using Deception. CERIAS Tech Report 2013-13, Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN.

[20] Banerjee, U., Batra, G. and Arya, K.V. (2012) Feedback Reliability Ratio of an Intrusion Detection System. *Journal of Information Security*, **3**, 238-244. https://doi.org/10.4236/jis.2012.33030

[21] Osanaiye, O., Kim-Kwang, R.C. and Mqhele, D. (2016) Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework. *Journal of Network and Computer Applications*, **67**, 147-165. https://doi.org/10.1016/j.jnca.2016.01.001

[22] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. https://doi.org/10.4236/jis.2015.62015

[23] Gagandeep, M.R. (2019) A Review of Intrusion Detection System in Cloud Computing. *International Conference on Sustainable Computing in Science, Technology & Management* (*SUSCOM*-2019), Amity University Rajasthan, Jaipur, India, 26-28 February 2019, 770-776.

[24] Alam, S., Shuaib, M. and Samad, A. (2019) A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing. *International Conference on Innovative Computing and Communications*, *Lecture Notes in Networks and Systems*, **55**, 231-240. https://doi.org/10.1007/978-981-13-2324-9_23

[25] Chourasiya, P. (2018) A Survey on Intrusion Detection Technique in Cloud Computing System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* (2018 *IJSRCSEIT*), **3**, 526-531.

[26] Nagaraja, A. and Kumar, S.T. (2018) An Extensive Survey on Intrusion Detection—Past, Present, Future. *Proceedings of the* 4*th International Conference on Engineering & MIS*, Istanbul, 19-20 June 2018, Article No. 45. https://doi.org/10.1145/3234698.3234743

[27] Pawlick, J., Colbert, E. and Zhu, Q. (2017) A Game-Theoretic Taxonomy and Survey of Defensive Deception for Cybersecurity and Privacy. *ACM Computing Surveys*, **52**, Article No. 82. https://doi.org/10.1145/3337772

[28] Virvilis-Kollitiris, N. (2015) Detecting Advanced Persistent Threats through Deception Techniques. PhD Thesis, Information Security and Critical Infrastructure Pro-

tection (INFOSEC) Laboratory, Department of Informatics, Athens University of Economics & Business, Athens, 1-174.

[29] Efendi, A.I.M., Ibrahim, Z., Zawawi, M.N.A., Rahim, F.A., Pahri, N.A.M. and Ismail, A. (2019) A Survey of Deception Techniques for Securing Web Applications. 2019 *IEEE 5th Intl Conference on Big Data Security on Cloud* (*BigDataSecurity*), *IEEE Intl Conference on High Performance and Smart Computing*, (*HPSC*) *and IEEE Intl Conference on Intelligent Data and Security* (*IDS*), Washington DC, 27-29 May 2019, 328-331. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00066

[30] Park, K., Woo, S., Moon, D. and Choi, H. (2018) Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat. *Symmetry*, **10**, 14. https://doi.org/10.3390/sym10010014

[31] 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

[32] Fraunholz, D., Anton, D.S., Lipps, C., Reti, D., Krohmer, D., Pohl, F., Tammen, M. and Schotten, D.H. (2018) Demystifying Deception Technology: A Survey. arXiv:1804.06196

[33] Urias, E.V., Stout, W.M.S., Luc-Watson, J., Grim, J., Liebrock, L. and Merza, M. (2017) Technologies to Enable Cyber Deception. 2017 *International Carnahan Conference on Security Technology* (*ICCST*), Madrid, 23-26 October 2017, 1-6. https://doi.org/10.1109/CCST.2017.8167793

[34] Han, X., Kheir, N. and Balzarotti, D. (2018) Deception Techniques in Computer Security: A Research Perspective. *ACM Computing Surveys*, **51**, Article 80. https://doi.org/10.1145/3214305

[35] Steingartner, W., Galinec, D. and Kozina, A. (2021) Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry*, **13**, 597. https://doi.org/10.3390/sym13040597

[36] Varghese, B. and Buyya, R. (2018) Next Generation Cloud Computing: New Trends and Research Directions. *Future Generation Computer Systems*, **79**, 849-861. https://doi.org/10.1016/j.future.2017.09.020

[37] Shendre, K. (2015) Intrusion Detection Using Honeypot and Support Vector Machine Classifier. Master Thesis, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, India, 1-58.

[38] Sanders, M.E. (2015) Unknown Threat Detection with Honeypot Ensemble Analysis Using Big Datasecurity Architecture. Master Thesis, Illinois State University, Normal, IL, 1-77.

[39] Samu, F. (2016) Design and Implementation of a Real-Time Honeypot System for the Detection and Prevention of Systems Attacks. Master Thesis, St. Cloud State University, St Cloud, MN, 1-129.

[40] Vasilomanolakis, E. (2016) On Collaborative Intrusion Detection. PhD Thesis, Technische Universität Darmstadt, Darmstadt, 1-233.

[41] Bar, A., Shapira, B., Rokach, L. and Unger, M. (2016) Identifying Attack Propagation Patterns in Honeypots Using Markov Chains Modeling and Complex Networks Analysis. 2016 *IEEE International Conference on Software Science*, *Technology and Engineering*, Beer-Sheva, Israel, 23-24 June 2016, 28-36. https://doi.org/10.1109/SWSTE.2016.13

[42] De Faveri, C., Moreira, A. and Amaral, V. (2018) Multi-Paradigm Deception Modeling for Cyber Defense. *The Journal of Systems & Software*, **141**, 32-51.

https://doi.org/10.1016/j.jss.2018.03.031

[43] Jafarian, J.H., Al-Shaer, E. and Duan, Q. (2012) Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking. *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, Helsinki, 13 August 2012, 127-132. https://doi.org/10.1145/2342441.2342467

[44] Karlin, J., Ellard, D., Jackson, W.A., Jones, C.E., Lauer, G., Mankins, D. and Strayer W.T. (2011) Decoy Routing: Toward Unblockable Internet Communication. *USENIX Workshop on Free and Open Communications on the Internet* (*FOCI*), San Francisco, CA, 1-6.
https://www.usenix.org/legacy/events/foci11/tech/final_files/Karlin.pdf

[45] Nasr, M., Zolfaghari, H. and Houmansadr, A. (2017) The Waterfall of Liberty: Decoy Routing Circumvention That Resists Routing Attacks. *Proceedings of the* 2017 *ACM SIGSAC Conference on Computer and Communications Security*, Dallas, TX, 30 October 2017-3 November 2017, 2037-2052.
https://doi.org/10.1145/3133956.3134075

[46] Adili, T.M.T., Mohammadi, A., Manshaei, H.M. and Rahman, A.M. (2017) A Cost-Effective Security Management for Clouds: A Game-Theoretic Deception Mechanism. 2017 *IFIP/IEEE Symposium on Integrated Network and Service Management* (*IM*), Lisbon, 8-12 May 2017, 98-106.
https://doi.org/10.23919/INM.2017.7987269

[47] Chen, Z., Wei, S., Yu, W., Nguyen, J.H. and Hatcher, W.G. (2018) A Cloud/Edge Computing Streaming System for Network Traffic Monitoring and Threat Detection. *International Journal of Security and Networks*, **13**, 169-186.
https://doi.org/10.1504/IJSN.2018.10014317

[48] Baykara, M. and Das, R. (2018) A Novel Honeypot Based Security Approach for Real-Time Intrusion Detection and Prevention Systems. *Journal of Information Security and Applications*, **41**, 103-116. https://doi.org/10.1016/j.jisa.2018.06.004

[49] Almomani, A., Alauthman, M., Albalas, F., Dorgham, O. and Obeidat, A. (2018) An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms. *International Journal of Cloud Applications and Computing*, **8**, Article 5.
https://doi.org/10.4018/IJCAC.2018040105

[50] Shrivastav, S. and Dhawan, G. (2018) Detection of Intrusion Detection System in Cloud Using Artificial Intelligence. *International Journal of Advanced Computronics and Management Studies* (*IJACMS*), **3**, 43-50.

[51] Hajimirzaei, B. and Navimipour, N.J. (2018) Intrusion Detection for Cloud Computing Using Neural Networks and Artificial Bee Colony Optimization Algorithm. *ICT Express*, **5**, 56-59. https://doi.org/10.1016/j.icte.2018.01.014

[52] Mehibs, M.S. and Hashim, H.S. (2018) Proposed Network Intrusion Detection System Based on Fuzzy C Mean Algorithm in Cloud Computing Environment. *Journal of Babylon University/Pure and Applied Sciences*, **26**, 29-40.
https://doi.org/10.29196/jub.v26i1.351

[53] Aldribi, A., Traore, I., Moa, B. and Nwamuo, O. (2019) Hypervisor-Based Cloud Intrusion Detection through Online Multivariate Statistical Change Tracking. *Computers & Security*, **88**, Article ID: 101646. https://doi.org/10.1016/j.cose.2019.101646

[54] Joseph, L. and Mukesh, R. (2018) Detection of Malware Attacks on Virtual Machines for a Self Heal Approach in Cloud Computing Using VM Snapshots. *Journal of Communications Software and Systems*, **14**, 249-257.
https://doi.org/10.24138/jcomss.v14i3.537

[55] Qasem, M. and Almohri, M.J.H. (2019) An Efficient Deception Architecture for Cloud-Based Virtual Networks. *Kuwait Journal of Science*, **46**, 40-52.

[56] Jelidi, M., Ghourabi, A. and Gasmi, K. (2019) A Hybrid Intrusion Detection System for Cloud Computing Environments. 2019 *International Conference on Computer and Information Sciences* (*ICCIS*), Sakaka, 3-4 April 2019, 1-6. https://doi.org/10.1109/ICCISci.2019.8716422

[57] Li, Y., Shi, L. and Feng, H. (2019) A Game-Theoretic Analysis for Distributed Honeypots. *Future Internet*, **11**, 65. https://doi.org/10.3390/fi11030065

[58] Fraunholz, D., Zimmermann, M., Hafner, A. and Schotten, D.H. (2017) Data Mining in Long-Term Honeypot Data. 2017 *IEEE International Conference on Data Mining Workshops* (*ICDMW*), New Orleans, LA, 18-21 November 2017, 649-656. https://doi.org/10.1109/ICDMW.2017.92

[59] Fraunholz, D., Zimmermann, M., Hafner, A. and Schotten, D.H. (2017) An Adaptive Honeypot Configuration, Deployment and Maintenance Strategy. 2017 19*th International Conference on Advanced Communication Technology* (*ICACT*), Pyeong-Chang, 19-22 February 2017, 53-57. https://doi.org/10.23919/ICACT.2017.7890056

[60] Schlenker, A., Fang, F. and Tambe, M. (2018) Deceiving Cyber Adversaries: A Game Theoretic Approach. *Proceedings of the* 17*th International Conference on Autonomous Agents and Multiagent Systems* (*AAMAS* 2018), Stockholm, Sweden, 10-15 July 2018, 9 p.

[61] Durkota, K., Lisý, V., Bošanský, B. and Kiekintveld, C. (2015) Optimal Network Security Hardening Using Attack Graph Games. *Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence*, Buenos Aires, 25-31 July 2015, 526-532.

[62] Fraunholz, D. and Schotten, D.H. (2018) Strategic Defense and Attack in Deception Based Network Security. *International Conference on Information Networking*, Chiang Mai, 10-12 January 2018, 156-161. https://doi.org/10.1109/ICOIN.2018.8343103

[63] Çeker, H., Zhuang, J., Upadhyaya, S., La, Q. and Soong, B.-H. (2016) Deception-Based Game Theoretical Approach to Mitigate DoS Attacks. In: Zhu, Q., Alpcan, T., Panaousis, E., Tambe, M. and Casey, W., Eds., *Decision and Game Theory for Security*. *GameSec* 2016. *Lecture Notes in Computer Science*, Vol. 9996, Springer, Cham, 18-38. https://doi.org/10.1007/978-3-319-47413-7_2

[64] Wang, K., Du, M., Maharjan, S. and Sun, Y. (2017) Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. *IEEE Transactions on Smart Grid*, **8**, 2474-2482. https://doi.org/10.1109/TSG.2017.2670144

[65] Horák, K., Zhu, Q. and Bošanský, B. (2017) Manipulating Adversary's Belief: A Dynamic Game Approach to Deception by Design for Proactive Network Security. In: Rass, S., *et al.*, Eds., *Proceedings of the International Conference on Decision and Game Theory for Security*, Springer, Berlin, 273-294. https://doi.org/10.1007/978-3-319-68711-7_15

[66] Sokol, P., Míšek, J. and Husák, M. (2017) Honeypots and Honeynets: Issues of Privacy. *EURASIP Journal on Information Security*, **2017**, Article No. 4. https://doi.org/10.1186/s13635-017-0057-4

[67] Sokol, P. (2014) Legal Issues of Honeynet's Generations. *Proceedings of the* 2014 6*th International Conference on Electronics, Computers and Artificial Intelligence* (*ECAI*), Bucharest, 23-25 October 2014, 63-69. https://doi.org/10.1109/ECAI.2014.7090212

[68] Nance, K. and Ryan, D.J. (2011) Legal Aspects of Digital Forensics: A Research

Agenda. 2011 44*th Hawaii International Conference on System Sciences*, Kauai, HI, 4-7 January 2011, 1-6. https://doi.org/10.1109/HICSS.2011.282

[69] Burstein, A.J. (2008) Conducting Cybersecurity Research Legally and Ethically. *LEET'*08: *Proceedings of the* 1*st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, San Francisco, CA, 15 April 2008, Article No. 8.

[70] Sicker, D.C., Ohm, P. and Grunwald, D. (2007) Legal Issues Surrounding Monitoring during Network Research. *IMC'*07: *Proceedings of the* 7*th ACM SIGCOMM Conference on Internet Measurement*, San Francisco, CA, 24-26 October 2007, 141-148. https://doi.org/10.1145/1298306.1298307

[71] Oluoha, O. and Ebem, D. (2019) A Proposed Framework for Smart Home Systems Design & Adoption. *Computing, Information Systems & Development Informatics Journal*, **10**, 15-28. https://doi.org/10.22624/AIMS/CISDI/V10N1P3

[72] Okereke, G.E. and Oluoha, O. (2017) Security Strategies in Embedded Systems. *International Journal of Current Science and Technology*, **5**, 431-437.