Review of Cyber Attack Detection: Honeypot System

M.R. Amal
Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, India
E-mail: amalmr2010@gmail.com

P. Venkadesh
Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, India.
E-mail: pvenkadesh2002@gmail.com

Received October 07, 2021; Accepted December 24, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19370

Abstract

The number of connected devices in the network is growing day by day, and as the number of linked devices grows, so will the number of cyberattacks. All devices connected to the Internet has become a target of cyberattacks as network attack methods have developed. As a result, the security of network data cannot be neglected. To handle the future threats in this way, we employ honeypots, which are conceptual framework traps designed to block unauthorized access to both PCs and data. Every day, a large number of people access the internet throughout the world. Honeypot, also known as Intrusion Detection Technology, is a type of security technology that screens devices to prevent unwanted activities. This article will provide an overview of cyber security as well as a discussion of machine learning, cyber threats, and honeypot system-based techniques. This review paper was the result of a lot of research, and in assessing honeypots, the researchers found that they are becoming more of a concern for experts as an important security tool that can halt or limit system attacks and provide analysts with insights into the origins and behaviours of such attacks.

Keywords

Cyber Security, Cyber Attack, Clod Computing, Machine Learning, Honeypot.

Introduction

Cloud computing is a network access strategy that allows quick, on-demand network connectivity to a shared network. It can be readily provided and published with minimal administrative work or service provider participation. Many of us will witness a fundamental shift in information technology in our lifetimes. Current improvements in

computing may have drastically affected the way computing is done, as well as the notion of capital in computing. The services in a cloud computing network are often located on someone else's premise or network and are accessible remotely by Cloud users.

As per GDATA (Ameen et al.,2021) the number of new threats is rapidly increasing, with millions of threats being detected each year (Figure 1), requiring quite advanced and fully automated analysis techniques. In the case of large amounts of information or with new types of attacks, traditional tools are limited. An expert-based approach is time-consuming and difficult to identify attacks, which are its primary drawbacks (Alhayani et al., 2021). In addition to identifying and stopping attacks against our systems, understanding the motivations, aims, and strategies of adversaries are essential to finding new and predicting attacks that might be launched against our systems. Honeypot technology has been in use since 1992 (Lallie et al.,2021), as a powerful data system that monitors, detects, and analyzes malicious behaviours. Traditional approaches such as intrusion detection systems (IDS) and system logs, which cannot handle the large volume of data, false alarms, and inability to identify new threats (four), are supplemented with this technology. It was designed not to be interrogated, attacked or compromised (Zhang et al.,2021; Shaw et al.,2021). By using this, the administrator network can determine the identity, intentions, and strategies used by attackers to penetrate the system, as well as the type of attack they used.

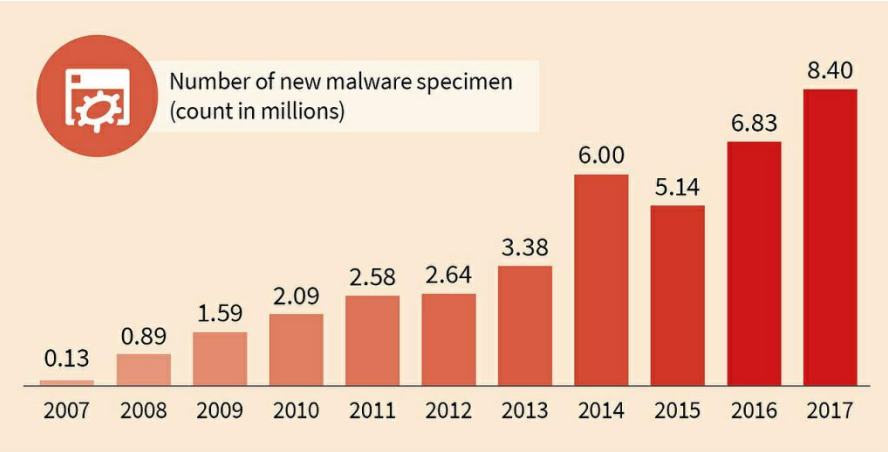

Figure 1 New attacks evolution

The goal of this study is to provide an evaluation of the instances and progress of honeypots for different research agencies at the time. Researchers in the future who wish to study networks security will find the study valuable as it discusses the application, benefits, and implementation of computer security, intrusion detection systems, and honeypots. Overall this article is arranged as follows: Section 2 discusses some

introduction to cyber security and cloud computing, Sections 3 and 4 are dedicated to the history of cyber security threats and solutions, and Section 3 discusses related work. Section 4 concludes the work.

Background of Study

1. Cyber Security

Privacy and data security might be the key security behaviours that every firm is concerned with daily. In today's largely digital or cyber-specific world, where all data is stored, we tend to encircle measures. Although social networking sites offer a safe place for users to interact with family and friends, cyber thieves also utilize social media sites to collect sensitive data's (Dixit et al., 2021; Ghiasi et al., 2021; Kilincer et al., 2021).

2. Types of Cyber Attack

- **Denial-of-service (DoS) and Distributed Denial of- Service (DDoS) Attacks**

A Denial-of-Service exploit exhausts the system's capacity, preventing it from responding to service requests. A DDoS attack is launched by a host system that has been infected with malicious programs and is managed by an attacker. In this type of cyber-attack, the computer or networks resources are rendered inaccessible to the desired user by interfering with the services of the hosts that are connected to the network. Various sorts of DoS and DDoS attacks include TCP SYN flood attacks, teardrop attacks, smurf attacks, ping-of-death attacks, and botnets.

- **Man-in-the-Middle (MitM) Attack**

A Man-In-The-Middle attack occurs whenever a third person intervenes inside the communications between a client and the server. The third-party pretends to be the client as well as the server to obtain access to the data shared among them. This type of attack causes a threat actor to grab, send, and receive information meant for someone else. A MITM technique takes advantage of real-time communications, transactions, or the exchange of information.

- **Phishing Attacks**

False messages that appear to be from trusted sources are called Phishing. Its primary goal is to obtain sensitive information such as personal information and credentials. It is a type

of social engineering or technological deception that uses emails with embedded URLs to send malicious files to our system.

- **Drive-by- Download Attack**

  Drive-by-Download attacks are indeed a prevalent type of cyber-attack used by hackers to propagate viruses and acquire illicit access. This type of attack happens whenever a computer is compromised with malicious programs merely by browsing a website.

- **Password Attack**

  Passwords are the more commonly used means of user authentication, and acquiring such credentials is an effective attacking strategy. A credential hack is a process where a user's credentials are stolen or decoded illegally. Checking all around the user's desk, assuming, obtaining a login database, monitoring the network connection to retrieve the plaintext password, and so on may all be used to discover the user's password.

- **SQL Injection Attack**

  An attacker who wishes to do SQL injection may alter a regular SQL query to exploit unsubstantiated weaknesses in a database. Misfiltered characters can also be used by attackers to change SQL statements. There are various viable methods for preventing and defending against SQLI attacks if they occur.

- **Cross-Site Scripting (XSS) Attack**

  Cross-Site Scripting is a form of injecting technique in which a malicious script is inserted into a trusted website or a sensitive online application. In other words, XSS happens when an attacker injects malicious script or JavaScript into the database of a website. The victim's browser runs the infected script inside the response, transmitting the victim's cookies to the attacker's server.

- **Eavesdropping Attack**

  The same thing is known as snooping attacks or spying attacks. Eavesdropping attacks involve hackers compromising data delivered through digital devices. Attackers exchange communications over an unsecured network and examine data sent and received. An attacker may use a sniffer to eavesdrop on a computer or server to grab data while it is being transmitted during this type of attack, which is hard to identify since it exhibits no anomalous behaviour during network transmission.

- **Birthday Attack**

Birthday attacks are a type of cryptographic attack that falls into the brute force attack category. It is based on the birthday problem premise from probability theory. This technique could be used to exploit the sharing of data among more than 2 parties. Birthday attacks are performed out by employing hash methods to validate the message's authenticity, program, or cryptographic signature.

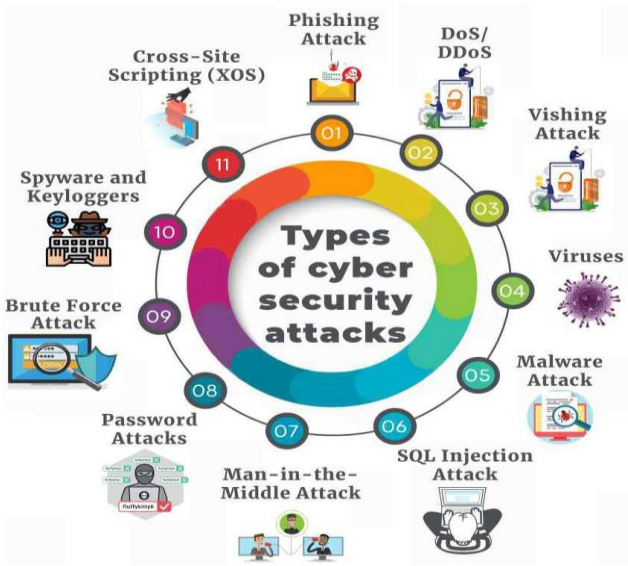

Figure 2 Different attack types

- **Malware Attack**

Malware attacks are a type of cyber threat wherein a harmful program is placed on the victim's machine even without the user knowing or agreement. Viruses, malware, and ransomware are just some of the terms we use today when referring to pernicious software. Malicious software propagates itself and executes by itself. Through malware, access to a private network can be gained, disrupted, and personal data can be taken as shown in figure 2 or other user information can be accessed, making it possible to illegally earn money. Malware now mostly targets commercial or financial data rather than personal sensitive information. The most frequent types of malware are:

- Virus: a harmful program that attaches itself to any system program and replicates and modifies instructions when run. It may spread by accessing files or by launching any software.
- Worms: are viruses that propagate through devices or the internet via email attachments. This might lead to denial-of-service attacks.

- A malware called Trojan Horses is malicious software that masquerades as helpful software and does not spread like viruses.
- Ransomware: Malicious software that encrypts user data and threatens the user until a ransom is paid. Even though the code is basic, it is quite difficult to avoid this attack.
- Spyware: Malware that examines user activities without the user's permission and reports this to the hacker.

3. Trends Changing Cyber Security

Below are a few factors having a significant impact on cyber security:

- Mobile Networks: Now we can communicate with any person in the world anywhere. However, security is a troubling issue for these mobile networks. Firewalls and other security protections are becoming increasingly permeable as people use smartphones, tablets, PCs, and so on.
- Web servers: Web servers are vulnerable to web application hacks that can steal data or distribute harmful code.
- Cloud computing and its services: Businesses of all sizes are gradually adopting cloud-based services these days. In other words, the entire planet is gradually moving toward the clouds.
- APTs and targeted attacks: There is a completely new type of cybercrime ware known as APT (Advanced Persistent Threat).
- Code encryption: Communication (or information) is encrypted so that it cannot be interpreted by eavesdroppers or attackers.
- IPv6: 'IPv6' stands for 'Internet Protocol 6'. It will replace IPv4, which has served as the foundation of our networks and the Internet in general.

4. Cyber Security Techniques

Cyber-attacks on the internet can expand by using new approaches. To exploit new technological flaws, cybercriminals would constantly modify existing malware fingerprints. In other cases, they look for unique properties of new technologies to uncover flaws in virus insertion. Cyber thieves are trying to take benefit of developing Internet technology and millions or billions of active users to gain easy and efficient access to a large number of individuals.

- Access control and password security
- Data authentication

- Malware scanners
- Anti-virus software
- Firewalls

5. Honeypot

The main purpose of an information security policy is to ensure that services are safe, secure, authentic, available, and accessible. Attacks rely on programs that search a network looking for vulnerabilities (Kim et al., 2021), so the honeypot's distinctiveness lies in the fact that it openly displays itself as a vulnerable system likely to attract the attention of hackers. The basic objective of honeypots is to fool the attacker into thinking he can gain control of a genuine operational computer, allowing the admin to study the methods of exposing the attackers, protect against fresh threats, and provide them additional time to react. Honeypots are extremely adaptable and come in a variety of shapes and sizes. Most works define honeypots in 2 directions: the first classifies them based on the interactions they enable, and the second classifies them based on their utility.

A honeypot is a security resource whose value is determined by its ability to be explored, exploited, or hacked. This implies that whatever we identify as a honeypot, we anticipate and intend for the system to be examined, attacked, and potentially exploited. Honeypot is primarily a detection and reaction tool, with minimal utility in preventive. Honeypots do not block specific intrusions or the transmission of viruses or worms. Instead, they gather data and detect attack trends. After that, defenders can respond to this evidence by constructing stronger defences and countermeasures against future security threats. A honeypot is a tool used to gather evidence or information and to learn as much as possible about attack patterns, hacker purposes and motives, and widely utilized programs launched by them. We can also learn more about the hacker's abilities, particularly their technical understanding, based on the information we have acquired.

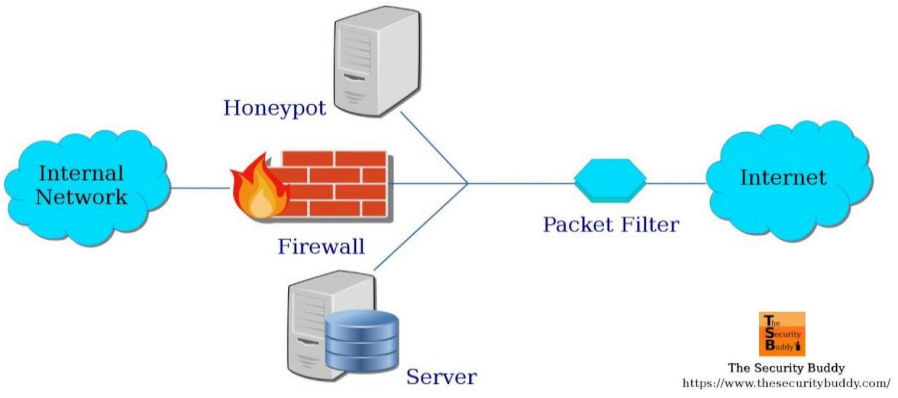

Figure 3 Honeypot for improving security

Honeypots could also be used to capture attackers while they are in the network and to steer attackers from the real production system to the honeypot system. The ideal people to handle the honeypot are those who have a substantial understanding of three crucial areas: security, systems and networks. In the proper hands, a honeypot may be a powerful tool for information collection. In the wrong, unskilled hands, a honeypot can become infiltrating machinery and an instrument for the black-hat group. Honeypots rarely help to improve a group's network security. Rather, they invite intruders into the network. Honeypots are security tools as shown in figure 3 with no actual or production value. It should not be conveyed by anybody. If there is activity or traffic to the honeypot, this might be interpreted as an intrusion, illegal access, or a probing effort. Instead, if the honeypot initiates any outgoing connections, the honeypot has likely been hijacked and taken over. Honeypots are available in a variety of styles and sizes. Honeypots are classified into two types: low-interaction honeypots and high-interaction honeypots (Chesney et al., 2020; Mohammadpourfard et al., 2020).

Literature Review

Honeypots have become increasingly important in information security as Internet technology has advanced. Nevertheless, hackers could simply determine whether or not the server had deployed honeypot capabilities. Many academics (Poorvika et al., 2020; Feifei et al., 2019; Yicheng et al., 2019) have recently begun focusing on how to automatically detect a honeypot server to address such a threat. Researchers must improve their honeypot services by making them realistic, as well as improving their internal mechanism and external interface. Comparative study of different methods are shown in table 1.

Table 1 Comparison study of different methods

Authors	Title	Method	Outcome
(Yicheng et. Al, 2019)	In an IoT-based cloud computing environment, secure authentication and key agreement scheme is presented	AKAP	Low accuracy
(Poorvika et.al, 2020)	Detecting and preventing cloud intruders by using a honeypot network	Honeypot Protocol	Reduce attack rate
(Feifei Wang et. Al, 2019)	Authentication Protocol Based on ECC with High Security and Efficient Performance	ECC based AAP	Low throughput
(Yang et.al, 2019)	Security and privacy in VANETs with a certificate-less conditional authentication scheme	CPPAP (Conditional Privacy-Preserving Authentication Protocol)	Reduce communication cost

1. Cyber Security Trends and Recent Developments

New algorithms, methods, and systems have made many recent breakthroughs in cyber security possible (Kapczynski et al., 2019; Huang et al., 2019; Dwivedi et al.,2011). The world is entering a new era of asymmetrical schemes that promise to provide solutions to inherently insecure systems (Barbulescu et al., 2017). Different methods and their features are shown in table 2.

Table 2 Different methods and their features

Paper	Method detail	Mitigated attacks	Vulnerabilities/Limitation
(Kapczynski and Lawnik, 2019)	The use of variable key length cyphers	This system is designed to resist various attacks, such as side-channel attacks, related-key attacks, and plain text attacks	Execution time and space are vastly increased.
(Aggarwal and Maurer, 2016)	RSA factoring using the generic ring algorithm	RSA mitigation of factoring issues	Various cryptoanalysis attacks are possible.
(Hwang et al., 2016)	Using pairless cryptography to encrypt certificates	Protects against attacks using chosen cypher texts	Due to its reliance on bandwidth, the architecture is prone to Denial-of-Service attacks.
(Fujisaki, 2018)	Based on a binary string, this method involves public-key encryption with apt length.	A defence against man-in-the-middle attacks.	Attacks that interfere with service may result in denial of service.
(Hazay et al., 2018)	Utilize two-party distributed factoring to resolve the factoring problem.	Defend yourself against malicious attacks.	The size of the application and the execution time increases dramatically.
(Dwivedi, 2011)	Distributed-transforming encoders for message recovery.	Ensure security against brute force attacks.	This vulnerability can be exploited by known plain text attacks.
(Biswas and Mohit, 2016)	Implementing RSA within DES	Protection against a variety of threats.	An attack using known-cypher text is possible, as well as brute force attacks
(Chie, 2018)	Generating session keys based on key agreement schemes.	Passive and active defence models.	Attacks by third parties are possible.
(Barbulescu and Duquesne, 2017)	Using a variant of NFS, suggest a novel key size.	Reduce the risk of DOS, impersonation and replay attacks.	It cannot be accessed by a multi-server environment.
(Thangarasu and Selvakumar, 2018)	Modifying the ECC algorithm to secure session keys.	Intruder attacks can be mitigated.	Attacked by traditional methods.

2. Survey on Various IDS Techniques

According to Roschke et al. (2009), cloud-based IDS deployment is necessary by presenting an extensible IDS architecture that can be utilized in a distributed cloud infrastructure. Using virtual servers provided by Amazon's Elastic Compute Cloud service, Noah Guilbault and Ratan Guha can create a distributed intrusion detection system that utilizes the distributed grid as a detection mechanism. Using an Intrusion Detection System (IDS) within a virtual machine, Bakshi et al. (2010) suggested a strategy to protect the cloud against DDoS attacks. It is possible to implement both solutions with IDS, and you only need to implement as many IDS as virtual machines. Comparitive study of different algorithms are shown in table 3.To implement this in a virtual machine sniffing network traffic and analyzing packets sent over the Internet, you can implement Snort intrusion detection sensors.

Based on Claudio Mazzariello et al. 's work, Snort serves as a NIDS for the switch component of the physical machine. This system uses Eucalyptus, a cloud computing platform for running client virtual machines. An intrusion detection system developed by Kleber Vieira et al. (2010) uses signature-based techniques for detecting intrusions in cloud computing networks to combat DDoS attacks. This strategy, however, works best if used with PaaS platforms.

Table 3: Comparative study of different techniques

Algorithm / Technique Used	**Reference Paper**	**Purpose of IDS**	**Advantage**	**Limitation/ Future Scope**
KDD and clustering	(Chen et al. 2017)	Detecting novel anomalies referred to as NEC	It is not necessary to have quality labelled datasets.	A large number of false positives and a high number of false positives.
Decision tree, random forest, K-NN	(Anbar et al. 2016)	To accurately detect potential attack	Produce impressive and efficient results in detecting IPV4-based attacks.	IPV6 attack cannot be detected yet.
GPFISClass (genetic programming fuzzy inference system for classification)	(Ahmim, A., & Zine, N.G. 2015)	Solving the classification problem in IDS.	Higher classification accuracy.	Introducing the new hybrid GFS that combines neural networks with GFS.
Epigenetic algorithm	(Ghazi et al. 2016)	The future offspring of this couple.	By preventing diseases based on environmental factors that are not related to the sequenced genes, it helps prevent more preciously the curable.	A shorter time is spent to obtain optimal solutions when there are fewer iterations.

3. Review based on Machine Learning Algorithms

Nowadays, machine learning methods are widely used in many network intrusion detection system investigations. Due to the availability of numerous open-source datasets, a variety of strategies have been developed to solve the challenge of locating and avoiding threats. Methods such as machine learning and standalone data science methods are frequently combined to develop hybrid approaches that utilize layered and hierarchical models, detect anomalies, and enhance machine learning approaches by incorporating knowledge-based methods. Generally speaking, the majority of these techniques are geared toward identifying unusual attacks while reducing false alarms resulting from recurring attacks. Various machine learning algorithms are used in intrusion detection, including SVMs, fuzzy logic approaches, and neural network-based algorithms.

Based on rule-based and decision tree approaches, Ahmed et al. developed IDS by combining multiple classification techniques, including J-Rip, REP trees, and Forest PA. Input characteristics are used to categorize the first two methods as benign or hostile. As opposed to REP trees, Forest PA uses the original input characteristics and both the first and second classifiers' output. We have achieved 97% accuracy with the CICIDS-2017 dataset, and we scored a 95% detection rate. If compared to other methods, we achieved better results. Various studies use hybrid methods rather than single ones. According to Sharma et al. (1998), NBC and NB-Tree combined to improve both the recall of attacks (attack detection ratio) and the accuracy of minority class attacks (including R2L and U2R). By using reduced feature sets to forecast each type of attack using periodic tests and domain knowledge, this system combines both accuracy and recall for small and critical threats. False positives in the IDS are kept to a manageable level. According to the study, this methodology achieves 99.05% accuracy overall and is better at categorizing minor groups when compared to the usual methods.

The neural network-based intrusion detection system developed by Moradi and Zulkernine manages to handle a multi-class issue by detecting attack types as well. To determine the optimal number of hidden layers, different neural network topologies are evaluated to detect intrusions. The authors used MLP to detect intrusions based on offline assessment strategies. To improve the neural network's rationalization capabilities, they also used a preliminary validation strategy during the training. Based on the testing results, a neural network with two hidden layers was able to correctly identify the logs with 91% accuracy, and with just one layer, it achieved 87 % accuracy. The proposed solution is suitable for a three-class problem, but it does not cover all classes. Among the findings of Zhang et al. is the need for artificial neural networks to detect intrusions. Unfortunately, it is rather difficult to select the most general and practical framework for

the neural network. Although they can often cope with noisy data quite well, they require a large quantity of data.

They intended to propose a more precise and computationally expensive technique based on Gupta et al. 's standardized and simpler tiered technique for detecting intrusions. Using three layers of security, the company describes data integrity, confidentiality, and integrity. In the first layer, features such as connection establishment, user identification, and destination layer IP addresses are managed at the packet level. The availability layer further detects attacks like a probe, U2R, R2L, and DoS attacks. It implements aspects such as what data is obtained, how many files have been viewed, etc. Ibrahim et al. addressed the problem of IDS performance optimization and presented a multi-layered methodology for detecting intrusions (Ibrahim et al., 2012). Using machine learning algorithms, the authors determine which features are optimal for each layer, based on data integrity, permissions, and file changes. To maximize storage space and achieve better performance, they used Nave Bayes, C5 decision tree approaches, and MLP neural networks algorithms to determine which features are optimal. Utilizing Naive Bayes, C5 decision tree approaches, and MLP neural networks utilizing gain ratios, the authors optimized the limited storage space and maximized performance in determining optimal features for each layer. Using gain ratio as a feature selection strategy, the proposed multiple-layer model was more accurate than MLP neural networks and Nave Bayes approaches and hence resulted in fewer false alarms than other approaches such as MLP neural networks and Nave Bayes. A limited number of invasions can, however, be identified by this system.

4. Review based on the Honeypot Techniques

Because the identification of hostile breaches has received a lot of attention recently, protecting the privacy of sensitive information in network infrastructures has become difficult. Although several security measures are presented, they all have a few limitations. Comparitive study of different approaches are shown in table 4. The majority of current research projects rely on machine learning algorithms to identify intrusions through data collecting utilizing various information technologies, specifically honeypots.

Based on machine learning, Luo et al. (2017) proposed an intelligent honeypot that improves the security of IoT devices. To save each device response, an IoT scanner was developed to scan the internet for potentially harmful interactions and teach the honeypot how to use an IoT learner model that can optimize a model to respond to each interaction. Using unsupervised anomaly data and honeypot data, (Owezarski et al., 2014) presents a method for categorizing assaults using clustering techniques such as density-based

clustering, subspace clustering, and evidence accumulation. By leveraging social honeypots to find out about harmful accounts on social networks such as Facebook and MySpace, the authors of (Lee et al., 2010) propose an automatic classification of spam utilizing machine learning techniques (e.g., SVMs).

In this paper, the authors propose a linkage protection-based honeypot that circumvents the inadequacies of existing techniques. A linkage management protocol provides a method of bringing honeypots into communication with the defence system components. Choosing to block or not block attacks depends on the honeypot's state regarding detecting new threats. The system is a centroid honeypot, which processes suspicious flows coming through the traditional defensive system. "CloudAV- N Version Antivirus System in the Network" by Oberheide et al. (2008) proposes a new paradigm for AV installations and scanning in the cloud if the honeypot is damaged. A new technique developed by the researcher outperformed typical host-based anti-virus scanner capabilities, including enhanced abilities to detect and manage retroactive detection of harmful software. Demonstrate a real-world implementation and deployment of the Cloud AV platform.

In his paper, Schmidt et al. (2009) proposed a combined solution for malware detection and kernel rootkit avoidance by intercepting all executing binary programs from virtual instances and submitting them to a variety of analysis engines. Each system call is examined in real-time in addition to checking against a signature database to uncover undetected vulnerabilities or malware. A honeypot is a security resource that is used to investigate, attack, and discover vulnerabilities and malware. Having a honeypot deployed serves the purpose of enticing attackers to capture, register, and analyze their activities for incident response. Using an unsupervised anomaly learning approach and honeypots, Wezarski et al. (2014) developed a self-governing solution to detect attacks. The authors used cluster-based techniques to classify items during diverse traffic sources, such as subspace clustering, evidence accumulation, and density conscious clustering. This strategy has the advantage that it does not require prior training. To improve the security of IoT-based devices, Luo et al employed machine-learning methodologies to create a smart honeypot-based model. The honeypot is employed in this strategy to manage invasions through model optimization. Through the use of machine learning methodologies, Lee and colleagues (Lee et al., 2010) developed a model that can be applied to a range of social media platforms, including MySpace, Facebook, and Twitter, to gather data about anomalous intrusions.

Li. et. al adapted Feng's link protection system to develop a honeypot model that overcomes the shortcomings of existing tools. That model enables the authors to increase

communication and administration among the defensive mechanisms by utilizing the standard SNMP protocol. As a defence system, a honeypot monitors the defensive system and determines whether to block or allow attacks based on its condition. Qiul et al. (2016) established a model to predict attacks using machine learning methods. This project proposes using machine learning and honeypot algorithms to create an intrusion prevention system. By using this hybrid strategy, a machine-learning algorithm combines with a honeypot algorithm to prevent intrusions.

Honeyed honeypots have been studied for their latency analysis by Fu et al. (2006). In some virtual networks, the link latency is a multiple of one millisecond or ten milliseconds due to the very high stimulus accuracy of honeypots such as honeyd. As a result of their strategy, they acquired a high detection rate using the Neyman-Pearson decision theory. By evaluating network monitoring characteristics or analyzing the virtual environment, users can identify honeypots, according to Wenda and Ning (2012). By taking advantage of the fact that interactive honeypots are always deployed with firewalls and intrusion detection systems, Defibaugh-Chavez et al. (2006) presented a method of identifying honeypot network-level actions and providing services. Using user-mode Linux and virtual machine files, Holz and Raynal developed a honeypot detection method based on the feedback information.

Table 4 Comparitive study of different approaches

Ref.	Approaches	Strengths	Weaknesses
(Choi et al, 2018)	Botnet, IoT botnet	Web service is available for easy monitoring of IoT device health and is useful for smart factories with many IoT devices.	Limited capacity
(Park et al., 2018)	Smart factory detection using machine learning.	Cost reduction	Low detection rate, high complexity and uncertainty.
(Wang et al.,2020)	Exploiting IoT honeypots for detection.	In addition, since only parts of the system are implemented, the gathering of information is rapid.	Stacks of unneeded data accumulate.
(Wang et al., 2020)	Botnet detection using Machine learning.	In this case, the combination of a flow-based and a graph-based analysis achieves a detection accuracy of 99.94%, exceeding individual detectors at each stage.	To ensure security, it is necessary to randomly specify the size of the packets and the number of packets in each flow so that they are not detected. Flow-based detectors cannot be quickly applied.
(Vishwakarma, 2019)	Machine learning detection with the Honey Pot	With the help of machine learning, it has developed a solution to detect botnets using honeypots. Honeypots log newly released malware functions so that they can be identified in the future.	The functions of the system vary depending on how well it performs.

The number of attacks on these platforms has risen dramatically in recent years. In addition, cloud cyber attacks will account for 20% of all cyberattacks in 2020. Therefore it is important to devise a system that can act as a decoy to the attacker and let the system monitor the attack in detail while collecting actionable information for preventing future attacks. This is where honeypots come in handy as they are specifically designed virtual systems which mimic the behaviour of the real assets that we have to protect. No system is perfect, and honeypots have significant drawbacks. One of the main issues is that the system is designed to be attacked, so attacks are likely to occur. Once the honeypot has been compromised, it could be used as a launchpad for additional attacks. These attacks could be carried out against an internal system or another company. As a result, honeypots introduce risk. As a result, there is a legal liability issue. You could be sued if your honeypot is used in an attack on another company. The level of risk introduced will be determined by the honeypot.

The number of people exploiting cloud infrastructure to implement their complex solutions to various problems is growing exponentially. One disadvantage of this change is that no system is indestructible there for there always pose a threat of cyber attacks to these cloud solutions. As we already know that these cloud systems come with built-in defensive systems but the use of a honeypot ensures that extra layer of security all while providing us with valuable information about the attack vector. To overcome the above problem implement a hybrid honeynet system in future, this can incorporate the best of different types of honeypots to build a better difference system.

Conclusion

Here, an introduction to cyber-attacks, security, and honeypots as cyber security remedies is offered, as well as an efficient algorithm that returns to crucial facts, those for creating a profile and those for categorizing it. Using honeypots and machine learning algorithms, you can detect and categorize suspicious profiles and build strong models and predictions. To measure how effective, the Hybrid Honeypot is against future attacks and zero-day attacks, it will be subjected to a real-world test to evaluate its performance against future attacks. This suggested honeypot will be used as an investigation tool to collect additional data regarding the growing number of system attacks that occur regularly.

References

Ameen, Nisreen, Ali Tarhini, Mahmood Hussain Shah, Nnamdi Madichie, Justin Paul, and Jyoti Choudrie. "Keeping customers' data secure: A cross-cultural study of cybersecurity

compliance among the Gen-Mobile workforce." *Computers in Human Behavior* 114 (2021): 106531.

Alhayani, Bilal, Husam Jasim Mohammed, Ibrahim Zeghaiton Chaloob, and Jehan Saleh Ahmed. "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry." *Materials Today: Proceedings* (2021).

Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." *Computers & Security* 105 (2021): 102248.

Zhang, Dan, Gang Feng, Yang Shi, and Dipti Srinivasan. "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances." *IEEE/CAA Journal of Automatica Sinica 8*, no. 2 (2021): 319-333.

Dixit, Priyanka, and Sanjay Silakari. "Deep learning algorithms for cybersecurity applications: A technological and status review." *Computer Science Review* 39 (2021): 100317.

Anthi, Eirini, Lowri Williams, Matilda Rhode, Pete Burnap, and Adam Wedgbury. "Adversarial attacks on machine learning cybersecurity defences in industrial control systems." *Journal of Information Security and Applications* 58 (2021): 102717.

Kim, Kyounggon, Faisal Abdulaziz Alfouzan, and Huykang Kim. "Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework." *Applied Sciences* 11, no. 16 (2021): 7738.

Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on a smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094.

He, Qiyi, Xiaolin Meng, Rong Qu, and Ruijie Xi. "Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles." *Mathematics* 8, no. 8 (2020): 1311.

Poorvika Singh Negi, Aditya Garg and Roshan Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security", *IEEE Conference on data security,* 2020.

Yang Ming and Hongliang Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs", *Hindawi Mobile Information Systems,* 2019.

Feifei Wang, Guoai Xu and Lize Gu. "A Secure and Efficient ECC-Based Anonymous Authentication Protocol", *Security and Communication Networks* Volume 2019.

Huang, X., Liu, J., Ma, J., Xiang, Y., Zhou, W., Data Authentication with Privacy Protection. *In Advances in Cyber Security: Principles, Techniques, and Applications.*115-142. 2019. Springer, Singapore. DOI: 10.1007/978-981-13-1483-4_6.

Fujisaki, E., 2018. All-but-many encryption. *J. Cryptol. 31*(1), 226–275. https://doi. org/10.1007/s00145-017-9256-x.

Dwivedi, A., 2011. A model of key agreement protocol using polynomials over non-commutative division semirings. *J. Global Res. Comput. Sci. 2*(3).

Biswas, G. P., Mohit, P., Modification of Symmetric-Key DES into Efficient Asymmetric-Key DES using RSA. *In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.* ACM, New York, NY, USA .136. (2016). DOI: 10.1145/2905055.2905352.UKI

Chie, H., 2018. Using the modified Diffie-Hellman problem to enhance client computational performance in a three-party authenticated key agreement. Arab. J. Sci. Eng. 43 (2), 637–644. https://doi.org/10.1007/s13369-017-2725-6.

Thangarasu, N., Selvakumar, A.A.L., 2018. Improved elliptical curve cryptography and abelian group theory to resolve linear system problems in sensor-cloud cluster computing. *Cluster Comput. 1*. https://doi.org/10.1007/s10586-017-1573-1.

Barbulescu, R., Duquesne, S., 2017. Updating key size estimations for pairings. *J. Cryptol.* 1–39. https://doi.org/10.1007/s00145-018-9280-5.

Bakshi, A., Dujodwala, Y.B.: Securing cloud from DDoS attacks using intrusion detection system in the virtual machine. *In: International Conference on Communication Software and Networks*, pp. 260–264 (2010)

Mazzariello, C., Bifulco, R., Canonico, R.: Integrating a network ids into an open-source cloud computing environment. *In: Sixth International Conference on Information Assurance and Security (IAS)*, pp. 265–270 (2010)

Lo, C.C., Huang, C.C., Ku, J.: A cooperative intrusion detection system framework for cloud computing networks. *In: Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, ICPPW* 2010, pp. 280–284. IEEE Computer Society (2010)

W. Chen, F. Kong, F. Mei, G. Yuan, and B. Li, "A novel unsupervised Anomaly detection Approach for Intrusion Detection System," *IEEE 3rd International Conference on big data security on the cloud, Zhejiang, China,* 2017.

Ahmim, A., Maglaras, L., Ferrag, M.A., Derdour, M., & Janicke, H. (2019). A novel hierarchical intrusion detection system based on decision trees and rules-based models. *In 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 228-233.

Moradi, M., & Zulkernine, M. (2004). A neural network-based system for intrusion detection and classification of attacks. *In Proceedings of the IEEE international conference on advances in intelligent systems-theory and applications* 15-18.

Debar, H., Zhang, M., & Siboni, D. (1992). A neural network component for an intrusion detection system. *In Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE,* 240-250.

T. Luo, Z. Xu, X. Jin, Y. Jia, and X. Ouyang, "Iotcandyjar: towards an intelligent-interaction honeypot for IoT devices," in Proceedings of the Black Hat, Las Vegas, NV, USA, 2017.

P. Owezarski, "Unsupervised classification and characterization of honeypot attacks," *in Proceedings of 10th International Conference on Network and Service Management (CNSM) and Workshop, pp. 10–18, Rio de Janeiro, Brazil, November 2014.*

K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots+ machine learning," *in Proceeding of the 33rd international ACM SIGIR conference on Research and development in information retrieval - SIGIR'10, pp. 435–442)* e ACM Digital Library, New York; NY, USA, July 2010.

G. Feng, C. Zhang, and Q. Zhang, A Design of Linkage Security Defense System Based on Honeypot: Trustworthy Computing and Services, Springer, Berlin, Heidelberg, Germany, 2014.

J. Oberheide, E. Cooke, and F. Jahanian "CloudAV: N-Version Antivirus in the Network Cloud", *In Proceedings of the 17th USENIX Security Symposium (Security'08). San Jose, CA, 2008.*

L. Spitzner, *Honeypots: Tracking Hackers.* Addison Wesley, 2002.

Lee, K., Caverlee, J., & Webb, S. (2010). Uncovering social spammers: social honeypots+ machine learning. *In Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval,* 435-442.

Feng, G., Zhang, C., & Zhang, Q. (2013). A design of linkage security defence system based on the honeypot. *In International Conference on Trustworthy Computing and Services,* 70-77.

X. Fu, W. Yu, D. Cheng, X. Tan, K. Streff, and S. Graham, "On recognizing virtual honeypots and countermeasures," *in Proceedings of the 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing,* pp. 211–218, IEEE, Indianapolis, IN, USA, September 2006.

D. Wenda and D. Ning, "A honeypot detection method based on characteristic analysis and environment detection," *In 2011 International Conference in Electrics, Communication and Automatic Control Proceedings,* pp. 201–206, Springer, Berlin, Germany, 2012.

P. Defibaugh-Chavez, R. Veeraghattam, M. Kannappa, S. Mukkamala, and A. Sung, "Network-based detection of virtual environments and low interaction honeypots," *in Proceedings of the 2006 IEEE SMC Information Assurance Workshop,* pp. 283–289, IEEE, West Point, NY, USA, June 2006.

S.T. Park, G. Li, and J.C. Hong, "A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning," *Journal of Ambient Intelligence and Humanized Computing, vol. 0, no. 0, Springer Berlin Heidelberg,* 2018.

W. Wang, Y. Shang, Y. He, Y. Li, and J. Liu, "BotMark: Automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviours," *Inf. Sci. (NY).,* vol. 511, pp. 284–296, 2020.

R. Vishwakarma, "A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks," *2019 3rd Int. Conf. Trends Electron. Informatics, no. Icoei,* pp. 1019–1024, 2019.