frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 08 April 2024
DOI 10.3389/fcomp.2024.1381351

EDITED BY
Javed Ali Khan,
University of Hertfordshire, United Kingdom

REVIEWED BY
Hafsa Shareef Dar,
University of Gujrat, Pakistan
Tawfik Al-Hadhrami,
Nottingham Trent University, United Kingdom

*CORRESPONDENCE
Osama Sohaib
✉ osama.sohaib@uts.edu.au

RECEIVED 03 February 2024
ACCEPTED 22 March 2024
PUBLISHED 08 April 2024

CITATION
Hani U, Sohaib O, Khan K, Aleidi A and Islam N (2024) Psychological profiling of hackers via machine learning toward sustainable cybersecurity. *Front. Comput. Sci.* 6:1381351. doi: 10.3389/fcomp.2024.1381351

Psychological profiling of hackers via machine learning toward sustainable cybersecurity

Umema Hani[1], Osama Sohaib[2,3]*, Khalid Khan[1], Asma Aleidi[4] and Noman Islam[1]

[1]College of Computing and Information Sciences, Karachi Institute of Economics and Technology, Karachi, Pakistan, [2]School of Business, American University of Ras Al Khaimah, Ras Al Khaimah, United Arab Emirates, [3]Department of Computer Science, University of Technology Sydney, Sydney, NSW, Australia, [4]College of Humanities and Social Sciences, Libraries and Information Department, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia

This research addresses a challenge of the hacker classification framework based on the "big five personality traits" model (OCEAN) and explores associations between personality traits and hacker types. The method's application prediction performance was evaluated in two groups: Students with hacking experience who intend to pursue information security and ethical hacking and industry professionals who work as White Hat hackers. These professionals were further categorized based on their behavioral tendencies, incorporating Gray Hat traits. The k-means algorithm analyzed intra-cluster dependencies, elucidating variations within different clusters and their correlation with Hat types. The study achieved an 88% accuracy in mapping clusters with Hat types, effectively identifying cyber-criminal behaviors. Ethical considerations regarding privacy and bias in personality profiling methodologies within cybersecurity are discussed, emphasizing the importance of informed consent, transparency, and accountability in data management practices. Furthermore, the research underscores the need for sustainable cybersecurity practices, integrating environmental and societal impacts into security frameworks. This study aims to advance responsible cybersecurity practices by promoting awareness and ethical considerations and prioritizing privacy, equity, and sustainability principles.

KEYWORDS

hacker identification, personality traits, K-means clustering, cyber security, social engineering

1 Introduction

The rise of the Internet has led to a corresponding surge in cybercrime instances, as computers have become integral to various facets of life, including commerce, entertainment, and government operations (Siddiqi et al., 2022). Additionally, the emergence of novel networking models such as mobile, wireless, cognitive, mesh, Internet of Things (IoT), and cloud technologies has further complicated the landscape of cybersecurity (Islam and Shaikh, 2016; Tandera et al., 2017; Wong et al., 2020). This evolving scenario poses significant challenges in combating cyber threats. Cybercrime utilizes computers as tools and mediums for criminal activities, targeting security objectives such as privacy, confidentiality, availability, and integrity of information. Common cyber crimes encompass phishing, honeypots, social engineering, spoofing, and disseminating viruses or worms.

The discussion on cybercrimes highlights previous research findings indicating that these activities are primarily carried out by individuals with low technical sophistication and are driven by motivations such as fame, financial gain, revenge, and self-satisfaction (John et al., 1999; Gulati et al., 2016; Buch et al., 2017; Matulessy and Humaira, 2017; Suryapranata et al., 2017). Hacking, a specialized form of cybercrime, involves illegally accessing personal or sensitive data using technology and knowledge, with various countermeasures such as firewalls and intrusion detection systems in place to mitigate such threats (Gulati et al., 2016; Akdag, 2020). Building on this understanding, the concept of "sustainable cybersecurity" is introduced in this study, emphasizing the need for enduring and efficient strategies to adapt to the evolving challenges posed by hackers (Shackelford et al., 2016; Medoh and Telukdarie, 2022). This approach aligns with corporate social responsibility (CSR) practices, with an increasing number of managers recognizing cybersecurity as integral to safeguarding customers and the public, thereby expanding risk management practices to encompass the prevention of social-engineering-linked attacks (Shackelford et al., 2016; Medoh and Telukdarie, 2022).

In this study, the term "sustainable" indicates the formulation of enduring and efficient cybersecurity strategies. Within this framework, sustainability encompasses the creation of practices, methodologies, and tools capable of persisting and adjusting over time to adeptly confront the continuously evolving challenges presented by hackers. The concept of "Sustainable Cybersecurity" suggests implementing robust and resilient defense mechanisms designed not only to react to existing threats but also to foresee and alleviate potential risks. For instance, social engineering, which focuses on exploiting human psychology to both perpetrate and prevent cyberattacks, diverges from relying solely on technical hacking methods. It is associated with attacks such as phishing emails, deepfakes, and spear phishing (Siddiqi et al., 2022). This field also underscores the application of social psychology to reinforce cybersecurity policies within organizations. Tools such as the Cyber Risk Index (CRI) and the Cybercrime Rapid Identification Tool (CRIT) (Buch et al., 2017) can be implemented and utilized to bolster this approach. The gap between "social engineering" linked attacks and their avoidance measures creates an ongoing challenge for security experts. Therefore, security through technology is not the sole solution; it is the much-needed side to sustain the cyber security world. Even the World Economic Forum declares social engineering cyber-attacks as the reason for organizations' alarming security situation.

This study is grounded in research utilizing data collected from personality trait rating scales (Buch et al., 2017; Novikova and Alexandra, 2019; Wong et al., 2020), with Matulessy and Humaira (2017) providing insight into hacker personality profiles based on the Big Five Personality Traits model. The aim is to construct a machine learning model capable of predicting and analyzing the personality profiles of hackers, utilizing the Big Five personality model and validating its reliability. Understanding the psychology or personality of hackers is essential for implementing effective preventive measures (Javaid, 2013; Ali et al., 2020). The research inquiry addresses the dominant personality traits (openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism) abbreviated as OCEAN that are exhibited by various hacker types (White, Black, and Gray Hats) and how these traits can be accurately identified and categorized through a machine learning-based approach. This identification mechanism holds promise for informing targeted cybercrime prevention strategies. Figure 1 illustrates the research flow and target, detailing a secure model for predicting personality traits. The authors devised a questionnaire based on the OCEAN model and applied machine learning models to classify hacker types.

Different sections in this article are as follows. The section covers relevant literature, Section 3 covers the research method, Section 4 covers experimentation and results of the secure model, Section 5 covers discussions on results and threats to validity, and Section 6 concludes the study and highlights potential future work.

2 Literature review

In today's technologically advancing world, cybercrimes are on the rise. This section discusses targeted studies published previously to investigate contemporary cybercriminal acts.

In the realm of cybersecurity research, many studies have leveraged machine learning methodologies to delve into the intricacies of cybercrime data analysis. Concurrently, Geluvaraj et al. (2019) have tackled prevalent cybersecurity challenges, proposing innovative machine-learning solutions for their mitigation. Drawing from diverse machine learning techniques, Zheng et al. (2003) have unraveled concealed patterns within crime data, underscoring the indispensability of data-driven approaches in cybercrime investigations. Meanwhile, Islam et al. (2021) have explored the transformative potential of artificial intelligence and deep learning in bolstering cybersecurity frameworks. Adewumi and Akinyelu (2017) have harnessed machine learning algorithms to discern distinctive authorship patterns and shed light on attributing illicit messages in cyberspace. Pastrana et al. (2018) proposed a comprehensive approach to counter the spread of fake news online, leveraging machine learning technologies. This effort aligns with the rise of blockchain technology, which has become a cornerstone in fortifying applications across mobile and cloud networks, exemplified by the study by Mohammed et al. (2023) and Tamboli et al. (2023). Furthermore, pioneering approaches, such as the Low-Latency and High-Throughput Multipath routing technique, as elucidated by Ramachandran et al. (2022), have been devised to counter novel threats such as black hole attacks. Meanwhile, Imran et al. (2019) have employed machine learning and nature-inspired algorithms to scrutinize credit card data, fortifying fraud prevention measures. Against this backdrop, integrating artificial intelligence, machine learning, and IoT technologies has heralded a new era in cybercrime analysis and cybersecurity enhancement, a paradigm eloquently underscored by Sood and Enbody (2013) and epitomized in the broader research landscape.

Bridging the gap between psychology and information security, investigations by Del Pozo et al. (2018) and Chayal and Patel (2021) have illuminated the psychological underpinnings crucial to fortifying cyber defenses. Suryapranata et al. (2017) studied the activities of a user forum to identify the variables that can be used to predict the likelihood of a user being involved in cybercrime.

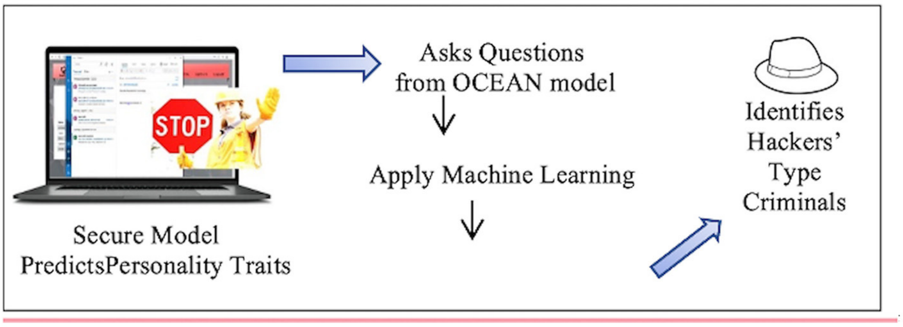


FIGURE 1
Research flow and target.

An intervention can benefit in avoiding a crime. The study reports users in an underground forum as providers, advertisers, and buyers (Fox and Holt, 2021). Alashti et al. (2022) employed logistic regression and latent class analysis to identify risk factors associated with juvenile hacking. Odemis et al. (2022) observed the behaviors of Iranian hackers via interviews. It was found that young hackers enjoyed the pleasure of cybercrime. Back et al. (2019) addresses whether we can analyze the psychology and behavior of a hacker by investigating their computer logs. A honeypot system was created for this purpose. Suryapranata et al. (2017) built profiles of cybercriminals by analyzing court records and media documents for incidents in South Korea. It was found that there is a difference in motivation between young and adult hackers.

The hidden Markov Model has been used in various studies to identify the personality traits of cybercriminals over social media networks (Xie and Wei, 2022). The method comprises a training and identification phase. The average likelihood of the observation sequence is performed in the identification phase. The text information posted by users over social media, blogs, and language characteristics can be analyzed using neural networks, logistic regression, and support vector machines for personality analysis (Golbeck et al., 2011; Adali and Golbeck, 2012; Lima and De Castro, 2014).

Novikova and Alexandra (2019) discuss the Five Factor Model in detail. The Five Factor Model suggests that all people, regardless of their age, gender, or culture, share some essential traits, but every person differs in their degree of manifestation. John et al. (1999) discuss the result of an eight-item Cybercrime Rapid Identification Tool (CRIT). It evaluates the psychometric properties of the proposed scale on samples of secondary school and university students. A study on Personality Prediction Systems from Facebook Users attempts to build a system to predict a person's personality based on user information (Buch et al., 2017). The research mentioned in the above studies discusses cybercrimes in general. This includes the essential five personality traits all humans are divided into, the tool for identifying Cybercrimes, and especially the personality profiles of the hackers.

In the realm of hacker classification, researchers often employ a framework akin to the concept of White, Black, and Gray Hats (Buch et al., 2017). White Hat Hackers, the first category, embody ethical hacking practices. Despite engaging in illegal activities, they channel their skills toward constructive and positive ends, often for the betterment of security systems. Contrastingly, Black Hat Hackers, the second category, operate with nefarious intent, breaching security measures for personal gain. Their activities typically involve theft, exploitation, and the illicit sale of data driven by self-interest. Gray Hat Hackers constitute the third category, occupying a space between the ethical and the malicious. While they may identify and exploit vulnerabilities, their actions are not motivated by financial gain. However, their endeavors still fall within the realm of illegality, as they typically lack consent from the system's owner. Gray Hats often have associations with Black Hat hackers, blurring the lines between ethical and unethical practices. In another perspective Javaid (2013) offered, Gray Hats are portrayed as reformed Black Hats. These individuals, often independent security experts, consultants, or corporate researchers, transition from illicit activities to a more legitimate stance. Notable figures such as Kevin Mitnick exemplify this transformation.

In summary, the delineation between White, Black, and Gray Hats provides a nuanced understanding of hacker motivations and behaviors, shedding light on the spectrum between ethical and malicious hacking practices. Each of the three types of hackers utilizes their skills for different purposes. The previous research defines that each possesses other personality profiles regarding Big Five Personality Traits (OCEAN Model). The research study conducted by Matulessy and Humaira (2017) described the personality profiles of the hackers concerning the Big Five Personality Traits model using 30 hacker subjects and utilized descriptive qualitative research.

The research claims that hackers are positioned in the middle of the personality trait of extraversion regardless of the categories of hackers. White Hats have more dominant personality traits of agreeableness, and Black Hats have more dominant personality traits of openness to experience. In contrast, Gray Hats have more dominant personality traits in terms of neuroticism (see Table 1). Table 2 presents the summary of the previous research.

Previous researchers have primarily focused on broad aspects of cybercrime identification and personality prediction. While some studies have explored personality prediction systems utilizing social media platforms (Buch et al., 2017), others have theorized based on research findings obtained from personality trait rating scales, interviews, surveys, and questionnaires (Matulessy

TABLE 1 OCEAN traits claimed in earlier research (Matulessy and Humaira, 2017).

	Extroversion	Neurotic	Agreeable	Conscientious	Openness
White hat	**Average**	**Average**	**High**	**Average**	**Average**
Interview-beginner	H	H	H	H	H
Interview-elite	H			H	H
Gray hat	**Average**	**High**	**Average**	**Average**	**Average**
interview-beginner	H	H		H	L
Interview-elite	A			H	H
Black Hat	**Average**	**Average**	**Average**	**Average**	**High**
Interview-Beginner	A				H
Interview-elite	H	H	H	H	A

and Humaira, 2017; Novikova and Alexandra, 2019). However, the scope of investigation in these studies remains somewhat limited, predominantly addressing general trends rather than delving into nuanced aspects of cybercriminal behavior and personality profiling.

This research implements a machine learning-based model that predicts and analyzes the personality profiles of hackers using the Big Five personality model, and it also validates the model on real-life datasets. This study mainly targets White and Gray hackers who either use hacking as their profession or have career motivation to adopt it professionally. For detailed classification, refer to the study by Martineau et al. (2023) and Chng et al. (2022) w.r.t hacker type, their possible motivations, and personality type.

3 Research methodology

Figure 2 shows the research method adopted in this study (McAlaney et al., 2020; Bakas et al., 2021). This study uses a machine learning-based approach to validate the classification of different hacker types (White, Black, and Gray Hats) based on their dominant personality traits (openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism).

The K-means algorithm was chosen for its simplicity, ease of implementation, and speed. It is widely used for clustering tasks, including in high-volume datasets such as those associated with criminal data, as described by Aldhyani and Alkahtani (2022). K-means can generate clusters based on similarities in the data, aiming to group data points close to each other while being far from points in other clusters. This study applied K-means to cluster individuals based on their responses to personality trait questions. By clustering individuals with similar personality trait profiles together, the algorithm aids in identifying distinct groups or "clusters" that may correspond to different types of hackers based on their dominant personality traits. The study also seeks to develop an effective hacker identification mechanism that can accurately categorize these traits and contribute to developing targeted cybercrime prevention strategies related to social policies.

The Big Five Inventory is a 44-item inventory that measures an individual on the Big Five Factors (dimensions or traits) of personality. Each of the five factors is then further divided into personality characteristics. The inventory shares some questions for generic OCEAN personality traits. These are given in the dataset of Kaggle (Akdag, 2020). A reduced set of questions was used from the Five Personality questionnaire comprising 40 questions (Akdag, 2020). The users were asked to indicate their favorable responses to the questionnaire items by selecting an appropriate score. After collecting the questions' responses, a machine learning code runs and predicts results against all five personality traits. Based on the results, different hacker types are identified.

3.1 Research questionnaire

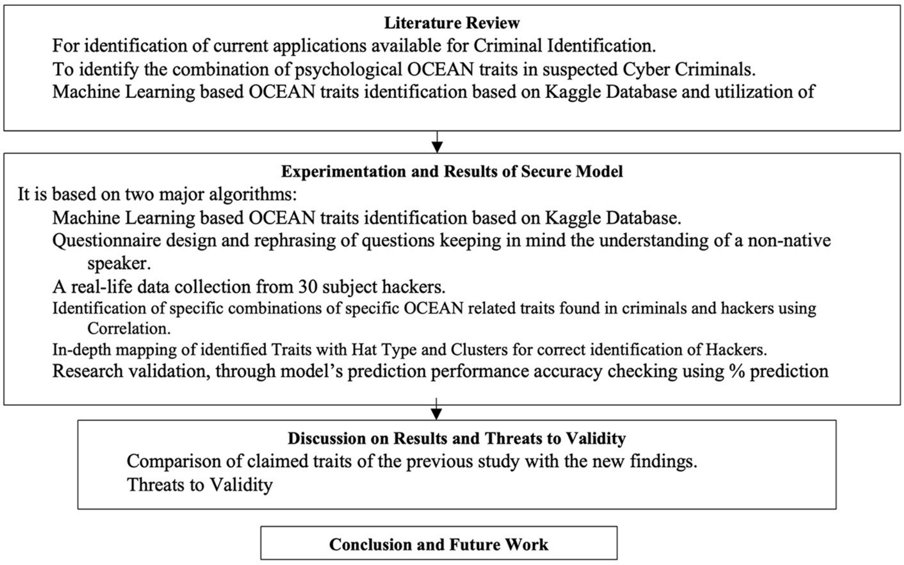
There are several instruments to measure the Big Five Trait Factors, such as the Big Five Inventory (BFI), the NEO Personality Inventory-Revised (NEO-PI-R), and the International Personality Item Tool (IPIP). This study used the dataset constructed from the IPIP for our research. This dataset was collected (2016–2018) through an interactive online personality test and comprises 10,12,050 records (Akdag, 2020). The training dataset trains the clustering model for OCEAN trait prediction.

Following the points concluded in the research mentioned in Table 1, 21 questions were selected. Redundant reverse questions were not included to reduce user frustration. In the questionnaire development process, the reverse questions are normally designed to verify the authenticity of answers recorded by random users.

Suárez Álvarez et al. (2018) demonstrated the conventional way of handling reverse coding. Here, the reduction was made for all reverse-scored questions included in the 40 questions. These were negatively phrased to ensure the user knew his point of view. Including such questions requires reserve scoring. The negative consequences of using the reverse scoring include a) the flawed measurement precision of the instrument, b) the variance of the combined form is reduced, c) examinees' scores differ significantly from those obtained in tests where all of the items are of a similar form, and d) verbal skills influence examinees' responses (Suárez Álvarez et al., 2018). Minor changes in wording can also have a significant effect on responses. One should, therefore, be careful when looking at alternative wordings. Negative words such as "not" should be avoided in questions as respondents easily miss them. In addition, using "not" in a scale such as "Satisfied," "Neither," and "Not satisfied" does not provide a true opposite as defined by

TABLE 2 Summary of previous research and hacker profiling gap analysis.

References	Main theme of the study	Hacker profiling research using personality traits	
	Technology used	Status (Yes/No)	Statistical justification (Yes/No)
Mohammed et al. (2023)	Implementation of secure applications using blockchain technology.	No	N/A
Tamboli et al. (2023)	Utilization of blockchain technology for secure applications over mobile and cloud networks.	No	N/A
Ramachandran et al. (2022)	Identification and handling of black hole attacks using Low-Latency and High-Throughput Multipath routing techniques.	No	N/A
Alashti et al. (2022)	Identification of risk factors associated with juvenile hacking using logistic regression and latent class analysis.	No	N/A
Chayal and Patel (2021)	Examination of psychology for information security to predict different cyber attacks.	No	N/A
Islam et al. (2021)	Exploration of the role of artificial intelligence and deep learning in cybersecurity.	No	N/A
Geluvaraj et al. (2019)	Discussion of various cybersecurity issues and the use of machine learning to address them.	No	N/A
Imran et al. (2019)	Application of machine learning and nature-inspired algorithms to analyze credit card data for fraud prevention.	No	N/A
Pastrana et al. (2018)	Identification of fake news spreading over the Internet using machine learning algorithms.	No	N/A
Sood and Enbody (2013)	Utilization of AI, machine learning, and IoT for cybersecurity; Deep understanding of cybersecurity.	No	N/A
Odemis et al. (2022)	Observation of behaviors of Iranian hackers via interviews; Analysis of young hackers' enjoyment of cybercrime.	No personality traits used	N/A
Back et al. (2019)	Analysis of hacker psychology and behavior through computer logs using a honeypot system.	No personality traits	N/A
Buch et al. (2017)	Investigation of personality prediction systems using social media data; Categorization of hackers into White Hat, Black Hat, and Gray Hat.	No personality traits used	N/A
Suryapranata et al. (2017)	Study of user forum activities to predict involvement in cybercrime; Profiling of cybercriminals using court records and media documents.	No personality traits used	N/A
Xie and Wei (2022)	Utilization of Hidden Markov Models to identify cybercriminal personality traits. It does not explicitly mention **hacker profiling**, but it does contribute to enhancing security within OSNs by improving the ability to identify fraudulent behavior	No hackers identification	N/A
Novikova and Alexandra (2019)	Discussion of the Five Factor Model and its application in personality analysis. It contributes valuable insights to the broader field of personality theory and cross-cultural psychology.	No hackers identification	N/A
Larose and Chantal (2014)	Examination of the impact of personality type and matching messaging on password strength.	No hackers identification	N/A
Adali and Golbeck (2012)	Analysis of text data from social media, blogs, and language characteristics for personality analysis using neural networks, logistic regression, etc.	No hackers identification	N/A
Zheng et al. (2003)	Exploration of techniques (classification, association rules mining, clustering) to identify hidden patterns in crime data.	No hackers identification	N/A
John et al. (1999)	Evaluation of Cybercrime Rapid Identification Tool (CRIT) on *second*ary school and university students.	No hackers identification	N/A
Del Pozo et al. (2018)	Study of psychology for information security; Application of machine learning in cybersecurity. It highlights the critical role of understanding human psychology in fortifying information security against social engineering attacks	No	N/A
Golbeck et al. (2011)	Analysis of text data from social media, blogs, and language characteristics for personality analysis using neural networks, logistic regression, etc. It highlights the implications of personality insights for social media design and broader domains	No	N/A
Matulessy and Humaira (2017)	Description of hacker personality profiles using the Big *Five* Personality Traits model; Utilization of descriptive qualitative research.	Yes	No Statistical Analysis



Literature Review

For identification of current applications available for Criminal Identification.

To identify the combination of psychological OCEAN traits in suspected Cyber Criminals.

Machine Learning based OCEAN traits identification based on Kaggle Database and utilization of

Experimentation and Results of Secure Model

It is based on two major algorithms:

Machine Learning based OCEAN traits identification based on Kaggle Database.

Questionnaire design and rephrasing of questions keeping in mind the understanding of a non-native speaker.

A real-life data collection from 30 subject hackers.

Identification of specific combinations of specific OCEAN related traits found in criminals and hackers using Correlation.

In-depth mapping of identified Traits with Hat Type and Clusters for correct identification of Hackers.

Research validation, through model's prediction performance accuracy checking using % prediction

Discussion on Results and Threats to Validity

Comparison of claimed traits of the previous study with the new findings.

Threats to Validity

Conclusion and Future Work

FIGURE 2
Research method.

the Australian Statistic Bureau (Corallo et al., 2022). The questions were then rephrased from native English speakers' style into a more understandable one for non-native speakers. See Table 3 for a detailed set of questions used in this study.

3.2 Questionnaire reliability

The questionnaire's accuracy and precision, i.e., its internal validity (consistency) or reliability, have been checked using Cronbach's alpha score. Its value was reported as 0.874 in previous research (Matulessy and Humaira, 2017) on 40 questions. In this research's reduced set of 21 questions, its value is 0.82, which shows acceptable reliability, i.e., >0.7. It always gives the same results when applied to the same group at different times or circumstances (Matulessy and Humaira, 2017).

4 Experimentation of results of secure model

4.1 Algorithms used and experimentation

The research experimentation is based on two algorithms:

1. The machine learning-based OCEAN traits identification dataset is from Kaggle, developed by Akdag (2020).
2. Identification of specific OCEAN traits-related combinations found in criminals and hackers.

The experiment starts with creating an optimal number of clusters on the training dataset downloaded from Kaggle (Akdag, 2020). The k-means algorithm generates clusters (groups of similar data) because of its ease of implementation, simplicity, and speed, which is very appealing in practice. This has been described in detail by Aldhyani and Alkahtani (2022), who targeted the classification of criminal data. According to the study, K-means is suitable for high-volume crime datasets and can help to extract useful information.

K-means applied in this research is a complete, partitioned clustering technique that attempts to find user-specified clusters (K) represented by their centroids. The distance between any two points in different groups is larger than the distance between any two points within a group. Well-separated clusters do not need to be spherical but can have any shape (Tan et al., 2016).

Figure 3 shows methods Python uses to calculate an optimum cluster value. The KElbowVisualizer or elbow method selects the optimal number of clusters by fitting the model with a range of values for K, which shows that the calculated value of K is 6. The Silhouette coefficient method is used to know the truth about the dataset by computing the density of clusters. This produces a score between 1 and -1, where 1 is a highly dense cluster and -1 is a completely incorrect cluster. Here, the value is approximately 0.06, which shows that the number of clusters in this research is dense and thus correct.

After clustering the training dataset on 6 clusters (0–5), the score of the five personality traits is calculated individually based on the responses to the questions. Then, the system is trained to predict the cluster for each dataset and calculate each trait's score respectively (see Figure 4). Figure 4 shows how many datasets were assigned to identify each cluster; even the worst count shows 6,200 records.

4.2 Scoring values to identify hackers

The same technique is applied to the responses taken from the test datasets, which were collected on 21 questions and converted into responses. According to the user's responses, the system calculates the score of each personality trait. It determines the

TABLE 3 Research questions with no reverse questions.

- EXT1: I am the life of the party. I am interactive and never mind being the center of attention.
- EXT2: I talk a lot, even around strangers.
- EXT5: I start a conversation.
- EST1: I get stressed out easily.
- EST3: I often worry about things.
- EST7: I change my mood a lot.
- EST9: I get irritated and annoyed easily.
- AGR2: I care about people as humans and their lives and what they do and say.
- AGR4: I can understand what someone is feeling
- AGR6: I have a soft heart.
- AGR8: I take time out for others and give high priority to others in need.
- CSN1: I am always prepared.
- CSN2: I am careless and unsystematic about the things in my ownership.
- CSN3: I pay attention to details in my work as I am demanding.
- CSN5: I get my work done right away.
- CSN7: I like doing things in an organized manner.
- CSN9: I follow a schedule.
- OPN1: I have a rich vocabulary and communicate more engagingly.
- OPN3: I have a vivid (intense) imagination.
- OPN7: I am quick to understand things.
- OPN10: I am full of ideas.

cluster where the user belongs to three types of hackers who have one most dominant personality trait among all. In previous research (Matulessy and Humaira, 2017), as shown in Table 1, for OCEAN traits, the generalized most dominant traits are agreeableness for the White hacker, openness to experience for the Black hacker, and neuroticism for the Gray Hackers. If any of these traits have the maximum score among all four traits, there is a strong possibility that the person can be a hacker or have any illegal intentions.

4.3 Organizational preventive measures

If the user is found to be suspicious, the system temporarily holds that user on a "watch list" before granting further access to the site or organizational sensitive resources. The organization can add its name to the social policy list to use resources under organizational or web access monitoring software. As mentioned earlier, proper social security and communication policies should be designed based on identified "social psychology" and Crime Risk Index, as suggested by Siddiqi et al. (2022), or Cybercrime Rapid Identification Tool (CRIT), as suggested by Buch et al. (2017), must be maintained to differentiate naïve users from the one who can harm other colleagues or employer organization.

5 Validation of secure model

Rather than blindly implementing clusters on previous research claims (Matulessy and Humaira, 2017), its proper validation is performed on (a) average scores as well as on (b) clusters using a prediction performance accuracy measurement of machine learning (Matulessy and Humaira, 2017). In validating the secure model, several techniques are applied to ensure the reliability and accuracy of the model's predictions. These include comparing average scores of the test dataset with established category claims for hacker types, validating clustering outcomes through cluster predictions on the test dataset, analyzing correlations between personality traits using Spearman's rho, quantitatively measuring model performance, examining demographic information, and mapping clusters to hacker types based on observed traits. Collectively, these validation techniques ensure the effectiveness and robustness of the model in identifying hacker types based on personality traits.

5.1 Data collection for test set

Test data were collected reliably for a major research project to gather personality traits data across various professional domains in computer science. These data were used to develop a career counseling system for final-year students in higher education institutions. It included responses from final-year students and professionals in domains such as information security, such as hackers, auditors, trainers, and security administrators. The response rate was highly encouraging. Out of 300 records, around 32 were related to hackers, with 30 ultimately included after data cleaning. This aligns with validation criteria from previous psychology research. Despite the lack of progressive research in hacker personality detection, the study aimed to contribute positively to career counseling. The data collection process was based on high trust, as participants and the research team belonged to the same information security professionals community. Data collected from final-year students were deemed reliable due to their field of interest and relevant academic projects noted during their tenure.

5.2 Demographics on test data

Demographics and frequency scores of the collected dataset for Gray and White hackers are given in Table 4. The total respondents for this study were 30 professionals and final-year students who intend to adopt hacking as their profession. The majority of them were male respondents, whereas only two were female respondents. Table 5 shows all possible details of the collected test dataset.

5.3 Cluster trends on test dataset with hat type mapping for validation

First, the test dataset was given as an input in the clustering algorithm generated, as discussed in Section 4, and clusters were predicted on all datasets. The cluster distribution will be discussed in detail in later sections.

To better understand the cluster trends and establish their mapping with Hat types, there was a need to consider the correlation between the traits on test data. Correlation is a statistical measure that measures the extent to which two variables are in a linear relationship without calculating cause and effect. This means

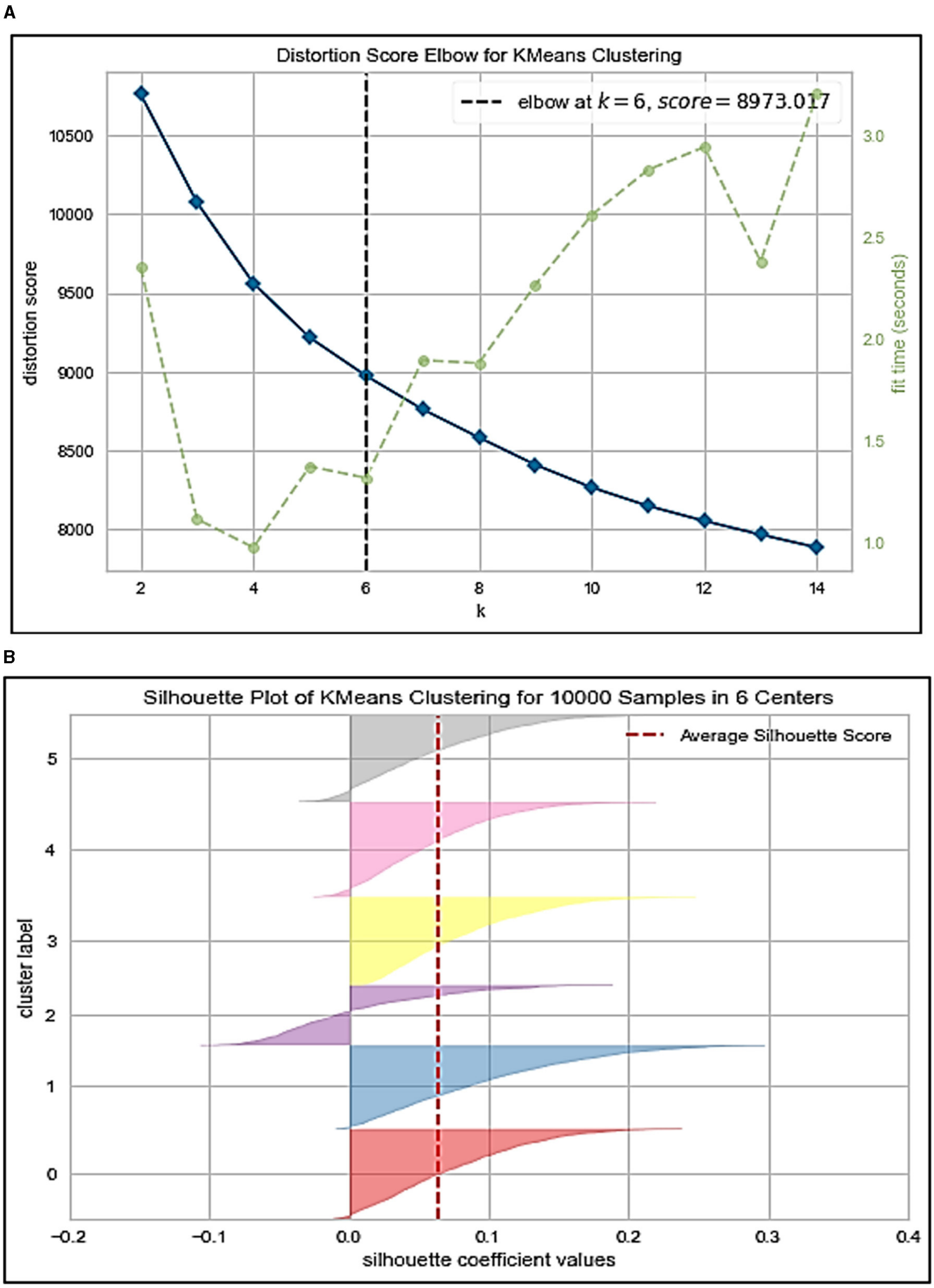
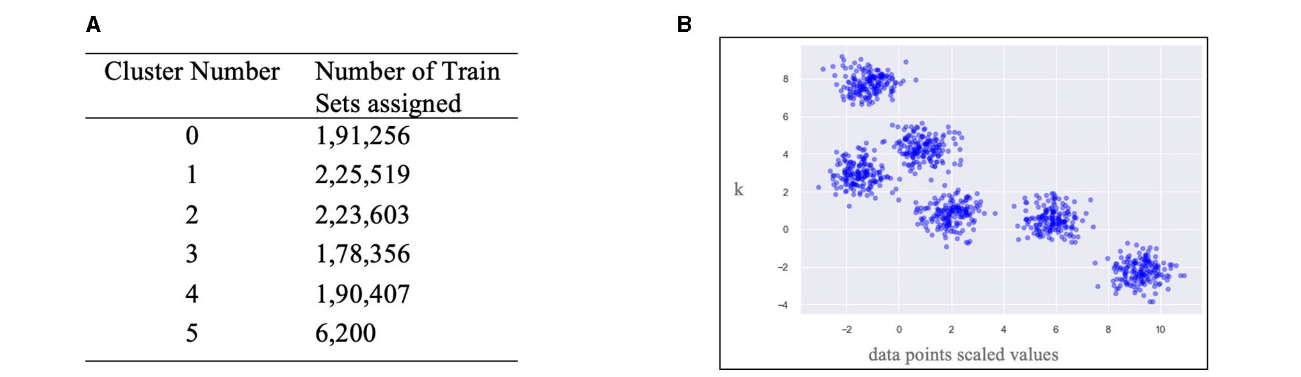


FIGURE 3
Optimal cluster number. **(A)** KElbowVisualizar; **(B)** Silhouette coefficient.

they constantly change; when one changes, the other also changes. It is measured on a scale of −1/0/+1, which means an indirect, no, or a direct relationship. For the stated reason, Spearman's correlation was applied to the test dataset (see Table 6), showing a few other significant but moderate level inter-dependencies between traits in the correlation coefficient range +/– 0.4.



Cluster Number	Number of Train Sets assigned
0	1,91,256
1	2,25,519
2	2,23,603
3	1,78,356
4	1,90,407
5	6,200

FIGURE 4
Cluster's centers picked by K-means Python estimator. **(A)** Training data distribution across calculated clusters. **(B)** Train data points spread across calculated clusters.

TABLE 4 Hacker type, motivations, and common strategies.

Hacker type	Motivations	Common strategies
White hat hackers	- Enhance cybersecurity. - Identify and fix vulnerabilities.	- Conduct ethical hacking. - Collaborate with organizations to strengthen defenses.
Black hat hackers	- Financial gain. - Data theft. - Disruption.	- Exploit vulnerabilities maliciously. - Engage in cybercriminal activities.
Gray hat hackers	- Curiosity. - Seeking recognition. - Responsible disclosure.	- Discover vulnerabilities without authorization. - Disclose responsibly.
Script kiddies	- Mischief. - Curiosity.	- Use pre-written scripts or tools without deep understanding.

TABLE 5 Number of test datasets and their demographics.

Respondents		Number of professional/elite	Number of final year student
Test data		**13**	**17**
Age in years		21–25	18–50
Sex	Male	13	15
	Female	0	2
City type	Urban	13	15
	Rural	0	2
Income range		0–above 200,000 PKR/Month	0–25,000 PKR/Month
Financial satisfaction	Yes	6	15
	No	7	2 (fresh in job)
Experience in years		0–1	0–28

These visible correlations can be generalized as given by Matulessy and Humaira (2017):

a. The openness to experience keeps conscientiousness closer. High openness was claimed to be the major trait of Black Hats.
b. Neuroticism depends directly on no other traits. High neuroticism was claimed to be the major trait of Gray Hats.
c. Agreeableness keeps extroversion closer. High agreeable was claimed to be the major trait of White Hats.

Figure 5 graphically shows all 6 clusters with average score values and reflects apparent behavior across each cluster on both training and test datasets. It is visible from the two graphs that the K-means clustering algorithm does not just check the average score values while designating the cluster numbers but also reflects intra-cluster trends within specific clusters. Following are the conclusions to map the cluster numbers with the Hat types purely over hacker's data:

1. The first cluster, "Cluster-0," shows the same trend among both datasets. Still, the training dataset has shown less sense of taking creative challenges by the White Hats because their job demands carefully defined method's adaptation. In this combination, the highest level starts with an extra high level of neuroticism, then comes a high level of agreeableness, conscientiousness, openness, and the last somewhat above-average level of extroversion.

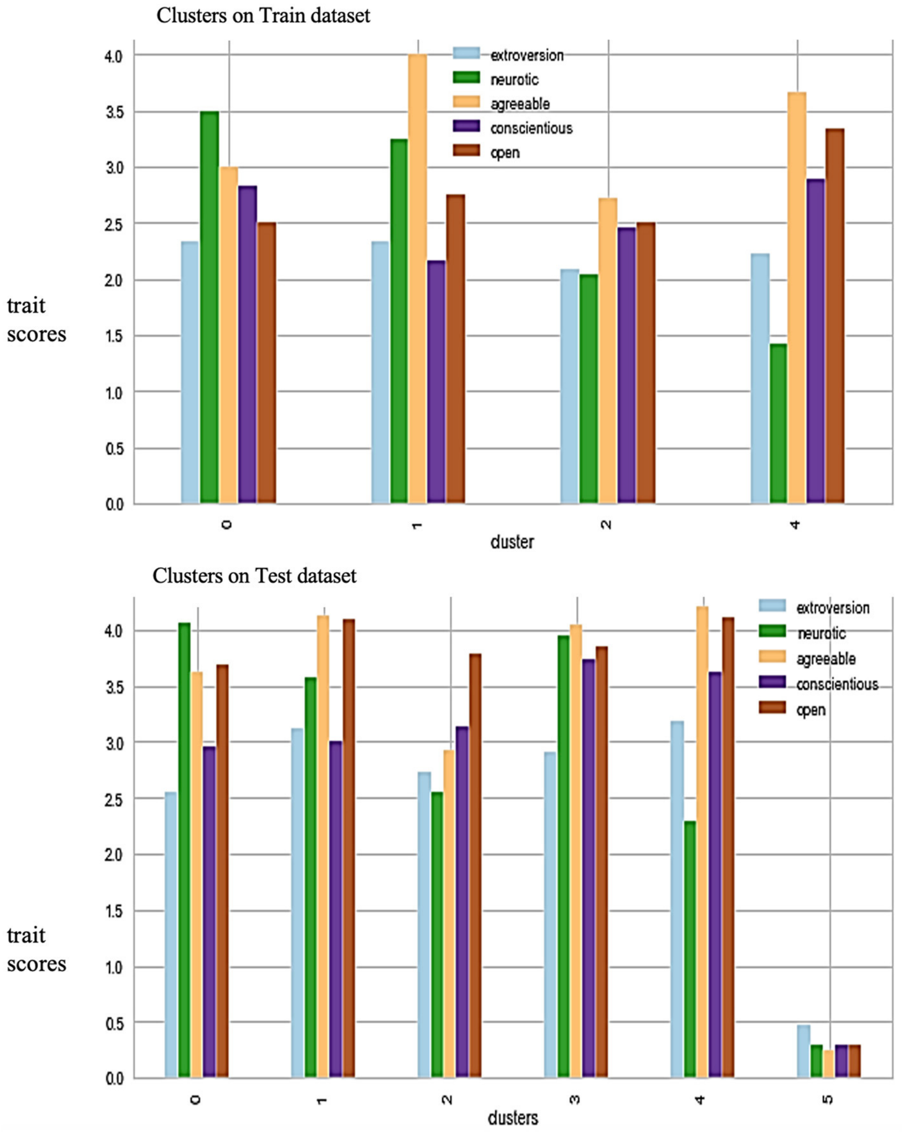


FIGURE 5
Average score value against each cluster for OCEAN traits prediction on training data.

- Conclusion: "Cluster-0" represents Gray Hats with the highest neuroticism; therefore, it does not depend on other traits.

2. The second cluster, which is "Cluster-1," is closer to the first cluster but has high neuroticism and agreeableness.

   - Conclusion: "Cluster-0" represents a switching behavior of White Hats with a Gray Hat tendency. White has the highest level of agreeableness but also has a high level of neuroticism; therefore, it does not depend on any other traits.

3. The third cluster, "Cluster-2," is closer to the fourth cluster but has an average level of neuroticism.

   - Conclusion: "Cluster-2" represents White Hats with average neurotic tendencies and with high agreeableness and average values of extroversion.

4. The fifth cluster, "Cluster-4," shows the same trend captured on the training and test datasets. The highest trait is agreeableness, followed by openness, an average level of conscientiousness, and an average value of extroversion.

   - Conclusion: "Cluster-4" represents White Hats with low neuroticism, high agreeableness, and average values of extroversion.

See Table 7 for clusters to Hat-type mapping with quantitative values of average scores across each trait for all clusters predicted on the test dataset.

10.3389/fcomp.2024.1381351

TABLE 6 Spearman's rho correlation checking to make multiple trait-based Hat-type selections.

		Extroversion	Neurotic	Agreeable	Conscientious	Open
Extroversion	Correlation coefficient	1.000	−0.117	0.422*	−0.100	−0.170
	Sig. (two-tailed)		0.553	0.025	0.614	0.387
Neurotic	Correlation coefficient	−0.117	1.000	−0.035	−0.284	−0.311
	Sig. (two-tailed)	0.553		0.861	0.143	0.107
Agreeable	Correlation coefficient	0.422*	−0.035	1.000	−0.077	0.224
	Sig. (two-tailed)	0.025	0.861		0.697	0.253
Conscientious	Correlation coefficient	−0.100	−0.284	−0.077	1.000	0.410*
	Sig. (two-tailed)	0.614	0.143	0.697		0.030
Open	Correlation coefficient	−0.170	−0.311	0.224	0.410*	1.000
	Sig. (two-tailed)	0.387	0.107	0.253	0.030	

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

5.4 Validation of average scores

A test dataset of 30 records is collected to check the claims of previous research (Matulessy and Humaira, 2017) without applying the clustering algorithm. In Table 7, the test dataset matches the previous research's (Matulessy and Humaira, 2017) generalized category claim of White Hats, as shown in Table 1.

After the detailed experimentation performed in Section 4, a better interpretation of validation results on test data can be made based on Table 7 cluster to Hat-type mappings (see Table 8).

1. The average scores of the test dataset for professionals match the generalized score claim for White Hats in previous research (Matulessy and Humaira, 2017) but show an average extroversion value (see Table 6); therefore, after the following cluster-level validation, it could be placed under Cluster-4.
2. The average scores of the test dataset for student hackers match the generalized score claim for White hackers (Matulessy and Humaira, 2017) but show an average neuroticism value (see Table 6). Therefore, the student's class belongs to the White Hats but tilts toward Gray Hat traits, and after performing the cluster-level validation, it will be placed under Cluster-2.

5.5 Secure model's clustering model validation

The secure model uses the clusters to predict the criminal's or hacker's personality type.

In this section, the clustering outcomes are validated to visualize the cluster's outcome spread when run over the test dataset (see Figure 6). Validation was performed by making cluster predictions over the test dataset using a 6-clusters-based model trained on 21 factors-based train datasets. As shown in Table 9, the overall prediction performance accuracy is 100% of the time. This can be seen when using the correlation information in Table 6 to better understand the varying trait-wise mapping for hackers in the test dataset.

1. The professional dataset has shown 100% accuracy as they are all White Hats since Cluster-2 and Cluster-4 represent White Hats.
2. The student's dataset predicts 88% of White Hats and 11.7% of Gray Hats or White Hats with Gray Hat tendency. Both Cluster-0 and Cluster-1 show Gray Hat tendencies.

6 Discussion

This research uses machine learning to validate the proposed approach on approximately 30 real-life datasets. The application prediction performance was evaluated on (a) the final-year students who have some experience in hacking and intend to choose information security and ethical hacking as their profession and (b) professionals from the industry who are working as White Hackers. The study aimed to understand cluster trends and their association with different Hat types, requiring consideration of trait correlations in the test data. Spearman's correlation analysis was conducted, revealing moderate inter-dependencies between traits. These correlations were generalized, associating certain traits with specific Hat types.

The clustering analysis highlighted distinct trends across datasets, with clusters exhibiting varying trait compositions. The validation of these clusters using a 6-cluster model showed a high prediction accuracy of 100%, with professionals predominantly classified as White Hats and students displaying a mix of White Hat and Gray Hat tendencies. It has successfully mapped the different clusters with the different Hat types in the test dataset (see Table 9) with 88% accuracy. This can predict 11.7% of our false understanding of test data to consider two correctly predicted students as we conceived Gray Hats as White Hats. Previous research (Matulessy and Humaira, 2017) being conducted under the psychology domain only discusses results at generalized higher levels, covers no scientific experimentation, and has no detail of cluster assignments; therefore, it was neither possible to correctly understand individual tests nor the implementation done for cyber-criminal identification as hackers.

TABLE 7 Cluster to Hat-types mapping.

Cluster	Extroversion	Neurotic	Agreeable	Conscientious	Openness	Comments with hat mapping
0	2.33	3.50	3.00	2.83	2.50	Gray hats
1	2.33	3.25	4.00	2.17	2.75	White hat with gray hat tendency
2	2.08	2.05	2.73	2.47	2.50	White Hat with an average neurotic tendency (0.20 points difference in magnitude between traits)
4	2.22	1.42	3.67	2.89	3.33	White Hat with a low neurotic tendency (0.80 point difference in magnitude between traits)

TABLE 8 Validation of average trait scores on test datasets about previous research (Matulessy and Humaira, 2017).

	Extraversion	Neuroticism	Agreeableness	Conscientious	Openness	Hat type
Professional's data 13 records	1.99	1.71	2.5	2.37	2.48	White Hats with low Neurotic behavior (later will be generalized to cluster-4)
	Average	Low→ Average	High	Average → High	Average → High	
Student's data 17 records	2.12	2.12	3.20	2.54	2.68	White Hats with average Neurotic behavior (later will be generalized to cluster-2)
	Average	Average	High	Average → High	Average → High	

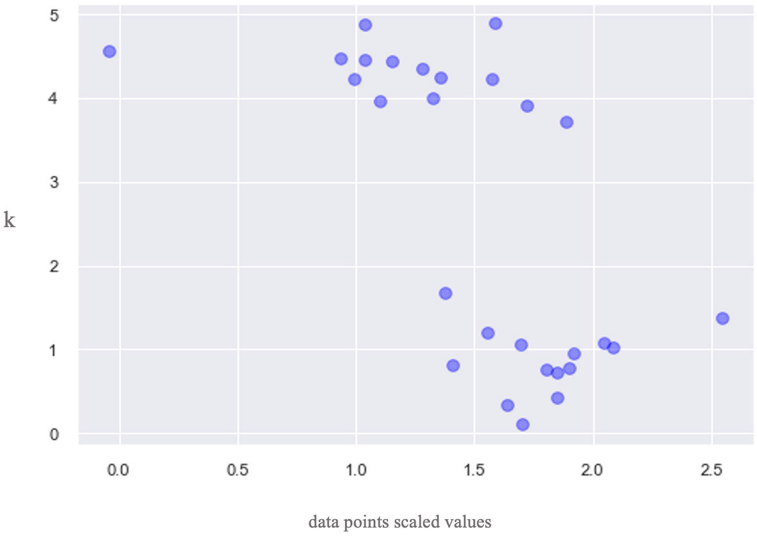


FIGURE 6
Test data points spread across the predicted clusters.

6.1 Implications

Incorporating personality profiling methodologies within the realm of cybersecurity elicits profound ethical inquiries necessitating meticulous examination. Chief among these concerns is the pivotal issue of privacy, wherein the acquisition and scrutiny of individuals' personality traits may encroach upon their privacy entitlements, and absent explicit consent and robust protective measures, with a palpable risk of unauthorized access to sensitive personal data, potentially precipitating privacy breaches and data misuse. Additionally, the deployment of personality profiling algorithms introduces the specter of bias, engendering the prospect of unjust treatment or discriminatory practices targeting specific individuals or demographic groups.

Securing informed consent stands as a crucial element in navigating these ethical challenges. Organizations are responsible for ensuring that individuals are comprehensively informed about the intentions and potential consequences of gathering and scrutinizing their personality data for cybersecurity aims. This empowers individuals to make informed decisions regarding their participation, allowing them to grant consent or abstain. Transparency and accountability take center stage in this process,

TABLE 9 Distribution of test dataset on 5 and 6 cluster-based hacker identification models.

5 Cluster	Total data	Number of test sets for professionals	Number of test sets for students	Hat types
4	6	3	3	White Hats with low Neurotic behavior
1	3	1	2	White Hat with Gray Hat tendency
0	3	1	2	Gray Hats
2	18	8	10	White Hats with average Neurotic behavior
Performance accuracy on a 6 cluster model	100%	100%	88% White Hats; 11.7% Gray Hats	

compelling organizations to openly disclose their data management procedures and to shoulder accountability for any ethical implications arising from the application of personality profiling.

Moreover, the cultivation of sustainable cybersecurity practices assumes critical importance in ensuring that security measures are deployed to minimize adverse environmental and societal impacts. This necessitates concerted efforts to curtail the environmental footprint associated with cybersecurity operations, promote social responsibility, and fortify resilience against cyber threats over the long term. Organizations can bolster security postures by integrating sustainability imperatives into cybersecurity frameworks while advancing equitable and environmentally conscious digital ecosystems.

The implications of our research underscore the imperative of comprehending hacker behavior, advocating for ethical considerations in cybersecurity practices, and promoting sustainable security paradigms. Through the dissemination of awareness on these issues, our endeavor is to facilitate informed decision-making and foster responsible cybersecurity practices that accord primacy to principles of privacy, equity, and sustainability.

6.2 Conclusion and future work

Following the research, it can be concluded that at a higher level, the hackers possess personality traits of agreeableness, neuroticism, and openness to experience. K-means algorithm of machine learning can be used to detect the personality traits of hackers. This research is an in-depth study to establish a quantitative and statistically significant mapping between predicted clusters and their respective Hat types using machine learning and correlation techniques. The mapping established in this research justifies the test dataset prediction performance accuracy of ∼94%. Cross-validation was not utilized due to the ample size of the training set. Additionally, the training and test sets were distinct. For future work, it is suggested that if reliable access to hackers becomes available, the training set could primarily consist of hacker data, which would then be validated using cross-validation techniques.

The model must also validate the test dataset for Black Hat types from reliable resources. Further work can be done to make this approach more advanced by replacing the questionnaire with some other graphical or pictorial techniques to judge the personalities of employees before the contract signup stage or at the time of the signup process on office systems.

Despite the strength of our approach and findings, it is important to recognize some limitations. One key issue is the size and diversity of our sample. Our study's sample might not be big or varied enough to apply our findings to all hackers. Most of our participants were final-year students and cybersecurity professionals, so our conclusions might not fully represent all hacker personality traits. In addition, since our sample was mostly male, we might not have captured the full range of hacker demographics. Additionally, relying on self-reported data and personality tests could introduce biases. Participants might try to give answers they think are socially desirable, affecting the accuracy of our data.

Finally, our study focused on specific personality traits linked to hackers, but there could be other factors at play in cybersecurity behavior. Future research should aim to overcome these limitations by using more diverse samples, which would help make our findings more reliable and widely applicable.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. Written informed consent from the [patients/ participants OR patients/participants legal guardian/next of kin] was not required to participate in this study in accordance with the national legislation and the institutional requirements.

Author contributions

UH: Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review and editing. OS: Methodology, Supervision, Validation, Writing – review and editing. KK: Methodology, Supervision, Writing – review and editing. AA: Methodology, Resources, Writing – review and editing. NI: Methodology, Supervision, Writing – review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Adali, S., and Golbeck, J. (2012). "Predicting personality with social behavior," in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (Istanbul: IEEE), 302–309.

Adewumi, A. O., and Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *Int. J. Syst. Assurance Eng. Manage.*8, 937–953. doi: 10.1007/s13198-016-0551-y

Akdag, M. (2020). *Open Psychometrics, Big Five Personality Test, International Personality Item Pool IPIP-BFFM*. Available online at: https://www.kaggle.com/akdagmelih/five-personality-clusters-k-means (accessed November 27, 2023).

Alashti, Z. F., Bojnordi, A. J. J., and Sani, S. M. S. (2022). Toward a carnivalesque analysis of hacking: a qualitative study of Iranian hackers. *Asian J. Soc. Sci.* 50, 147–155. doi: 10.1016/j.ajss.2022.01.001

Aldhyani, T. H., and Alkahtani, H. (2022). Attacks to autonomous vehicles: a deep learning algorithm for cybersecurity. *Sensors* 22, 360. doi: 10.3390/s22010360

Ali, A., Wasim, A., Husam, A., and Manasa, K. N. (2020). Crime analysis and prediction using K-means clustering technique. *EPRA Int. J. Econ. Business Rev.* 3, 2925–2929. doi: 10.36713/epra2016

Back, S., LaPrade, J., Shehadeh, L., and Kim, M. (2019). "Youth hackers and adult hackers in South Korea: An application of cybercriminal profiling," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (Stockholm: IEEE), 410–413.

Bakas, A., Wagner, A., Johnston, S., Kennison, S., and Chan-Tin, E. (2021). Impact of personality types and matching messaging on password strength. *EAI Endors. Trans. Secur. Safety.* 8, e1-e1. doi: 10.4108/eai.1-6-2021.170012

Buch, R., Dhatri, G., Pooja, K., and Nirali, B. (2017). World of cyber security and cybercrime. *RTPL* 4, 18–23.

Chayal, N. M., and Patel, N. P. (2021). Review of machine learning and data mining methods to predict different cyberattacks. *Data Sci. Intellig. Applicat.* 43–51. doi: 10.1007/978-981-15-4474-3_5

Chng, S., Lu, H. Y., Kumar, A., and Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Comp. Human Behav. Rep.* 5, 100167. doi: 10.1016/j.chbr.2022.100167

Corallo, A., Lazoi, M., Lezzi, M., and Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: a systematic literature review. *Comp. Indust.* 137, 103614. doi: 10.1016/j.compind.2022.103614

Del Pozo, I., Iturralde, M., and Restrepo, F. (2018). "Social engineering: Application of psychology to information security," in *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (Barcelona: IEEE), 108–114.

Fox, B., and Holt, T. J. (2021). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Crim. Justice Behav.* 48, 943–963. doi: 10.1177/0093854820969754

Geluvaraj, B., Satwik, P. M., and Ashok Kumar, T. A. (2019). "The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace," in *International Conference on Computer Networks and Communication Technologies* (Cham: Springer), 739–747.

Golbeck, J., Robles, C., Edmondson, M., and Turner, K. (2011). "Predicting personality from twitter," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (Boston: IEEE), 149–156.

Gulati, J., Priya, B., Bharti, S., and Anu, S. L. (2016). A study of the relationship between performance, temperament, and personality of a software programmer. *ACM SIGSOFT Softw. Eng. Notes* 41, 1–5. doi: 10.1145/2853073.2853089

Imran, M., Faisal, M., and Islam, N. (2019). "Problems and vulnerabilities of ethical hacking in Pakistan," in *2019 Second International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT)* (Karachi: IEEE), 1–6.

Islam, N., Shaikh, A., Qaiser, A., Asiri, Y., Almakdi, S., Sulaiman, A., et al. (2021). Ternion: an autonomous model for fake news detection. *Appl. Sci.* 11, 9292. doi: 10.3390/app11199292

Islam, N., and Shaikh, Z. A. (2016). "A study of research trends and issues in wireless ad hoc networks," in *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications*, ed I. Management Association (IGI Global), 1819–1859. doi: 10.4018/978-1-4666-8751-6.ch081

Javaid, M. A. (2013). Psychology of hackers. *SSRN Electr. J.* 15, 26. doi: 10.2139/ssrn.2342620

John, P., Oliver, and Sanjay, S. (1999). *The Big-Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives*. Berkeley: University of California. Available online at: https://personality-project.org/revelle/syllabi/classreadings/john.pdf (accessed March 10, 2024).

Larose, D. T., and Chantal, D. L. (2014). "Discovering knowledge in data: an introduction to data mining," in *IEEE Computer Society, 2nd ed.* Hoboken: John Wiley and Sons.

Lima, A. C. E., and De Castro, L. N. (2014). A multi-label, semi-supervised classification approach applied to personality prediction in social media. *Neural Netw.* 58, 122–130. doi: 10.1016/j.neunet.2014.05.020

Martineau, M., Spiridon, E., and Aiken, M. (2023). A comprehensive framework for cyber behavioral analysis based on a systematic review of cyber profiling literature. *Forens. Sci.* 3, 452–477 doi: 10.3390/forensicsci3030032

Matulessy, A., and Humaira. N. H. (2017). Hacker personality profiles reviewed in terms of the big five personality traits. *Psychol. Behav. Sci.* 5, 137–142. doi: 10.11648/j.pbs.20160506.12

McAlaney, J., Hambidge, S., Kimpton, E., and Thackray, H. (2020). "Knowledge is power: an analysis of discussions on hacking forums," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (Genoa: IEEE), 477–483.

Medoh, C., and Telukdarie, A. (2022). The future of cybersecurity: a system dynamics approach. *Procedia Comp. Sci.* 200, 318–326. doi: 10.1016/j.procs.2022.01.230

Mohammed, Z. H., Chankaew, K., Vallabhuni, R. R., Sonawane, V. R., Ambala, S., and Markkandan, S. (2023). Blockchain-enabled bioacoustics signal authentication for cloud-based electronic medical records. *Measurem. Sens.* 26, 100706. doi: 10.1016/j.measen.2023.100706

Novikova, I. A., and Alexandra, A. V. (2019). "The five-factor model: contemporary personality theory," in *Cross-Cultural Psychology: Contemporary Themes and Perspectives* (Hoboken: John Wiley and Sons Press), 685–706.

Odemis, M., Yucel, C., and Koltuksuz, A. (2022). Detecting user behavior in cyber threat intelligence: development of honeypsy system. *Secur Commun. Netw.* 2022, 7620125. doi: 10.1155/2022/7620125

Pastrana, S., Hutchings, A., Caines, A., and Buttery, P. (2018). "Characterizing eve: Analysing cybercrime actors in a large underground forum," in *International Symposium on Research in Attacks, Intrusions, and Defenses (Cham:* Springer), 207–227.

Ramachandran, D., Rajeev Ratna, V., PT, V. R., and Garip, I. (2022). A low-latency and high-throughput multipath technique to overcome black hole attack in mobile *ad hoc* network (MTBD). *Secur. Commun. Netw*. 2022, 8067447. doi: 10.1155/2022/8067447

Shackelford, S. J., Raymond, A., Fort, T. L., and Charoen, D. A. (2016). *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*. Chicago: University of Illinios Law Review. Available online at: https://illinoislawrev.web.illinois.edu/wp-content/uploads/2016/10/Shackelford.pdf (accessed March 10, 2024).

Siddiqi, M. A., Pak, W., and Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Appl. Sci*. 12, 6042. doi: 10.3390/app12126042

Sood, A. K., and Enbody, R. J. (2013). Crimeware-as-a-service: a survey of commoditized crimeware in the underground market. *Int. J. Criti. Infrastruct. Protect.* 6, 28–38. doi: 10.1016/j.ijcip.2013.01.002

Suárez Álvarez, J., Pedrosa, I., Lozano, L. M., García Cueto, E., Cuesta Izquierdo, M., and Muñiz Fernández, J. (2018). "Using reversed items in Likert scales: A questionable practice," in *Psicothema*, 30. Available online at: https://digibuo.uniovi.es/dspace/bitstream/handle/10651/48979/Using%20.pdf?sequence=1 (accessed March 10, 2024).

Suryapranata, K. P., Louis, P. K., Gede, H., Yaya, H., Bahtiar, S. A., et al. (2017). "Personality trait prediction based on game character design using a machine learning approach," in *Proc. ICITech* (Salatiga: IEEE), 1–5.

Tamboli, M. S., Vallabhuni, R. R., Shinde, A., Kataraki, K., and Makineedi, R. B. (2023). Block chain based integrated data aggregation and segmentation framework by reputation metrics for mobile adhoc networks. *Measurem.: Sens.* 27, 100803. doi: 10.1016/j.measen.2023.100803

Tan, P. N., Steinbach, M., and Kumar, V. (2016). *Introduction to Data Mining*. Washington DC: Pearson Education India. Available online at: https://www-users.cse.umn.edu/$\sim$kumar001/dmbook/ch7_clustering.pdf (accessed March 10, 2024).

Tandera, T., Derwin, S., Rini, W., and Yen, L. P. (2017). Personality prediction system from Facebook users. *Procedia Comp. Sci.* 116, 604–611. doi: 10.1016/j.procs.2017.10.016

Wong, S., Dennis, and Sai-fu, F. (2020). Development of the cybercrime rapid identification tool for adolescents. *Int. J. Environ. Res. Public Health* 17, 4691. doi: 10.3390/ijerph17134691

Xie, B., and Wei, N. (2022). "Personality trait identification based on hidden semi-Markov model in online social networks," in *Proceedings of the 2022 7th International Conference on Intelligent Information Technology (ICIIT '22)* (New York, NY: Association for Computing Machinery), 52–58. doi: 10.1145/3524889.3524898

Zheng, R., Qin, Y., Huang, Z., and Chen, H. (2003). "Authorship analysis in cybercrime investigation," in *International Conference on Intelligence and Security Informatics* (Berlin: Springer), 59–73.