Hindawi
Security and Communication Networks
Volume 2022, Article ID 7620125, 28 pages
https://doi.org/10.1155/2022/7620125

Research Article

Detecting User Behavior in Cyber Threat Intelligence: Development of Honeypsy System

Murat Odemis,[1] **Cagatay Yucel**,[2] **and Ahmet Koltuksuz**[1]

[1]*Department of Computer Engineering, Yasar University, Izmir 35530, Turkey*
[2]*Department of Computing and Informatics, Bournemouth University, Poole BH12 5BB, UK*

Correspondence should be addressed to Murat Odemis; murat.odemis@yasar.edu.tr

Received 22 October 2021; Accepted 21 December 2021; Published 27 January 2022

Academic Editor: Konstantinos Demertzis

This research demonstrates a design of an experiment of a hacker infiltrating a server where it is assumed that the communication between the hacker and the target server is established, and the hacker also escalated his rights on the server. Therefore, the honeypot server setup has been designed to reveal the correlation of a hacker's actions with that of the hacker's experience, personality, expertise, and psychology. To the best of our knowledge, such a design of experiment has never been tested rigorously on a honeypot implementation except for self-reporting tests applied to hackers in the literature. However, no study evaluates the actual data of these hackers and these tests. This study also provides a honeypot design to understand the personality and expertise of the hacker and displays the correlation of these data with the tests. Our Honeypsy system is composed of a Big-5 personality test, a cyber expertise test, and a capture-the-flag (CTF) event to collect logs with honeypot applied in this sequence. These three steps generate data on the expertise and psychology of known cyber hackers. The logs of the known hacker activities on honeypots are obtained through the CTF event that they have participated in. The design and deployment of a honeypot, as well as the CTF event, were specifically prepared for this research. Our aim is to predict an unknown hacker's expertise and personality by analyzing these data. By examining/analyzing the data of the known hackers, it is now possible to make predictions about the expertise and personality of the unknown hackers. The same logic applies when one tries to predict the next move of the unknown hackers attacking the server. We have aimed to underline the details of the personalities and expertise of hackers and thus help the defense experts of victimized institutions to develop their cyber defense strategies in accordance with the *modus operandi* of the hackers.

1. Introduction

By the growth and variety of the hefty volume of data to track users' behavior, novel research opportunities have been built for researchers. The request to learn about a person is a multidisciplinary subject. This requirement has been included in the designs of research in various domains such as marketing, e-commerce, psychology, cyber security, and computer forensics. The benefits of collaborating across disciplines, such as social sciences, applied statistics, and computer science, primarily affect the security arena regarding the fields of open-source intelligence, information warfare, and strategic studies of security. Most of the existing studies aim to predict the next move of users from their actions. The prediction of user behavior has been the main research question in user and customer experience analysis [1].

The main question in this research is whether we can analyze the experiences and psychology of the hackers by looking at their computer logs and vice versa. This research is targeted towards analyzing the characteristics of a hacker, such as psychology, personality, and experience, and thus establishing a correlation between them with server logs. Therefore, for this aim, establishing a connection between the psychology and expertise of the hacker with the honeypot logs is the main contribution of this research. The new dimension and perspectives stemming from this connection are presented in this research.

This paper tries to find answers to these questions:

Is there a relation between hacker expertise and hacker psychology?

Is there a relation between hacker expertise and the operations performed on the server?

If there is a relation between expertise and psychology, what characteristics indicate that this hacker is an expert on cyberattacks?

If there is a relation between expertise and operations, what kinds of operations on the computer (logs) indicate that this is an expert hacker on cyberattacks?

Can the personality/psychology and expertise of an unknown hacker who is not in the dataset be predicted by looking at the logs he left?

We designed a system to find answers to these questions. Our testing system is composed of a Big-5 personality test, a cyber expertise test, and a capture-the-flag (CTF) event applied in this sequence. These three steps generate data on the expertise and psychology of known cyber hackers. In other words, the honeypot logs of the known hackers are obtained through the CTF events that they have participated in.

By analyzing these elements, we create a trained dataset. Furthermore, with these analyses, we have aimed to see significant findings on the personalities and expertise of hackers and thus shed light on the strategies of those experts.

We wanted to make sense of the logs left by unknown hackers on any server according to this trained data. The overall design of log collection, test result collection, and the respective analysis of them are depicted in Figure 1. The overall design of the part where data are collected is shown in Figure 1, and the detailed explanation of the flowchart of the system can be examined in Section 4.

The prediction pattern of an unknown hacker is given in Figure 2. This diagram shows how we collect data from unknown hackers and put them into the analysis/prediction phase. Finally, the design of the system and detailed flowchart explanation is provided in Section 4.

In the literature, some studies perform a hacker psychology test or expertise test [1]. However, to the best of our knowledge, no study connects these results with the same hackers' actual computer/server logs. Therefore, the novelty of this research is the demonstration of the possibility of predicting the psychology and expertise of the hacker through the logs of the server in question. Once this connection of psychology with expertise is established, then the behavior of an unknown/untested hacker can be predicted by acquiring the trained data set of known hackers.

In a nutshell, this study analyzes hackers who log on to a honeypot and leave traces, and their personalities and behaviors are predicted from these logs and traces. Therefore, one of the main outcomes of this research is the design of a honeypot that collects the behavioral characteristics of a hacker. Moreover, some of these hackers are interviewed by CTF competitions and tests to gather information about hackers' Big-5 [1] personalities and expertise. Then, a relationship between logs and tests in the system is compared and analyzed. At the end of these steps, when a new and unknown hacker enters the system, we demonstrate that it is possible to estimate that person's expertise and psychology, without extensive surveying but by considering their server logs instead. In the comparison and the analysis steps, the study includes a "Cyber Psychology and Personality Analysis Test (Big-5 Test)," a "Cyber Expertise Test," and a "Honeypot Server to Store Logs, using a CTF to store the logs of participants to server."

At first, the "Cyber Psychology and Personality Analysis Test (Big-5 Test)" and "Cyber Expertise Test" are conducted with a volunteer group consisting of known hackers, computer experts, and engineering students. The same participants were later taken to the honeypot server to take the CTF. The logs were generated while the group was dealing with CTF. Thus, a correlation was established and analyzed between the self-reporting tests and the data left on the server by the known hackers. All these data were brought together, and a model was trained with data mining algorithms/machine learning. Thus, from the logs left by hackers to the server, the psychology and expertise can be estimated. Likewise, by looking at their expertise, the logs they left to the server can also be estimated. Furthermore, by examining some of the steps of commands, it is possible to predict the actions that this person will take in later stages. This acquired power of prediction makes it possible to be proactive and thus be decisive when it comes to making a decision about that persons' actions.

By applying this proactive approach, the information about the hacker's expertise and psychology can be obtained easily and quickly when an unknown hacker, who has not done a survey or test on that server before, is in action. Hence, not even a past kept log might be necessary since the log that is currently being generated at that specific real-time of action is there to be utilized, as explained above. Then, in line with this information, measures can be taken, and a defense strategy can be constituted.

We think it is essential to understand whether the hacker is an expert at attacking a server to control this cyberattack. In order to analyze this, we need to have logs, tests, and surveys. By analyzing these accumulated data, it will be possible to predict the attacks in real time in the future.

The contributions of this research are three-fold:

A honeypot design that is capable of capturing relevant logs from an interaction with the attacker

Correlation of these logs with Cyber Psychology and Personality Analysis Test (Big-5 Test) and Cyber Expertise Test analysis

The evaluation of these results and the expertise and personality tests applied to the known participants to predict personality and expertise from unknown hacker logs and vice versa

The remainder of the paper is organized as follows. The background and the literature review relevant to this study are presented in Section 2. Problem definition with the used materials and methods were explained in Section 3. Section 4 is the detailed results and analysis of the computational

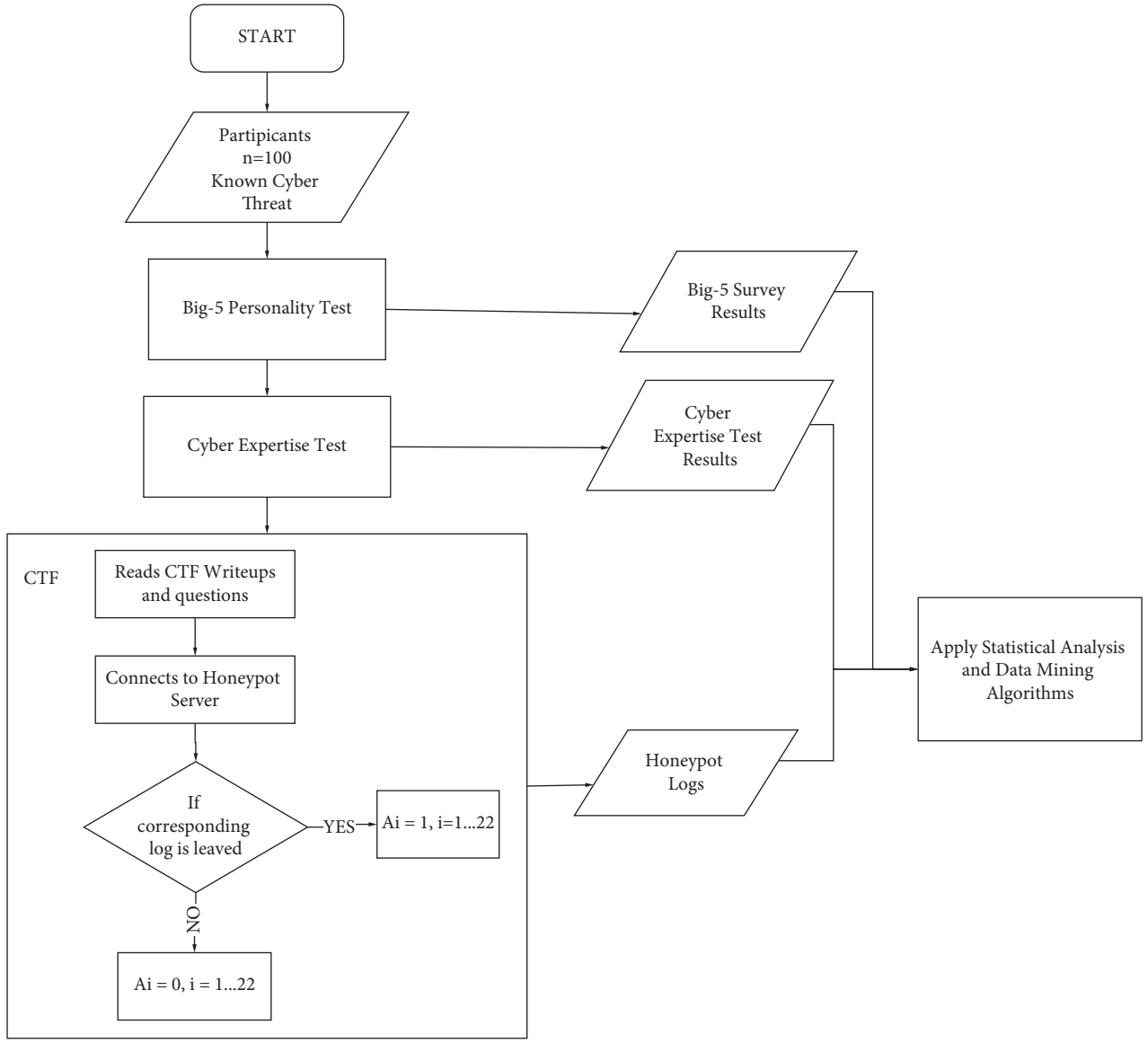

Figure 1: Log collection and test result collection diagram of known participants.

experiments for all presented materials and methods. Section 5 has a discussion and limitations of our system. Finally, Section 6 provides conclusions and future work.

2. Background and Literature Review

Since the Big-5 psychology/personality test, which is the starting point of the idea, was applied to a hacker, the scientific papers of this field were examined first. Then, the previous research on Cyber Expertise Detection was covered. As the last stage, the literature on Honeypots was extensively examined.

2.1. Background and Relevant Studies on Hacker Psychology Analysis. Psychology is one of the exciting fields that can work together with computer science. The question of whether a user's psychology can be detected via computers may come to mind, like a question of whether it is detectable that a user is neurotic, happy, depressive, or maybe not. As a result of predicting the users' psychological states, information can be obtained about whether the users are open-minded, extroverted, etc. With the power of computer science, these personality-related analyses can be applied cost effectively. As it plays an essential role in understanding a cyber threat, it is a necessity for psychoanalysis to become more proactive in the world of cyber security.

Hackers are one of the most curious types of actors in the tech world. Hackers can bypass the firewalls, and sometimes they can pass through insurmountable barriers. Some leave traces behind or get caught. The question is as follows: can the behavior, expertise or psychology, and personality of hackers be predicted with the data left behind?

In order to investigate the psychology of users, their website usage information, mobile phone cellular usage logs, IoT device logs, and network logs were taken into consideration. All of the following data metrics are currently

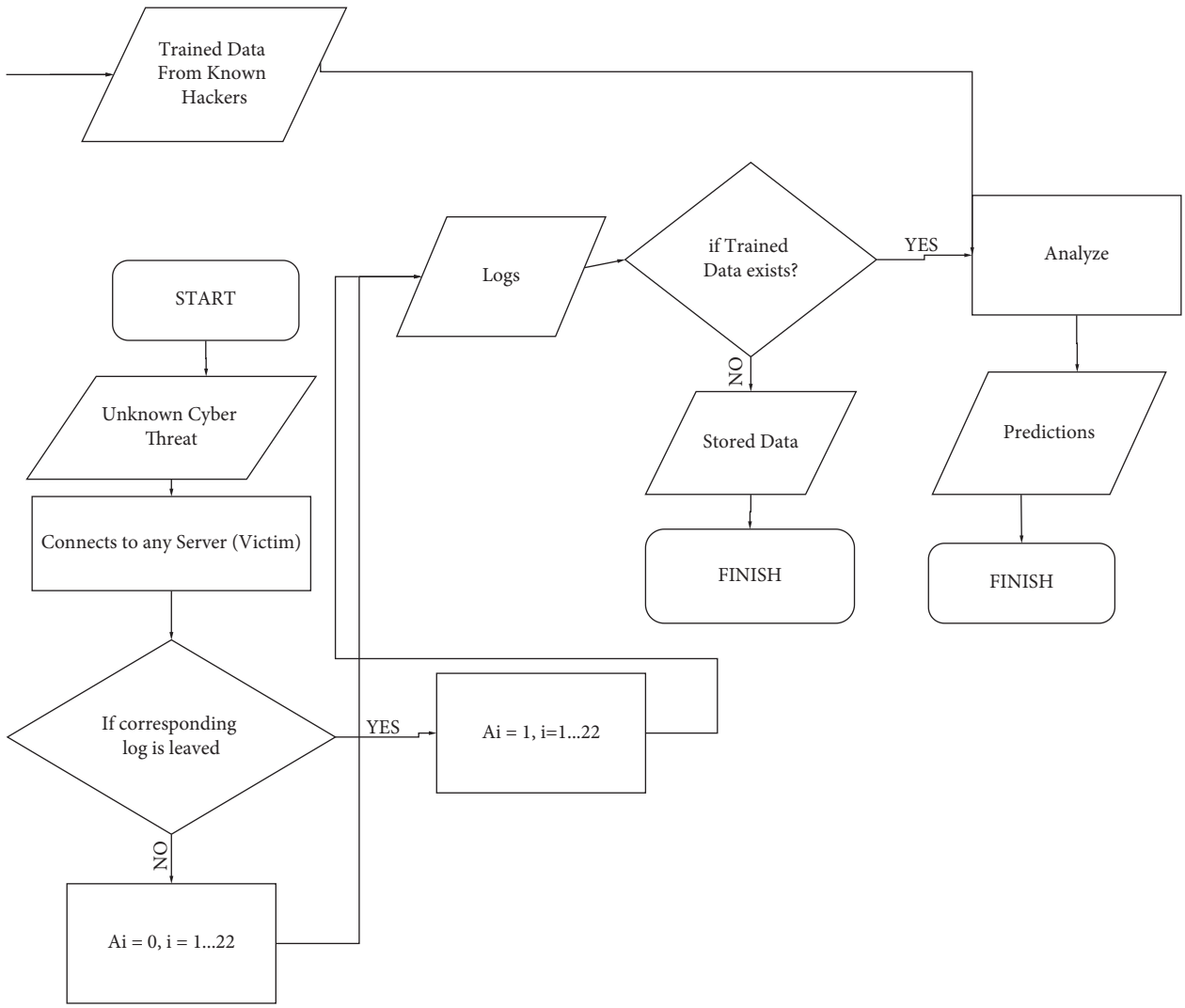

Figure 2: Diagram of prediction on unknown hackers and collecting his logs.

utilized in many domains: Heatmaps based on website clicks, standard phone logs, accelerometers, heart rates, blood pressures, breath monitoring, GPS tracking, locations, diversity, activity tracking, lengths between phone sessions, interevent timing, social media usage, body temperatures, users' light exposure, regularities, response rates, and latencies, the radius of gyration, Bluetooth scans, sleep patterns, daily walking distances, social media posts after traumatic events, music, code-switching, discovering neighbors, indoor localization with Wi-Fi fingerprint, and the number of unlocking trials and repetitions.

Some of the psychological symptoms that could be defined by the end of these examinations include neuroticism, extroversion, conscientiousness, agreeableness, openness, gender prediction, ethnicity prediction, political attitude prediction, depression, behavioral changes, workplace effects, motivations, confidence, one-sidedness, attitudes, experiences, vigor and fatigue, stress, guilt, and hostility.

The Big-5 personality theory gives a simple blueprint to understanding others, improving relationships by knowing why people behave the way they do. We asked psychology experts which psychology test we should use for our study. As a result of the answers and research we received, we decided to use the Big-5 test. The Big-5 Personality model is an organization of personality traits that measures five dimensions of personalities:

Extroversion: this dimension measures one's level of being sociable, energetic, and outgoing. It determines whether the person is quiet or able to work in a crowded environment and enjoy accompanying others a lot.

Agreeableness: it is about being warm, compassionate, and cooperative and how well you deal with other people.

Conscientiousness: this is the tendency to show self-discipline, be organized, and aim for achievement. If a person has a high score on conscientiousness, it can be said that he/she is likely to be organized and thorough, plans well, and can comply with those plans.

Neuroticism: the model defines this as the tendency to experience negative feelings, emotional problems and changes, anxiety, anger or depression, and the frequency of bad moods.

Openness: one who scores high in this might be called curious, creative, intellectual, a stargazer, and devoted to knowledge and makeshift experiences.

Mazadi et al. [2] and Shi et al. [3] offered a study that included the psychological aspects of socially conducted agents. These two papers described ways to model a streamlined behavior of an agent in four critical cultural aspects, self-enhancement, openness to change, self-transcendence, and conservation, from the model of primary human values in [4]. Cyber behavioral and psychological studies remain up to date. With COVID-19, a study shows the correlation between Internet, security use, loneliness, and satisfaction [5].

A well-detailed study that primarily worked on mobile data provided the personality evidence from mobile phone logs and used the data available from carriers to predict users' personalities. It was stated that an evaluation of these records, along with country-scaled datasets, may lead to unprecedented discoveries in psychology. The information can also help detect country-wide user behaviors and profiles. Montjoye et al. [6] used mobile phones to predict Big-5 personality factors: neuroticism, extroversion, conscientiousness, agreeableness, and openness. The entropy of their usage enabled them to indicate both extroversion and agreeableness. The variance between sessions and phone calls showed their conscientiousness; answering the questions and texts was the predictor for openness. Extroversion was a strong predictor of positive emotions, and neuroticism was associated with negative emotions [6].

The studies we have detailed so far constitute self-reporting tests performed on a hacker. The accuracy can decrease since there is no connection between these tests and the hacking data/logs of the hackers. We built a fake-honeypot server to increase accuracy and correlate self-reporting tests with actual data/logs of hackers.

This research contributes to the corresponding literature by adding the following values to a honeypot system: (i) novelty in integrating the Big-5 personality concept to a honeypot (neuroticism, extroversion, conscientiousness, agreeableness, and openness) and (ii) compare it with the expertise of participants.

2.2. Background and Relevant Studies on Hacker Expertise Analysis. A common aim of the hackers to target organizations is data theft [7], resulting in billions of dollars in losses each year [8]. Due to hackers' threat to companies, researchers have begun to investigate hackers' motives and behaviors [9]. They have conducted different studies to understand hacker behavior better [9, 10, 11]. These studies are based on data collected from self-reported hackers. However, these data have the problem of not verifying whether the participants are real hackers and categorizing them according to their level of knowledge. A hacker's level of expertise is determined by the ability to write code or scripts without being caught that can circumvent security protocols, disrupt a system's intended functions, or gather valuable information [12].

In order to differentiate between novice and expert hackers, SEAM [13] can be used. This tool provides two critical capabilities to information systems researchers. One is to verify the identity of the hackers involved in the data collection, and the other is to separate the samples of the hackers into different groups. Thus, novice and expert hackers are tried to be identified with more detailed analysis and insights. The authors of the SEAM state that there are some shortcomings in the article: "a common concern was that our approach might only measure how well a hacker conceptually understands hacking methods without directly assessing a hacker's actual ability."

In this paper, we developed our Honeypsy framework and methodology to solve the mentioned shortcomings in SEAM. Although HAIS-Q [14] is not precisely a hacker expertise test, it does provide insight as it is used to measure computer usage ability. The difference between the tests such as SEAM [13], HAIS-Q [14], and HONEYPSY, which is proposed in this study, is depicted in Table 1.

The purpose of the Cyber Expertise test is to measure how skilled, knowledgeable, and experienced the hacker is. We have implemented a widely accepted method by experts and hackers on this topic for the cyber expertise test. For this reason, we came up with the idea of devising a test on the MITRE ATT&CK Framework [15], a generally accepted framework for systematically providing a categorized adversary behavior. The ATT&CK test developed in this research includes ordering randomly chosen techniques and placing them into tactics.

2.3. Background and Relevant Studies on Honeypots and Collecting Hacker Logs and Behavior. The term "honeypot" or "honey trap" refers to a strategy where an attractive agent is deployed to lure individuals and exploit their vulnerabilities (mostly sexual) and relationships to push the individuals to comply with them. A honeypot system is camouflaged as a host or a service on the Internet that is deliberately left vulnerable. Honeypot systems have these decoy-based aspects developed to lure the attackers into its vulnerable surface and record information about the attack and attackers. Therefore, honeypots can be considered passive traps for attackers. Their designs aim to unlock and reveal actionable cyber threat intelligence about the techniques, tactics, procedures, origins, attributions, and motivations of the adversaries [16].

Honeypots are categorized to their interaction levels and service types. A low-interaction honeypot presents just a few levels of steps and replies of the targeted host, network protocol, and stack. Conversely, a high-interaction honeypot fully emulates the intended service. A high-interaction honeypot can reveal many significant characteristics such as the amount of data that has been sent and received from the server, failed logins, CPU, and memory usage, whether the attacker has been typing on the server or automation is

Table 1: Comparison of related works with our system.

Study	Participants	Test	Method	Area
SEAM	35 (students and experts)	Expertise test	Regression analysis	Hacker expertise
HAIS-Q	112 (students)	Computer usage expertise test	Regression analysis	Computer usage expertise
HONEYPSY (our work)	100 (experts + students)	Expertise test + Big5 test + server logs	Regression analysis + machine learning	Hacker expertise and hacker personality

utilized, and the level of sophistication for the exploration of the attacker on the honeypot. These characteristics about the attackers can be crafted into actionable intelligence; it reveals the modus operandi of the attacker, gives insights about their motivations, and, more importantly, identifies the source of the attack by tracking down the network connections of the attacker, such as connecting to the Command and Control (C&C) and downloading malware from a public server.

The honeypot research has been shifted to the profiling of the attacker based on their behaviors in recent years. A honeypot design to identify an attacker's attribution using heatmaps created by the threat and capability of the attacker is given by the study of [17]. The basis for the profiling model is created from the collected logs of attackers, captured as capabilities, skills, motivation, and intentions, and mapped onto capability and threat ratings. A low interaction honeypot for Ethereum networks has been designed [18]. In this research, the attackers are characterized utilizing the communication logs, the analysis of the Ethereum network, and the IP addresses belonging to the Darknet.

Correlation of cyber threat intelligence from high interaction honeypots from six different locations is conducted, and the results are presented in [19]. The attack patterns identified by the commands are analyzed, and patterns of actions are extracted and correlated. In addition, network communications, daily events, and sessions from the honeypots have also been analyzed and represented in this research. Similarly, in [20], sessions constructed with the chain of commands are collected from high interaction honeypots. A prediction model based on the frequency analysis of the commands is presented.

As far as the authors know, no study in the literature analyzes computer logs, expertise, and psychology altogether. This study was conducted to fill this gap in the literature. In order to conduct an analysis, it is necessary to obtain the computer logs of a person who has undergone a psychology test. Therefore, a CTF has been developed. A honeypot is designed to collect the logs that were generated by the unknown hackers who did the CTF. So, the binary representation of these logs in the form of True (=1) or False (=0) is analyzed. For this reason, this study differs from the literature and thus bears originality.

Table 2 summarizes the methodology and usage area of the works mentioned in this paper.

3. Materials and Methods

The design of the devised system and the interaction between the tests and the logs can be seen in Figure 3. Honeypots are designed to collect logs. The Expertise test and Big-5 test were designed to draw inferences about the psychology and expertise of the potential cyber threat.

In this study, 100 participants were tested. The properties of these participants are described in Section 5. To be able to match the data of the participants from three separate tests with each other, we want the participant to write his name in each test, and they are given a unique ID.

(1) The participant first solves the Big-5 Personality Test, which is given to him as an online form. The definition of the Big-5 Personality test, its evaluation, and the analysis results of our target group are explained in detail in Sections 3.2 and 4.1, respectively. These data will also be used for the predictions.

(1.1) After solving the Big-5 Personality Test, we have Big-5 and Facets results for that user. The detailed information of facets is given in Section 3.2.1. Here is an example result for a user named Joe H., given in Table 3. In Table 3 and the following tables, the abbreviations for the Big-5 (extraversion: E, agreeableness: A, openness: O, conscientiousness: C, and neuroticism: N) personalities and the Facets (sociability: Soc, assertiveness: Asse, energy level: EnL, compassion: Com, respectfulness: Res, trust: Tru, organization: Org, productiveness: Pro, anxiety: Anx, depression: Dep, emotional volatility: Emo, intellectual curiosity: IntC, aesthetic sensitivity: AeS, and creative imagination: CreI) are used.
These results were collected for 100 participants, and the results are organized in Table 4.

(2) After the Big-5 test, the participant completes the 4-part cyber expertise test. The definition of the cyber expertise tTest, its analysis, and the correlation results of our target group are explained in detail in Sections 4.2 and 4.1, respectively. These data will also be used for the predictions as well.

(2.1) After solving the cyber expertise tTest, we obtained the results in the following form, as depicted in Table 5.

(3) The participant is then taken to the CTF we designed. The definition of the CTF, its preparation process, and its analysis are explained in Sections 3.1 and 4.1, respectively. The user is directed to honeypot to solve CTF questions. Honeypot design

Table 2: Used methodologies, tools, and areas of related works in literature.

Tools	References	Methods	Areas
Survey	[8]	Machine learning	Security
Survey	[9]	Regression analysis	Security
Survey	[10]	Regression analysis	Security
Survey	[14]	Regression analysis	Psychology
Survey	[13]	Regression analysis	Security
Survey	[12]	Regression analysis	Security
Logs + Surveys	Honeypsy (our work)	Machine learning/regression analysis	Security

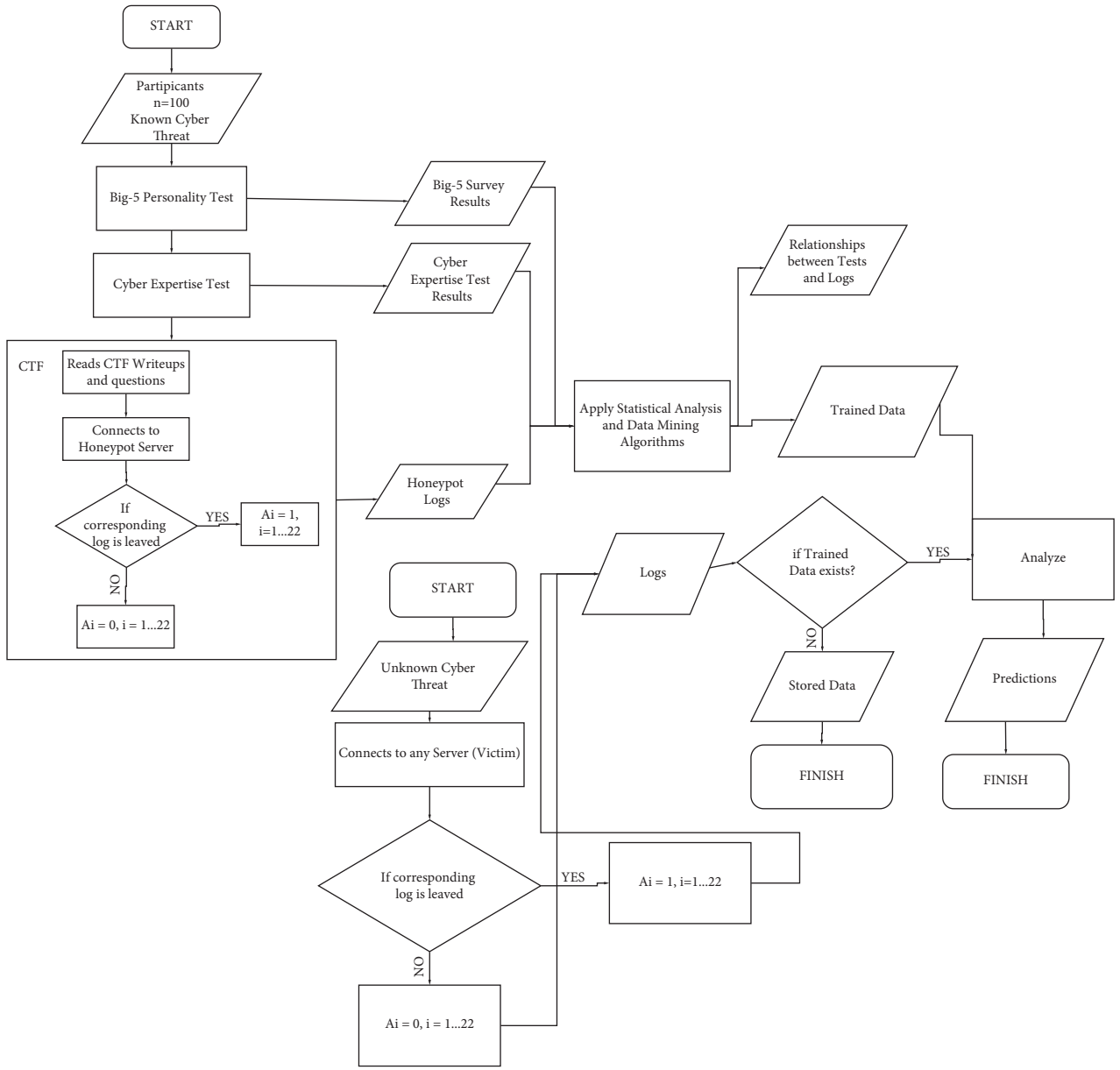

Figure 3: Log collection and test result collection and prediction diagram of our system.

Table 3: Example personality results of a known participant named Joe H.

Name	E	A	O	C	N	Soc	Asse	EnL	Com
Joe H.	0.75	0.64	0.43	0.12	0.7	0.8	0.7	0.1	0.2

Table 4: Example personality of results of all known participants 1...100.

ID	Name	E	A	O	C	N	Soc	Asse	EnL	Com
1	Joe H.	0.75	0.64	0.43	0.12	0.7	0.8	0.7	0.1	0.2
2	Che N.	0.65	0.12	0.43	0.12	0.12	0.11	0.97	0.88	0.1
	...	...	...	...	...	...	...	...	...	...
100	Kol X.	0.44	0.15	0.17	0.18	0.32	0.77	0.77	0.22	0.12

Table 5: Example cyber expertise result of a known participant named Joe H.

ID	Name	Cyber expertise test score	Cyber expertise test class
1	Joe H.	75	Expert
2	Che N.	65	Medium
..	..	..	...
100	Kol X	44	Low

is described in Section 3.1. The participant marks the specifications in the honeypot while solving the CTF questions. An example scenario and two questions are as follows.

CTF QUESTION #7

There are many files that include btc wallets in the system. Try to remove just all of them, but not delete the other necessary files.

CTF QUESTION #8

We understand your ambition, do not let anyone win! We seriously think that you should do some harm to the SSH server! Try to remove all files.

While answering questions 7 or 8, the user will type commands. If at least one of the corresponding commands is typed, then, in the result, table A7 (used for question 7) will be marked as 1, otherwise 0.

After participants have solved all of the CTF questions, we will have a log table designed in Table 6. In this table, the meanings of columns shown by A1...A22 are explained in Section 4.1. The detailed explanation for A1...A22 is provided in Section 4.1. This binary representation allows us to analyze the user's server and computer logs. Only A14 is numerical data, which defines the user's keyboard speed and the time between two subsequent commands entered by the hacker. The information obtained from the typing speed and the time interval between commands gives us the ability to predict the expertise and the personality of that hacker.

(4) After we have all the test results, we now have the logs of all the participants and then combine the logs. As a result, we will have the information of the participants as represented in Table 7. After that, we applied statistical analysis to see if there exists any correlation between the test results.

Table 6: Honeypot logs of known participants.

ID	Name	A2	A3	A4	A5	A6	A7	A11	A12	A14
1	Joe H.	1	0	1	0	0	1	0	1	0.4
2	Che N.	0	0	0	0	0	1	1	1	0.3
	...	...	...	...	...	...	...	...	...	...
100	Kol X.	0	1	1	1	0	1	0	1	0.4

In the statistical analysis phase, the data mining algorithms were also applied to the obtained and edited test results to train the data besides checking the correlations. In this way, we obtained the trained data, which will enable us to predict the expertise and psychology of unknown hackers with a certain accuracy in the future.

The following scenario is explained in the lower START section of the flowchart. This section describes the steps of an anonymous attack by someone other than the participants we tested. The purpose of this section is to explain the behavior of the method we developed during an attack and to show what kind of results we will get in these cases.

(1) The unknown cyber threat, whose identity is not known, enters any server where our Honeypsy system is installed. This server does not need to be a honeypot.

(2) According to the logs written by the hacker on the server, the following steps are applied:

(a) If a hacker enters a command that we have specified, the corresponding commands (A1, ..., A22) will be marked as 1.

(b) All logs are recorded to catch adversary attacks.

(c) Most attacks on a server are made by bots. With the help of these markings, it can be interpreted whether the attacker is human or not. The logs of the hacker who marked A1, ..., A22 can be examined in detail, and also, other methods and commands used can be analyzed.

(3) As a result of an unknown cyber threat, we get a log like in Table 8.

(4) Next, using these logs, we tried to estimate the hacker's expertise and psychology.

(a) If trained data are available, analysis and predictions are made based on this data.

According to the data seen in Table 9, the following predictions having root mean square error (RMSE) of 9.1123 can be made:

Unknown cyber threat has a cyber expertise score of 81/100, which indicates that he can be an expert.

Unknown cyber threat can be neurotic because its neuroticism score prediction is 78/100, which is borderline class.

(b) Based on these data, the institution can develop a defense strategy or put its predetermined procedures to use.

The accuracy of the predictions is explained with an example as follows. Among our participants,

Table 7: Combination of logs and test results of example known participants in one table.

ID	Name	A2	A3	A4	...	A22	Expertise score	E	A	O	C	N	Soc
1	Joe H.	1	0	1	0	0	75	0.75	0.64	0.43	0.12	0.7	0.8
2	Che N.	0	0	0	0	0	65	0.55	0.34	0.43	0.12	0.7	0.8
	...	...	...	...	...	...	..						
100	Kol X.	0	1	1	1	0	44	0.35	0.24	0.43	0.12	0.7	0.8

Table 8: Logs of unknown hacker that signs predefined honeypot specs.

	IP	A2	A3	A4	...	A22
Unknown hacker	22.1.11.222	1	0	1	0	0

Table 9: Real data/results of a known participant from our dataset.

ID	Name	A2	A3	A4	...	A22	Expertise score	E	A	O	C	N	Soc
17	M.K	1	0	1	0	0	75	0.75	0.64	0.43	0.12	0.7	0.8

the results of the person with participant ID number 17 are shown in Table 9.

Sample log of an unknown hacker, other than our participants, who marks the same logs with participant 17, is shown in Table 10:

This person's expertise score is estimated as 72/100 with our system. While the known hacker's expertise score was 78/100, the unknown hacker's expertise score is generated respecting to known hacker results as 72/100 due to the accuracy of the data mining algorithm. This example indicates that the predictions are compatible with our examined sample data. The details of the predictions can be seen in Section 4.3.

Apart from these estimations, general analyzes are also made on our sample group of participants. These general analyzes are described in Section 4.1.

If the hackers do not want to provide their name or nickname, they get a unique ID when they complete the tests. To do that, they enter the same ID as they connected to the honeypot. In this way, a correlation can be established between tests and honeypot logs.

3.1. Honeypot Requirements, Specifications, Marking Commands, and Features. The process of designing our honeypot system started in early 2019. Two honeypots have been set up on Amazon Web Clouds and Digital Ocean Servers. The interactions with the hackers and adversaries in the wild have been collected through those servers. We set up and modified Cowrie [21] to be a basis for the honeypot to collect logs. Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks plus the shell interaction performed by the attacker. The purpose of building this honeypot is to mark the behavior of hackers. However, this honeypot also collects data from the Internet and is open to examining unknown cyber threats. We use SPLUNK to monitor and visualize the honeypot data. Since we would know the volunteers who entered this SSH Honeypot, we can infer their personality and expertise by looking at their operations on the server.

Table 10: Sample logs to make a prediction of an unknown hacker.

ID	Name	A2	A3	A4	...	A22
Unknown	Unknown	1	0	1	0	0

In order to analyze the hacker operations, we defined a standard table of requirements and specifications in Table 11.

These requirements and specifications have been crafted by scrutinizing and categorizing the collected logs and traces. The specifications given here are the definitions of the hacker actions that we have collected from the honeypots. Although the specification such as 'search commands' listed as item A9 in Table 11 seems one, it includes all the terminal-based search commands observed from our systems. User behavior in the honeypot marks these specifications as "True, False, Duration."

Example 1. A9. Search commands such as "grep."

Suppose that a hacker enters honeypot and types one of the commands below:

grep
awk
sed
tail
head
Cat

A9 ⟶ True. A9 is marked as true.

These commands are crafted by the cyber security experts as well as by the hackers, plus by utilizing GitHub sources [21, 22].

Honeypot is designed to mark the specifications given in Table 11 by looking at the logs of unknown or known hackers entering the server. The system includes multiple Cowrie honeypots, and we have implemented a script to sign and output the logs that combine and process the data from these honeypots.

Table 11: Requirement description.

Requirement description
R1. Source IP must be logged
R2. Services that are tried on the server must be logged
R3. Detection of a file-malware-rootkit upload
R4. Nothing will be deleted about the activities of hackers
R5. Keyboard speed-frequency-command copy-parting must be understood
R6. Operations after a successful intrusion must be logged as well
A1. Software should analyze if the code is entered manually or via a script
A2. The same commands have been tried more than once
A3. Command similarity (% sudo ~ sudp) must be checked for erroneous commands
A4. A command database must be created for similar commands for several systems; an erroneous command can be a legit command in another system which in return shows skill
A5. If 'passwd' is entered or attempted
A7. Signs for a virtual machine are checked
A8. Do commands such as nmap, network detection, and ettercap which are tried
A9. Search commands such as "grep"
A10. Any command follows IP addresses found on the honeypot
A11. Harming commands such as "rm–rf"
A12. Download commands should be added
A13. Installation of DDoS methods
A14. Event/command interarrival times
A15. The file system is tested
A16. Leaving a file/trace for fame
A17. Deleting tracks and history when exiting–att&ck
A18. Is reverse-shell used? (persistence)
A19. Determining the Linux distro?
A20. Collecting system information
A21. Collecting network information
A22. Collecting user information

The number of honeypots might be easily increased by cloning, and a new honeypot can be set up with a single click through a script. Thus, no new configuration is required. Suppose we say N is the number of honeypots. We have a cluster of N+1 machines. We connect to our N honeypot servers through our load balancer server working with HAproxy. This load balancer distributes the hackers to the servers by the leastconn algorithm with the least connection. In this way, it will be sufficient to specify the IPs of the new machines in our load balancer config instead of distributing the IPs of the new devices that we will open under heavy load.

A file structure is needed to use the specifications. We have developed a file structure and embedded it in Cowrie. A plugin system was developed by forking the Cowrie honeypot system, and each specification was turned into a plugin. The plugin system has been designed using the strategy pattern. Plugins can be quickly produced from the main class. Thus, if the number of specifications increases, they can be reproduced. When Cowrie receives an input, it also transmits the input to our plugins. In this way, we can make the necessary checks and markings.

The data collection script collects and aggregates logs from all Cowrie instances. It reads the files one by one, analyzes the logs and event durations we marked, and outputs a CSV and JSON file:

The plugin trigger mechanism awakes when user inputs start to be processed.

Plugins can be implemented according to need from the prepared BasePlugin class.

Plugins are processed in the process_event method.

Cowrie simulates the layout of the files placed in the Honeyfs folder.

Files uploaded to connect/to the directory for CTF. The python bin/createfs -l honeyfs -o share/cowrie/fs.pickle command generates the directory's memory to be kept in memory.

The honeypots are created to be reached online. For this study, the honeypots have been running since early 2019.

In order to analyze the collected data from known hackers, they were invited to the CTF. While solving the CTF, they connected to the honeypot. Then, the specifications are marked respecting the operations of known hackers on CTF. Besides these known hackers, any hacker/instance of the Internet can connect to the honeypot since the honeypots are online and reachable. From January 2019 to September 2021, ~1M logs have been collected. SPLUNK has been installed on the servers to monitor this collected extensive data and to search on this data.

The server specifications of the HAProxy machine are 2 GB ram and 1 CPU. All servers have Ubuntu 11 operating systems on them. No transaction takes place on this machine, and it only provides a proxy. Machines with honeypots consist of 4 GB ram and two premium CPUs. Currently, one HAproxy server and four honeypot machines

are open and stored in Digitalocean. Its monthly expense is about $60. It has been observed that up to 50 users can connect to a server simultaneously with these features.

3.1.1. Log Collection with Honeypot and CTF Evaluation. The "Capture-the-Flag (CTF)" contest is a special kind of cybersecurity competition designed to challenge its participants to solve computer security problems and/or capture and defend computer systems. The CTF aims to provide general knowledge on Capture-the-Flag (CTF) exercises. The CTF contains questions about general hacking knowledge, computer forensics, reverse engineering, web hacking, and cryptosystems. The volunteer hackers' personalities and experiments were learned with the Big-5 test and the Hacker Expertise test. By including the same people in the CTF, a connection will be established between their server logs and these test results. The methods, commands, and behaviors that users apply to find answers to the CTF questions will mark the honeypot specifications.

The information containing the honeypot logs of the same students was extracted, and a result file was created as in the example in Table 12. In Table 12, "F" represents "FALSE," "T" represents "TRUE," and "s." represents "seconds."

The cyber expertise rest, Big-5 Test, and Honeypot Logs are combined in a single spreadsheet, as depicted in Figure 4. The individual results of these tests were explained in the following sections.

3.2. Big-5 Personality Test and Cyber Expertise Test. In order to correlate the server behaviors and logs of the volunteer hacker group with their expertise and psychology, firstly, these people were taken to self-prepared tests. These tests are the 60-question Big-5 test and the 4-part cyber expertise test. After solving the test, we collect their logs to honeypot with a CTF.

3.2.1. Big-5 Personality Test and Evaluation. It is aimed to generate an idea about hackers' personalities without examining every hacker entering the system. There are different types of Big-5 tests in the literature as follows:

10 Question TIPI Big-5 Test

44 Question Big-5 Test

60 Question Big-5 Test (BFI-2)

50 Question new version of Big-5 Test

With these tests, different information about users can also be obtained using these additional features. Some of these other personalities (=facets), which are subgroups of the Big-5 personalities, are below:

Extraversion facets: sociability, assertiveness, and energy level

Agreeableness facets: compassion, respectfulness, and trust

Conscientiousness facets: organization, productiveness, and responsibility

Neuroticism facets: anxiety, depression, and emotional volatility

Openness facets: intellectual curiosity, aesthetic sensitivity, and creative imagination

This study has applied the 60 questions Big-5 Test named BFI-2 [23], providing the most comprehensive results for facets. Table 13 shows the example results of one participant's Big-5 test result.

The benchmark results include the following considerations for the participants:

Big-5: extraversion, agreeableness, openness, conscientiousness, and neuroticism

Facets: sociability, assertiveness, energy level, compassion, respectfulness, trust, organization, productiveness, anxiety, depression, emotional volatility, intellectual curiosity, aesthetic sensitivity, and creative imagination

(i) Evaluations are used in psychological assessment, respecting all the participants

(ii) Evaluations are based on the z and t-scores conducted in light of the test results from [23]

(iii) Numerical evaluations are determined as percent scores as conducted in literature

According to the Big-5 and facets test result, a score is calculated for each participant and question defined by Soto and John [23]. For instance, for the "extraversion", the following scores for the indicated question numbers are considered: 1, 6, 11R, 16 R, 21, 26R, 31 R, 36R, 41, 46, 51R, 56. For each of these question numbers, a score between 1 and 5 is given respecting the answers of the participants. If there exists a letter "R" near the question number, it means that the reverse score should be taken into account. If a score equals 5, then its reverse equals 1, and vice versa. Similarly, when R appears, score 4 indicates score 2 and score 3 does not change. For the characteristics of "extraversion," if a participant has the scores of (1, 2, 2, 3, 1, 4, 3, 5, 2, 2, 3, 3) for the question numbers given above, then its score is converted to (1, 2, 4, 3, 1, 2, 3, 1, 2, 2, 3, 3) respecting the reverse values indicated as "R" near the question numbers.

In order to conduct the first (i) analysis on the test results, the average value of the scores for each criterion and participant is calculated. For the above example the average score of the participant (*Pscore*) for the "extraversion" is $(1 + 2+4 + 3+1 + 2+3 + 1+2 + 2+3 + 3)/9 = 3$. Then, the average (*mean*) of all participants for the same criterion and the standard deviation (*std*) is calculated, i.e., *mean = 3.42 and std = 1.14*. After that, the corresponding z-score is calculated. After calculating the z-score, it is also converted to the t-score, which is generally used in the psychometric analysis.

With the help of the psychometric conversion table, the corresponding description to the calculated scores is determined, which is "average" for the calculated t-score. As a result, the extraversion characteristics of a participant can be stated as the "average" respecting all the participants that

Table 12: Example representation of Honeypot logs.

ID	A3	A5	A7	A8	A9	A10	A11	A12	A13	A14	A15	A17	A19	A20	A22
P1	T	T	F	T	F	F	T	F	T	9.0s.	T	F	T	F	T
P2	T	F	T	F	T	F	T	F	F	1.1s.	T	T	F	F	F
P3	T	F	F	T	F	T	T	F	T	1.6s.	F	F	T	F	F
P4	T	F	T	F	T	F	T	F	F	1.4s.	F	T	T	T	F
P5	T	F	T	T	T	F	T	F	F	21.6s.	F	F	F	T	F

	HONEYPOT LOGS (SIGNED SPECS)					C. EXPERT. TEST RES.	BIG-5 TEST RESULTS				
UNIQ-ID	|__A2	|__A3	|__A5	|__A7	|__A8	RESULTS	E	A	O	C	N
1	1	1	1	1	1	80	35,42	54,17	52,08	45,83	47,92
2	1	1	1	0	1	97	41,67	56,25	58,33	79,17	52,08
3	1	1	1	0	0	60	66,67	70,83	68,75	79,17	25,00
4	1	1	1	0	0	30	62,50	56,25	47,92	79,17	56,25
5	1	1	1	0	0	95	66,67	62,50	75,00	64,58	52,08
6	0	0	0	0	0	15	50,00	60,42	72,92	60,42	39,58
7	1	1	1	1	0	90	64,58	62,50	64,58	52,08	41,67
8	1	1	0	1	1	80	8,33	64,58	37,50	68,75	33,33
9	0	0	0	0	0	50	52,08	66,67	56,25	95,83	39,58
10	1	1	1	1	1	80	54,17	56,25	81,25	33,33	66,67
11	1	0	1	0	1	50	50,00	50,00	39,58	68,75	58,33
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
100	1	0	0	1	0	70	60,42	60,42	70,83	72,92	41,67

Figure 4: Example results of cyber expertise test, Big-5 test, and Honeypot Log.

Table 13: Example of the results.

User ID	Openness	Conscientiousness	Extraversion	Agreeableness	Neuroticism
A754abs1a	85.22	46.31	58.00	62.50	32.50

apply the tests. The same procedure is applied to all the participants for all big five and facet characteristics.

Besides gathering the results by respecting the average results of all participants, the descriptions are determined according to the results obtained by Soto and John [23], which is mentioned as the second analysis (ii). Thus, instead of using the calculated mean and standard deviation, the mean and standard deviation of the participants of the Soto and John [23] are used. Since the questions are the same as those of Soto and John [23], there is no need to use the results of these authors. The score of our participants, Pscore, does not change. Therefore, it can be inferred that we will test the results of our participants with respect to another group (a group that Soto and John [23] apply their tests) to see if we obtain similar descriptions. Likewise, the previous calculations, z-score, and t-score are calculated, and the description is determined concerning the psychometric conversion Table 14. In this table, the description correspondences of the participants' Big-5 and facet characteristics are determined according to the ranges.

Finally, another analysis that is independent of the other participants was applied, calculating the participant's compliance with the specified characters as a percentage.

Table 14: Psychometric conversion table description ranges.

Range (t-score)	Percentile rank	Description
>69	>97	Very superior
64–69	92–97	Superior
58–63	77–91	High average
43–57	25–76	Average
37–42	9–24	Low average
30–36	3–8	Borderline
28–29	2–2	Impaired
27–28	1–1	Mild
26–27	1–1	Moderate
24–25	1–1	Severe
<24	<1	Profound

Since this percent score does not depend on scores of other participants, it is referred to as individual score (i-score) and inspired from [23] calculated using equation (1), where $score_j$ is the score that the participant obtains from the question j of corresponding characteristic and nQ_k represents the total number of questions for the corresponding characteristic k. The constant value K is calculated as in equation (2):

$$i - \text{score} = \frac{K * \left(\sum_j \text{score}_j - nQ_k\right)}{96} * 100, \quad (1)$$

$$K = \frac{96}{4 * nQ_k}. \quad (2)$$

For example, Big-5 characteristics have 12 questions with different combinations (for some questions, their reverse values are calculated). Considering the above example, the total score of the participant is 27 $(1+2+4+3+1+2+3+1+2+2+3+3)$, $nQ_k = 12$, and $K = 2$; thus, the i-score of this participant is 31.25, which indicates that the participant is extroverted with a probability of 31%.

f the participant gets 1 point from all the related questions, he/she does not have that character at all, but if the participant gets 5 points from all the questions, it means that he/she has that character with 100% probability. In order to achieve this, in Equation (1), the total number of questions was subtracted from the total score. If the participant's all scores are 1, then he/she can get as many points as the total number of questions, and the difference between these two terms is equal to zero, so we can say that he has this character with 0 probability. Similarly, suppose the participant scores full points on all questions. In that case, the upper part of the equation will always equal 96 because the constant K value is calculated as 96 when the full score is taken (see equation (2)). Thus, we can say that the participant has this character 100%. The part of the results for these three criteria is given in Table 15. Results of the five participants are presented, and the descriptions are determined respecting the t-scores according to the first criterion. According to this small part of the results, we can conclude that both t-scores are similar. Thus, the corresponding descriptions are the same except for participant 3.

Big-5 results of the five participants were presented in Table 16. The participants' scores (i-score) and the descriptions were summarized for each characteristic of the Big-5.

3.2.2. Cyber Expertise Test and Evaluation. In the Big-5 Test, we obtained data about the hacker's personality, whose behavior we logged on the server. In this way, we aim to find out hackers' expertise, in another way of saying, how experienced, knowledgeable, and thus how dangerous they are. We searched for answers to these kinds of questions. Then, we can recognize whether the person who voluntarily takes the test and leaves the server's logs is the same person with a unique id and IP address or not.

Although there are studies in the literature on hacker expertise, there is no standard and widely used test such as the Big-5 test. The studies in the literature focus more on what kind of computer user he/she is [14]. However, these studies try to infer how immeasurable a computer user is rather than a hacker's experience. After the literature review, we selected the SEAM test for Cyber Expertise Test Methodology with our additions. We create our version of the security expertise test, combining current security expertise tests with inspiration of MITRE ATT&CK MATRIX [15]. The hacker expertise test consists of 4 parts.

Part 1: Security Expertise Scenario Test

Part 2: Techniques with Tactics Matching Test

Part 3: Tool Knowledge Test

Part 4: Attack Knowledge Test (MITRE ATT&CK MATRIX)

Security Expertise Scenario Test is performed using 3×5 cards relevant scenarios written on them; each scenario contains one deep feature and one surface feature [24]. SEAM created validated scenarios. The scenarios point to a hacking concept, as given in Table 17. We have obtained the scenarios from the SEAM test. An example scenario is also in Table 17, column number 3.

An example of a hacking scenario with both a deep feature (system resource consumption) and a surface feature (financial data) is presented in Table 18.

The SEAM test wants to group these scenarios. Users are rated according to the deep and surface features they find. We also applied the same test in this part and graded the users for part 1. This test seems to be scientifically one of the most validated publications in the literature. Unfortunately, there are not many publications that one can find about the detection of hacker expertise. For this reason, the test is applied to volunteers, but we enhanced this test with other parts that we created.

Users are required to compose a group and use the suggested technique. With this method, we can use the same methodology with the SEAM test by using MITRE ATT&CK Matrix, which is considered the de facto standard for classifying adversary behaviors. For this aim, we have devised a test for grouping these behaviors and actions defined by ATT&CK techniques and procedures into ATT&CK tactics. Since some techniques can be grouped into more than one tactic in the ATT&CK framework, this test is also designed to accommodate this requirement. The groups are retrieved from ATT&CK Enterprise, and the techniques and procedures are randomly selected from the available methods. The questions in "Part 2: Techniques with Tactics Matching Test", "Part 3: Tool Knowledge Test", and "Part 4: Attack Knowledge Test" include multiple-choice and fill-the-matrix questions.

As a result of this test, we evaluate expert skills by the knowledge and fluency over the ATT&CK framework. The utilization of this framework as such is also one of the novel approaches that this research undertakes.

An example result of known hackers' cyber expertise test evaluation is in Table 19.

Cyber expertise test results: the 4-part exam questions were normalized between 0 and 1, resulting in a single result. In order to be able to classify with these results in Matlab, they are labeled as follows:

0–25 ⟶ low

25–50 ⟶ moderate

50–75 ⟶ good

75–100 ⟶ expert

Table 15: Example results of the participants.

ID	*P*-score	*z*-score	*t*-score	*z*-score [23]	*t*-score [23]	*i*-score %	Description
P1	2.33	−0.96	40.41	−1.34	36.62	33.33	Low average
P2	2.42	−0.89	41.15	−1.22	37.76	35.42	Low average
P3	4.83	1.24	62.40	2.09	70.87	95.83	High average
P4	2.83	−0.52	44.81	−0.65	43.47	45.83	Average
P5	2.75	−0.59	44.08	−0.77	42.33	43.75	Average

Table 16: Example results for the Big-5 test.

ID	Extraversion		Agreeableness		Openness		Conscientiousness		Neuroticism	
P1	33.3	Avg.	45.8	Avg.	45.8	Avg.	45.8	Avg.	45.8	Avg.
P2	35.4	Avg.	43.8	Avg.	58.3	Avg.	39.6	Avg.	47.9	Avg.
P3	95.8	Superior	91.7	Superior	64.8	Avg.	70.8	Avg.	10.4	Low avg.
P4	45.8	Avg.	52.8	Avg.	54.7	Avg.	52.1	Avg.	56.3	Avg.
P5	43.8	Avg.	47.9	Avg.	56.5	Avg.	50.0	Avg.	43.8	Avg.

Table 17: Hacking conceptual expertise scenarios.

Hack	#	Scenario
Removing log files	A	Eve compromises a machine looking for tax returns and modifies log files before exiting the system
Port scanning	B	Eve downloads the automated tool to scan for open ports of visitors
Phishing	C	Eve creates an e-mail mimicking a national bank and sends it to Kelly, asking her to send an overdraft payment to another account

Table 18: Hacking scenario matrix.

		Hypothesized surface features		
		Using prebuilt tools	Social media	Financial data
Hypothesized deep features	Authentication/authorization	H	D	O
	Hiding tracks	F	N	A

Table 19: Example results for the cyber expertise test.

Participant ID	Part 1 normalized	Part 2 normalized	Part 3 normalized	Part 4 normalized
P1	22	32	1	0
P2	51	31	1	0
P3	92	100	5	5
P4	57	9	1	2
P5	59	58	3	1

Table 20: Detailed information of participants.

Total participants	100
#Undergraduate students	20
#Graduate students	15
#More than five years work experience in cyber security field	13
#More than five years work experience in computer technologies	40
#Participated in more than 3 CTFs	15
#Hacked somewhere before	11
#Outside the cyber security domain	40
#Outside the computer science domain	10

4. Results and Analysis

Within this research, a total of 100 people were chosen as a sample group of known hackers. Most of these groups are hackers, computer experts, IT professionals, engineering students, and engineers. The detailed information of the participants is summarized in Table 20.

Of the 100 participants in this study, 27 were female and 73 were male. Ninety percent of the participants are computer science/engineering graduates, employees, or students. Ten percent are outside this area. Forty participants have more than five years of experience in the field of computer

technologies. About 30 participants have previously dealt with hacking/cyber security.

CTF questions were sent to the participants via a website or writeups pdf containing the questions. Questionnaires were created in Microsoft Office. Some of the attendees are invited guests who are working in the cyber security domain. At the same time, participation information was distributed to hackers via Discord, Telegram, and Slack channels. A CTF invitation was also sent to the MDISEC discord group, with about 4000 cyber security enthusiasts or hackers.

The target group (known hackers) participated in the Big-5 personality test, explained in detail in Section 3.2.1, and the Cyber Expertise test, explained in detail in Section 3.2.2. The log analysis of the target group was also examined by taking them to the honeypot with CTF.

In the results and analyses, we first examined the Big-5 personality, expertise test results of known hackers that we know are experienced in cyber security and computer science. Then, we have examined the logs they left via CTF.

We then examined the correlations between the logs and these tests. Finally, we trained the data, applied machine learning algorithms, made predictions for an unknown hacker, and examined the success of these predictions.

The following sections include the analysis results, the relative effects of the personalities and hacker expertise, and the prediction of the characteristics of a person who has an unknown attack on the systems.

First, the target group's analysis is provided to get information about their experience level and personality. Those analyses provide information about whether there is a relationship between personality classifications and levels of expertise of the target group. Based on the results of this analysis, we aimed to make various comments about whether personality tests can determine the level of expertise of an unknown person or vice versa. At the same time, A1...A22, marked from the logs left by known hackers via CTF, were examined. The correlations between these logs and their correlations with the tests were examined.

These analysis results led us to make predictions with data mining. Data mining has two functions: one is descriptive and the other is prediction. In this study, we used the methods of estimation with the help of the MATLAB program. We determined an unknown person's level of expertise and personality estimation using various classification and regression algorithms in this context. The machine learning algorithms are applied to the obtained data from the target group. The aim here is to determine how accurately we can predict the psychology and expertise of an unknown hacker when this person comes to the system.

The Sections 4.1 and 4.2 include the following analysis.

- The target group analyses of Big-5 Personalities and Expertise Tests
- Correlation within honeypot logs
- Correlation between Big-5 Personalities and honeypot logs
- Correlation between honeypot logs and Expertise Tests
- Correlation within Big-5 Personalities
- Correlation between Big-5 Personalities and Expertise Tests
- Correlation between Big-5 Facets and Expertise Tests

Moreover, double and triple correlations were examined, besides the single correlation analysis, and the interaction effects were also obtained in some cases.

Section 4.3 includes the following predictions using data mining algorithms:

- Predicting the expertise level and considering Honeypot logs
- Predicting the honeypot log from the Expertise test
- Predicting the expertise level and using Big-5 Personality

4.1. Big-5 Personality, Cyber Expertise, and Honeypot Log Analysis of Known Hackers. This section will examine the results of the tests we have done on our known hacker group consisting of 100 people. In this section, only the internal interpretations of the tests are included.

Table 21 presents the average results of participants' Big-5 (extraversion: E, agreeableness: A, openness: O, conscientiousness: C, and neuroticism: N) personalities. Table 22 presents the Facets (sociability: Soc, assertiveness: Asse, energy level: EnL, compassion: Com, respectfulness: Res, trust: Tru, organization: Org, productiveness: Pro, anxiety: Anx, depression: Dep, emotional volatility: Emo, intellectual curiosity: IntC, aesthetic sensitivity: AeS, and creative imagination: CreI) results of the same sample group.

As explained in the previous sections, the average results shown in Table 21 and 22 are calculated over 100 points. As seen from the table, the highest average value belongs to IntC, and the lowest average value belongs to depression, which gives an opinion on the personalities of our known hackers.

The correlations in Big-5 personalities are analyzed using SPSS program version 28.0. The significance test is conducted under a 95% confidence interval. Figure 5 displays the correlations between Big-5 personalities of our target group.

If the significance level is lower than 0.05, then we can say that the correlation is significant. Otherwise, we could not conclude any meaningful correlation between personality labels. As seen from Figure 5, agreeableness and openness are highly positively correlated on our data of known hackers. Neuroticism and Extraversion are highly negatively correlated. Since facets are subpersonalities of Big-5, the correlation results between the facets will follow a similar pattern as the Big-5 correlations.

As already underlined, one of the primary purposes of this article is to relate the hackers' operations on the server to Big-5 and expertise. In the previous section, it was explained how these logs were collected. The correlation between the logs is shown in Figure 6.

Table 21: Average Big-5 results of known hackers.

	E	A	O	C	N
AVG	60.63	65.24	68.20	67.74	44.97

Table 22: Average Big-5 results with facets of known hackers.

Soc	Asse	EnL	Com	Res	Tru	Org	Pro	Anx	Dep	Emo	IntC	AeS	CreI
56.63	61.99	68.88	63.26	71.65	58.52	67.55	66.41	54.29	37.31	43.31	71.21	62.94	68.94

Correlations of Big-5

		E	A	O	C	N
E	Pearson Correlation	1	.307**	.302**	.134	-.288**
	Sig. (2-tailed)		.002	.002	.185	.004
	N	99	99	99	99	99
A	Pearson Correlation	.307**	1	.362**	.343**	-.176
	Sig. (2-tailed)	.002		<.001	<.001	.082
	N	99	99	99	99	99
O	Pearson Correlation	.302**	.362**	1	.080	-.025
	Sig. (2-tailed)	.002	<.001		.430	.809
	N	99	99	99	99	99
C	Pearson Correlation	.134	.343**	.080	1	-.380**
	Sig. (2-tailed)	.185	<.001	.430		<.001
	N	99	99	99	99	99
N	Pearson Correlation	-.288**	-.176	-.025	-.380**	1
	Sig. (2-tailed)	.004	.082	.809	<.001	
	N	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 5: Correlations within Big-5 personalities.

Figure 6 shows several positive correlations between the logs, but the higher correlation belongs to A12 (download commands should be added) and A15 (file system is tested). Also, A15 is highly correlated with A5 (if "passwd" is entered or attempted). Also, there is a correlation between A9 (search commands such as "grep") and A17 (deleting tracks and history when exiting att&ck) that is meaningful because of our knowledge, and it can be assumed that, to realize A17, A9 must also occur. Another interesting result is that almost all the logs positively correlate with each other, and only A14 negatively correlates with the other logs. A14 is numeric, and it is event/command interarrival times. We expect that if the event-command interarrival times are short because the typing speed is high. Explanations of A1. . .A22 can be found In Section 4.1.

Honeypot design, creation, and marking of specifications are the highlights of our work. For this reason, the Cronbach alpha method was applied to measure the reliability of the CTF questions by looking at the specifications marked according to the CTF results. The results of the Cronbach alpha method are shown in Figure 7.

The table shows that the questions are consistent, looking at the specifications that hackers have flagged by solving CTF questions.

4.2. Correlations between the Tests and Server Logs of Known Hackers. In the previous section, the correlations within the tests and the averages of results were interpreted for known hackers. This section seeks a correlation between the binary represented logs (A1. . .A22) left by known hackers via CTF with Big-5 test and cyber expertise test. Likewise, it was investigated whether there could be a connection between Expertise and Big-5 Personalities.

Figure 8 presents the correlations between the logs and expertise. All the logs, except A14, are significantly positively correlated with the expertise. Log A14 negatively correlates with the expertise, which is an expected result since it is also negatively correlated with the other logs. We can interpret these results as the expertise of hackers increases as they mark the logs and write the correct commands to hack the server.

Figure 9 displays the correlations between the Logs and Big-5 personalities. Extraversion negatively correlates with A3, A7, and A15, and it does not have any positive correlation with the other logs. Conscientiousness positively correlates with the A5, A10, A15, and A20 and does not negatively. Finally, neuroticism negatively correlates with A9, A19, and A20 and does not positively correlate with the other logs.

Correlations of Logs

		A2	A3	A5	A7	A8	A11	A10	A9	A12	A13	A14	A15	A17	A19	A20	A22
A2	Pearson Correlation	1	.410**	.551**	.413**	.369**	.b	.226*	.438**	.440**	.344**	-.384**	.481**	.395**	.344**	.335**	.b
	Sig. (2-tailed)		<.001	<.001	<.001	<.001	.	.025	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A3	Pearson Correlation	.410**	1	.219*	.309**	.368**	.b	.321**	.141	.501**	.615**	-.236*	.377**	.391**	.256*	.326**	.b
	Sig. (2-tailed)	<.001		.029	.002	<.001	.	.001	.164	<.001	<.001	.019	<.001	<.001	.011	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A5	Pearson Correlation	.551**	.219*	1	.332**	.411**	.b	.241*	.169	.552**	.314**	-.289**	.637**	.295**	.447**	.319**	.b
	Sig. (2-tailed)	<.001	.029		<.001	<.001	.	.016	.094	<.001	.002	.004	<.001	.003	<.001	.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A7	Pearson Correlation	.413**	.309**	.332**	1	.404**	.b	.431**	.480**	.428**	.512**	-.240*	.446**	.652**	.558**	.453**	.b
	Sig. (2-tailed)	<.001	.002	<.001		<.001	.	<.001	<.001	<.001	<.001	.017	<.001	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A8	Pearson Correlation	.369**	.368**	.411**	.404**	1	.b	.491**	.318**	.311**	.504**	-.184	.353**	.438**	.552**	.410**	.b
	Sig. (2-tailed)	<.001	<.001	<.001	<.001		.	<.001	.001	-.002	<.001	.068	<.001	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A11	Pearson Correlation	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.	.	.	.	.		.	.	.	.	.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A10	Pearson Correlation	.226*	.321**	.241*	.431**	.491**	.b	1	.184	.226*	.471**	-.133	.314**	.336**	.409**	.466**	.b
	Sig. (2-tailed)	.025	.001	.016	<.001	<.001	.		.069	.024	<.001	.190	.002	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A9	Pearson Correlation	.438**	.141	.169	.480**	.318**	.b	.184	1	.316**	.316**	-.254*	.176	.493**	.406**	.479**	.b
	Sig. (2-tailed)	<.001	.164	.094	<.001	.001	.	.069		.001	.001	.011	.081	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A12	Pearson Correlation	.440**	.501**	.552**	.428**	.311**	.b	.226*	.316**	1	.420**	-.257*	.667**	.511**	.375**	.575**	.b
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	.002	.	.024	.001		<.001	.010	<.001	<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A13	Pearson Correlation	.344**	.615**	.314**	.512**	.504**	.b	.471**	.316**	.420**	1	-.200*	.339**	.406**	.561**	.236*	.b
	Sig. (2-tailed)	<.001	<.001	.002	<.001	<.001	.	<.001	.001	<.001		.047	<.001	<.001	<.001	.019	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A14	Pearson Correlation	-.384**	-.236*	-.289**	-.240*	-.184	.b	-.133	-.254*	-.257*	-.200*	1	-.251*	-.229*	-.199*	-.224*	.b
	Sig. (2-tailed)	<.001	.019	.004	.017	.068	.	.190	.011	.010	.047		.012	.023	.048	.026	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A15	Pearson Correlation	.481**	.377**	.637**	.446**	.353**	.b	.314**	.176	.667**	.339**	-.251*	1	.367**	.428**	.433**	.b
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	.	.002	.081	<.001	<.001	.012		<.001	<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A17	Pearson Correlation	.395**	.391**	.295**	.652**	.438**	.b	.336**	.493**	.511**	.406**	-.229*	.367**	1	.406**	.578**	.b
	Sig. (2-tailed)	<.001	<.001	.003	<.001	<.001	.	<.001	<.001	<.001	<.001	.023	<.001		<.001	<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A19	Pearson Correlation	.344**	.256*	.447**	.558**	.552**	.b	.409**	.406**	.375**	.561**	-.199*	.428**	.406**	1	.376**	.b
	Sig. (2-tailed)	<.001	.011	<.001	<.001	<.001	.	<.001	<.001	<.001	<.001	.048	<.001	<.001		<.001	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A20	Pearson Correlation	.335**	.326**	.319**	.453**	.410**	.b	.466**	.479**	.575**	.236*	-.224*	.433**	.578**	.376**	1	.b
	Sig. (2-tailed)	<.001	<.001	.001	<.001	<.001	.	<.001	<.001	<.001	.019	.026	<.001	<.001	<.001		.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A22	Pearson Correlation	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).
b. Cannot be computed because at least one of the variables is constant.

Figure 6: Correlations within the logs.

Figure 10 indicates the correlations between the logs, Big-5 personalities, and expertise together.

Figure 11 presents that, as the marked logs increase, the expertise increases. Thus, the experts are expected to mark more logs in the honeypot. Similarly, as the marked logs increase, the participants' average keyboard time (A14) increases, which indicates that those who leave more logs write faster code. Thus, the correlation results also state that these people are experts.

After analyzing logs with tests, our expectation here is to find a connection between the Big-5 personalities and the expertise of the target group. First, we will investigate the result of the target group by performing correlation analysis. Thus, by applying machine learning, we can make a Big-5 prediction of a person who does not know by looking at their expertise and making an expertise prediction by looking at the Big-5 personality and logs.

Figure 12 represents the correlation between the Big-5 personalities and the expertise. However, no significant correlation was found between expertise and any personality traits. In this case, we can say that no personality

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.897	.897	13

Item Statistics

	Mean	Std. Deviation	N
A2	.7778	.41786	99
A3	.4242	.49674	99
A5	.5152	.50231	99
A7	.3737	.48626	99
A8	.3232	.47009	99
A9	.5859	.49508	99
A10	.1515	.36037	99
A12	.4040	.49320	99
A13	.2929	.45742	99
A15	.4949	.50252	99
A17	.3535	.48050	99
A19	.2929	.45742	99
A20	.3434	.47727	99

Figure 7: Cronbach alpha reliability analysis of CTF questions.

trait gives us direct information about the level of expertise.

When we examined the results, we consider that there may be a dual effect of Neuroticism-Extraversion (N_E) and Neuroticism-Openness (N_O) on the level of expertise. This dual effect was analyzed, and the result is shown in Figure 13. According to Figure 13, it was seen that N_E has a negative correlation with expertise. This correlation indicates that the level of expertise increases as the N_E level decreases.

Figure 14 shows the correlation between the Big-5 facets and the expertise. An interesting result is achieved, which is a negative correlation between the organization and the expertise. Although expertise did not significantly correlate with conscientiousness, which is in the upper category of organization, there was a negative correlation between the expertise and the organization.

Table 23 summarizes the results of the expertise and Big-5 personalities. The average results of all the participants are given in the "AVGALL" row. In contrast, the other rows indicate the average results for the expertise levels greater than 70, 85, and 95, lower than 30, and between 50 and 70, respectively.

Table 23 indicates that, as the expertise level of the participants increases, the conscientiousness personality results also increase. However, a higher expertise level leads to lower neuroticism for the target group.

4.3. Predictions on Unknown Hackers with Data Mining Algorithms. The paper's main aim is to predict the expertise and psychology of an unknown hacker by looking at their behavior (logs) on the honeypot. Thus, in Sections 4.3.1 and 4.3.2, prediction methods are described.

4.3.1. Predicting with Regression Learner. We used the predictive methods in data mining on MATLAB 2020b. First, we applied the regression learner method. We prepared our data for Matlab. Since we will be using regression learner, we have prepared all the data numerically. Thus, the regression learner will be able to make numerical predictions for us. Evaluation of regression models differs according to classification. MSE (mean squared error) and RMSE (root mean square error) are two methods used to evaluate regression models.

The first prediction is between honeypot logs and the expertise test. Estimation was made using the regression learning algorithms indicated in Figure 15. Note that the cross validation is defined as 10.

Correlations Logs and Expertise

		A2	A3	A5	A7	A8	A11	A10	A9	A12	A13	A14	A15	A17	A19	A20	A22	Expertise
A2	Pearson Correlation	1	.410**	.551**	.413**	.369**	.b	.226*	.438**	.440**	.344**	-.384**	.481**	.395**	.344**	.335**	.b	.634**
	Sig. (2-tailed)		<.001	<.001	<.001	<.001	.	.025	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A3	Pearson Correlation	.410**	1	.219*	.309**	.368**	.b	.321**	.141	.501**	.615**	-.236*	.377**	.391**	.256*	.326**	.b	.471**
	Sig. (2-tailed)	<.001		.029	.002	<.001	.	.001	.164	<.001	<.001	.019	<.001	<.001	.011	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A5	Pearson Correlation	.551**	.219*	1	.332**	.411**	.b	.241*	.169	.552**	.314**	-.289**	.637**	.295**	.447**	.319**	.b	.642**
	Sig. (2-tailed)	<.001	.029		<.001	<.001	.	.016	.094	<.001	.002	.004	<.001	.003	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A7	Pearson Correlation	.413**	.309**	.332**	1	.404**	.b	.431**	.480**	.428**	.512**	-.240*	.446**	.652**	.558**	.453**	.b	.549**
	Sig. (2-tailed)	<.001	.002	<.001		<.001	.	<.001	<.001	<.001	<.001	.017	<.001	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A8	Pearson Correlation	.369**	.368**	.411**	.404**	1	.b	.491**	.318**	.311**	.504**	-.184	.353**	.438**	.552**	.410**	.b	.631**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001		.	<.001	.001	.002	<.001	.068	<.001	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A11	Pearson Correlation	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.	.	.	.	.		.	.	.	.	.	.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A10	Pearson Correlation	.226*	.321**	.241*	.431**	.491**	.b	1	.184	.226*	.471**	-.133	.314**	.336**	.409**	.466**	.b	.421**
	Sig. (2-tailed)	.025	.001	.016	<.001	<.001	.		.069	.024	<.001	.190	.002	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A9	Pearson Correlation	.438**	.141	.169	.480**	.318**	.b	.184	1	.316**	.316**	-.254*	.176	.493**	.406**	.479**	.b	.457**
	Sig. (2-tailed)	<.001	.164	.094	<.001	.001	.	.069		.001	.001	.011	.081	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A12	Pearson Correlation	.440**	.501**	.552**	.428**	.311**	.b	.226*	.316**	1	.420**	-.257*	.667**	.511**	.375**	.575**	.b	.604**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	.002	.	.024	.001		<.001	.010	<.001	<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A13	Pearson Correlation	.344**	.615**	.314**	.512**	.504**	.b	.471**	.316**	.420**	1	-.200*	.339**	.406**	.561**	.236*	.b	.613**
	Sig. (2-tailed)	<.001	<.001	.002	<.001	<.001	.	<.001	.001	<.001		.047	<.001	<.001	<.001	.019	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A14	Pearson Correlation	-.384**	-.236*	-.289**	-.240*	-.184	.b	-.133	-.254*	-.257*	-.200*	1	-.251*	-.229*	-.199*	-.224*	.b	-.227*
	Sig. (2-tailed)	<.001	.019	.004	.017	.068	.	.190	.011	.010	.047		.012	.023	.048	.026	.	.024
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A15	Pearson Correlation	.481**	.377**	.637**	.446**	.353**	.b	.314**	.176	.667**	.339**	-.251*	1	.367**	.428**	.433**	.b	.602**
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	.	.002	.081	<.001	<.001	.012		<.001	<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A17	Pearson Correlation	.395**	.391**	.295**	.652**	.438**	.b	.336**	.493**	.511**	.406**	-.229*	.367**	1	.406**	.578**	.b	.431**
	Sig. (2-tailed)	<.001	<.001	.003	<.001	<.001	.	<.001	<.001	<.001	<.001	.023	<.001		<.001	<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A19	Pearson Correlation	.344**	.256*	.447**	.558**	.552**	.b	.409**	.406**	.375**	.561**	-.199*	.428**	.406**	1	.376**	.b	.693**
	Sig. (2-tailed)	<.001	.011	<.001	<.001	<.001	.	<.001	<.001	<.001	<.001	.048	<.001	<.001		<.001	.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A20	Pearson Correlation	.335**	.326**	.319**	.453**	.410**	.b	.466**	.479**	.575**	.236*	-.224*	.433**	.578**	.376**	1	.b	.521**
	Sig. (2-tailed)	<.001	<.001	.001	<.001	<.001	.	<.001	<.001	<.001	.019	.026	<.001	<.001	<.001		.	<.001
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A22	Pearson Correlation	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b	.b
	Sig. (2-tailed)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.		.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
Expertise	Pearson Correlation	.634**	.471**	.642**	.549**	.631**	.b	.421**	.457**	.604**	.613**	-.227*	.602**	.431**	.693**	.521**	.b	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	.	<.001	<.001	<.001	<.001	.024	<.001	<.001	<.001	<.001	.	
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).
b. Cannot be computed because at least one of the variables is constant.

Figure 8: Correlations between the logs and expertise.

The minimum RMSE is obtained as 9.6591 determined by Gaussian process regression, which indicates that this algorithm is the best performing. It means that, with the 9.6591 RMSE, we can predict expertise by looking at the honeypot logs. The RMSE value is between 0 and 100; close to 0 indicates its performance.

The results of the regression learning algorithm applied to the Big-5, Honeypot Logs. Expertise test results are given in Table 24. We can predict expertise from honeypot logs, honeypot logs from the expertise, and Big-5 results and vice versa. In the following table, predictors are the data to predict, and predicted response is the data we try to predict.

Correlations Logs with Big-5

		A2	A3	A5	A7	A8	A9	A10	A11	A12	A13	A14	A15	A17	A19	A20	A22	E	A	O	C	N
A2	Pearson Correlation	1	.410**	.551**	.413**	.369**	.438**	.226*	.c	.440**	.344**	-.384**	.481**	.395**	.344**	.335**	.c	-.153	-.083	-.175	.030	.042
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.025	.	.000	.000	.000	000	.000	.000	.001	.	.130	.415	.084	.765	.681
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A3	Pearson Correlation	.410**	1	.219*	.309**	.368**	.141	.321**	.c	.501**	.615**	-.236*	.377**	.391**	.256*	.326**	.c	-.223*	-.111	-.079	.001	.135
	Sig. (2-tailed)	.000		.029	.002	.000	.164	.001	.	.000	.000	.019	.000	.000	.011	.001	.	.027	.275	.434	.993	.183
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A5	Pearson Correlation	.551**	.219*	1	.332**	.411**	.169	.241*	.c	.552**	.314**	-.289**	.637**	.295**	.447**	.319**	.c	-.019	.028	-.036	.273**	-.107
	Sig. (2-tailed)	.000	.029		.001	.000	.094	.016	.	.000	.002	.004	.000	.003	.000	.001	.	.853	.781	.724	.006	.291
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A7	Pearson Correlation	.413**	.309**	.332**	1	.404**	.480**	.431**	.c	.428**	.512**	-.240*	.446**	.652**	.558**	.453**	.c	-.235*	-.007	.022	-.028	-.069
	Sig. (2-tailed)	.000	.002	.001		.000	.000	.000	.	.000	.000	.017	.000	.000	.000	.000	.	.019	.947	.828	.782	.498
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A8	Pearson Correlation	.369**	.368**	.411**	.404**	1	.318**	.491**	.c	.311**	.504**	-.184	.353**	.438**	.552**	.410**	.c	-.138	.030	-.118	.184	-.117
	Sig. (2-tailed)	.000	.000	.000	.000		.001	.000	.	.002	.000	.068	.000	.000	.000	.000	.	.174	.768	.243	.069	.249
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A9	Pearson Correlation	.438**	.141	.169	.480**	.318**	1	.184	.c	.316**	.316**	-.254*	.176	.493**	.406**	.479**	.c	-.003	-.066	-.026	-.046	-.223*
	Sig. (2-tailed)	.000	.164	.094	.000	.001		.069	.	.001	.001	.011	.081	.000	.000	.000	.	.979	.515	.800	.649	.026
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A10	Pearson Correlation	.226*	.321**	.241*	.431**	.491**	.184	1	.c	.226*	.471**	-.133	.314**	.336**	.409**	.466**	.c	-.130	.018	.021	.209*	-.066
	Sig. (2-tailed)	.025	.001	.016	.000	.000	.069		.	.024	.000	.190	.002	.001	.000	.000	.	.201	.856	.835	.038	.519
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A11	Pearson Correlation	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c
	Sig. (2-tailed)	.	.	.	.	.	.	.		.	.	.	.	.	.	.	.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A12	Pearson Correlation	.440**	.501**	.552**	.428**	.311**	.316**	.226*	.c	1	.420**	-.257*	.667**	.511**	.375**	.575**	.c	-.180	-.130	-.063	.114	.045
	Sig. (2-tailed)	.000	.000	.000	.000	.002	.001	.024	.		.000	.010	.000	.000	.000	.000	.	.074	.201	.536	.261	.660
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A13	Pearson Correlation	.344**	.615**	.314**	.512**	.504**	.316**	.471**	.c	.420**	1	-.200*	.339**	.406**	.561**	.236*	.c	-.150	-.062	.011	.024	.011
	Sig. (2-tailed)	.000	.000	.002	.000	.000	.001	.000	.	.000		.047	.001	.000	.000	.019	.	.137	.539	.916	.814	.914
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A14	Pearson Correlation	-.384**	-.236*	-.289**	-.240*	-.184	-.254*	-.133	.c	-.257*	-.200*	1	-.251*	-.229*	-.199*	-.224*	.c	.145	.125	.068	.046	.072
	Sig. (2-tailed)	.000	.019	.004	.017	.068	.011	.190	.	.010	.047		.012	.023	.048	.026	.	.153	.218	.502	.655	.480
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A15	Pearson Correlation	.481**	.377**	.637	.446**	.353**	.176	.314**	.c	.667**	.339**	-.251*	1	.367**	.428**	.433**	.c	-.222*	-.046	-.053	.227*	.072
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.081	.002	.	.000	.001	.012		.000	.000	.000	.	.027	.654	.603	.024	.480
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A17	Pearson Correlation	.395**	.391**	.295**	.652**	.438**	.493**	.336**	.c	.511**	.406**	-.229*	.367**	1	.406**	.578**	.c	-.065	-.042	.052	-.017	-.046
	Sig. (2-tailed)	.000	.000	.003	.000	.000	.000	.001	.	.000	.000	.023	.000		.000	.000	.	.520	.679	.611	.867	.653
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A19	Pearson Correlation	.344**	.256*	.447**	.558**	.552**	.406**	.409**	.c	.375**	.561**	-.199*	.428**	.406**	1	.376**	.c	-.043	.053	.007	.152	-.211*
	Sig. (2-tailed)	.000	.011	.000	.000	.000	.000	.000	.	.000	.000	.048	.000	.000		.000	.	.670	.605	.948	.134	.036
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A20	Pearson Correlation	.335**	.326**	.319**	.453**	.410**	.479**	.466**	.c	.575**	.236*	-.224*	.433**	.578**	.376**	1	.c	-.033	.078	.031	.198*	-.208*
	Sig. (2-tailed)	.001	.001	.001	.000	.000	.000	.000	.	.000	.019	.026	.000	.000	.000		.	.742	.444	.759	.050	.039
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A22	Pearson Correlation	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c
	Sig. (2-tailed)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
E	Pearson Correlation	-.153	-.223*	-.019	-.235*	-.138	-.003	-.130	.c	-.180	-.150	.145	-.222*	-.065	-.043	-.033	.c	1	.307**	.302**	.134	-.288**
	Sig. (2-tailed)	.130	.027	.853	.019	.174	.979	.201	.	.074	.137	.153	.027	.520	.670	.742	.		.002	.002	.185	.004
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A	Pearson Correlation	.083	-.111	.028	-.007	.030	-.066	.018	.c	-.130	-.062	.125	-.046	-.042	.053	.078	.c	.307**	1	.362**	.343**	-.176
	Sig. (2-tailed)	.415	.275	.781	.947	.768	.515	.856	.	.201	.539	.218	.654	.679	.605	.444	.	.002		.000	.001	.082
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
O	Pearson Correlation	-.175	-.079	-.036	.022	-.118	-.026	-.021	.c	-.063	.011	.068	-.053	.052	.007	.031	.c	.302**	.362**	1	.080	-.025
	Sig. (2-tailed)	.084	.434	.724	.828	.243	.800	.835	.	.536	.916	.502	.603	.611	.948	.759	.	.002	.000		.430	.809
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
C	Pearson Correlation	.030	.001	.273**	-.028	.184	-.046	.209*	.c	.114	.024	.046	.227*	-.017	.152	.198*	.c	.134	.343**	.080	1	-.380**
	Sig. (2-tailed)	.765	.993	.006	.782	.069	.649	.038	.	.261	.814	.655	.024	.867	.134	.050	.	.185	.001	.430		.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
N	Pearson Correlation	.042	.135	-.107	-.069	-.117	-.223*	-.066	.c	.045	.011	.072	.072	.046	-.211*	-.208*	.c	-.288**	.176	.025	-.380**	1
	Sig. (2-tailed)	.681	.183	.291	.498	.249	.026	.519	.	660	.914	.480	.480	.653	.036	.039	.	.004	.082	.809	.000	
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).
c. Cannot be computed because at least one of the variables is constant.

Figure 9: Correlations between the logs and Big-5 personalities.

Table 24 summarizes the best performing algorithms with their RMSE values for different predictors on different responses. The following data mining algorithms are tried for regression learner: Linear Regression (Linear, Interactions Linear, and Robust Linear), Stepwise Linear Regression (Stepwise Linear), Tree (Fine Tree, Medium Tree, and Coarse Tree), SVM (Linear SVM, Quadratic SVM, Cubic SVM, Fine Gaussian SVM, Medium Gaussian SVM, and Coarse Gaussian SVM), Ensemble (Boasted Trees and Bagged Trees), and Gaussian Process Regression (Squared Exponential GPR, Matern 5/2 GPR, Exponential GPR, and Rational Quadratic GPR).

Correlations Big5-Logs-Exp

		A2	A3	A5	A7	A8	A9	A10	A11	A12	A13	A14	A15	A17	A19	A20	A22	E	A	O	C	N	Expertise
A2	Pearson Correlation	1	.410**	.551	.413**	.369**	.438**	.226*	.c	.440**	.344**	-.384**	.481**	.395**	.344**	.335**	.c	-.153	-.083	-.175	.030	.042	.634**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.025	.	.000	.000	.000	.000	.000	.000	.001	.	.130	.415	.084	.765	.681	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A3	Pearson Correlation	.410**	1	.219*	.309**	.368**	.141	.321**	.c	.501**	.615**	-.236*	.377**	.391**	.256*	.326**	.c	-.223*	-.111	-.079	.001	.135	.471**
	Sig. (2-tailed)	.000		.029	.002	.000	.164	.001	.	.000	.000	.019	.000	.000	.011	.001	.	.027	.275	.434	.993	.183	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A5	Pearson Correlation	.551**	.219*	1	.332**	.411**	.169	.241*	.c	.552**	.314**	-.289**	.637**	.295**	.447**	.319**	.c	-.019	.028	-.036	.273**	-.107	.642**
	Sig. (2-tailed)	.000	.029		.001	.000	.094	.016	.	.000	.002	.004	.000	.003	.000	.001	.	.853	.781	.724	.006	.291	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A7	Pearson Correlation	.413**	.309**	.332**	1	.404**	.480**	.431**	.c	.428**	.512**	-.240*	.446**	.652**	.558**	.453**	.c	-.235*	-.007	.022	-.028	-.069	.549**
	Sig. (2-tailed)	.000	.002	.001		.000	.000	.000	.	.000	.000	.017	.000	.000	.000	.000	.	.019	.947	.828	.782	.498	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A8	Pearson Correlation	.369**	.368**	.411**	.404**	1	.318**	.491**	.c	.311**	.504**	-.184	.353**	.438**	.552**	.410**	.c	-.138	.030	-.118	.184	-.117	.631**
	Sig. (2-tailed)	.000	.000	.000	.000		.001	.000	.	.002	.000	.068	.000	.000	.000	.000	.	.174	.768	.243	.069	.249	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A9	Pearson Correlation	.438**	.141	.169	.480**	.318**	1	.184	.c	.316**	.316**	-.254*	.176	.493**	.406**	.479**	.c	-.003	-.066	-.026	-.046	-.223*	.457**
	Sig. (2-tailed)	.000	.164	.094	.000	.001		.069	.	.001	.001	.011	.081	.000	.000	.000	.	.979	.515	.800	.649	.026	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A10	Pearson Correlation	.226*	.321**	.241*	.431**	.491**	.184	1	.c	.226*	.471**	-.133	.314**	.336**	.409**	.466**	.c	-.130	.018	-.021	.209*	-.066	.421**
	Sig. (2-tailed)	.025	.001	.016	.000	.000	.069		.	.024	.000	.190	.002	.001	.000	.000	.	.201	.856	.835	.038	.519	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A11	Pearson Correlation	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c
	Sig. (2-tailed)	.	.	.	.	.	.	.		.	.	.	.	.	.	.	.	.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A12	Pearson Correlation	.440**	.501**	.552**	.428**	.311**	.316**	.226*	.c	1	.420**	-.257*	.667**	.511**	.375**	.575**	ç	-.180	-.130	-.063	.114	.045	.604**
	Sig. (2-tailed)	.000	.000	.000	.000	.002	.001	.024	.		.000	.010	.000	.000	.000	.000	.	.074	.201	.536	.261	.660	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A13	Pearson Correlation	.344**	.615**	.314**	.512**	.504**	.316**	.471**	.c	.420**	1	-.200*	.339**	.406**	.561**	.236*	.c	-.150	-.062	.011	.024	.011	.613**
	Sig. (2-tailed)	.000	.000	.002	.000	.000	.001	.000	.	.000		.047	.001	.000	.000	.019	.	.137	.539	.916	.814	.914	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A14	Pearson Correlation	-.384**	-.236*	-.289**	-.240*	-.184	-.254*	-.133	.c	-.257*	-.200*	1	-.251*	-.229*	-.199*	-.224*	.c	.145	.125	.068	.046	-.072	-.227*
	Sig. (2-tailed)	.000	.019	.004	.017	.068	.011	.190	.	.010	.047		.012	.023	.048	.026	.	.153	.218	.502	.655	.480	.024
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A15	Pearson Correlation	.481**	.377**	.637**	.446**	.353**	.176	.314**	.c	.667**	.339**	-.251*	1	.367**	.428**	.433**	.c	-.222*	-.046	-.053	.227*	-.072	.602**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.081	.002	.	.000	.001	.012		.000	.000	.000	.	.027	.654	.603	.024	.480	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A17	Pearson Correlation	.395**	.391**	.295**	.652**	.438**	.493**	.336**	.c	.511**	.406**	-.229*	.367**	1	.406**	.578**	.c	-.065	-.042	.052	-.017	-.046	.431**
	Sig. (2-tailed)	.000	.000	.003	.000	.000	.000	.001	.	.000	.000	.023	.000		.000	.000	.	.520	.679	.611	.867	.653	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A19	Pearson Correlation	.344**	.256*	.447**	.558**	.552**	.406**	.409**	.c	.375**	.561**	-.199*	.428**	.406**	1	.376**	.c	-.043	.053	.007	.152	-.211*	.693**
	Sig. (2-tailed)	.000	.011	.000	.000	.000	.000	.000	.	.000	.000	.048	.000	.000		.000	.	.670	.605	.948	.134	.036	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A20	Pearson Correlation	.335**	.326**	.319**	.453**	.410**	.479**	.466**	.c	.575**	.236*	-.224*	.433**	.578**	.376**	1	.c	-.033	.078	.031	.198*	-.208*	.521**
	Sig. (2-tailed)	.001	.001	.001	.000	.000	.000	.000	.	.000	.019	.026	.000	.000	.000		.	.742	.444	.759	.050	.039	.000
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A22	Pearson Correlation	.	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c	.c
	Sig. (2-tailed)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.		.	.	.	.	.	.
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
E	Pearson Correlation	-.153	-.223*	-.019	-.235*	-.138	-.003	-.130	.c	-.180	-.150	.145	-.222*	-.065	-.043	-.033	.c	1	.307**	.302**	.134	-.288**	-.101
	Sig. (2-tailed)	.130	.027	.853	.019	.174	.979	.201	.	.074	.137	.153	.027	.520	.670	.742	.		.002	.002	.185	.004	.318
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
A	Pearson Correlation	-.083	-.111	.028	-.007	.030	-.066	.018	.c	-.130	-.062	.125	-.046	-.042	.053	.078	.c	.307**	1	.362**	.343**	.176	-.056
	Sig. (2-tailed)	.415	.275	.781	.947	.768	.515	.856	.	.201	.539	.218	.654	.679	.605	.444	.	.002		.000	.001	.082	.579
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
O	Pearson Correlation	-.175	-.079	-.036	.022	-.118	-.026	-.021	.c	-.063	.011	.068	-.053	.052	.007	.031	.c	.302**	.362**	1	.080	-.025	-.086
	Sig. (2-tailed)	.084	.434	.724	.828	.243	.800	.835	.	.536	.916	.502	.603	.611	.948	.759	.	.002	.000		.430	.809	.399
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
C	Pearson Correlation	.030	.001	.273**	-.028	.184	-.046	.209*	.c	.114	.024	.046	.227*	-.017	.152	.198*	.c	.134	.343**	.080	1	-.380**	.184
	Sig. (2-tailed)	.765	.993	.006	.782	.069	.649	.038	.	.261	.814	.655	.024	.867	.134	.050	.	.185	.001	.430		.000	.068
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
N	Pearson Correlation	.042	.135	-.107	-.069	-.117	-.223*	.066	.c	.045	.011	-.072	-.072	-.046	-.211*	-.208*	.c	-.288**	-.176	-.025	-.380**	1	-.139
	Sig. (2-tailed)	.681	.183	.291	.498	.249	.026	.519	.	.660	.914	.480	.480	.653	.036	.039	.	.004	.082	.809	.000		.168
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99
Expertise	Pearson Correlation	.634**	.471**	.642**	.549**	.631**	.457**	.421**	.c	.604**	.613**	-.227*	.602**	.431**	.693**	.521**	.c	-.101	-.056	-.086	.184	-.139	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.	.000	.000	.024	.000	.000	.000	.000	.	.318	.579	.399	.068	.168	
	N	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).
c. Cannot be computed because at least one of the variables is constant.

Figure 10: Correlations between the logs, Big-5 personalities, and expertise.

The trained model is used to make predictions that give insights for unknown hackers. We composed a new example that is not included in our dataset. In order to verify the effectiveness of our predictions, our new example is generated respecting data from our dataset, which has an expertise result of 95.

The generated honeypot logs of the unknown hacker are presented in Table 25. After applying the trained model to

Correlations

		SignedHoneypLabel	Expertise	AvgTimeKeyboard
SignedHoneypLabel	Pearson Correlation	1	.836**	-.402**
	Sig. (2 -tailed)		<.001	<.001
	N	99	99	99
Expertise	Pearson Correlation	.836**	1	-.307**
	Sig. (2-tailed)	<.001		.002
	N	99	99	99
AvgTimeKeyboard	Pearson Correlation	-.402**	-.307**	1
	Sig. (2-tailed)	<.001	.002	
	N	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 11: Correlations between marked logs, expertise, and keyboard times.

Correlations Big5 Exp

		E	A	O	C	N	Expertise
E	Pearson Correlation	1	.307**	.302**	.134	-.288**	-.101
	Sig. (2-tailed)		.002	.002	.185	.004	.318
	N	99	99	99	99	99	99
A	Pearson Correlation	.307**	1	.362**	.343**	-.176	-.056
	Sig. (2-tailed)	.002		<.001	<.001	.082	.579
	N	99	99	99	99	99	99
O	Pearson Correlation	.302**	.362**	1	.080	-.025	-.086
	Sig. (2-tailed)	.002	<.001		.430	.809	.399
	N	99	99	99	99	99	99
C	Pearson Correlation	.134	.343**	.080	1	-.380**	.184
	Sig. (2-tailed)	.185	<.001	.430		<.001	.068
	N	99	99	99	99	99	99
N	Pearson Correlation	-.288**	-.176	-.025	-.380**	1	-.139
	Sig. (2-tailed)	.004	.082	.809	<.001		.168
	N	99	99	99	99	99	99
Expertise	Pearson Correlation	-.101	-.056	-.086	.184	-.139	1
	Sig. (2-tailed)	.318	.579	.399	.068	.168	
	N	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 12: Correlations between Big-5 and expertise.

the new data below, we obtained its expertise grade as 93.4854, similar to the known hackers 95. Therefore, we achieved the desired result.

Likewise, we will try to predict neuroticism with any log. The same example with Table 25 indicates a neuroticism value of 34.5368. When we look at the real neuroticism value of a participant with similar data, we obtain 33.33. These comparisons give us the chance to make predictions about psychology and expertise by looking at the logs and vice versa.

4.3.2. Predicting with Classification Learner. In Section 4.3.1, analysis using the regression learner was mentioned. In order to strengthen the analysis and compare the methods, classification learner algorithms have also been tried. For this, the data were prepared categorically. Since it gave numerical results in regression learning tried in Section 4.2, the data were prepared numerically. Our dataset has been trained and analyzed with Tree (Fine, Medium, and Coarse), Naive Bayes (Gaussian and Kernel), SVM (Linear, Quadratic, Cubic, and Fine Gaussian), and Ensemble (Boasted, Bagged, and RUBoasted Trees) classification learning methods.

The success of the classifier is determined by the area under the curve (AUC). Therefore, the larger the field, the more successful the classifier (model). The fact that the area under the curve is 1 (which is not a very realistic value) means

Correlations

		E	A	O	C	N	N_E	N_O	Expertise
E	Pearson Correlation	1	.307**	.302**	.134	-.288**	.282**	-.163	-.101
	Sig. (2-tailed)		.002	.002	.185	.004	.005	.107	.318
	N	99	99	99	99	99	99	99	99
A	Pearson Correlation	.307**	1	.362**	.343**	-.176	-.004	-.022	-.056
	Sig. (2-tailed)	.002		<.001	<.001	.082	.965	.828	.579
	N	99	99	99	99	99	99	99	99
O	Pearson Correlation	.302**	.362**	1	.080	-.025	.112	.365**	-.086
	Sig. (2-tailed)	.002	<.001		.430	.809	.269	<.001	.399
	N	99	99	99	99	99	99	99	99
C	Pearson Correlation	.134	.343**	.080	1	-.380**	-.298**	-.325**	.184
	Sig. (2-tailed)	.185	.001	.430		<.001	.003	.001	.068
	N	99	99	99	99	99	99	99	99
N	Pearson Correlation	-.288**	-.176	-.025	-.380**	1	.818**	.914**	-.139
	Sig. (2-tailed)	.004	.082	.809	<.001		<.001	<.001	.168
	N	99	99	99	99	99	99	99	99
N_E	Pearson Correlation	.282**	-.004	.112	-.298**	.818**	1	.801**	-.215*
	Sig. (2-tailed)	.005	.965	.269	.003	<.001		<.001	.033
	N	99	99	99	99	99	99	99	99
N_O	Pearson Correlation	-.163	-.022	.365**	-.325**	.914**	.801**	1	-.168
	Sig. (2-tailed)	.107	.828	<.001	.001	<.001	<.001		.097
	N	99	99	99	99	99	99	99	99
Expertise	Pearson Correlation	-.101	-.056	-.086	.184	-.139	-.215*	-.168	1
	Sig. (2-tailed)	.318	.579	.399	.068	.168	.033	.097	
	N	99	99	99	99	99	99	99	99

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Figure 13: Correlations between Big-5 and expertise, including the dual effect.

that the classifier correctly classifies all samples without making any mistakes. An example of how classification performance can be interpreted according to the area under the curve is presented in Table 26. AUC values and performance class names in this table are subject to change.

The most accurate values were given by SVM. Figure 16 shows the "expert" class estimate as AUC = 0.89 according to the ROC Curve. The assessment of the "good" class" is 0.71.

In order to test the algorithm results, the same algorithms were tried again on a dataset with an expertise score of more than 40 and known to be experienced in the field of cyber security. Naive Bayes, Ensemble (Bagged Tree), and SVM (CUBIC) gave the best results in this trial, and accuracy increased by 11%. The predictive AUC of the Expert class improved to = 0.91. The good class was estimated at 0.86. These results show that better results can be obtained if the people participating in the tests are selected from people knowledgeable in the field of cyber security.

When regression learner mentioned in Section 4.3.1 and the classification learner method are compared, it is seen that they have similar accuracy by looking at AUC and RMSE values.

5. Discussion and Limitations

The proposed methodology combines the Big-5 Personality Test, cyber expertise test, and CTF test to have information about the multiple areas of expertise in computers by looking at people's character analysis and also have information about hacker psychology by looking at their expertise on the computers. The strengths of the proposed model are listed below:

The major strength of the study is that there is no similar study in the literature. However, this can also be considered a weakness in which the results of the study are not comparable with any existing studies as yet.

In the study, a honeypot was developed, and CTF questions were created. These questions are original and are first posed by this article.

Thanks to hacker psychology analysis; when an unknown person is encountered, it is aimed to understand the possibility of an attack from the behavior of the person and his expertise in this attack. Similarly, it is desired to determine the likelihood of a cyberattack by looking at the logs left by a person in any system. In addition to these, a psychological analysis of this person was also provided.

The study wants to show that these relationships can be an element of attack prevention for institutions by analyzing the relevance of any cyberattack to the

Correlations

		Soc	Asse	Enl	Com	Res	Tru	Org	Pro	Anx	Dep	Emo	IntC	AeS	CreI	Expertise
Soc	Pearson Correlation	1	.467**	.241*	-.063	-.146	.228*	-.142	-.015	-.208*	-.328**	-.009	.137	-.048	.156	.023
	Sig. (2-tailed)		<.001	.013	.522	.136	.019	.147	.882	.032	<.001	.924	.163	.624	.111	.839
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Asse	Pearson Correlation	.467**	1	.335**	.157	-.170	.098	.155	.203*	-.220*	-.382**	-.222*	.182	-.023	.249*	.065
	Sig. (2-tailed)	<.001		<.001	.108	.082	.316	.113	.037	.023	<.001	.022	.062	.814	.010	.561
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Enl	Pearson Correlation	.241*	.335**	1	.343**	.126	.261**	.134	.222*	.048	-.154	.002	.357**	.254**	.312**	-.127
	Sig. (2-tailed)	.013	<.001		<.001	.197	.007	.169	.022	.625	.114	.984	<.001	.009	.001	.251
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Com	Pearson Correlation	-.063	.157	.343**	1	.203*	.148	.083	.109	.011	-.031	.095	.167	.160	.047	-.101
	Sig. (2-tailed)	.522	.108	<.001		.037	.131	.398	.265	.908	.751	.333	.087	.102	.631	.365
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Res	Pearson Correlation	-.146	-.170	.126	.203*	1	.417**	.403**	.376**	-.188	-.282**	-.353**	.093	.190	.165	-.215
	Sig. (2-tailed)	.136	.082	.197	.037		<.001	<.001	<.001	.054	.003	<.001	.346	.051	.091	.051
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Tru	Pearson Correlation	.228*	.098	.261**	.148	.417**	1	.077	.174	-.286**	-.234*	-.244*	.133	.047	.282**	.016
	Sig. (2-tailed)	.019	.316	.007	.131	<.001		.430	.075	.003	.016	.012	.174	.630	.003	.883
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Org	Pearson Correlation	-.142	.155	.134	.083	.403**	.077	1	.562**	-.090	-.213*	-.291**	-.070	.138	-.014	-.224*
	Sig. (2-tailed)	.147	.113	.169	.398	<.001	.430		<.001	.357	.029	.003	.475	.158	.883	.042
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Pro	Pearson Correlation	-.015	.203*	.222*	.109	.376**	.174	.562**	1	-.107	-.343**	-.443**	-.029	.180	.071	-.101
	Sig. (2-tailed)	.882	.037	.022	.265	<.001	.075	<.001		.274	<.001	<.001	.770	.065	.471	.365
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Anx	Pearson Correlation	-.208*	-.220*	.048	.011	-.188	-.286**	-.090	-.107	1	.495**	.462**	.056	.047	-.241*	.006
	Sig. (2-tailed)	.032	.023	.625	.908	.054	.003	.357	.274		<.001	<.001	.569	.630	.013	.955
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Dep	Pearson Correlation	-.328**	-.382**	-.154	-.031	-.282**	-.234*	-.213*	-.343**	.495**	1	.560**	-.088	-.047	-.144	-.036
	Sig. (2-tailed)	<.001	<.001	.114	.751	.003	.016	.029	<.001	<.001		<.001	.369	.630	.141	.748
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Emo	Pearson Correlation	-.009	-.222*	.002	.095	-.353**	-.244*	-.291**	-.443**	.462**	.560**	1	-.018	-.094	.176	.096
	Sig. (2-tailed)	.924	.022	.984	.333	.000	.012	.003	<.001	<.001	<.001		.851	.336	.071	.390
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
IntC	Pearson Correlation	.137	.182	.357**	.167	.093	.133	-.070	-.029	.056	-.088	-.018	1	.338**	.432**	-.015
	Sig. (2-tailed)	.163	.062	<.001	.087	.346	.174	.475	.770	.569	.369	.851		<.001	<.001	.891
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
AeS	Pearson Correlation	-.048	-.023	.254**	.160	.190	.047	.138	.180	.047	-.047	-.094	.338**	1	.112	-.176
	Sig. (2-tailed)	.624	.814	.009	.102	.051	.630	.158	.065	.630	.630	.336	<.001		.253	.112
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
CreI	Pearson Correlation	.156	.249*	.312**	.047	.165	.282**	-.014	.071	-.241*	-.144	-.176	.432**	.112	1	.010
	Sig. (2-tailed)	.111	.010	.001	.631	.091	.003	.883	.471	.013	.141	.071	<.001	.253		.926
	N	106	106	106	106	106	106	106	106	106	106	106	106	106	106	83
Expertise	Pearson Correlation	.023	.065	-.127	-.101	-.215	.016	-.224*	-.101	.006	-.036	.096	-.015	-.176	.010	1
	Sig. (2-tailed)	.839	.561	.251	.365	.051	.883	.042	.365	.955	.748	.390	.891	.112	.926	
	N	83	83	83	83	83	83	83	83	83	83	83	83	83	83	106

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Figure 14: Correlations between Big-5 facets and expertise.

psychology of individuals and their actions (logs) in the system.

In addition to the advantages and ramifications of the designed system compared with the literature, the system can also be discussed at the technical-software level. As a developed monitoring system, every requirement for the behavioral analysis is added as a plugin to the existing high-level honeypot system. This has provided the flexibility and agility needed in the software. Another essential repercussion of this modular design comes when scaling to the honeynets; the system allows us to distribute the plugins modularly to

Table 23: Average of Big-5 respecting to different expertises.

	Expertise	E	A	O	C	N
AVGALL	53.49	60.63	65.24	68.20	67.74	44.98
AVG > 70	83.91	59.57	64.58	67.71	70.90	40.04
AVG > 85	92.06	59.77	62.50	70.31	74.22	43.10
AVG > 95	95.78	59.95	64.35	70.60	78.01	42.13
AVG ≤ 30	19.92	62.83	65.42	71.50	67.25	44.33
AVG:50–70	59.14	60.12	66.89	67.49	69.20	44.95

1.1	Linear Regression	RMSE:13.938
Last change: Linear		16/16 features
1.2	Linear Regression	RMSE:179.48
Last change: Interactions Linear		16/16 features
1.3	Linear Regression	RMSE:14.059
Last change: Robust Linear		16/16 features
1.4	Stepwise Linear Regression	Failed
Last change: Stepwise Linear		16/16 features
1.5	Tree	RMSE:14.533
Last change: Fine Tree		16/16 features
1.6	Tree	RMSE:14.544
Last change: Medium Tree		16/16 features
1.7	Tree	RMSE:20.259
Last change: Coarse Tree		16/16 features
1.8	SVM	RMSE:13.548
Last change: Linear SVM		16/16 features
1.9	SVM	RMSE:17.639
Last change: Quadratic SVM		16/16 features
1.10	SVM	RMSE:146.97
Last change: Cubic SVM		16/16 features
1.11	SVM	RMSE:13.758
Last change: Fine Gaussian SVM		16/16 features
1.11	SVM	RMSE:13.233
Last change: Medium Gaussian SVM		16/16 features
1.12	SVM	RMSE:14.696
Last change: Coarse Gaussian SVM		16/16 features
1.13	Ensemble	RMSE:12.873
Last change: Boasted Trees		16/16 features
1.14	Ensemble	RMSE:14.147
Last change: Bagged Trees		16/16 features
1.15	Gaussian Process Regression	RMSE:12.798
Last change: Squared Exponential GPR		16/16 features
1.16	Gaussian Process Regression	RMSE: 12.014
Last change: Matern 5/2 GPR		16/16 features
1.17	Gaussian Process Regression	RMSE: 9.6591
Last change: Exponential GPR		16/16 features
1.19	Gaussian Process Regression	RMSE: 10.943
Last change: Rational Quadratic GPR		16/16 features

Figure 15: RMSE of regression learning algorithms.

Table 24: Regression learning algorithm results.

Predictors	Predicted response	RMSE	Algorithm
All Honeypot_Logs	Expertise	9.659	Gaussian process regression (GPR)
Expertise	Honeypot_Logs(A14)	13.69	Linear SVM
Expertise + Honeypot_Logs(A2 ∗ A3 ∗ A7 ∗ A8 ∗ A9 ∗ A19)	Honeypot_Logs(A5)	0.345	Gaussian process regression (GPR)
Honeypot_Logs + exp	Big-5(Extravert)	13.515	Gaussian process regression (GPR)
All Honeypot_Logs	Big-5(Extravert)	13.309	Gaussian process regression (GPR)
All Honeypot_Logs + Big-5	Expertise	12.039	Gaussian process regression (GPR)

Table 25: A example of generated trial honeypot logs of an unknown hacker.

A2	A3	A5	A7	A8	A9	A10	A11	A12	A13	A14	A15	A17	A19	A20	A22
1	1	1	1	1	1	0	0	1	1	4.42	1	1	1	1	0

Table 26: Interpretation of AUC.

AUC (area under the curve)	Classification performance
0.91 - 1.00	Very good
0.81 - 0.90	Good
0.71 - 0.80	Mediocre - fair
0.61 - 0.70	Very poor
≤0.50	Valueless

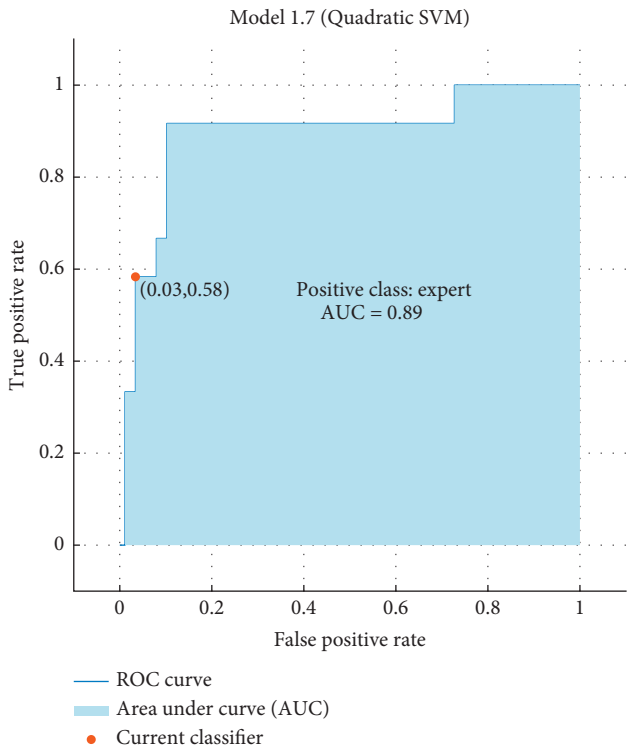

Figure 16: AUC result of expert class.

a network of honeypots and monitor different behaviors on subnetwork of honeypots.

The only limitation of the proposed method is conducting all the analyses based on the results from different tests:

Test participation or answering questions is often low, and questions are not answered by carefully reading them. Therefore, the reliability of the questionnaire decreases. To provide reliability, we have to reduce the sample space.

Giving random answers to test questions is another handicap. Apart from people who do this voluntarily, it is another fact that there are subjects who follow such a path because they cannot fully grasp the question. In order to overcome this issue, a knowledgeable group of participants is chosen.

Governance models can be created with the policies that are in turn developed on the logs from real life. These policies can be fed to CERT/CSIRT teams depending on the alarm state of the enterprise. Extra security measures such as extreme DDoS protection, strict IPS/IDS rules, and security as an infrastructure service can be enabled depending on the peculiarity of the profiles and the contemporary users.

Adversarial attacks aim to manipulate the machine learning engine by feeding false/fabricated input to the machine learning training. In this research, the data fed to the ML engine has been captured after the Big-5 and cyber expertise tests; the input has been crafted from the actions that the hacker input in the honeypot system. During the training session, the honeypots work as an outward-facing server that has been compromised, and the tasks of the CTF are accomplished using this compromised server. The requirements and specifications are calculated offline from the traces left by the attacker. These traces are matched with the personality test and expertise test from the unique ID and IP addresses provided by the CTF organizers. This countermeasure, therefore, renders the adversarial attacks infeasible on our systems.

We think that it is essential to determine whether the hacker is an expert or not, for this underlines the level of measures to be taken by victim institutions. By analyzing these results, predictions will be made in real time of a possible attack in the future. Moreover, we feel that it could help to decide about the appropriate defense mechanism if we have some information about the personality of a hacker while under attack.

6. Conclusions and Future Work

This study aims to find a correlation between a hacker's behavior/logs on the server and the personality, expertise, and psychology of the hacker. There are self-reporting surveys applied to hackers in the literature. However, no study evaluates the accurate data of these hackers considering these surveys, which cause to reduce accuracy in finding the characteristics of the hackers.

In this study, the following tests are first applied to a volunteer group consisting of hackers, computer experts, and computer engineering students:

Big-5 Psychology test

Expertise test

Later, the same people were directed to a fake-honeypot server and were requested that they solve the CTF questions and leave their respective logs at the server. As for the processing, all the accumulated data were brought together as a first step. We then analyzed the current data. By utilizing data mining techniques, we were able to develop a model to predict the hacker's expertise and personality from the logs and vice versa.

When a system encounters an unknown hacker, the information regarding his expertise and psychology might be established readily by examining the logs he has left behind on the server. So, the necessary cyber security precautions can be taken on a timely basis even if that hacker has not taken a survey or a test before or has never shown up on that specific server before.

The tests and the CTF takes approximately 2 hours to complete. As the number of participants increases, the results will undoubtedly improve. As seen in Section 4.3, the closer the participants are to cybersecurity, the more accurate the results are. It is planned to improve the results with more participants and/or hackers.

It is also aimed that our study will be performing a real-time log analysis in the future. Thus, a proactive response can be established at the time of the attack. Moreover, our Honeypsy system will be integrated into a SIEM (Security Information and Event Management) tool and thus be monitored online in the future.

In this paper, data mining techniques are applied to make predictions. In order to obtain trained data, a fuzzy logic model can be proposed in the future.

These tests and results can also be utilized in real cases. Our Honeypsy system can be installed easily in any institution or organization within 5 minutes. It can collect logs and sign the specifications. When a server is attacked, the expertise of the cyber threat and/or cyberattack can be determined by utilizing our trained data in the Honeypsy system. Based on this expertise, the organization can then define its defense methodology without killing a mosquito with a machine gun.

Data Availability

The authors have refrained from disclosing the data gathered in this study due to psychology data's sensitive and private nature. Nevertheless, the data can be obtained from the corresponding author upon request.

Conflicts of Interest

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

Acknowledgments

As this work is part of an ongoing Ph.D. research, the authors would like to express their gratitude to thesis jury committee members Dr. Beyazıt, Dr. Kose, and Dr. Eren. This work has received funding from the European Union's Horizon 2020 research and innovation program, under the Grant agreement no. 830943(ECHO).

References

[1] M. Odemis, C. Yucel, A. Koltuksuz, and İ. Ozbilgin, "Suggesting a honeypot design to capture hacker psychology, personality and sophistication," in *Proceedings of the ICCWS 2018*, Washington DC, USA, May 2019.

[2] Z. Mazadi, N. Ghasem-Aghaee, and T. Ören, "Prelude to cultural software agents: cultural backgrounds in agent simulation," in *Proceedings of the 2008 Spring simulation multiconference*, Ottawa Canada, April 2008.

[3] P. Shi, F. Liu, M. Yang, and Z. Wang, "A fuzzy rules-based approach to analyzing human behavior models," in *Proceedings of the 2009 11th International Conference on Computer Modelling and Simulation*, Cambridge, UK, March 2009.

[4] E. Davidov, P. Schmidt, and S. H. Schwartz, "Bringing values back in: the adequacy of the European social survey to measure values in 20 countries," *Public Opinion Quarterly*, vol. 72, no. 3, pp. 420–445, 2009.

[5] J. Deutrom, V. Katos, and R. Ali, "Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19," *Behaviour & Information Technology*, pp. 1–15, 2021.

[6] Y.-A. De Montjoye, J. Quoidbach, F. Robic, and A. Pentland, "Predicting personality using novel mobile phone-based metrics," in *Social Computing, Behavioral-Cultural Modeling and Prediction*, A. M. Greenberg, W. G. Kennedy, and N. D. Bos, Eds., vol. 7812, pp. 48–55, Springer, Berlin, Germany, 2013.

[7] S. Widup, J. Wade, S. Jay et al., "Verizon data breach investigations report," 2014.

[8] D. Dey, A. Lahiri, and G. Zhang, "Hacker behavior, network effects, and the security software market," *Journal of Management Information Systems*, vol. 29, no. 2, pp. 77–108, 2012.

[9] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, and T. S. Raghu, "Moving toward black hat research in information systems security: an editorial introduction to the special issue," *MIS Quarterly*, vol. 34, no. 3, pp. 431–433, Oct. 2010.

[10] J. Giboney, A. Durcikova, and R. Zmud, "What motivates hackers? Insights from the awareness-motivation-capability framework and the general theory of crime," in *Proceedings of the Dewald Roode information security research workshop*, pp. 1–40, Amsterdam, Netherland, October 2013.

[11] Z. Xu, Q. Hu, and C. Zhang, "Why computer talents become computer hackers," *Communications of the ACM*, vol. 56, no. 4, pp. 64–74, 2013.

[12] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation*, vol. 3, no. 2, pp. 97–102, 2006.

[13] J. S. Giboney, J. G. Proudfoot, S. Goel, and J. S. Valacich, "The security expertise assessment measure (SEAM): developing a scale for hacker expertise," *Computers & Security*, vol. 60, pp. 37–51, 2016.

[14] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, 2017.

[15] MITRE, "Mitre att&ck framework," 2021, https://attack.mitre.org/.

[16] Ç. Yücel, A. Koltuksuz, M. Ödemiş, A. Muazu Kademi, and G. Özbilgin, "A programmable threat intelligence framework for containerized clouds," in *Proceedings of the 13th International Conference on Cyber Warfare and Security (ICCWS 2018)*, Washington, DC, USA, March 2018.

[17] D. Fraunholz, D. Krohmer, S. D. Antón, and H. D. Schotten, "Yaas - on the attribution of honeypot data," *International Journal on Cyber Situational Awareness*, vol. 2, no. 1, pp. 31–48, 2017.

[18] K. Hara, T. Sato, M. Imamura, and K. Omote, "Profiling of malicious users using simple honeypots on the Ethereum blockchain network," in *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020*, pp. 22–24, Toronto, Canada, May 2020.

[19] J. Thom, Y. Shah, and S. Sengupta, "Correlation of cyber threat intelligence data across global honeypots," in *Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) 2021*, pp. 766–772, December 2021.

[20] F. Sadique and S. Sengupta, "Modeling and Analyzing Attacker Behavior in IoT Botnet Using Temporal Convolution Network (TCN) Modeling and Analyzing Attacker Behavior in IoT Botnet Using Temporal Convolution Network (TCN)," 2021, https://arxiv.org/abs/2108.12479.

[21] Z. C. Schreuders, "Post-exloitation," 2013, http://z.cliffe.schreuders.org/edu/DSL/Post-exploitation.pdf.

[22] S. Aliaksei, "Linux post exploitation command list," 2019, https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List#paths.

[23] C. J. Soto and O. P. John, "The next big five inventory (BFI-2): developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power," *Journal of Personality and Social Psychology*, vol. 113, no. 1, pp. 117–143, Jul 2017.

[24] S. A. Bissonnette, E. D. Combs, P. H. Nagami et al., "Using the biology card sorting task to measure changes in conceptual expertise during postsecondary biology education," *CBE-life Sciences Education*, vol. 16, no. 1, p. ar14, 2017.