World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

# Literature review on advanced persistent threats management with deception techniques

Chukwuebuka Bartholomew Onah *, Chukwudi Linda Nnadi *and* Chimezie Fredrick Ugwu

*Department of Computer Science, Faculty of Faculty of Technology, Institute of Management and Technology, (IMT), Nigeria.*

World Journal of Advanced Research and Reviews, 2025, 27(01), 2005-2017

Publication history: Received on 21 May 2025; revised on 08 July 2025; accepted on 11 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2509

## Abstract

This study investigates the dynamic threat landscape of cybersecurity, with a particular focus on Advanced Persistent Threats (APTs) and various web-based and network-based attacks. Through a theoretical approach, it examines key attack vectors including structural query language (SQL) Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Directory Traversal, Server-Side Request Forgery (SSRF), and Command Injection, highlighting the mechanisms through which attackers exploit vulnerabilities in web and network systems. To counter these evolving threats, the research explores theoretical frameworks such as Game Theory and Reinforcement Learning (RL). Game Theory is applied to honeypot optimisation, modelling strategic interactions between attackers and defenders, while RL enables adaptive learning for dynamic defence configurations. The integration of these concepts presents a proactive cybersecurity approach, improving detection capabilities, resource allocation, and system resilience. This study concludes that combining strategic modelling with intelligent learning systems is vital for building robust cybersecurity defences capable of addressing modern and emerging threats.

**Keywords:** Advanced Persistent Threat; Cybersecurity; Network-Based Attacks; Structural Query Language; Injection

## 1. Introduction

Deception as a fundamental concept in cybersecurity involves the strategic deployment of deceptive techniques to mislead adversaries and protect critical assets. At its core, deception security aims to create uncertainty and confusion for attackers, making it harder for them to achieve their objectives while providing defenders with valuable intelligence on adversary tactics and motivations (Feng et al., 2020).

To start with, deception security relies on the creation of decoy systems, such as honeypots and honeytokens, that mimic legitimate assets within a network. These decoys appear to be genuine to potential attackers but are designed to attract and engage them. By luring attackers away from real assets, decoys buy time for defenders to detect, analyse, and respond to threats effectively (Khoje, 2023).

In the ever-evolving landscape of cybersecurity, organisations face an incessant barrage of sophisticated threats from malicious actors seeking unauthorised access to sensitive data and systems. To combat these threats effectively, cybersecurity professionals employ a variety of innovative techniques, including the strategic use of deception. Deception techniques involve the deliberate creation of false information or resources to mislead attackers, gather intelligence, and enhance threat detection capabilities. The common cyber deception techniques employed are Honeypots, honey nets, mimicking, dazzling, and repackaging (Feng et al., 2020).

* Corresponding author: Onah C.B

Honeypots serve as decoy systems or resources designed to mimic legitimate targets, enticing attackers to interact with them. These traps are isolated and monitored, providing valuable insights into attackers' tactics and behaviours without jeopardising actual assets. Honeypots fulfil three primary functions: Detection, Prevention, and Research. Notably, their detection capability excels due to a minimal rate of false positives, as legitimate users typically refrain from interacting with them. This attribute grants honeypots a distinct advantage in identifying zero-day attacks compared to conventional security tools. In terms of prevention, honeypots serve as a proactive deterrent, dissuading adversaries through the perception of risk and uncertainty, thus fortifying network defences against potential breaches. Honeypots assume a pivotal role in cybersecurity research by amassing comprehensive data on adversaries' actions and responses (Armal and Venkadesh, 2022).

Despite the increasing adoption of deceptive cybersecurity technologies like honeypots, there exists a significant weakness in understanding the behaviour of attackers and also that of normal users, which presents the issues of false alarms as a major problem in this study. Another notable problem identified is the static nature of existing honeypot security solutions, which are mostly identified by attackers due to their inability to replicate real network behaviour. Due to this effect, attackers easily detect them and avoid them, hence presenting another issue.

The implication of these problems of false alarm and lack of adaptive behaviour, impacts on the reliability of the existing honeypot security solution as they do not provide the desired security solution needed and also do not effective divert attackers; hence there is need for a more advance solution capable of diverting attackers to a decoy facility and also very difficult to be detected and differentiate from original network by attackers. This study is focused on honeypots and their deception techniques. While several surveys exist in this domain, including recent works by (Ilg et al., 2023; Zuzcak and Zenka, 2020; Zhang et al., 2023), none delve into honeynets' deception techniques. This study concentrates on a review related to honeypot, their challenges, classification, deceptive techniques and recommended solutions to these problems.

## 2. Literature review

Ilg et al. (2023) surveyed the frameworks and tools of contemporary open-source honeypots. The study addressed open-source honeypots with varying degrees of complexity and attention in our study. For the majority of use cases, there are solutions available, whether one is looking for a web application honeypot, a Secure Shell (SSH) honeypot, or a honeypot that looks like a mail server. Larger open-source projects, in particular, provide excellent quality because of their large contributor base. The study found that there is a trade-off between deceptiveness and customisation for various use cases when interacting with installed honeypots. Recent studies on honeypot finding support this: honeypots that imitate a particular system or service are harder to find than their customizable equivalents. The extensive use of container technology is another finding. The majority of honeypots provide dummy images or even use containers as a proxy or honeypot. There isn't a technique implementation report or outcome evaluation in the study, nevertheless.

Aggarwal et al. (2022) researched the design of an effective masking strategy for cyber defence on human experimentation and cognitive models. In this research, two problems that impede the development of successful masking tactics against human attackers are addressed, building on earlier work in cyber-deception (masking techniques). First, consideration is given to the majority of machine learning and game theory protection strategies' presumption of adversary rationality. In a novel person-in-the-loop experiment, the study investigated human attacker behaviour in more detail and contrasted the new risk-averse masking technique with a logical masking method. The study also shows how to use a well-calibrated cognitive model of attacker conduct to provide copious quantities of data, which can be used to develop game theory and machine learning protection systems. To show off the cognitive model's capacity to mimic the attacker's activities gathered from a human experiment, the study created an instance-based learning (IBL) model of a human attacker. According to the research's findings, this model can help adaptive cybersecurity algorithms and be used to create a lot of fake data about an attacker's movements to enhance ML-based bounded rational masking algorithms.

Zhang et al. (2023) present a masking and purifying approach for cyber defence against adversarial attacks. Developing approved defensive strategies is essential to securing DNNs from adversarial assaults. Nevertheless, certified defences have received little attention in the research that is currently accessible, and certified defences frequently rely on erroneous presumptions and previous information, which is limited in real-world situations. In this study, we offer a certified defensive mechanism that applies demonising and refactoring of input samples through the Makser and the Purifier, without regard to the model or the attack. The whole implementation is independent of any target models or attack techniques, with the Makser being rule-based and the Purifier being trained via self-supervised fine-tuning on

the enhanced BERT Masked Language Model (BERT-MLM). After the study was put into practice, the system demonstrated a 92.8% clean accuracy and a 66.1% defence against hostile attack.

Zuzcák and Zenka (2020) researched the use of an expert system for the assessment of the threat level of attacks on a hybrid SSH honeynet. Using an expert system based on EMYCIN and rules from earlier research, the suggested solution, which is based on a hybrid SSH honeypot, evaluates existing methods for network traffic analysis and offers a new one. The following is a presentation of the study's key points: As of right now, there is no way to divide incoming connections into two categories according to the amount of activity they require for analysis and the type of analysis they need. A medium degree of contact is necessary for connections that might be the target of basic assaults, while a high level of engagement is necessary for sophisticated attacks. (B) - A connection classification expert system was created. It makes use of two different kinds of attacker data. The study's conclusion said that the honeynet is always being improved and enhanced. The efficient observation of an attacker inside a high-interaction honeypot is the current development emphasis.

Papaspirou et al. (2021) present a novel Two-Factor Authentication (2FA) approach based on the HoneyToken mechanism. This work offers a prototype of a unique security mechanism based on these discoveries, aiming to combine the capabilities of 2FAs and honeywords while making the system easy to incorporate into any current platform or system. The research put out and created a novel security feature for online apps that generates passwords and QR codes for various login options. The suggested approach combines the benefits of Honeyword and two-factor authentication. In the produced prototype, the user receives an SMS with three OTP passwords that match three QR codes. The proper token must be used to proceed is just one of these three components. The suggested 2FHA technique makes the authentication bypass impractical, if not impossible, even in the unlikely event that the attacker gains access to the device that gets the token, for example, through SIM cloning. The work was completed with the method being implemented and demonstrating the effectiveness of 2FA; hence, it is suggested that future work include the approach in Google and Microsoft authenticators.

Khoje (2023) developed a secure platform based on a strategic masking technique for ensuring privacy and security in Business-to-Business (B2B) enterprise data. In particular, this article will examine how data masking strategies integrated into data platforms might be a potent tool to improve sensitive data protection in these intricate B2B ecosystems. Data masking is used to generate a cleaned-up version of the data that may be utilised for analytics, software testing, and user training without revealing the real sensitive data. In this work, data masking may be conceptualised in two stages. Sensitive information in the raw data must first be identified and secured. Then, using the bloom filter approach, the data may be transformed or hidden without compromising its value. Finally, this work simultaneously serves as a clear demand for continued attention and evolution, while also charting a road towards solid data security inside data platforms using efficient masking mechanisms. Businesses will be able to confidently and honourably traverse the next digital era thanks to this unwavering commitment.

Feng et al. (2020) present a model for mimic defence technology for the protection of multimedia cloud servers. In this work, a distinct modelling paradigm was produced by a thorough analysis of the modelling challenges and attack problems. A straightforward mathematical expression was created by severing the model from the particular system input and output situations, hence bypassing the modelling challenges. Moreover, the attack's process features were emphasised through the development of a particular mathematical mapping technique. The suggested model was used to illustrate Cyber Mimic Defence's (CMD) superior security capabilities. Ultimately, a unique and intuitive mathematical model for CMD was developed, one that could mathematically represent the CMD mechanism and convert the CMD's attack and defence game problems into corresponding mathematical sub-problems. This allowed for a qualitative evaluation of the CMD safety capacities. The decomposition problem of large prime factors is a prerequisite for the suggested mathematical model of the CMD, which is based on the convolution process. The Large-Number Convolutional Mimic Defence (LNCMD) is the name given to the model. The system suggests that the suggested LNCMD model be directly applied through programming in the next work. The next stage is to programme the LNCMD model to investigate the CMD framework's primary technologies in more detail.

Amal and Venkadesh (2022) reviewed cyber-attack detection using a honeypot system. With the development of network attack techniques, every device linked to the Internet has become a potential target for attacks. Thus, it is impossible to overlook network data security. The study uses honeypots, which are conceptual framework traps made to prevent unauthorised access to both PCs and data, to counteract potential risks in this manner. Worldwide, a sizable portion of the population uses the internet each day. A sort of security equipment called a honeypot, also referred to as intrusion detection technology, screens devices to stop undesirable activity. An introduction to cybersecurity, a study of machine learning, cyber threats, and strategies based on honeypot systems are all included in this article. The review study is the outcome of extensive research, and in evaluating honeypots, the researchers found that experts are starting

to worry more about them as a crucial security tool that can prevent or restrict system attacks and give analysts insights into the causes and tactics of such attacks. The results of this study will help influence the direction of future research projects.

Aggarwal et al. (2020) explored the use of a masking strategy of cyber-deception using CyberVAN. The Cyber Virtual Ad hoc Network (CyberVAN) testbed was used to conduct an exploratory experiment. CyberVAN can be used to carry out several deception strategies, including decoying and masking. In this experiment, we tested the efficacy of masking tactics against human volunteers (as attackers) using CyberVAN. We used CyberVAN to alter the TC characteristics by employing the Π matrices generated by the random and optimum masking techniques. Using CyberVAN's Honeyd service, TCs of virtual computers are disguised to appear as fictitious OCs. To trick network scanning tools, the honeyed configuration file hides the operating systems and ports of TCs with OCs. According to the study's findings, 90% of the attempts made were successful.

Khader et al. (2023) researched the assessment of masking and encryption techniques for effectiveness in safeguarding the identity of social media publishers from advanced metadata analysis. To identify anonymous publishers or online users, the study uses machine learning algorithms like K-Nearest Neighbour (KNN), Support Vector Machine (SVM), Multilayer Perceptron (MLP), Random Forest (RF), and Multinomial Logistic Regression (MLR) to extract useful information from shared digital data on social media platforms through their APIs. The study shows how various forms of metadata from social media accounts may be extracted and used for the identification of users on Twitter. The study then demonstrates how anonymising the metadata and assessing the possible impact on information loss might stop this identification. The study looked at how well these methods work when text and picture tweets from Twitter are used to hide or encrypt important information elements. The study's findings showed that while SVM obtained the highest identity identification rate of 50.24% when combining data masking and the AES encryption method, it also earned the highest accuracy rate of 95.81% when neither technique was used.

**Table 1 Summary of literature review**

| Author(s) and Year | Techniques | Work Done | Findings | Weaknesses |
|---|---|---|---|---|
| Lee and Park (2024) | Stability and stabilisation criteria, Sector bound function, Bernoulli distribution, Novel LKFs | Proposed criteria for networked control systems with delays and deception attacks, using LKFs combining mixed delay and sampling patterns. | Numerical examples showed asymptotic stability of NCSs with the proposed controller gain matrix. | Limited to periodic sampling scenarios and may not generalise to non-periodic systems. |
| Hu et al. (2021) | Discrete-time approach, Security control, Law of total expectation | Addressed security control for systems with deception attacks and packet dropouts, and developed sufficient conditions for security. | Control performance degraded under deception attacks; effectiveness shown through simulations on power grids and energy generators. | Control strategy is less effective under high deception attack levels, limited to specific system types. |
| Zhang et al. (2024) | Resilient distributed state estimation, IEKF, HCMCIA | Proposed IRDSEA for resilient state estimation in moving robots under attacks, compared with HCMCIA. | IRDSEA effectively estimates states under attack; HCMCIA failed during attacks but performed well without them. | HCMCIA's limited performance under attacks; IRDSEA's effectiveness may vary with attack intensity. |
| Chen and Wei (2024) | Optimal adaptive back-stepping control, Reinforcement learning | Developed an adaptive back-stepping control strategy using RL for nonlinear systems under deception attacks. | The strategy achieved bounded state and control inputs, with effective performance in simulations. | RL-based approach might require extensive training data and computational resources. |
| Gao et al. (2020) | Network-based modelling, | Addressed steering control for electric | Improved steering stability and | Focused on specific vehicle types, real- |

| | | | | |
|---|---|---|---|---|
| | Distributed ADRC, Extended State Observer (ESO) | vehicles with unknown tire forces and random attacks using ESO and ADRC. | robustness with fast convergence and effective disturbance rejection. | world applications might face practical challenges. |
| Ge et al. (2019) | Distributed resilient estimation, Attack detection framework, Finite horizon estimators | Developed a framework for distributed attack detection and estimation, with efficient recursive algorithms. | Effective attack detection and estimation, with superior performance over previous methods. | Complexity of implementation and potential computational demands for large systems. |
| Seungjin et al. (2021) | Machine learning honeypot for IoT security | To achieve this, two machine learning algorithms, which are R-studio and Weka, were trained to generate two separate models of botnet attack detection. | Comparative analyses were performed on the models, and the R-studio model stood out as he best. | Honeypot is static and prone to false alarms. |
| Tian and Zhao (2024) | Event-based adaptive NN control, Bounded estimation, Back-stepping method | Proposed a control strategy for nonlinear CPSs with unknown attacks, incorporating adaptive tracking and ETM. | Achieved asymptotic tracking control and reduced data transmission load, effective under attacks. | Limited testing under varying attack scenarios and system complexities. |
| Yuan, et al. (2022) | Distributed time-varying filtering, Quantisation, Event-triggered communication | Established a distributed filtering system with deception attacks in channels, using quantisation and event-triggered protocols. | Better filtering performance with increased attack probability and reduced network congestion. | Performance degradation with higher attack probability and model uncertainties. |
| Tian, et al. (2024) | Dynamic event-triggered control, RDFNNs, Secure tracking | Developed an adaptive secure tracking control for nonlinear CPSs, addressing unknown attacks with ETM. | Effective tracking control with bounded states and reduced transmission load, even under attacks. | Tracking error may converge to a neighbourhood of zero, limited to specific attack models. |

## 3. The concept of advanced persistent threat (APT)

The Theory of Advanced Persistent Threat (APT) refers to a sophisticated and targeted cyber-attack, typically carried out by nation-state actors or organised crime groups. These threats are characterised by their persistence, stealth, and adaptability, allowing attackers to evade detection and remain within a compromised system for extended periods (Bartwal et al., 2022).

According to Diamantoulakis et al. (2020), APTs typically involve a series of coordinated attacks, using multiple vectors such as phishing, exploitation of vulnerabilities, and social engineering. Once inside, attackers move laterally, escalating privileges and gaining access to sensitive data and systems. Their goals may include espionage, data theft, or disruption of critical infrastructure (Du and Wang, 2020; Anwar et al., 2020). The APT theory highlights the importance of understanding the attacker's motivations, tactics, and techniques. This includes identifying the initial compromise, tracking lateral movement, and detecting data exfiltration. APTs require a comprehensive defence strategy, incorporating threat intelligence, incident response, and continuous monitoring (Franco et al., 2021). The APT theory has evolved to address emerging threats, such as fileless malware, living-off-the-land tactics, and supply chain attacks. As APTs continue to adapt, it's essential to stay ahead of these threats through advanced threat detection, AI-powered analytics, and collaborative information sharing among organisations and governments (Gokhale et al., 2021). Figure 1 presents the different types of APTs.

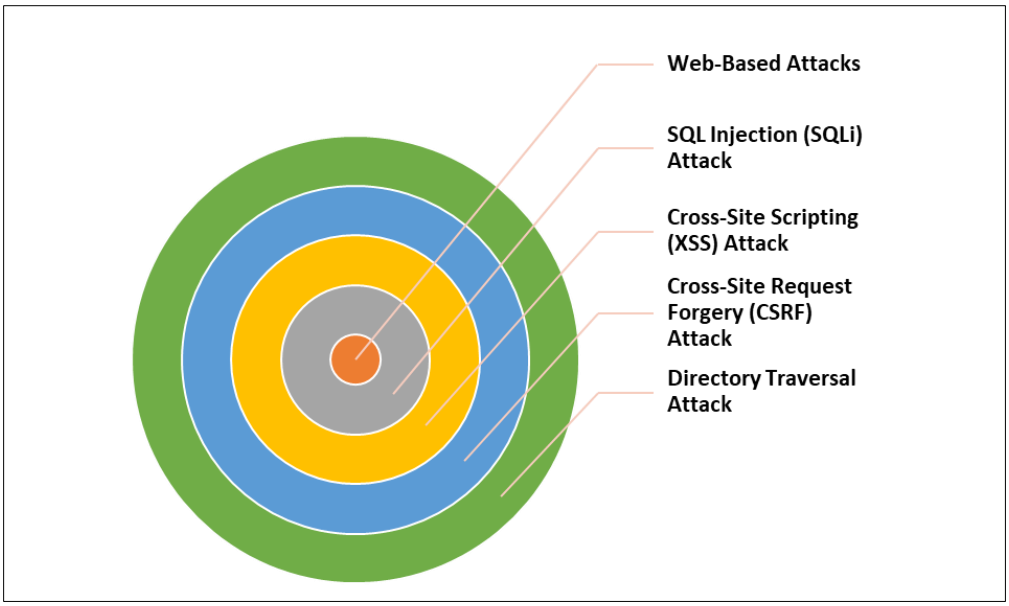


**Figure 1** Type of APTs **Diamantoulakis et al. (2020)**

### 3.1. Web-Based Attacks

Web-based attacks target applications, websites, and online platforms by exploiting vulnerabilities in web servers, application logic, or user input validation mechanisms. These attacks aim to steal sensitive data, manipulate web content, or gain unauthorised access to systems. Attackers often use malicious scripts, injection techniques, and authentication bypass strategies to compromise web applications.

### 3.2. SQL Injection (SQLi) Attack

An SQL Injection (SQLi) attack is a technique where an attacker injects malicious SQL queries into input fields of a web application to manipulate or extract data from a database. Many web applications use Structured Query Language (SQL) to communicate with databases, and when input validation is weak, attackers can exploit these queries to gain unauthorised access. One of the most common forms of SQL Injection is Error-Based SQLi, where an attacker crafts SQL queries that cause the database to return error messages, revealing valuable information about the database structure. By analysing these error messages, attackers can refine their queries to extract user credentials, payment details, or other sensitive records.

### 3.3. Cross-Site Scripting (XSS) Attack

A Cross-Site Scripting (XSS) attack is a web security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. This attack enables the execution of unauthorised JavaScript code, which can steal user credentials, manipulate website content, or redirect users to malicious websites. XSS attacks occur due to improper handling of user input and inadequate content sanitisation in web applications. There are three main types of XSS attacks: Stored XSS, Reflected XSS, and DOM-Based XSS. In a stored XSS attack, the malicious script is permanently stored in the website's database or message boards. When other users visit the infected page, the script executes automatically in their browsers, often stealing session cookies or injecting keyloggers. In Reflected XSS, the attacker tricks the victim into clicking on a maliciously crafted URL containing JavaScript code.

### 3.4. Cross-Site Request Forgery (CSRF) Attack

A Cross-Site Request Forgery (CSRF) attack tricks a logged-in user into performing unwanted actions on a trusted website without their knowledge. The attacker exploits the trust that a website has in the user's browser session by sending unauthorised requests disguised as legitimate ones. If a victim is authenticated on a site and unknowingly clicks on a malicious link, the attacker can force the website to execute actions such as changing passwords, transferring funds, or modifying account settings.

### 3.5. Directory Traversal Attack

A Directory Traversal attack, also known as Path Traversal, occurs when an attacker manipulates file paths in web applications to access restricted directories and retrieve sensitive files. This attack exploits insufficient input validation in web applications that use file inclusion mechanisms. By using special character sequences such as (dot-dot-slash), an attacker can navigate beyond the intended directory structure and access system files such as password configurations, logs, or source code.

### 3.6. Server-Side Request Forgery (SSRF) Attack

A Server-Side Request Forgery (SSRF) attack occurs when an attacker manipulates a web application to send requests to unintended external or internal systems. This vulnerability arises when a server fetches resources from user-supplied URLs without proper validation. Attackers exploit SSRF to bypass access controls, retrieve internal files, or interact with restricted networks.

### 3.7. Network-Based Attacks

Network-based attacks are a category of cyber threats that target the communication infrastructure of a system. These attacks aim to disrupt, intercept, manipulate, or overload networks, causing service denial or unauthorised data access. Hackers exploit vulnerabilities in networking protocols, IP configurations, and server communications to execute these attacks. One of the most common consequences of network-based attacks is service downtime, which can significantly affect businesses, government institutions, and individuals relying on uninterrupted online access.

## 4. Game theory for honeypot optimization

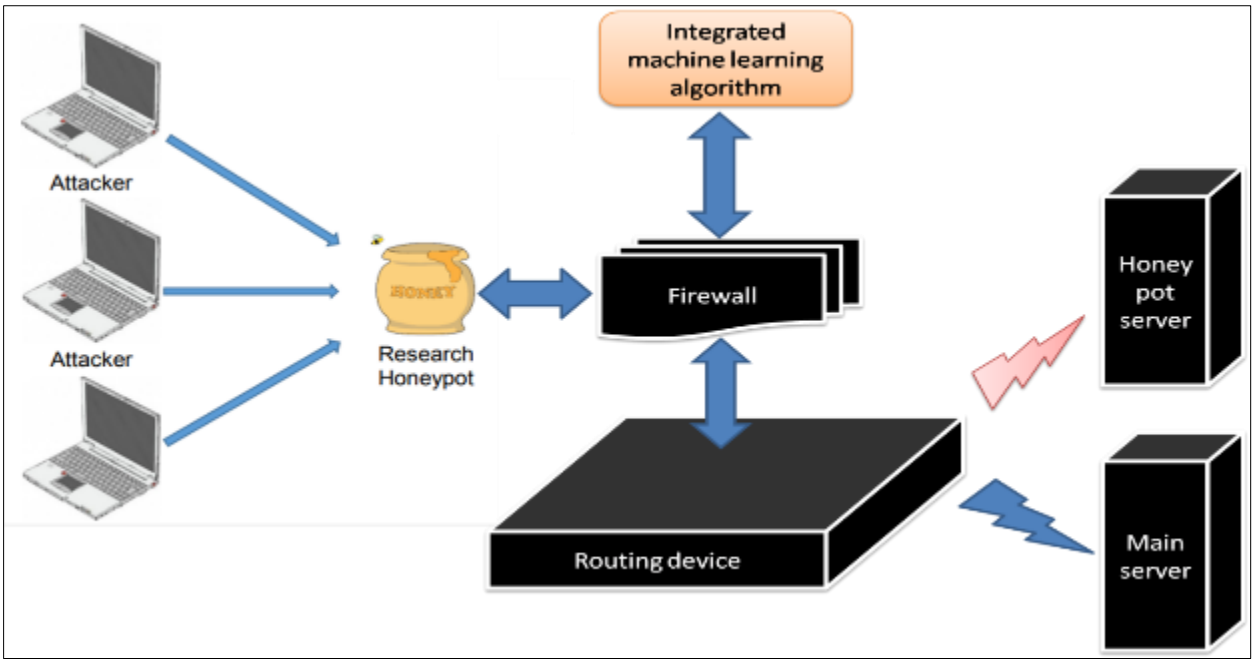


**Figure 2** Machine learning based honeypot model **(Grammatikis et al., 2021)**

Game theory provides a mathematical framework for analysing strategic decision-making in honeypot security. It models the interactions between attackers and defenders, helping defenders optimise honeypot deployment and configuration to detect and respond to threats more effectively (Grammatikis et al., 2021). In honeypot security, game theory can be used to analyse the strategic interactions between attackers and defenders. Attackers aim to evade detection and compromise the system, while defenders aim to detect and respond to threats. By understanding the attacker's motivations and tactics, defenders can optimise honeypot configuration to increase detection rates and reduce false positives (Grammatikis et al., 2020). The Stackelberg game model is particularly relevant to honeypot security. In this model, the defender leads by setting honeypot configurations, and the attacker responds by adapting their strategies. This model helps defenders optimise honeypot deployment to maximise detection rates and minimise resource usage (Radoglou et al., 2021). Figure 2 presents the architecture of a machine learning based honeypot model for network security.

Game theory also helps defenders understand the attacker's perspective, allowing them to anticipate and prepare for potential attacks. By analysing the attacker's payoffs and strategies, defenders can identify the most effective honeypot configurations and deployment strategies. This enables defenders to stay one step ahead of attackers and improve overall system security (Tiwaeri and Kumar, 2020). The application of game theory to honeypot security has several benefits, including improved detection rates, enhanced deterrence, and optimised resource allocation (Zhang et al., 2020). By using game theory to model the strategic interactions between attackers and defenders, defenders can develop more effective honeypot security strategies and improve overall system resilience (Uprety and Rawat, 2021).

### 4.1. Reinforcement learning (RL) for honeypot update

Reinforcement learning (RL) is a powerful technique to update the honeypot environment, enabling it to adapt to changing attacker tactics and evolve its defences accordingly. By training an agent to take actions in the honeypot environment, RL optimises honeypot configuration, deployment, and response strategies to detect and respond to threats more effectively (Sochima et al., 2025). The RL agent learns through trial and error, receiving rewards or penalties for its actions. The goal is to learn an optimal policy that maximises the cumulative reward over time. This approach enables the honeypot to improve its detection rates, reduce false positives, and enhance its overall effectiveness. Figure 3 presents the integration of RL with a honeypot as an intrusion detection system.

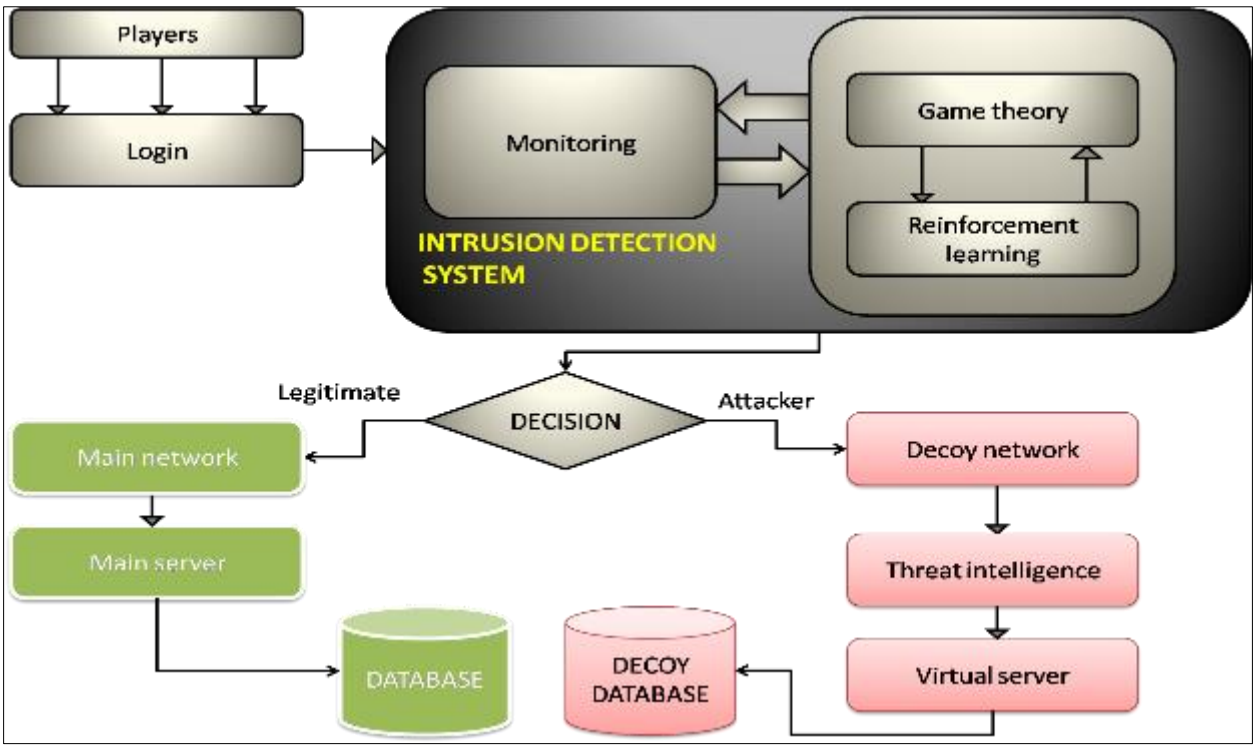


**Figure 3** RL with a honeypot for an intrusion detection system

RL techniques, such as Q-learning and Deep Q-Networks (DQN), can be applied to honeypot security to optimise honeypot configuration, improve deployment strategies, enhance response mechanisms, and adapt to changing threats. By leveraging RL, defenders can create a robust and adaptive honeypot security system that stays ahead of emerging threats. The combination of game theory and RL provides a comprehensive framework for honeypot security. Game theory offers a strategic understanding of the attacker's motivations and tactics, while RL optimises the honeypot environment to detect and respond to threats more effectively. This integrated approach enables defenders to develop proactive and adaptive defence strategies. By applying a combination of RL and game theory, organisations can significantly enhance their honeypot security capabilities, improving their ability to detect and respond to sophisticated threats. As the threat landscape continues to evolve, the integration of RL and game theory will play a critical role in developing robust and effective honeypot security systems.

## 5. Research observations

From the comprehensive review presented in this study, various findings have been identified in the field of study. The observations from the review are as follows:

### 5.1. Advanced Persistent Threats

Advanced Persistent Threats (APTs) are distinguished by their high level of sophistication, stealth, and persistence. The literature reveals that APTs are often perpetrated by well-funded actors such as nation-states or organised cybercriminal groups. These threats aim to infiltrate systems and remain undetected for extended periods, often with the goal of espionage, data theft, or sabotage. The theoretical concept of APTs emphasises a lifecycle-based approach involving initial compromise, lateral movement, privilege escalation, and data exfiltration. This underlines the need for organisations to go beyond traditional security tools and adopt holistic, intelligence-driven defence mechanisms.

### 5.2. Web and Network Attacks Exploit Weaknesses in Application and Infrastructure Layers

The review identifies a broad spectrum of web-based attacks such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and Server-Side Request Forgery (SSRF). These attacks often exploit weak input validation, authentication flaws, or poor configuration in web applications. On the other hand, network-based attacks like Denial of Service (DoS) and packet sniffing target communication infrastructures, aiming to intercept, disrupt, or overload data transmissions. This highlights the need for a security strategy that protects both application logic and the underlying network infrastructure.

### 5.3. Traditional Security Measures Are Insufficient for Modern Threats

A key observation is that traditional, static cybersecurity measures (e.g., firewalls, antivirus software) are no longer adequate. APTs and other modern cyber threats leverage dynamic and evasive tactics, which require advanced tools like behaviour-based anomaly detection, intrusion detection systems (IDS), and AI-powered monitoring solutions. Continuous threat hunting and adaptive security postures are becoming essential to stay ahead of ever-evolving threats.

### 5.4. The Importance of Understanding the Attacker's Lifecycle and Behaviour

Understanding how attackers operateespecially in APT scenarios crucial for timely detection and response. The APT theoretical framework helps organisations identify critical stages in the attack process, such as the method of initial entry, the pattern of lateral movement, and the technique used for data exfiltration. Recognising these behavioural patterns enables cybersecurity teams to deploy targeted countermeasures and shorten the dwell time of attackers in the system.

### 5.5. Game Theory Provides Strategic Insight into Attacker-Defender Interactions

The application of game theory introduces a strategic layer to cybersecurity defence. Models like the Stackelberg game simulate a scenario where the defender moves first by deploying honeypots or configuring system defences the attacker reacts based on observed defences. This strategic foresight enables defenders to make calculated decisions that can confuse, deter, or entrap attackers. Game theory aids in rationalising security investments by quantifying attacker payoffs and predicting likely attack vectors.

### 5.6. Reinforcement Learning (RL) Enhances Honeypot Adaptability and Responsiveness

Reinforcement Learning is observed as a powerful tool for adapting honeypot systems in real-time. RL agents learn optimal honeypot configurations and response strategies through interaction with attackers. This learning is reward-basedactions that successfully detect or deceive an attacker are reinforced. Techniques like Q-learning and Deep Q-Networks (DQN) allow honeypots to dynamically evolve in response to new threat patterns, thereby improving detection rates and reducing false positives.

### 5.7. Combining Game Theory and Reinforcement Learning Improves System Robustness

An important theoretical observation is the synergy between game theory and reinforcement learning. While game theory models strategic interactions and provides predictive insights into attacker behaviour, RL ensures adaptive learning and system evolution. Together, they enable the design of intelligent, self-learning honeypot systems capable of proactive defence. This combined approach is particularly effective in detecting zero-day threats and thwarting sophisticated adversaries.

### 5.8. A Multi-Layered, Proactive Defence Model Is Essential

Both the literature and theoretical insights emphasise the need for a multi-layered defence strategy. This includes endpoint protection, web application security, network monitoring, deception technologies (e.g., honeypots), and AI-based threat detection. Integration of these components enhances threat visibility and resilience. Proactivityanticipating and preparing for attacks rather than simply reacting central to modern cybersecurity.

### 5.9. Cybersecurity is a Dynamic Field Requiring Continuous Adaptation

The final observation is that cybersecurity is an ever-evolving discipline. New tactics, techniques, and procedures (TTPs) continue to emerge, making static defences obsolete. Both the literature and theoretical perspectives underscore the importance of continuous monitoring, adaptive learning, and collaborative information sharing among organisations and governments to stay ahead of threats. As threat actors innovate, so too must defenders evolve their tools and strategies.

## 6. Conclusion

This study has explored the evolving landscape of cybersecurity threats, focusing on Advanced Persistent Threats (APTs), web-based and network-based attack vectors, and the application of theoretical models such as Game Theory and Reinforcement Learning (RL) in enhancing cyber defence mechanisms. APTs, characterised by their stealth, persistence, and sophistication, underscore the inadequacy of traditional, reactive security approaches. The review reveals that modern cyber threats exploit both application and infrastructure-level vulnerabilities using techniques like SQL injection, XSS, CSRF, SSRF, and command injection, necessitating a proactive, multilayered security strategy.

Several studies on the application of honeypots as a smart security solution for persistent threats have been presented over the years. Among the studies, one of the most recent is Seungjin et al. (2021), who applied a hybrid machine learning algorithm and a honeypot as a holistic solution to mitigate cyberattacks. However, there is a gap in the static nature of the honeypot; also, there is a gap in the false alarm of the honeypot decision to classify normal attackers and normal users. Therefore, this project recommends the need for a reinforced honeypot model which is reliable to differentiate normal attackers and users and more so, adapt to the dynamic nature of network infrastructure in real time.

The theoretical frameworks discussed provide strategic and adaptive solutions to counter these threats. Game Theory offers a robust model for anticipating attacker behaviour and optimising defence strategies, particularly through the use of honeypots. Reinforcement Learning enhances this approach by enabling dynamic, self-improving systems that adapt to evolving attacker tactics in real-time. Together, these models foster the development of intelligent, proactive cybersecurity solutions capable of withstanding sophisticated and adaptive threats.

Ultimately, the integration of strategic modelling (Game Theory) and adaptive learning (RL) represents a significant advancement in the field of cybersecurity. As threats continue to grow in complexity, the findings of this study highlight the critical need for organisations to adopt innovative, intelligent, and forward-thinking security frameworks. Future cybersecurity resilience depends not only on robust technologies but also on strategic thinking, adaptive learning, and continuous collaboration across sectors.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict-of-interest to be disclosed. The authors have resolved that there no conflict of interest. All authors contributed with various percentage to put up this article

## References

[1] Aggarwal, P., Thakoor, O., Mate, A., Tambe, M., Cranford, E., Lebiere, C., & Gonzalez, C. (2020). An exploratory study of a masking strategy of cyberdeception using CyberVAN (Cooperative Agreement No. W911NF-13-2-0045). Army Research Laboratory, Cyber Security Collaborative Research Alliance (ARL Cyber Security CRA).

[2] Aggarwal, P., Thakoor, O., Jabbari, S., Cranford, E., Lebiere, C., Tambe, M., and Gonzalez, C. (2022). Designing effective masking strategies for cyber-defence through human experimentation and cognitive models. Computers and Security, 117, 102671. https://doi.org/10.1016/j.cose.2022.102671

[3] Aggarwal, P., Thakoor, O., Jabbari, S., Cranford, E., Lebiere, C., Tambe, M., and Gonzalez, C. (2022). Designing effective masking strategies for cyber defence through human experimentation and cognitive models. Computers and Security, 117, Article 102671. https://doi.org/10.1016/j.cose.2022.102671

[4] Aggarwal, P., Thakoor, O., Mate, A., Tambe, M., Cranford, E., Lebiere, C., and Gonzalez, C. (2020). An exploratory study of a masking strategy of cyberdeception using CyberVAN (Cooperative Agreement No. W911NF-13-2-0045). Army Research Laboratory, Cyber Security Collaborative Research Alliance (ARL Cyber Security CRA).

[5] Aggarwal, P., Thakoor, O., Mate, A., Tambe, M., Cranford, E., Lebiere, C., and Gonzalez, C. (2020). An exploratory study of a masking strategy of cyberdeception using CyberVAN (Cooperative Agreement No. W911NF 13 2 0045). Army Research Laboratory, Cyber Security Collaborative Research Alliance.

[6] Amal, M., andVenkadesh, P. (2022). Review of cyber attack detection: Honeypot system. Webology, 19(1). https://doi.org/10.14704/WEB/V19I1/WEB19370

[7] Amal, M., andVenkadesh, P. (2022). Review of cyber attack detection: Honeypot system. Webology, 19(1). https://doi.org/10.14704/WEB/V19I1/WEB19370

[8] Amal, M., andVenkadesh, P. (2022). Review of cyber attack detection: Honeypot system. Webology, 19(1). https://doi.org/10.14704/WEB/V19I1/WEB19370

[9] Anwar, A., Kamboua, C., and Nandi, L. (2020). Honeypot allocation over attack graphs in cyber deception games. In Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC): Communication and Information Security Symposium (pp. 1–6). Big Island, HI, USA.

[10] Anwar, A., Kamboua, C., and Nandi, L. (2020). Honeypot allocation over attack graphs in cyber deception games. In Proceedings of the 2020 International Conference on Computing, Networking and Communications (ICNC): Communication and Information Security Symposium (pp. 1–6). Big Island, HI, USA. [DOI unavailable]

[11] Bartwal, U., Mukhopadhyay, S., Negi, R., and Shukla, S. (2022). Security orchestration, automation, and response engine for deployment of behavioural honeypots. arXiv:2201.05326. https://doi.org/10.1109/DSC54232.2022.9888808

[12] Bartwal, U., Mukhopadhyay, S., Negi, R., and Shukla, S. (2022). Security orchestration, automation, and response engine for deployment of behavioural honeypots. arXiv:2201.05326. https://doi.org/10.1109/DSC54232.2022.9888808

[13] Chen, W., and Wei, Q. (2024). A new optimal adaptive backstepping control approach for nonlinear systems under deception attacks via reinforcement learning. Journal of Automation and Intelligence, 3, 34–39. https://www.keaipublishing.com/en/journals/journal-of-automation-and-intelligence/

[14] Chen, W., and Wei, Q. (2024). A new optimal adaptive backstepping control approach for nonlinear systems under deception attacks via reinforcement learning. Journal of Automation and Intelligence, 3, 34–39. https://www.keaipublishing.com/en/journals/journal-of-automation-and-intelligence/

[15] Diamantoulakis, P., Dalamagkas, C., Radoglou Grammatikis, P., Sarigiannidis, P., and Karagiannidis, G. (2020). Game-theoretic honeypot deployment in the smart grid. Sensors, 20, Article 4199. https://doi.org/10.3390/s20154199

[16] Du, M., and Wang, K. (2020). An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 16(1), 648–657. https://doi.org/10.1109/TII.2019.2917912

[17] Feng, F., Zhou, X., Li, B., and Zhou, Q. (2020). Modelling the mimic defence technology for multimedia cloud servers. Security and Communication Networks, 2020, Article 8819958. https://doi.org/10.1155/2020/8819958

[18] Franco, J., Aris, A., Canberk, B., andUluagac, A. S. (2021). A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems. IEEE Communications Surveys and Tutorials, 23, 2351–2383. https://doi.org/10.1109/COMST.2021.3106669

[19] Franco, J., Aris, A., Canberk, B., andUluagac, A. S. (2021). A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems. IEEE Communications Surveys and Tutorials, 23, 2351–2383. https://doi.org/10.1109/COMST.2021.3106669

[20] Gao, Z., Zhang, D., Zhu, S., and Feng, J. (2020). Distributed active disturbance rejection control for Ackermann steering of a four-in-wheel motor drive vehicle with deception attacks on controller area networks. Information Sciences, 540, 370–389. https://www.elsevier.com/locate/ins

[21] Ge, X., Han, Q.-L., Zhong, M., and Zhang, M.-X. (2019). Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica, 109, 108557. https://www.elsevier.com/locate/automatica

[22] Gokhale, S., Dalvi, A., & Siddavatam, I. (2021). Industrial control systems honeypot: A formal analysis of Conpot. International Journal of Computer Network and Information Security, 12, 44–56. https://doi.org/10.5815/ijcnis.2020.06.04

[23] Grammatikis, P. R., Sarigiannidis, P., Iturbe, E., Rios, E., Sarigiannidis, A., Nikolis, O., Ioannidis, D., Machamint, V., Tzifas, M., Giannakoulias, A., Angelopoulos, M., Papadopoulos, A., & Ramos, F. (2020). Secure and private smart grid: The SPEAR architecture. In Proceedings of the 6th IEEE Conference on Network Softwarization (pp. 450–456). https://doi.org/10.1109/NetSoft48620.2020.9165420

[24] Grammatikis, P. R., Sarigiannidis, P., Dalamagkas, C., Spyridis, Y., Lagkas, T., Efstathopoulos, G., ... Arce, A. (2021). SDN-based resilient smart grid: The SDN-microsense architecture. Digital, 1, 173–187. https://doi.org/10.3390/digital1040013

[25] Hu, Z., Deng, F., Su, Y., Zhang, J., and Hu, S. (2021). Security control of networked systems with deception attacks and packet dropouts: A discrete-time approach. Journal of the Franklin Institute, 358, 8193–8207. https://www.elsevier.com/locate/jfranklin

[26] Ilg, N., Duplys, P., Sisejkovic, D., and Menth, M. (2023). A survey of contemporary open-source honeypots, frameworks, and tools. Journal of Network and Computer Applications, 220, 103737. https://doi.org/10.1016/j.jnca.2023.103737

[27] Ilg, N., Duplys, P., Sisejkovic, D., and Menth, M. (2023). A survey of contemporary open source honeypots, frameworks, and tools. Journal of Network and Computer Applications, 220, Article 103737. https://doi.org/10.1016/j.jnca.2023.103737

[28] Ilg, N., Duplys, P., Sisejkovic, D., and Menth, M. (2023). A survey of contemporary open source honeypots, frameworks, and tools. Journal of Network and Computer Applications, 220, Article 103737. https://doi.org/10.1016/j.jnca.2023.103737

[29] Khader, M., & Karam, M. (2023). Assessing the effectiveness of masking and encryption in safeguarding the identity of social media publishers from advanced metadata analysis. Data, 8(6), 105. https://doi.org/10.3390/data8060105

[30] Khoje, M. (2023). Securing data platforms: Strategic masking techniques for privacy and security for B2B enterprise data. International Journal of Computer Trends and Technology, 71(11), 46–54. https://doi.org/10.14445/22312803/IJCTT-V71I11P107

[31] Lee, S. Y., & Park, J. M. (2024). Sampled-data stabilisation for networked control systems under deception attack and the transmission delay. Communications in Nonlinear Science and Numerical Simulation, 131, 107817. https://doi.org/10.1016/j.cnsns.2024.107817

[32] Papaspirou, V., Maglaras, L., Ferrag, M., Kantzavelou, I., Janicke, H., andDouligeris, C. (2021). A novel two-factor honeytoken authentication mechanism. arXiv. https://doi.org/10.48550/arXiv.2012.08782v3

[33] Papaspirou, V., Maglaras, L., Ferrag, M., Kantzavelou, I., Janicke, H., andDouligeris, C. (2021). A novel two-factor honeytoken authentication mechanism. arXiv. https://doi.org/10.48550/arXiv.2012.08782v3

[34] Radoglou-Grammatikis, P., Liatifis, A., Grigoriou, E., Saoulidis, T., Sarigiannidis, A., Lagkas, T., & Sarigiannidis, P. (2021). Trusty: A solution for threat hunting using data analysis in critical infrastructures. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (pp. 485–490). https://doi.org/10.1109/CSR51186.2021.9527936

[35] Sochima V.E., Asogwa T.C., Lois O.N., Onuigbo C.M., Frank E.O., Ozor G.O., Ebere U.C. (2025)" Comparing multi-control algorithms for complex nonlinear systems: An embedded programmable logic control application;

[36] TIan, Y., Zhang, H., Liu, Y., Zhao, N., & Kalidass, M. (2024). Event-triggered adaptive secure tracking control for nonlinear cyber–physical systems against unknown deception attacks. Mathematics and Computers in Simulation, 221, 79–93. https://doi.org/10.1016/j.matcom.2024.01.003

[37] Tian, Y., & Zhao, N. (2024). Event-based adaptive secure asymptotic tracking control for nonlinear cyber–physical systems against unknown deception attacks. Journal of the Franklin Institute, 361, 106766. https://doi.org/10.1016/j.jfranklin.2024.01.002

[38] Tiwari, A., & Kumar, D. (2020). Comparative study of various honeypot tools based on their classification & features. In Proceedings of the International Conference on Innovative Computing and Communications (pp. 1–6).

[39] Uprety, A., and Rawat, D. B. (2021). Reinforcement learning for IoT security: A comprehensive survey. IEEE Internet of Things Journal, 8(6), 8693–8706. https://doi.org/10.1109/JIOT.2020.3040957

[40] Yuan, H., Guo, Y., & Xia, Y. (2022). Event-based distributed filtering against deception attacks for sensor networks with quantisation effect. ISA Transactions, 126, 338–351. https://doi.org/10.1016/j.isatra.2021.12.024

[41] Zhang, W., Zhang, B., Zhou, Y., He, H., & Ding, Z. (2020). An IoT honeynet based on multiport honeypots for capturing IoT attacks. IEEE Internet of Things Journal, 7(5), 3991–3999. https://doi.org/10.1109/JIOT.2019.2956173

[42] Zhang, H., Gu, Z., Tan, H., Wang, H., Zhu, Z., Xie, Y., and Li, J. (2023). Masking and purifying inputs for blocking textual adversarial attacks. Information Sciences, 648, 119501. https://doi.org/10.1016/j.ins.2023.119501

[43] Zhang, H., Gu, Z., Tan, H., Wang, H., Zhu, Z., Xie, Y., and Li, J. (2023). Masking and purifying inputs for blocking textual adversarial attacks. Information Sciences, 648, Article 119501. https://doi.org/10.1016/j.ins.2023.119501

[44] Zhang, H., Gu, Z., Tan, H., Wang, H., Zhu, Z., Xie, Y., and Li, J. (2023). Masking and purifying inputs for blocking textual adversarial attacks. Information Sciences, 648, 119501. https://doi.org/10.1016/j.ins.2023.119501

[45] Zhang, C., Qin, J., Yan, C., Shi, Y., Wang, Y., & Li, M. (2024). Towards invariant extended Kalman filter-based resilient distributed state estimation for moving robots over mobile sensor networks under deception attacks. Automatica, 159, 111408. https://doi.org/10.1016/j.automatica.2024.111408

[46] Zuzcák, M., andZenka, M. (2020). An expert system assessing the threat level of attacks on a hybrid SSH honeynet. Computers and Security, 92, Article 101784. https://doi.org/10.1016/j.cose.2020.101784

[47] Zuzcák, M., andZenka, M. (2020). An expert system assessing the threat level of attacks on a hybrid SSH honeynet. Computers and Security, 92, Article 101784. https://doi.org/10.1016/j.cose.2020.101784