Classification of Cognitive Patterns of Hackers Using Machine Learning

Carlos Martinez-Santander[1-2], Myriam Hernández-Alvarez, Hugo Moreno Avilés[3], Ramiro Isa-Jara[3]

1 Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, Ecuador.
2 Carrera de Medicina, Universidad Católica de Cuenca, Cuenca, Ecuador.
3 Facultad de Informática y Electrónica, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador.

Abstract

Nowadays, computer security has become more crucial than ever. Beyond protecting digital assets, it is essential to safeguard financial institutions, companies, education, and defense sectors from increasingly sophisticated and evolving cyber threats. Addressing this challenge requires integrating various methodologies, techniques, and security tools. In this study, we utilize Honeypots, Machine Learning, and the ELK Stack, combined with an analysis of hacker psychology—understanding their motivations and behaviors—to develop more effective countermeasures. This research explores two key areas: the role of honeypots in cybersecurity and the psychological analysis of cyber attackers, examining their motivations and the tools used to measure these factors. Attack data was collected using the T-Pot Honeypot, while the Big Five Personality Traits instrument was applied to assess psychological patterns. A database was then generated, integrating this information for analysis through Machine Learning algorithms and neural networks, employing confusion matrices to compare predictions with actual data. The classification of cognitive patterns acquired through Honeypots and ML algorithms represents an emerging field that provides valuable insights into hacker behavior, enabling the development of more effective defensive strategies. Future research should focus on refining psychological assessment tools specifically designed for hackers. In our analysis, ML algorithms such as Neural Networks using a sequential model and Random Forest with 150 predictors demonstrated a strong fit for training and test datasets.

Keywords: Machine Learning, T-Pot, Hacker, Cognitive Patterns, Attacker, Investigative Psychology

Introduction

Nowadays, the Importance of IT security has risen to unparalleled levels [1], [2], [3], [4]; in addition to protecting digital assets, it is also necessary to safeguard the privacy of our financial institutions, businesses, education, and defense, among others, from recurrent, sophisticated, and constantly evolving cyber threats [5], [6], [7]. One of the innovative strategies that should employed in security systems is to understand and anticipate the cognitive patterns of hackers; hackers, with their different skills and motivations, can breach the security rules of systems and cause irreparable damage to the network or misuse the sensitive data found [8], [9]. Therefore, it is essential to understand their techniques and tools to get into their way of thinking and operating; classifying their cognitive patterns allows us to know their intentions and modus operandi, allowing security experts to anticipate their movements, develop solid preventive strategies, and reduce the potential risk of attack [10].

One strategy used for collecting the cognitive patterns of hackers is using Honeypots; these systems are designed with vulnerabilities, making them attractive to hackers [11], [12], [13]. Once the attacker interacts with these systems, they leave their footprint or trail, compared to a serial crime, meaning that hackers have unique behavior patterns for or against a cyber-attack. The two main constants of interest in criminology and now in computer security are the modus operandi and the signature, which reveal most information about the subject personality (hacker) [14]. On the other hand, the use of Machine Learning (ML) techniques as a tool with a wide range of applications in various fields to extract patterns and knowledge from data, likewise, able to perform the following operations with the same, classify and categorize, prediction and forecasting, sentiment analysis, fraud detection, computer vision, medicine and diagnostics, optimization and automation, among others. Therefore, ML has become a vital resource for effectively handling the new challenges of cybersecurity or computer security [15], [16], [17].

Therefore, to protect systems and information from cyber-attacks, combining several techniques and technologies, including implementing honeypots for data collection, ELK Stack for data analysis and visualization, and psychology of hackers and ML techniques, is necessary. This fusion allows us to analyze the behavior of hackers and elaborate preventive and corrective measures; that is why this research aims to evaluate the results of data collection, processing, and Analysis using ML to determine the cognitive patterns of hackers. For this, state-of-the-art Honeypots are first made, and it is also necessary to know about the personality of hackers. The rest of the article is organized as follows: Section 2 The Methodologies employed in the present research described. Section 3 discusses the results obtained; Section 4 discusses the main results, and finally, the conclusions and future work in this field.

State of the art

In this section, the use of honeypots in different investigations is equal to or similar to the field of study presented in this research. It also analyzes the most recent findings on the relationship between hackers' personalities and their behavior in cyberspace.

State of the art on Honeypots

It is important to note that the scientific production on the honeypot topic has been frequently addressed by researchers in the last decade because it is a technique widely used by information security managers to know the types of attacks a cyber attacker uses. In Figure 1, you will find publications from 2018 to 2023, where you will observe high and low peaks in certain years on the scientific production on this topic, a slight increase of publications in 2020, and, in the other years, a similar number of publications.

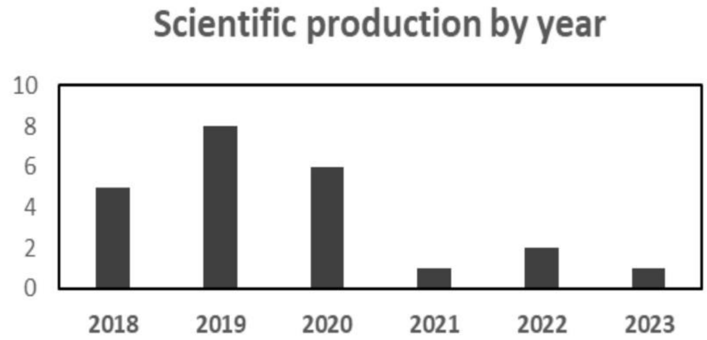

Figure 1 Primary studies, year of publications.

RQ01. What are the types of honeypots used in research?

There are honeypots [18] [19], high and low-interaction honeypots; the main difference is that high-interaction honeypots are more complex and expensive to implement. However, they provide a holistic and real view of the techniques and patterns used by attackers. In contrast, low-interaction honeypots are simpler and cheaper, which results in a less detailed view and can be easily detected by attackers [20], [21]. The selection for a high- or low-interaction Honeypot will depend on the needs [22], the objective, and the resources of the organization or research project. Table 1 compares these two technologies.

Table 1. A high and low interaction honeypot matching

LOW INTERACTION HONEYPOT	HIGH INTERACTION HONEYPOT
The attacker can detect it easily and quickly, which limits its efficiency.	Its detection is more difficult for the attacker, which translates into effectiveness in capturing and recording attacks and threats.
It requires the minimum investment of resources for its application and maintenance.	It requires a greater investment of resources and time for its implementation and maintenance.
It does not generate detailed data. That is, it provides an overview of the captured attacks.	Detailed and real data on attack methods and the tools used by the attackers.
It simulates a vulnerable system without allowing the attacker to develop his skills.	The attacker interacts with the system, leaving a record of the tactics and techniques used.
It can be deployed to existing operating systems and applications.	It requires a complete operating system environment and applications to be deployed.

Source: Author of the research, (Martínez C.2024)

T-Pot Honeypot is a honeypot hive; the main difference from other solutions of this type is the ability to emulate multiple services and operating systems, integrate with SIEM (Security Information and Event Management), install, and complete documentation. Below is a comparative table of some honeypots used in different research projects based on the bibliography consulted:

Table 2. Comparative table of the main Honeypots found in the literature.

HONEYPOT	INTERACTION	CUSTOMIZATION	INTEGRATION	VIRTUALIZATION	DIFFICULTY OF USE	INTEGRATION WITH SIEM
T-Pot Honeypot	High / Low	High	Yes	Yes	Medium	Yes

Honeyd	High	High	No	Yes	High	No
Dioneda	High	Medium	Yes	Yes	Medium	No
KFSensor	High	High	Yes	No	High	Yes
Glastopf	Low	Medium	No	Yes	Medium	No
Amun	Low	High	Yes	Yes	High	No

Source: Author of the research, (Martínez C.2024)

Table 3 presents the research works found, with information on the types of honeypots performed, the main objective, its contributions, limitations, and whether it uses a machine learning technique for the detection or intrusion of cyberattacks. It is important to highlight that most of the identified studies use high-interaction T-Pot because it is convenient for simulation in real services.

Table 3 Types, objectives, contribution, and Limitations of Honeypots

REFERENCE	YEAR	TITLE	HONEYPOT TYPE	PURPOSE	MACHINE LEARNING	CONTRIBUTION	LIMITATION
[23]	2018	Dynamic Honeypot Configuration for Intrusion Detection		Identify unauthorized access and network intruders.	N/A	Network activity and traffic can also be tracked through the dynamic honeypot configuration, which applies security to the protected network.	N/A
[24]	2018	Investigation of modern attacks using proxy honeypot		Implement a Honeypot on an open proxy server to identify patterns of offender behavior.	N/A	Records of user activity were collected, and then the respective Analysis was performed.	False positives in the identification of normal network traffic and network traffic under attack
[25]	2018	Hybrid System Between Anomaly-Based Detection System and Honeypot to Detect Zero-Day Attack		Protect your systems from a core exploit, the zero-day attack. The goal is to collect information from the attacker to prevent future attacks.	N/A	A hybrid model of anomaly-based detection and Honeypot are proposed as powerful mechanisms for zero-day detection.	Use Honeypot on the network.
[26]	2018	An SSH Honeypot Architecture Using Port Knocking and Intrusion Detection System	High-interaction	Obtain information about attacks on the SSH service and determine appropriate security	N/A	A Secure Shell (SSH) honeypot architecture using port knocking and Intrusion Detection (IDS), which combines port blocking and IDS	Ports 445 (SMB) and 23 (Telnet) are more vulnerable as they are only emulators.

REFERENCE	YEAR	TITLE	HONEYPOT TYPE	PURPOSE	MACHINE LEARNING	CONTRIBUTION	LIMITATION
				mechanisms to deal with attacks.			
[27]	2018	Honeypots That Bite Back: A Fuzzy Technique for Identifying and Inhibiting Fingerprinting Attacks on Low Interaction Honeypots	Low-interaction	They propose a fuzzy technique to correlate attack actions and predict the probability that an attack is a Fingerprint attack on the Honeypot.	N/A	The proposed fuzzy technique is used with any low-interaction honeypot to aid in the identification of the fingerprint attack as it is occurring.	It only works with low-interaction honeypots, which can be easily detected.
[28]	2019	Probabilistic Estimation of Honeypot Detection in the Internet of Things Environment	Medium-interaction	Analyzes techniques for detecting SSH and telnet honeypots.	N/A	Functional prototype, which allows the detection of honeypots with a certain degree of probability, with open-source implementation.	The use of additional methods in open-source implementation
[29]	2019	Multi-Platform Honeypot for the Generation of Cyber Threat Intelligence	Low-high interaction	Analyzes behaviors and deep learning methods to determine unknown threat patterns	N/A	Multi-honeypot platform	Consume resources and time
[30]	2019	A honeypot with machine learning-based Detection framework for defending IoT based botnet DDoS attacks	Combined	This article presents a honeypot that uses learning techniques for malware detection.	Yes	Honeypot-based solution for DDoS detection using real-time machine learning detection framework	Not applied in real environments
[31]	2019	A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure	Combined	This research aims to validate the honeypot's effectiveness and accuracy in a real traffic scenario for six months.		It implements the Conpot-based interactive ICS honeypot architecture.	Correct operation of the emulator
[22]	2019	Data Analytics Layer For high-interaction Honeypots	High-interaction	Integrating LibVMI with Volatility on a KVM, a Linux-	N/A	Detection mechanism for alerts when malware	High consumption of resources

REFERENCE	YEAR	TITLE	HONEYPOT TYPE	PURPOSE	MACHINE LEARNING	CONTRIBUTION	LIMITATION
				based hypervisor, to introspect the memory of virtual machines		attacks virtual machines.	
[32]	2019	HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design	Combined	A honeypot architecture called HoneyDOC is proposed.	N/A	It Leverages SDN technology and can be integrated into the versatile honeyDOC, which has three modules, Decoy, Captor, and Orchestrator, to support it.	Virtual environments
[33]	2019	The Security of Heterogeneous Systems based on Cluster High-interaction Hybrid Honeypot	High-interaction	Design a security system using the highly interactive Honeypot, which should comprehensively analyze attacks and threats.	N/A	N/A	N/A
[34]	2019	Automatic identification of honeypot server using machine learning techniques	High-interaction	This study looks for intelligent techniques to automatically check remotely if the server is running the honeypot service.	Yes	An automatic identification model based on the random forest algorithm with three features: application layer, network layer, and system layer.	Simulated environments
[35]	2020	Using Global Honeypot Networks to Detect Targeted ICS Attacks	High-interaction	It is demonstrated that a network of Internet-connected honeypots can be used to identify and profile targeted ICS attacks.	N/A	Common ICS protocols such as S7comm and Modbus	Bridging the gaps between ICS-aware and IoT-aware hosts
[36]	2020	Implementation of an insider threat detection system using honeypot-based sensors and threat analytics	Combined	The monitoring system functions to detect possible infiltration and discard false positives.	Yes	Proposes a new technique for insider detection using encrypted honeypots	Limited-form honeypot sensors
[37]	2020	HONEYDOS: a hybrid approach using data mining and Honeypot to counter	Low-interaction	An empirical comparison of the hybrid approach with previous methods used to	Yes	Support Vector Machine technique based on Honeypot and Data Mining,	HoneyDos is extremely elementary

REFERENCE	YEAR	TITLE	HONEYPOT TYPE	PURPOSE	MACHINE LEARNING	CONTRIBUTION	LIMITATION
		denial of service attacks and malicious packets		prevent denial of service attacks.			
[38]	2020	An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks	medium-high interaction	Analyze vulnerability CVE-2017-17215 exploited by large-scale botnets	N/A	A medium-high interaction honeypot was implemented to interact with SOAP services.	In the honeynet, system intelligence and automation require further reinforcement and eficiency.
[11]	2020	The Use of Honeypot in Machine Learning Based on Malware Detection: A Review	Combined	Use of Honeypot in machine learning to detect malware	Yes	N/A	N/A
[39]	2020	Enhanced attack blocking in IoT environments: Engaging honeypots and machine learning in SDN OpenFlow switches	Combined	Attack blocking to defend against unknown malicious attacks	Yes	Honeypot in each of the OF switchgear.	N/A
[40]	2021	Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis	Low-interaction	Detect the types of password attacks (brute force attack, dictionary attack, and social engineering) on real systems using Cowrie.	Yes	Production Honeypot or Research Honeypot	Passwords
[12]	2022	Semi-supervised approach for detecting distributed denial of service in SD-honeypot network environment	Combined	Detect attacks employing semi-supervised learning; for their classification, a combination of the pseudo-labeling model (Support Vector Machine (SVM) algorithm) and the Adaptive	Yes	Integration method between the honeypot sensor and the software-defined network (SDN) (SD-honeypot).	Packet loss/prediction occurred during the attack,

REFERENCE	YEAR	TITLE	HONEYPOT TYPE	PURPOSE	MACHINE LEARNING	CONTRIBUTION	LIMITATION
				Boosting method was used.			
[41]	2022	Predicting Attack Patterns via Machine Learning by Exploiting Stateful Firewall as Virtual Network Function in an SDN Network	Combined	Predict the susceptible host, which is extremely likely to be assaulted in the SDNFV network with distributed drivers.	Yes	Software-defined network function virtualization (SDNFV) network to improve network performance	Decrease in prediction accuracy with an increasing threshold.
[42]	2022	Threat prediction using Honeypot and machine learning	High-interaction	Configuration of honeypots in a cloud service and using machine learning algorithms to predict the type of threat detected in the honeypots.	Yes	Real-time Honeynet system using Machine learning using Apache Web Server, MYSQL, FTP, and SMTP system services.	Network system isolation
[43]	2022	A Passive OS-Fingerprinting framework using Honeypot	Combined	Identify network system vulnerabilities, as well as the ability to counter attacks by identifying your SO	N/A	Proposes a comprehensive OS passive fingerprinting framework counter-attacks on networked systems	Selection of countermeasures
[44]	2022	HoneyModels: Machine Learning Honeypots	medium-high interaction	It is a study of alternative honeypot-inspired approaches to detecting adversaries.	Yes	HoneyModels: Machine Learning Honeypots that detect adverse use of Machine Learning models	Keys with characteristics to be altered
[45]	2024	Integrating Machine Learning-Powered Smart Agents into Cyber Honeypots: Enhancing Security Frameworks	Combined	To monitor, identify, and analyze malicious activities by attracting potential attackers.	Yes	Enhances traditional honeypot systems by proactively predicting and mitigating future attacks through machine learning integration.	The available excerpts do not detail the specific limitations. To identify them, you must read the full article again.

Source: Author of the research, (Martínez C.2024)

RQ02. What are the study objectives of a honeypot?

The objectives agreed upon by researchers in different studies have been the detection and Analysis of attackers to the systems among them: Suleiman A. exposes that the purpose of his study is the identification of vulnerabilities of network systems and their ability to counter such attacks[44], in the same way [43], his approach is to predict susceptible hosts that will be assaulted by SDNFV mechanism that have distributed controllers. In addition, many studies agree on configuring and blocking honeypots with Machine learning to predict attack mechanisms, threats, and intrusion detection of cyber attackers [39] [40] [12] [41] [42] [43]. On the other hand, [11] focused their research on medium-high interaction honeypots to perform their Analysis of vulnerability CVE-2017-17215, which is exploited by botnets on a large scale [22] [32] [17] [34]. In the information collected, several authors' research objectives have been the design, architecture, and models that can be used to identify and profile attacks.

RQ03. What is the contribution of researchers to the detection of cyber-attacks?

Table 4 shows the different contributions that could be found in different studies in response to our research question (RQ3); among them are [7] and [24]. Their contribution focuses on the fact that while the cyber attacker is active within the network, the work of dynamic honeypots is to track and receive all their records, information, and types of attacks and then analyze and apply solutions to prevent a future attack. There are also several studies whose contributions are based on models, techniques, architectures, prototypes, platforms, methodologies, and algorithms combined with deep learning methods to determine the patterns of threats, attacks, vulnerabilities, and malware [9]-[16].

RQ04. What are the limitations of each research when using a honeypot as a decoy?

Regarding the limitations, in some cases, we found that they were applied in virtual environments. For example, [42], its objective was to predict the susceptible host, which in turn is extremely likely to be assaulted in the SDNFV network with distributed controllers, presenting its contribution to the application of a software-defined network functions virtualization network (SDNFV) to improve network performance, presenting its main limitation the decrease of the prediction accuracy with the increase of the threshold of false positives. Likewise, no solutions exist for applying Machine Learning techniques in the addressed subject.

The field of scientific research on the implementation of honeypots applied to computer security has evolved and grown in recent years. Among the most used techniques are the deployment techniques. We now have high-interaction honeypots that have proven more effective and realistic when deployed in network environments. Integration with security systems in such a way that honeypot alerts are interpreted by existing security systems such as Firewalls, IDS, IPS, and WAF. Attack analysis: Although most studies are still based on statistics for data analysis, there is research that applies Machine Learning techniques to improve results and decipher patterns that can be studied or inferred from them.

State-of-the-art cybercriminal personality

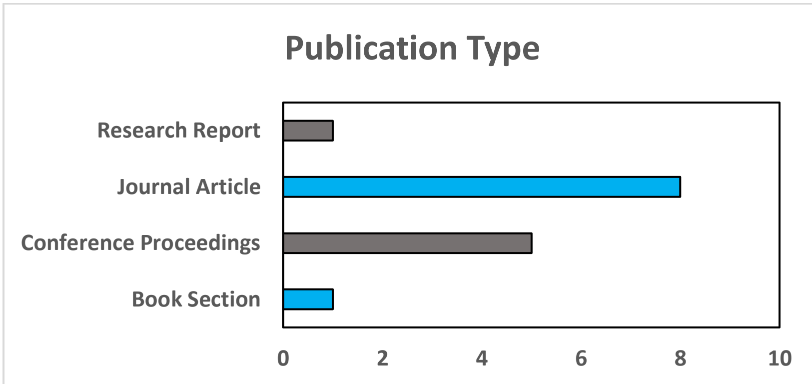

Figure 2. Primary studies, types of publication.

The scientific production on the personality of hackers or cybercriminals is not a very crowded topic by researchers; as seen in Figure 3, we found one publication in 2018, a slight increase of publications in 2020, and a similar number of publications in other years.

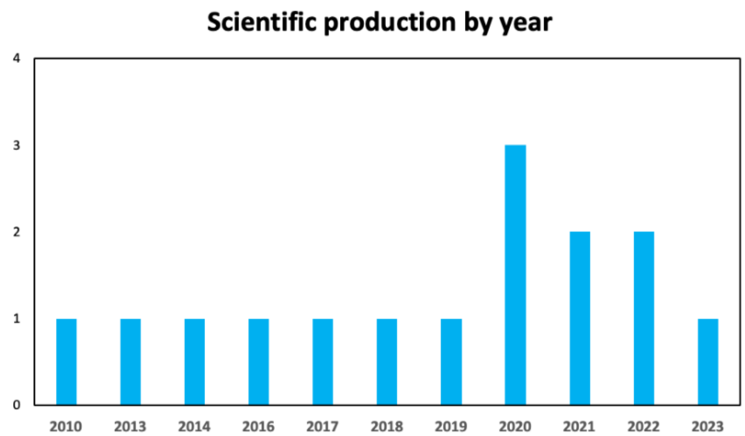

Figure 3. Primary studies, year of publications.

Results

RQ01. What are the methodologies used in the research conducted in this field?

Regarding scientific production in 2010 [46], a group of scientists interested in the subject conducted a quantitative study by applying a survey validated by experts. On the other hand, Summers et al. [47] conducted qualitative research based on Grounded Theory with a semi-structured interview with 18 hackers from a hacking community. In comparison, the other studies employed quantitative descriptive and analytical methodologies. Literature reviews were also included due to the scarcity of studies in this area, as shown in Table 4.

Table 4 Methods, Instruments, and Personality Classification of Hackers or Cybercriminals

REF	YEAR	TYPE	STUDY TYPE	TITLE	INSTRUMENT	SCALE	STUDY POPULATION	PERSONALITY CLASSIFICATION	HACKER MOTIVATION
[46]	2010	Journal Article	Quantitative	The Risk Propensity and Rationality of Computer Hackers	Itself Validated by experts	Regression Models	ShamooCon hacker convention	- Strong preference for rational decision-making processes - Pronounced risk propensity	N/A
[47]	2013	Research Report	Qualitative	How Hackers Think: A Study of Cybersecurity Experts and Their Mental Models	Semi-Structured interviews/open-ended questions	Grounded Theory /Triangulation	Members of the hacking community (18)	The hackers are Strategists (Patterning and Mental Logic), Comparative Analysis, and Understand their Adversaries.	N/A
[9]	2014	Book Section	Review	The Psychology of Computer Criminals	N/A	N/A	N/A	- The novice criminals - The students are electronic voyeurs - The tourists -The crashers - The Thieves	Addiction, curiosity, boredom, power, recognition, and politics//By dreed, revenge, problem resolution, and ego gratification
[48]	2016	Journal Article	Quantitative	Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits	Big five personality traits	Likert Scale	Six hacker subjects	-Hat white -Hat black	Hacking activity
[49]	2017	Journal Article	Analytical	Computer criminal behavior is related to psychopathy and other antisocial behavior	Elemental Psychopathy Assessment-Short Form (EPA-SF)	Likert Scale	250 Internet users	- Antagonism - Emotional Stability - Disinhibition - Narcissism	Intellectual curiosity

REF	YEAR	TYPE	STUDY TYPE	TITLE	INSTRUMENT	SCALE	STUDY POPULATION	PERSONALITY CLASSIFICATION	HACKER MOTIVATION
[50]	2018	Journal Article	Analytical	Human resources and their tendency to information security crimes based on Holland's theory	John Holland's Theory of Career Choice (RIASEC)	Statistical Analysis	N/A	- Realistic - Investigative - Artistic - Social - Enterprising - Conventional	N/A
[51]	2019	Conference Proceedings	Analytical	Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling	The FBI's criminal profiling framework	Descriptive Statistics	83 cybercriminals	N/A	Revenge, Exposure, Hacktivism, Ego, Monetary gain, Entertainment, , Extortion and exploitation, blackmail, Sabotage, Espionage
[52]	2020	Conference Proceedings	Analytical correlational study	Psychological Profiling of Hacking Potential	Dark Triad and the Capability, Motive, and Opportunity (CMO)	The average variance extracted (AVE)	474 computer science students	- White Hat (Machiavellianism, Narcissism, Psychopathy, and Thrill-Seeking) - Grey Hat (Opposition to Authority, Machiavellianism, and Psychopathy) - Black Hat Results (Thrill Seeking, Machiavellianism, Psychopathy)	Seeking, Revenge, Ideology, Fun, Thrills, Survival, Notoriety, Recreation, and Profit
[53]	2020	Conference Proceedings	Review	Measuring Psychosocial and Behavioral Factors Improves Attack Potential Estimates	Five-Factor Theory (FFT) model	N/A	N/A	- Agreeableness - Extraversion - Conscientiousness - Neuroticism - Openness to experiences	Political, Personal (Personal satisfaction, a feeling of accomplishment, boredom, competition), Social/Cultural, Philosophical/Theological
[54]	2020	Conference Proceedings	Review	Predicting personality from patterns of behavior	Big five personality traits	Descriptive Statistics	743 Volunteers	N/A	N/A

REF	YEAR	TYPE	STUDY TYPE	TITLE	INSTRUMENT	SCALE	STUDY POPULATION	PERSONALITY CLASSIFICATION	HACKER MOTIVATION
				collected with smartphones					
[55]	2021	Journal Article	Review	Profiling the Cybercriminal: A systematic review of research	N/A	Data collection process and data items	N/A	-White hat - Black hat - Gray hat	Ethics /malicious or ethical political views, cultural/religious beliefs, or terrorist ideology carding forums
[56]	2021	Journal Article	Analytical	Network discovery and scanning strategies and the Dark Triad	Building on Trait Activation Theory,	Mimicry Deception Theory Scale	268 f university students and Mechanical Turk	Dark triad	narcissism and psychopathy
[57]	2022	Journal Article	Review	Are you anonymous? Social-psychological processes of hacking groups	N/A	psychological research	N/A	-criminals -cyber warriors -hacktivists-insiders - coders	ideology, prestige, recreation, and revenge
[58]	2022	Conference Proceedings	Review	The Amorphous Nature of Hackers: An Exploratory Study	Hacker Perception Questionnaire	Neuroticism-Extraversion-Openness Inventory (NEO)	135 university students	-White hacker -Black hacker -Gray hacker	Hacking in the service of safety and/or justice Hacking is never okay. Hacking, when used to apprehend criminals
[59]	2023	Journal Article	Analytical description	Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets	Sample of respondents	HEXACO-PI-R questionnaire	928 individuals	Cyber offenders	ideology, prestige, recreation, and revenge

Source: Author of the research, (Martínez C.2024)

RQ02. What are the tools used to determine the personality of Cybercriminals?

The main instrument used in the different studies is An FBI criminal profiling framework [51]. On the other hand, most studies use the Big Five Personality Traits test [48], [51], [53], [54], composed of 132 items. Al-Ajilouni [50] The instrument used was John Holland's Career Choice Theory (RIASEC), which has 66 items. Normally, it serves to choose a specific career or profession. However, it also measures a set of elements and traits that constitute the personality, as in the research of Seigfried-Spellar et al. [49]. The Elementary Psychopathy Assessment (EPA), a 178-item self-report measure designed to assess the basic elements of psychopathy, was applied.

RQ03. What is the population to which the instrument has been applied?

Bachmann [47], at the ShammonCon hackers' annual convention. At the same time, they applied it to a population belonging to network professionals and hackers selected according to the researcher's criteria. Likewise, Matulessy et al. [48] used six hackers for their research. Seigfried-Spellar et al. [49] conducted their study on 250 Internet users who may or may not be considered hackers. In [51], the personality traits of 83 cybercriminals held in a prison in South Korea are evaluated. Consequently, in the research [52], [54], [56], [59], they measure the potential profile of cyber attackers in students of some technical careers and individuals in general.

RQ04. What is the classification of cybercriminal personality proposed by researchers based on the results of studies?

Once the different instruments have been applied to determine the personality of hackers or cybercriminals, researchers propose various classifications based on personality characteristics. However, it is necessary to avoid the repetition of the classification: White hacker, Black hacker, and Gray hacker [48], [52], [55], [58].

RQ05. What are the main motivations of cybercriminals?

Figure 4 shows that cybercriminals' main motivations include revenge, boredom, ideology, ego, sabotage, espionage, gratification, and blackmail.

Figure 4. Word diagram of the motivation of cybercriminals.

Once reviewing the field of hacker personality, it can be seen that it is currently being studied in various areas of knowledge, such as psychology, computer security, and criminology. However, it is important to emphasize that having a single or stereotypical profile that characterizes all hackers is impossible because they have different motivations and characteristics. In this sense, the personality of a hacker can evolve or, in turn, be influenced by contextual and social factors. Among the aspects to highlight is that hackers have a high technical capacity, i.e., skills in programming, computer networks, and operating systems. This is complemented by curiosity and thirst for knowledge, making them self-taught and motivated by intellectual challenge.

Hackers are owners of creative, divergent thinking, so they ingeniously see things from different perspectives, allowing effective solutions to overcome technical or security barriers. Their motivations are varied, ranging from financial gain, recognition, curiosity, activism, or desire to cause harm. They demonstrate low tolerance for authority or established norms, and some hackers may even experience intense emotions such as excitement or adrenaline when carrying out computer attacks. Finally, it can be analyzed that it has been difficult to have a population or sample directed to a single type of hacker; in this sense, researchers have sought ways to obtain data for further Analysis, from the inquiry of forums or hacker communities to people dedicated or related to technology. On the other hand, the instruments used have been developed in psychology and are suitable for identifying behavioral patterns in hackers; the instrument that has been able to classify the personality and extrapolate to white, gray, and black hat hackers has been the BIG FIVE model.

Big Five or Big Five Personality Traits is a widely accepted model in psychology that describes five main dimensions of human personality: Openness to experience; this trait is marked by an openness to explore and accept new ideas, experiences, and emotions; these people are imaginative, curious, creative and open to change; Responsibility related to organization, these people are very responsible, disciplined, follow through on commitments and are very orderly; Extroversion is the degree to which a person seeks stimulation and the company of others, they are sociable, energetic, assertive and like to be surrounded by more people; Kindness, they have kind attitudes towards others, are empathetic, cooperative, considerate and have a positive disposition; Neuroticism which is the degree to which a person experiences negative emotions, anxiety, emotional instability or tendencies to worry, to develop stress and sadness.

Table 5. Big Five Personality Traits

REFERENCE	MOTIVATION	DEFINITION	MESSAGE	JUSTIFY
Oxford Dictionary [9], [59]	Hacktivism Or Political	Hacktivism is defined as carrying out acts, usually malicious, on the Internet to promote political, religious, or social ideas. Hacktivists use electronic devices to carry out actions or attacks in cyberspace to propagate and defend specific ideals or values.	Loved By Linda Long Life vietnam | Moroccan Revolution	The hacker leaves a message about a social, political, or religious problem.
Oxford Dictionary [9], [49]	Ego	A person's sense of self-esteem or self-importance.	LapanWasTaken Here Whoopsss...Got Hacked	They leave messages to show capabilities and

REFERENCE	MOTIVATION	DEFINITION	MESSAGE	JUSTIFY
				certain talents that differentiate them from others and for which they stand out.
Oxford Dictionary [9], [51], [58], [59]	Revenge	The action of inflicting hurt or harm on someone for an injury or wrong suffered at their hands.	hacked by Salim Alk, ohh, sorry your security is gay	The hacker leaves a message with his identifier, usually a phrase making fun of the hacked site's security.
Oxford Dictionary [49], [59]	Entertainment	The action of providing or being provided with amusement or enjoyment.	Hacked by Phenix-TN Just for fun, HAHAHAHHA! ANYTIME I LIKE TO LOL, THANKS TO IMAM	A hacker who performs cyberattacks just for fun
[9], [52], [60]	Monetary	Connected with money	Hacked By Babacang07 - PhantomSec1337, icq: Gh05t11n6,telegram: Flavyy7	The only interest is for monetary gain, and he leaves his data to be contacted for data recovery or security patches.
Oxford Dictionary [9], [52], [53]	boredom	Feel weary because one is unoccupied or lacks interest in one's current activity.	Hacked By Ahd, Hacked By Ahd, This world is bad	A hacker who performs cyber-attacks to pass the time and be engaged in some activity other than boredom.
Oxford Dictionary /Google [8], [9], [47], [52], [57]	Recognition	To be recognized for an act or action that has been performed involves a great sacrifice of either intelligence or time.	Hacked by Mr.kro0oz.305	He wants to be recognized as the one who attacked the system, leaving a basic message of his Nickname.

Source: Author of the research, (Martínez C.2024)

Methodology Research

In the present research, it was necessary to divide the work into three phases: In the first phase, a T-Pot honeypot server implemented in the infrastructure of Escuela Superior Politécnica del Chimborazo and the Ecuadorian Corporation for the Development of Research, and the Academy of Ecuador CEDIA provided the bandwidth [10]. Afterward, a survey was developed based on Big Five personality traits, consisting of 132 questions related to personality and seven questions associated with the data obtained by the Honeypot; the survey was shared on the same sites in which the IP address of the T-Pot, as mentioned earlier. We proceeded to unify the database arranged in 18 columns by 500 rows, including the type of attack, tool, OS, IP, hacker personality, Nickname, and message, among other characteristics.

Subsequently, ML was applied to analyze the hacking patterns; for this, it was necessary to normalize the data in a language understandable by Python. The parameters used were (Tool Attack, IP address, Country, and Time) and neural Network Architecture used after reading and processing the data. The data was divided into four sets: 80% for training and 20% for testing. Likewise, to improve the results obtained from the previous model, the tree method (RANDOM FOREST) was used; here, the algorithm had 50 predictors. On the other hand, the following fields were used to evaluate correlation patterns between personality tests and cyberattacks (Personality, Train, Motivation, Country, Tool, Time).

Results

Data modeling

The following data were used for this process,

Table 6. Research parameters

Parameters	type of parameters
Tool Attack	Categorical or class
IP address	Integer
Country	Categorical or class
Time	Entero

Source: Author of the research, (Martínez C.2024)

The parameter to be classified is based on the type of attack, which is also considered category or class. A histogram of the existing data is made for categorical data, and the files are stored with the unique names in each field. For example, from the database for the Country parameter, the following is obtained:

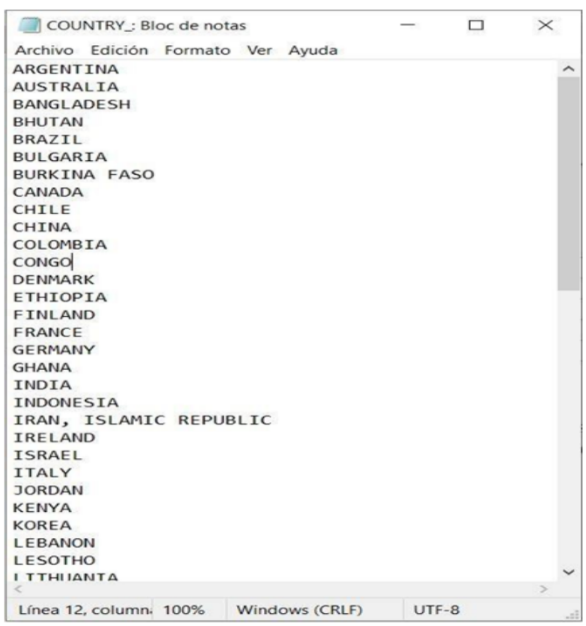
COUNTRY_: Bloc de notas
Archivo Edición Formato Ver Ayuda
ARGENTINA
AUSTRALIA
BANGLADESH
BHUTAN
BRAZIL
BULGARIA
BURKINA FASO
CANADA
CHILE
CHINA
COLOMBIA
CONGO
DENMARK
ETHIOPIA
FINLAND
FRANCE
GERMANY
GHANA
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC
IRELAND
ISRAEL
ITALY
JORDAN
KENYA
KOREA
LEBANON
LESOTHO
Línea 12, column 100% Windows (CRLF) UTF-8

Figure 5. Classifier parameter country

The parameter related to the IP address had to be converted to an integer value in order to have manageability with the data at the time of classification, as well as with the parameter time in hours, minutes and seconds. In addition, according to the data, there are 7 different types of attacks. According to the values taken by the IP Address, Country, Time and Attack Tool, the system should be able to predict what type of attack the server may suffer. The data are extracted from files with CSV extension, previously saved for each type using the PANDAS library in Python as can be seen in the following link: https://colab.research.google.com/drive/1bz__2YK1MJOZrSRXBQb3h-wdFaXxiEfI?usp=sharing

At this point, the performance metrics were defined to evaluate the machine learning algorithm implemented in this research is a neural network or Artificial Neural Networks (ANN). For which the confusion matrix is composed of prediction data (non-hacked data) and real data (hacked data), in this table for its classification are used logical values of 0 as negative and 1 as positive, where it is sought to facilitate the language as values of a "No and a Yes". Each of these applications is assigned a defined vector, which contains the information of the permissions and the classification labels.

Table 7. Structure of the confusion matrix

	REAL	
PREDICTION	DP	FN
	FP	DN

Source: Author of the research, (Martínez C.2024)

False positive (FP) are values that represent a yes, but in reality, is a no.

False negative (FN) values that represent a no, but in reality, is a yes.

Positive data (PD) values that represent a yes.

Negative data (ND) values that represent a no.

Four evaluation metrics Loss, Accuracy, Recall, Accuracy and F1 Score were used to evaluate the classification performance of the problem, which are defined as follows:

Loss is a penalty for misclassification. The Loss function to be used is binary crossentropy which is defined by the following formula.

$$y_{i,l} \in \{0,1\} \wedge l \in [1, L) \wedge i \in [1, N) \text{ Equation 1}$$

$$\text{binary crossentropy} = -\left(y_{i,l} * \ln(\hat{y}_{i,l}) + (1 - y_{i,l}) * \ln(1 - \hat{y}_{i,l})\right) \text{Equation2}$$

Accuracy this metric is calculated from the number of correctly classified values.

$$\text{Accuracy} = \frac{DP+DN}{DP+DN+FP+FN} \qquad \text{Equation 3}$$

Recall metric is calculated from correctly predicted positive data, over the total positive data plus the test set.

$$Recall = \frac{DP}{DP + FN}$$

Equation 4

Accuracy is calculated from correctly predicted positive data over total predicted positive data.

$$\text{Precisión} = \frac{DP}{DP + FP}$$

Equation 5

F1 Score is interpreted as the harmonic measure between accuracy and Racall, where F1 shows the best score and the worst score.

$$\text{F1 Score} = 2 + \frac{Precisión * Recall}{Precisión + Recall}$$

Equation 6

To improve the accuracy, Random Forests will be used, its representation is usually f_t (x)=f(x,θ) Equation 7, the whole forest is denoted by the form F={f_1..........f_T Equation 8, where T is the number of trees in the forest, with the following formula representing the probability of prediction of class k

$$p\,{}^{k}/_{x} = \frac{1}{T}\sum_{t=1}^{T} p_t\,{}^{k}/_{x}$$ Equation 9

Where $p_t\,{}^{k}/_{x}$ is the estimated density of data classification levels. The final functional is defined as

C(x)= arg max P${}^{k}/_{x}$ Equation 10
k∈ ϒ

As mentioned above, to develop the neural network architecture it was necessary to divide the data into four sets with the criterion of 80% of the data for training and 20% for testing. Also, the TENSORFLOW library was used, for this case the input layer must have 4 neurons, one for each parameter and 7 neurons in the output layer, each one will identify a type of attack, this model has two hidden layers to improve the results. The network architecture is presented in Fig. 6, which has been made using the playground_tensorflow tool.

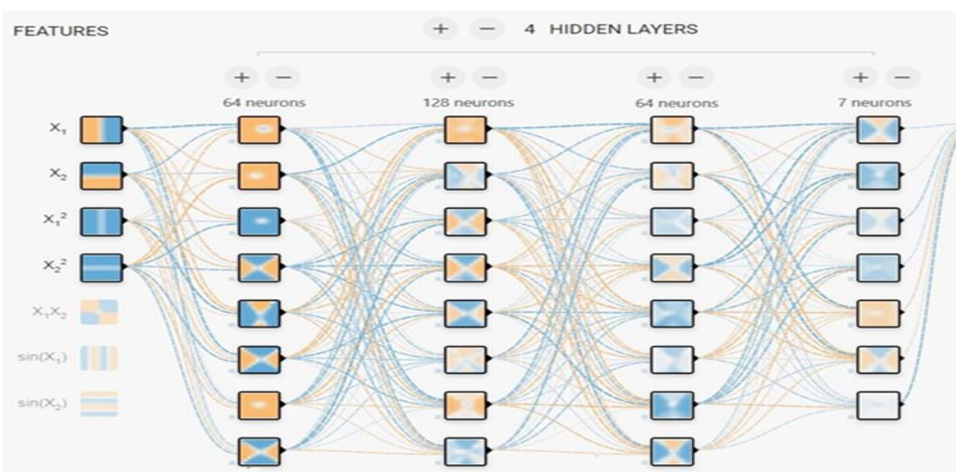

Figure 6. Architecture of the Neuroanl Network using a Sequential Model

On the other hand, the optimized RMSPROP was selected, the error known as the LOSS metric with the use of categorical cross-entropy and finally the metric to be evaluated is the accuracy (ACCURACY). The training process ran 100 epochs with a Batch of 16 data for each epoch, as the epochs pass it is expected that both the training error and the validation will decrease. For the evaluation of the model fit of the data, the confusion matrix was used to estimate the error at the time of classification, using the SEABORN library as shown in Figure 7.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	0.93	1.00	0.96	41
COMMAND INJECTION	1.00	1.00	1.00	31.00
CROSS-SITE SCRIPTING (XSS)	1.00	1.00	1.00	47.00
DDOS ATTACK	1.00	1.00	1.00	157.00
DEFACEMENT	1.00	1.00	1.00	25.00
SQL INJECTION	1.00	1.00	1.00	79.00
THE MAN IN THE MIDDLE	1.00	0.85	0.92	20.00
Accuracy			0.99	400
Macro avg	0.99	0.98	0.98	400
Weighted avg	0.99	0.99	0.99	400

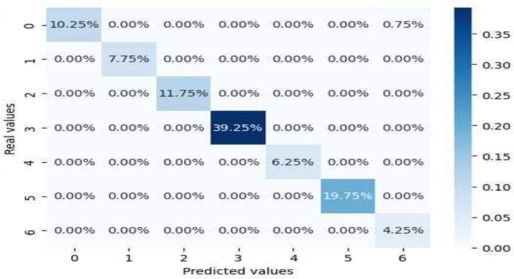

Figure 7. Matrix with the training data that the model already knew.

After that, the results are generally in line with expectations, but there is a problem in class four. One of the ways to evaluate the fit of the model to the data is to pay attention to the distribution of the observations using the density estimation by a KDE Kernel, as shown in the following plot.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	0.91	1.00	0.95	10
COMMAND INJECTION	1.00	1.00	1.00	5
CROSS-SITE SCRIPTING (XSS)	1.00	1.00	1.00	12
DDOS ATTACK	1.00	1.00	1.00	38
DEFACEMENT	0.67	1.00	0.80	2
SQL INJECTION	1.00	1.00	1.00	25
THE MAN IN THE MIDDLE	1.00	0.75	0.86	8
Accuracy			0.98	100
Macro avg	0.94	0.96	0.94	100
Weighted avg	0.98	0.98	0.98	100

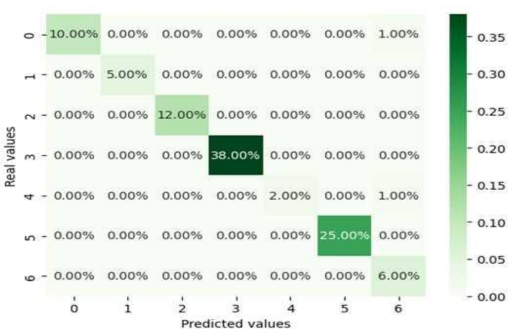

Figure 8. Matrix with training data not known to the model.

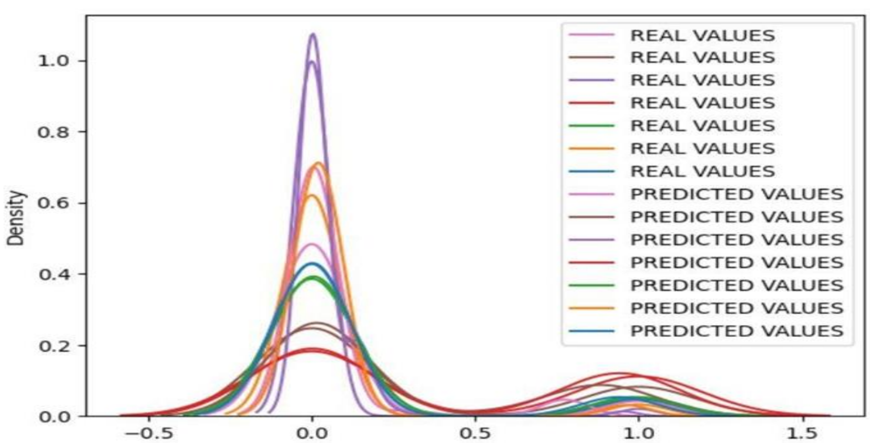

Figure 9. Density of model-predicted observations matched to actual observations. s.

To improve the results obtained with the previous architecture, we proceeded to use the RANDOM FOREST algorithm, in the same way, the data were normalized and divided into training and test sets. Moreover, for this problem it was used with 50 predictors. The prediction with the set that is already known is shown in the following chart.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	1.00	1.00	1.00	10
COMMAND INJECTION	1.00	1.00	1.00	5
CROSS-SITE SCRIPTING (XSS)	1.00	1.00	1.00	12
DDOS ATTACK	1.00	1.00	1.00	38
DEFACEMENT	1.00	1.00	0.80	2
SQL INJECTION	1.00	1.00	1.00	25
THE MAN IN THE MIDDLE	1.00	1.00	1.00	8
Accuracy			1.00	400
Macro avg	1.00	1.00	1.00	400
Weighted avg	1.00	1.00	1.00	400

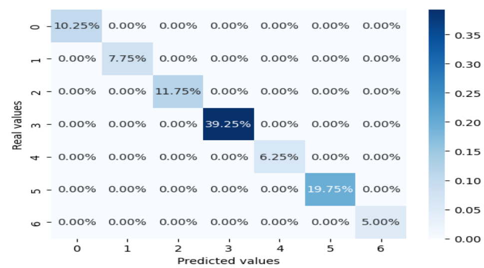

Figure 10. Matrix showing that the model differentiates all attack classes correctly with known data.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	0.91	1.00	0.95	10
COMMAND INJECTION	1.00	1.00	1.00	5
CROSS-SITE SCRIPTING (XSS)	1.00	1.00	1.00	12
DDOS ATTACK	1.00	1.00	1.00	38
DEFACEMENT	0.67	1.00	0.80	2
SQL INJECTION	1.00	1.00	1.00	25
THE MAN IN THE MIDDLE	1.00	0.75	0.86	8
Accuracy			0.98	100
Macro avg	0.94	0.96	0.94	100
Weighted avg	0.98	0.98	0.98	100

Figure 11. Matrix showing that the model differentiates all attack classes correctly with unknown data.

The system improves the results obtained previously, but with the unknown data it still maintains the error in differentiating class four. The decision tree is formed as follows

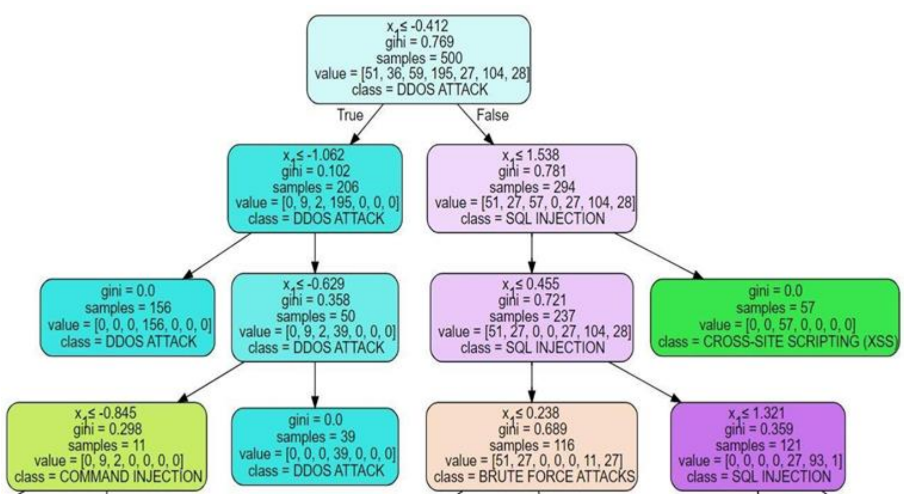

Figure 12. Classification decision tree

With regard to testing whether or not there is a relationship between the personality of the hackers or cybercriminals and the attacks carried out, the procedures described above are applied; the fields used are shown below in Table 8

Table 8. Type of parameters

Parameters	Type of parameters
Personality	Categorical or class
Trait	Categorical or class
Motivation	Categorical or class
Country	Categorical or class
Tool	Categorical or class
Time	Integer

Source: Author of the research, (Martínez C.2024)

In the same way, the corresponding histograms were obtained for each parameter, once the data was loaded, we proceeded to evaluate the correlation matrix between the indicated parameters. There is a multicorrelation between the parameters, six parameters are available for the case, the model is defined by 250 predictors, the following graph shows the results.

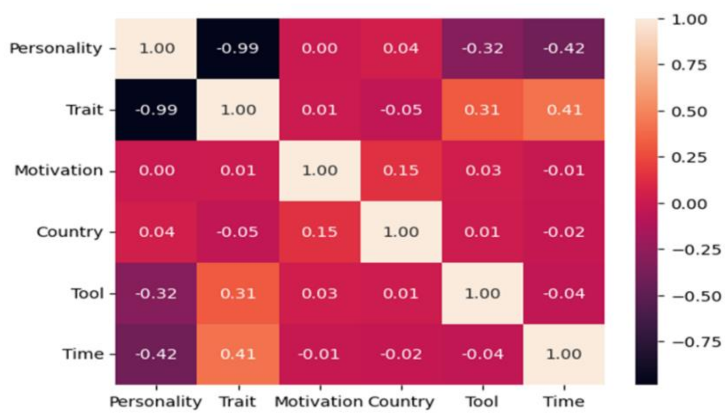

Figure 13. Multicorrelation between hackers' personality data

In this case, the model results in expected values to classify the seven types of attacks defined in this study, depending on certain personality traits and characteristics such as country or time of attack.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	1.00	1.00	1.00	41
COMMAND INJECTION	1.00	1.00	1.00	31
CROSS-SITE SCRIPTING (XSS)	1.00	1.00	1.00	47
DDOS ATTACK	1.00	1.00	1.00	157
DEFACEMENT	1.00	1.00	1.00	25
SQL INJECTION	1.00	1.00	1.00	79
THE MAN IN THE MIDDLE	1.00	1.00	1.00	20
Accuracy			1.00	400
Macro avg	1.00	1.00	1.00	400
Weighted avg	1.00	1.00	1.00	400

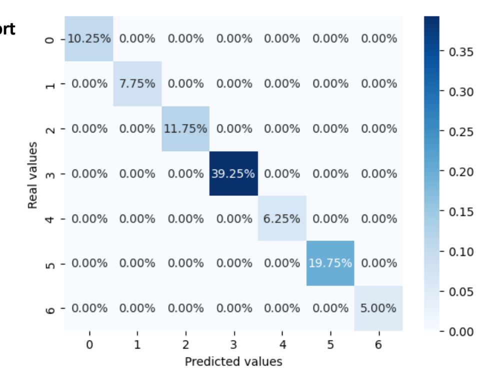

Figure 14. Matrix with the personality test data known to the model.

	Precision	Recall	F1-score	Support
BRUTE FORCE ATTACKS	0.90	0.82	0.86	11
COMMAND INJECTION	0.80	0.80	0.80	5
CROSS-SITE SCRIPTING (XSS)	1.00	0.92	0.96	13
DDOS ATTACK	1.00	1.00	1.00	38
DEFACEMENT	0.50	0.50	0.50	2
SQL INJECTION	0.96	0.92	0.94	26
THE MAN IN THE MIDDLE	0.62	1.00	0.77	5
Accuracy			1.00	100
Macro avg	1.00	1.00	1.00	100
Weighted avg	1.00	1.00	1.00	100

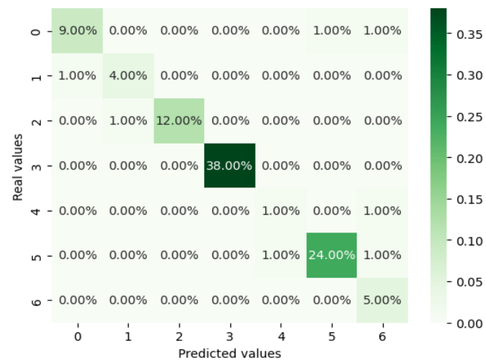

Figure 15. Matrix with the personality test data that the model does not know.

When evaluating the model, a distribution of the observations is observed by estimating the density by a KDE Kernel, it fits the data correctly with the predictions of the ML model, this is observed in Figure 16.

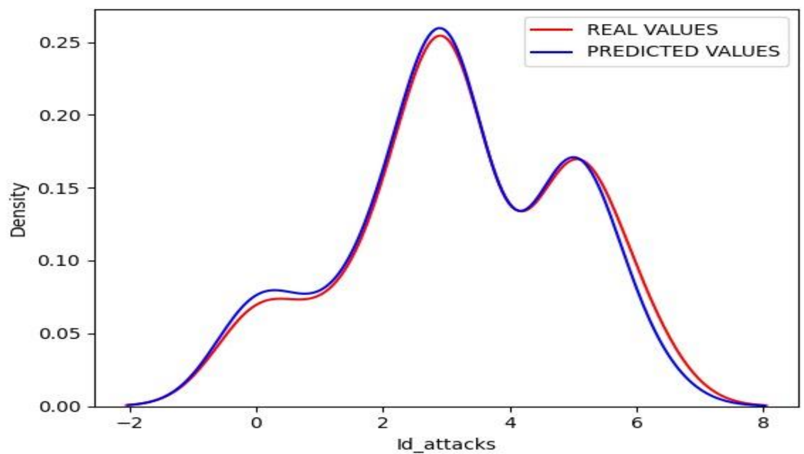

Figure 16. Density of observations predicted by the model matched to the actual observations of the hacker patterns.

Conclusion and Future Work

Regarding the classification of cognitive patterns acquired through Honeypots and ML algorithms for their processing, it is a new field that provides valuable information to understand better how cyber attackers or hackers operate and develop more effective countermeasures. The findings of this research can be shared with the cybersecurity community to develop advanced models that can identify patterns in real-time and mitigate them immediately or implement more effective security measures.

It is necessary to develop instruments (psychological tests) aimed at hackers to have better results in future research and, likewise, to delimit a study population or sample, thus avoiding the bias generated by applying the measurement instrument in hacker forums or sites. Currently, no single personality profile describes all hackers; common traits have been investigated, such as different motivations, which can be criminal, political, personal, or criminal situations; this tells us that we should not stereotype all hackers.

It also generates a process for automatically cleaning and constructing data from the patterns left by hackers in servers or honeypots. This will increase the database, which will allow for more accurate results by applying ML algorithms for processing, classification, and predictions.

ML algorithms, such as Neural Networks using a sequential model and Random Forest using 150 predictors, fit adequately to the training and test data as presented in Fig. 18. In the first analysis, the input parameters Country, Tool, IP, and Time have been used to model the seven types of attacks described. When evaluating the Neural Network with the training data, an average F1-score of 99% is obtained, where the lowest value obtained F1-score is 92% for the class 'THE MAN IN THE MIDDLE.' While with test data unknown to the Network, a 98% average F1-score is obtained, with the lowest value of 80% for the class 'DEFACEMENT.' Compared to Random Forest, the mean F1-score is 100% with training data, while it is 98% with test data. The lowest value obtained is 80% for the 'DEFACEMENT' class. The densities for these predictions are presented in Fig. 11. Comparing the performance of the two algorithms for the training data, Random Forest outperforms the Neural Network by 2%. In contrast, for the test data, the performance is similar.

For the second analysis, the input parameters Personality, Trait, Motivation, Country, Tool, and Time were used to model the seven types of attacks described based on the personality characteristics associated with the hacker. Since, in the previous case, Random Forest performed better, this algorithm was used with 250 predictors for the model. The average F1-score obtained is 100% for the training data, while 93% is obtained for the test data. The lowest value obtained is 50% for the 'DEFACEMENT' class. As can be noticed in the 2 analyses, the 'DEFACEMENT' class presents a high complexity at the time of classification. A larger amount of data associated with this type of attack could be obtained to improve this result.

It is recommended in future work to develop a model that converges all the tools applied in this research at a given time to have real-time results; in turn, it optimizes time, technological, and economic resources to have a complete and economical solution, unlike current defense systems that while it is true that already apply principles of artificial intelligence; however, they continue to work with known attack signatures leaving aside the entity responsible for the attacks as is the hacker or cybercriminal and with high costs of acquisition, maintenance and updating, unaffordable values for small and medium enterprises.

Bibliographical References

[1] C. Martínez, H. Moreno, and M. Hernández, "The evolution from Traditional to Intelligent Web Security : Systematic Literature Review," in *International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, pp. 1–9.

[2] C. Martínez Santander, S. G. Yoo, and H. O. Moreno, "Analysis of traditional web security solutions and proposal of a web attacks cognitive patterns classifier architecture," in *Communications in Computer and Information Science*, 2018, pp. 186–198. doi: 10.1007/978-3-030-00940-3_14.

[3] S. Saleem, M. Sheeraz, M. Hanif, and U. Farooq, "Web Server Attack Detection using Machine Learning," in *1st Annual International Conference on Cyber Warfare and Security*,

ICCWS 2020 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ICCWS48432.2020.9292393.

[4] A. A. Akinyelu and A. O. Adewumi, "Classification of phishing email using random forest machine learning technique," *J Appl Math*, vol. 2014, 2014, doi: 10.1155/2014/425731.

[5] C. Wang, T. T. N. Miu, X. Luo, and J. Wang, "SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 559–573, Mar. 2018, doi: 10.1109/TIFS.2017.2758754.

[6] D. Mitropoulos, P. Louridas, M. Polychronakis, and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," *IEEE Trans Dependable Secure Comput*, vol. 16, no. 2, pp. 188–203, Mar. 2019, doi: 10.1109/TDSC.2017.2665620.

[7] S. Salva and L. Regainia, "A security pattern classification based on data integration," in *Communications in Computer and Information Science*, 2018, pp. 105–129. doi: 10.1007/978-3-319-93354-2_6.

[8] R. Gabrys and K. Ferguson, "Emotional State Classification and Related Behaviors Among Cyber Attackers," 2023.

[9] Q. Campbell and D. M. Kennedy, "THE PSYCHOLOGY OF COMPUTER CRIMINALS," in *COMPUTER SECURITY HANDBOOK*, 2014.

[10] Martínez S Carlos José, H. A. Oswaldo Moreno, and M. A. Beatriz Hernández, "Analysis of intrusions into computer systems using honeypots."

[11] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks," *IEEE Internet Things J*, vol. 7, no. 5, pp. 3991–3999, May 2020, doi: 10.1109/JIOT.2019.2956173.

[12] H. TAŞÇI, S. GÖNEN, M. A. BARIŞKAN, G. KARACAYILMAZ, B. ALHAN, and E. N. YILMAZ, "Password Attack Analysis Over Honeypot Using Machine Learning Password Attack Analysis," *Turkish Journal of Mathematics and Computer Science*, Dec. 2021, doi: 10.47000/tjmcs.971141.

[13] A. Abdou, R. Sheatsley, Y. Beugin, T. Shipp, and P. McDaniel, "HoneyModels: Machine Learning Honeypots," Feb. 2022, doi: 10.1109/MILCOM52596.2021.9652947.

[14] "The Science of Criminal Profiling as Applied to the World of Hacking."

[15] Y. Ao, H. Li, L. Zhu, S. Ali, and Z. Yang, "The linear random forest algorithm and its advantages in machine learning assisted logging regression modeling," *J Pet Sci Eng*, vol. 174, pp. 776–789, Mar. 2019, doi: 10.1016/j.petrol.2018.11.067.

[16] G. Clark, M. Doran, and W. Glisson, "A Malicious Attack on the Machine Learning Policy of a Robotic System," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, no. Ml, pp. 516–521, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00079.

[17] D. Wu, C. Jennings, J. Terpenny, R. X. Gao, and S. Kumara, “A Comparative Study on Machine Learning Algorithms for Smart Manufacturing: Tool Wear Prediction Using Random Forests,” *Journal of Manufacturing Science and Engineering, Transactions of the ASME*, vol. 139, no. 7, Jul. 2017, doi: 10.1115/1.4036350.

[18] M. N. Hoda, I. Bharati Vidyapeeth’s Institute of Computer Applications and Management (New Delhi, Institute of Electrical and Electronics Engineers. Delhi Section, and I. International Conference on Computing for Sustainable Global Development (3rd : 2016 : New Delhi, “Honeypot-Based Intrusion Detection System: A Performance Analysis,” *Honeypot-Based Intrusion Detection System: A Performance Analysis*, vol. 16, no. 18, pp. 3947–3951, 2016.

[19] N. Eliot, D. Kendall, and M. Brockway, “A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills,” *IEEE Access*, vol. 6, pp. 34884–34895, Jun. 2018, doi: 10.1109/ACCESS.2018.2850839.

[20] X. Jiang, D. Xu, and Y.-M. Wang, “Collapsar: A VM-Based Honeyfarm and Reverse Honeyfarm Architecture for Network Attack Capture and Detention.”

[21] V. Nicomette *et al.*, “Set-up and deployment of a high-interaction honeypot: experiment and lessons learned Set-up and deployment of a high-interaction honeypot: experiment and lessons learned Set-up and deployment of a high-interaction honeypot: Experiment and lessons learned,” *Journal in Computer Virology*, vol. 7, no. 2, 2011, doi: 10.1007/s11416-010-0144-2ï.

[22] Iqra Khan, Hanif Durad, and Masoom Alam, *Data Analytics Layer For high-interaction Honeypots*. 2019.

[23] K. R. Sekar, V. Gayathri, G. Anisha, K. S. Ravichandran, and R. Manikandan, “Dynamic Honeypot Configuration for Intrusion Detection,” in *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018*, IEEE, May 2018, pp. 1397–1401. doi: 10.1109/ICOEI.2018.8553956.

[24] R. E. Mushtakov, D. S. Silnov, O. V. Tarakanov, and V. A. Bukharov, “Investigation of modern attacks using proxy honeypot,” in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, IEEE, Jan. 2018, pp. 86–89. doi: 10.1109/EIConRus.2018.8317036.

[25] N. Innab, E. Alomairy, and L. Alsheddi, “Hybrid System between Anomaly Based Detection System and Honeypot to Detect Zero Day Attack,” *21st Saudi Computer Society National Computer Conference, NCC 2018*, pp. 1–5, 2018, doi: 10.1109/NCG.2018.8593030.

[26] Ridho Maulana Arifianto, Parman Sukarno, and Erwid Musthofa Jadied, “An SSH Honeypot Architecture Using Port Knocking and Intrusion Detection System,” in *2018 6th International Conference on Information and Communication Technology (ICoICT)*, 2018, pp. 409–415.

[27] N. Naik, P. Jenkins, R. Cooke, and L. Yang, “Honeypots That Bite Back: A Fuzzy Technique for Identifying and Inhibiting Fingerprinting Attacks on Low Interaction Honeypots,” 2018.

[28] O. Surnin *et al.*, “Probabilistic Estimation of Honeypot Detection in Internet of Things Environment,” in *2019 International Conference on Computing, Networking and*

Communications, ICNC 2019, IEEE, Feb. 2019, pp. 191–196. doi: 10.1109/ICCNC.2019.8685566.

[29] S. Kumar, B. Janet, and R. Eswari, "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," *Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019*, pp. 25–29, 2019, doi: 10.1109/IACC48062.2019.8971584.

[30] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, no. Icoei, pp. 1019–1024, 2019, doi: 10.1109/ICOEI.2019.8862720.

[31] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thanasis Liatifis, Konstantinos Rompolos, and Ilias Siniosoglou, "A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure," in *IEEE COMMUNICATIONS SOCIETY, INSTITUTR OF ELECRICAL AND ELECTRONICS ENGENEERS*, 2019, pp. 1–6.

[32] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 683–697, Mar. 2019, doi: 10.1109/JSAC.2019.2894307.

[33] Eva Chovancová and Norbert Ádám, "The Security of Heterogeneous Systems based on Cluster High-interaction Hybrid Honeypot," in *IEEE Xplore. Restrictions apply*, 2019.

[34] C. Huang, J. Han, X. Zhang, and J. Liu, "Automatic identification of honeypot server using machine learning techniques," *Security and Communication Networks*, vol. 2019, 2019, doi: 10.1155/2019/2627608.

[35] M. Dodson, M. Vingaard, and A. R. Beresford, "Using Global Honeypot Networks to Detect Targeted ICS Attacks," *12th International Conference on Cyber Conflict*, pp. 275–291, 2020.

[36] M. Dodson, A. R. Beresford, and M. Vingaard, "Using Global Honeypot Networks to Detect Targeted ICS Attacks," *International Conference on Cyber Conflict, CYCON*, vol. 2020-May, pp. 275–291, 2020, doi: 10.23919/CyCon49761.2020.9131734.

[37] M. M. Yamin, B. Katt, K. Sattar, and M. Bin Ahmad, *Implementation of insider threat detection system using honeypot based sensors and threat analytics*, vol. 70. Springer International Publishing, 2020. doi: 10.1007/978-3-030-12385-7_56.

[38] P. Sharma and B. Nagpal, "HONEYDOS: a hybrid approach using data mining and honeypot to counter denial of service attack and malicious packets," *International Journal of Information Technology (Singapore)*, 2020, doi: 10.1007/s41870-018-0182-4.

[39] I. M. M. Matin and B. Rahardjo, "The Use of Honeypot in Machine Learning Based on Malware Detection: A Review," in *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/CITSM50537.2020.9268794.

[40] P. J. Chuang and T. C. Hung, "Enhanced attack blocking in iot environments: Engaging honeypots and machine learning in SDN OpenFlow switches," *Journal of Applied Science and Engineering*, vol. 23, no. 1, pp. 163–173, 2020, doi: 10.6180/jase.202003_23(1).0017.

[41] F. D. S. Sumadi, C. S. K. Aditya, A. A. Maulana, Syaifuddin, and V. Suryani, "Semi-supervised approach for detecting distributed denial of service in SD-honeypot network environment," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 3, pp. 1094–1100, Sep. 2022, doi: 10.11591/ijai.v11.i3.pp1094-1100.

[42] S. Prabakaran *et al.*, "Predicting Attack Pattern via Machine Learning by Exploiting Stateful Firewall as Virtual Network Function in an SDN Network," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030709.

[43] Prof. S. Aranjo, S. Maurya, C. Thakur, and M. Raju, "Threat Prediction using Honeypot and Machine Learning," *Int J Res Appl Sci Eng Technol*, vol. 10, no. 3, pp. 1838–1851, Mar. 2022, doi: 10.22214/ijraset.2022.41016.

[44] A. K. Suleiman, A. Kayed, R. A. Shamat, V. Jagni, I. Obaid, and A. Awad, "A Passive OS-Fingerprinting framework using Honeypot," in *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems, ICETSIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 178–185. doi: 10.1109/ICETSIS55481.2022.9888932.

[45] M. R. Siddique *et al.*, "Integrating Machine Learning-Powered Smart Agents into Cyber Honeypots: Enhancing Security Frameworks," *2024 IEEE 9th International Conference for Convergence in Technology, I2CT 2024*, 2024, doi: 10.1109/I2CT61223.2024.10543399.

[46] R. Chiesa, S. Ducci, and Ciappi Silvio, "The Science of Criminal Profiling as Applied to the World of Hacking," 2008.

[47] T. C. Summers, K. R. Lyytinen, T. Boland, E. Lingham, and D. M. Pierce, "HOW HACKERS THINK: A STUDY OF CYBERSECURITY EXPERTS AND THEIR MENTAL MODELS," 2013. [Online]. Available: http://ssrn.com/abstract=2326634http://ssrn.com/abstract=2326634http://ssrn.com/abstract=2326634

[48] A. Matulessy and N. H. Humaira, "Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits," *Psychology and Behavioral Sciences*, vol. 5, no. 6, pp. 137–142, 2016, doi: 10.11648/j.pbs.20160506.12.

[49] K. C. Seigfried-Spellar, N. Villacís-Vukadinović, and D. R. Lynam, "Computer criminal behavior is related to psychopathy and other antisocial behavior," *J Crim Justice*, vol. 51, pp. 67–73, Jul. 2017, doi: 10.1016/j.jcrimjus.2017.06.003.

[50] M. M. Al-Ajlouni, "Human resources and their tendency to information security crimes based on holland theory," *Information Resources Management Journal*, vol. 31, no. 4, pp. 44–58, Oct. 2018, doi: 10.4018/IRMJ.2018100103.

[51] S. Back, J. Laprade, L. Shehadeh, and M. Kim, "Youth hackers and adult hackers in south korea: An application of cybercriminal profiling," in *Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019*, Institute of Electrical and Electronics Engineers Inc., Jun. 2019, pp. 410–413. doi: 10.1109/EuroSPW.2019.00052.

[52] J. Gaia *et al.*, "Psychological Profiling of Hacking Potential," proceedings of the 53rd Hawaii International Conference on System Science, Ed., 2020.

[53] K. Kioskli and N. Polemi, "Measuring Psychosocial and Behavioural Factors Improves Attack Potential Estimates," in *2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.23919/ICITST51030.2020.9351343.

[54] C. Stachl *et al.*, "Predicting personality from patterns of behavior collected with smartphones," 2020, doi: 10.1073/pnas.1920484117/-/DCSupplemental.y.

[55] M. Bada and J. R. C. Nurse, "Profiling the Cybercriminal: A Systematic Review of Research," *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*, 2021, doi: 10.1109/CyberSA52016.2021.9478246.

[56] D. N. Jones, E. Padilla, S. R. Curtis, and C. Kiekintveld, "Network discovery and scanning strategies and the Dark Triad," *Comput Human Behav*, vol. 122, Sep. 2021, doi: 10.1016/j.chb.2021.106799.

[57] J. McAlaney, "Are you anonymous? Social-psychological processes of hacking groups," in *Cybersecurity and Cognitive Science*, Elsevier, 2022, pp. 139–155. doi: 10.1016/B978-0-323-90570-1.00003-6.

[58] K. Yasuhara *et al.*, "The Amorphous Nature of Hackers: An Exploratory Study," Other Computer Sciences Commons, and the Social Control, 2022. [Online]. Available: https://commons.erau.edu/adfsl/2022/presentations/1

[59] M. Weulen Kranenbarg, J. L. van Gelder, A. J. Barends, and R. E. de Vries, "Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets," *Comput Human Behav*, vol. 140, Mar. 2023, doi: 10.1016/j.chb.2022.107576.

[60] M. Bachmann, "The Risk Propensity and Rationality of Computer Hackers," *International Journal of Cyber Criminology*, vol. 4, no. 2, pp. 643–656, 2010.