Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7698993

EXAMINING THE ROLE OF ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

Yadav Sangeeta Ramchandra and Dr. Sanjay Singh Bhadoria
Department of Computer Application, Dr. A. P. J. Abdul Kalam University, Indore
Corresponding Author Email: ghodke.sangeeta@gmail.com

Abstract:

The complexity, frequency, and size of attacks on computer systems and infrastructure are all increasing. The goal of these attacks is to cause disruptions in vital infrastructure and get access to sensitive data, and novel attack tactics and the exploitation of new attack surfaces have been identified. Many other papers have summarized the history and current state of various types of cyber attacks. According to Microsoft's latest Digital Defense Report, hackers and nation-states are constantly changing their tactics to take advantage of emerging security holes and circumvent previously effective cyber defences. The goal of cybersecurity solutions should be to ensure that individuals can use a wide range of devices and access their data safely and securely from places outside the office. The benefits of using AI into cyber security applications are becoming more and more apparent. Artificial intelligence (AI) has various uses, one of which is the automated interpretation of signals produced during assaults, threat incident prioritisation, and adaptive responses to the pace and magnitude of hostile operations. These techniques show a lot of potential for quickly evaluating and correlating patterns across billions of data points, which may help in the detection of a broad range of cyber threats in a matter of seconds. In addition, AI is able to continuously learn and adapt to new attack patterns, using data collected in the past to help it identify similar assaults in the future. Due to this, machine learning has been increasingly integrated into modern cyber security tools. This study looks at how AI has affected cyber security in general.

Keywords: - Cybersecurity, Artificial Intelligence (AI), Cyber threats, Data Privacy

1. INTODUCTION

Cyberspace has had a profound effect on our society, ushering in a period of remarkable scientific and technological development. The rise of offensive cyber-tools and cyber-operations, however, poses a systemic danger that might undermine cyberspace's benefits. Networks, systems, and other forms of digital infrastructure must be protected by cyber security measures. Static management of security cyberspace monitoring according to pre-specified criteria is the backbone of conventional cyber security. However, with the emergence of more sophisticated cyber attacks, this passive defence strategy has become obsolete. In order to integrate malware categorization, intrusion detection, vulnerability, and threat identification, artificial intelligence technologies like deep learning have recently been brought into cyber security to develop smart models. Keep in mind, too, that AI may also be employed by attackers to hone their methods and develop more potent attacks. It is thus crucial to guarantee current cyber security is ready to handle the new risks permitted by malevolent applications of AI by studying the efficacy of both Defensive and Offensive AI. The potential and problems arising from the current state of artificial intelligence as they relate to cyber security are the primary subject of this special issue.

The use of artificial intelligence in cyber security is growing, for both positive and negative purposes. In order to safeguard their systems and data, businesses may use cutting-edge AI-based solutions to monitor for and identify potential dangers. However, this technology may also be used by cybercriminals to conduct more complex assaults. An increasing number of cyber attacks is contributing to the expansion of the market for security solutions powered by AI. The worldwide market was worth $14.9 billion in 2021, according to a research by Acumen Research and Consulting published in July 2022, and is projected to grow to $133.8 billion by 2030.

Distributed denial of service (DDoS) assaults and data breaches are on the rise, and they can be very expensive for the businesses they target. This has led to a need for more advanced solutions to combat these threats. The research also attributes the expansion of the business to the CoVD-19 epidemic and the subsequent rise of the telecommuting workforce. As a result, many businesses have begun to place a greater emphasis on cyber security and the use of AI-powered solutions to detect and thwart cyber attacks.

2. LITERATURE REVIEW

Tamanna Choithani (2022) In recent years, cryptocurrency has emerged as a primary digital money, financial asset, and system. Artificial intelligence methods are needed to anticipate price, trend, portfolio creation, and identify fraud in order to lower investing risk. This paper reviews the state of the art in artificial intelligence (AI) approaches applied to the cryptocurrency market, with a particular focus on Bitcoin. The article reviews and discusses the most significant works including AI and ML methods like SVM, ANN, LSTM, and GRU in the context of cryptocurrencies like Bitcoin. Some research avenues and places where findings may be used more effectively were also identified. AI and cyber security have both made rapid strides in recent years. Its adoption has been very helpful in the financial sector and has had significant effects on markets, institutions, and laws. It's a positive force that's helping the world improve. Intelligent simulations of robots that are like humans in every way save intelligence are the work of artificial intelligence. The use of AI in banking is reshaping monetary discourse. It aids in the simplification and improvement of credit decisions, quantitative analysis in marketing, and economic risk management, among other financial sector operations. The primary objective of this study has been to inquire into the effects of AI in the modern world. The allure of AI is explored along with its impact on the workforce and the opportunities it presents. The study explores how AI might help financial institutions attract and retain customers while also generating revenue. The digital implementation of the several banks that make up India's thriving banking industry (RBI, SBI, HDFC, etc.) employing chat-bots that have benefited clients is an integral part of daily life in India.

Binny Naik (2022) In light of the current condition of cyber security, it is not surprising that professionals in the sector are looking to artificial intelligence for help. Many technological advances have made a dent in the cyber security problems that have plagued the past. Big Data, Blockchain, and Behavioral Analytics, to mention a few, may all be used to realize these improvements. The report provides a summary of the results of using these technologies in cyber security. The primary objective of this study is to examine how different artificial intelligence methods have been used to investigate, identify, and counter cyber threats. Different cyber dangers have been examined in light of the installation of "distributed" AI techniques that are conditionally classed and "compact" AI methods that are readily classified. The potential and difficulties of using these methods in the future to cyber security are also highlighted. We have reached the end of our analysis, which aimed to evaluate the use of various AI developments in bettering cyber security.

Blessing Guembe (2022) In recent years, cyberattacks have increased in sophistication and frequency. As a result, cybercriminals are increasingly turning to AI methods to hide their tracks in cyberspace and inflict more widespread harm without being detected. The notion of AI-powered assaults has not been studied extensively enough by researchers in the cybersecurity space to comprehend the degree of complexity possessed by this form of attack. The purpose of this article is to delve into the rising problem of AI-powered cyberattacks and shed light on the potentially dangerous ways in which AI is already being utilised maliciously. The research used a three-stage procedure, during which only high-quality papers about AI-driven cyberattacks were chosen for inclusion. Relevant publications were retrieved via searches conducted in databases such as ACM's, arXiv Blackhat's, Scopus, Springer's, MDPI's, IEEE Xplore's, and others. Only 46 articles were chosen from the 936 that were initially considered after the first search. The findings show that throughout the cybersecurity kill chain, 56% of the AI-driven cyberattack techniques were demonstrated during the access and penetration stage, 12% during the exploitation stage, 12% during the command and control stage, 11% during the reconnaissance stage, and 9% during the delivery stage. According to the results, traditional cyber defences won't be able to keep up with the increased velocity and nuanced decision-making of AI-driven assaults. Therefore, businesses must make investments in AI cybersecurity infrastructures to counteract these new dangers.

Mujaheed Abdullahi (2022) With the advent of the fourth industrial revolution (Industry 4.0) in recent years, technological developments such as IoTs, fog computing, computer security, and cyberattacks have expanded at an exponential rate. The proliferation of IoT gadgets and networks calls for stringent measures to ensure the integrity of the vast quantities of data they produce. One of the most promising approaches to dealing with cybersecurity risks and ensuring security is the use of artificial intelligence (AI). We offer an SLR that organises, maps, and surveys the extant literature on artificial intelligence techniques for detecting cybersecurity threats in the Internet of Things setting. This SLR aims to cover a wide range of topics, from the history of cybersecurity to the current state of the art in artificial intelligence-based security. In order to get relevant results, a thorough search was conducted across several online resources (SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI). Eighty research published between 2016 and 2021 were randomly chosen from the retrieved data, surveyed, and evaluated. In this article, we looked at how successful deep learning (DL) and machine learning (ML) approaches are in spotting threats in the context of IoT security. However, a number of studies have developed smart intrusion detection systems (IDS) with intelligent architectural frameworks employing AI to address the current state of security and privacy concerns. High precision detection is likely one reason why support vector machines (SVM) and random forest (RF) are so popular, but they may also benefit from having a small memory footprint. Additionally, alternative approaches, such as extreme gradient boosting (XGBoost), neural networks (NN), and recurrent neural networks (RNN), give superior results (RNN). The AI development road plan for threat detection by attack category is also shown by this investigation. We conclude with several suggestions for follow-up research.

Mohammad Wazid (2022) Machine learning (ML) is a branch of AI that focuses on creating automated systems that can analyse large amounts of data in order to draw conclusions and make choices with little to no human input. Computers, servers, mobile devices, networks, and their related data are all vulnerable to cyber assaults, so it's important to take precautions to keep them safe. There are two main facets to merging cyber security with ML: taking into consideration the cyber security of the environment in which the ML is being used, and using the ML itself to enable cyber security. In addition to bolstering the safety of machine learning models, improving the efficiency of cyber security techniques, and facilitating the efficient detection of zero-day threats with little human interaction, we may benefit in a number of other ways from this coming together. By bringing together cyber security and machine learning, we are able to explore a wider range of topics than would normally be covered in a survey study. In addition, we talk about the benefits, concerns, and difficulties of combining cyber security with ML. We also compare and contrast a number of assaults across two main groups. Finally, we suggest several avenues for further study.

3. RESEARCH AND METHODOLOGY

Software that facilitates online social interaction, communication, and participation in group activities is known as "social networking software." This description encompasses all of the most well-known social networking platforms now available, from blogs and wikis to podcasts and tags, and even search engines themselves. The usage of online communities for the purpose of fostering relationships among people who have common interests has lately spread into the business sphere. Enterprise security and risk management professionals must face the reality that professional social networks such as LinkedIn and Blue Chip Expert, and professional groups on once-personal sites such as Facebook and MySpace, are emerging as a source for the unauthorised disclosure of confidential corporate information. There are many advantages to social network solutions, but users also need to be aware of the potential dangers presented by these platforms.

The purpose of this study is to examine certain concerns related to the safety and privacy of social networking sites. This survey-based investigation is both descriptive and quantitative in scope. Primary and secondary sources of information are used. Data for this study was gathered via a questionnaire. Random sampling is used to choose a sample of at least 500 people from the whole population of people who use social networking sites in India, who fall into categories such as students, researchers, scholars, workers, businessmen, businesswomen, and housewives.

4. DATA ANALYSIS

Table 1: Sample Profile

Particulars		Male	Female	Total	
Student	UG Student	120	88	208	250
	PG Student	24	18	42	
Non -Student	Businessman/Self-employed	9	4	13	250
	Employee	97	61	158	
	House Wife	0	79	79	
Total		250	250	N=500	

Table 2: Sample Distribution

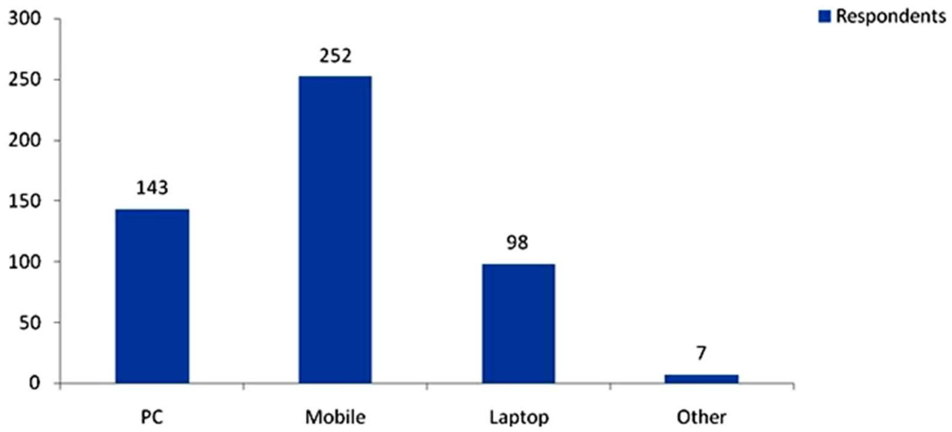
Category	Particulars	Respondents	Total
Gender	Male	250	500
	Female	250	
Occupation	UG Student	208	500
	PG Student	42	
	Employee	158	
	Businessman/Self-employed	13	
	House Wife	79	

Age	18-25	287	500
	26-35	54	
	36-50	143	
	Above 50	16	
Qualification	Non Matriculate	7	500
	Post Graduate	148	
	Matriculate	38	
	Graduate	307	

Table 3: Tools used to access Social Media

Sr.	Particulars	Respondents		Percentage
1	PC	217	143	29
2	Mobile	383	252	50
3	Laptop	149	98	20
4	Other	11	7	1
	Total	760	500	100

Fig.1 Tools used to access Social Networking Sites

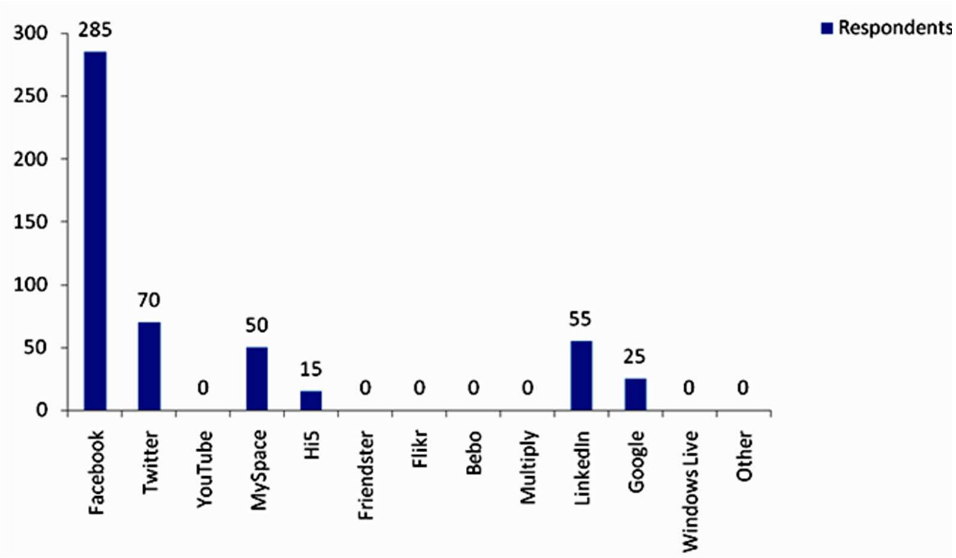


The data in the table above reveals that although 50% of respondents use their smartphones to access social media, 29% use a personal computer, 20% use a laptop, and 1% uses a smart television or other device. The Smartphone is becoming even more popular as the device of choice for accessing social networking sites. When using a mobile device, app access to social media is more popular than desktop access.

Table 4: Membership of Social Networking Sites

Sr.	Particulars	Respondents	Percentage
1	Facebook	285	57
2	Twitter	70	14
3	YouTube	0	0
4	MySpace	50	10
5	Hi5	15	3
6	Friendster	0	0
7	Flikr	0	0
8	Bebo	0	0
9	Multiply	0	0
10	LinkedIn	55	11
11	Google	25	5
12	Windows Live	0	0
13	Other	0	0
Total		500	100

Fig. 2 Membership of Social Networking Sites



According to the data, the vast majority (57%) of social networkers may be found on Facebook. Twitter accounts make up 14% of those surveyed, while 11% use LinkedIn, 10% report using MySpace, and 8% mention using other sites like Hi5 and Google. The vast majority of people who use social networks also have a profile on Facebook.

Table 5: Concern about the issues as a member of Social Networking Sites

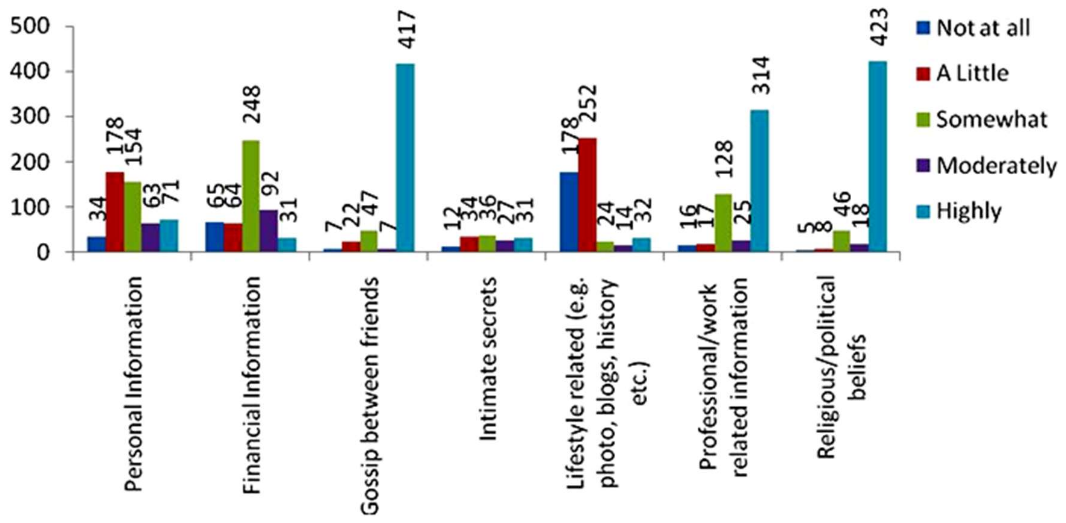
Sr.	Particulars	Not at all	A Little	Somewhat	Moderately	Highly	Total
		1	2	3	4	5	
1	Safe ways of using social networking sites.	78	134	118	90	80	500
2	Ways to behave towards other people on the social network.	34	128	203	64	71	500
3	Risks of using social networking services.	17	24	35	22	402	500
4	What to do if people you don’t know contact You online.	11	23	47	11	408	500

Concern about social media is fairly evenly distributed between those who are very concerned and those who are somewhat concerned. Forty-one percent of respondents reported being somewhat concerned about appropriate ways to interact with others online, and twenty-seven percent were concerned about using social networking safely. Females' natural shyness actually makes them better communicators and reduces the hazards associated with making contact with strangers and utilizing social networking sites, both of which have led to a general consensus of high worry across the population at large (80%).

Table 6: Concern about Privacy of information submitted on Social Networking Sites

Sr.	Particulars	Not at all	A Little	Somewhat	Moderately	Highly	Total
		1	2	3	4	5	
1	Personal Information	34	178	154	63	71	500
2	Financial Information	65	64	248	92	31	500
3	Gossip between friends	7	22	47	7	417	500
4	Intimate secrets	12	34	36	27	391	500
5	Lifestyle related (e.g. photo, blogs, history etc.)	178	252	24	14	32	500
6	Professional/work related information	16	17	128	25	314	500
7	Religious/political beliefs	5	8	46	18	423	500

Fig. 3 Concern about Privacy of information submitted on Social Networking Sites



Participants in the study feel secure in their capacity to keep safe online, despite the existence of some amount of online risk today; nonetheless, the above table demonstrates that they are less worried about their privacy on social networking sites. Some of the places where investigators raised concerns are listed below. Respondents were moderately worried about the protection of their personal information (67%), and had made a similar choice about their financial information (63%), when asked whether they had ever opted not to send it online. Most respondents were very worried about protecting their privacy by avoiding posting rumors and personal details about their acquaintances (83% and 78%, respectively).

Despite the fact that students are heavy social media users, it comes as a surprise that they are less concerned about privacy when disclosing information about their lifestyle (86%), whereas employees, businessmen, and self-employed users are very concerned about the privacy of their professional/work-related information (63%). Users wanted to find out why there was such a high level of anxiety about revealing religious/political ideas (85%) in the first place, and the media had a major role in raising people's knowledge of the problem.

Table 7: Activeness in disclosing information submitted on Social Networking Sites

Sr.	Particulars	Not at all	A Little	Somewhat	Moderately	Highly	Total
		1	2	3	4	5	
1	Personal Information	4	29	5	52	410	500
2	Financial Information	348	104	23	17	8	500
3	Gossip between friends	95	298	34	38	35	500

4	Intimate secrets	92	305	30	42	31	500
5	Lifestyle related (e.g. photo, blogs, history etc.)	5	12	3	72	406	500
6	Professional/work related information	167	64	14	87	168	500
7	Religious/political beliefs	405	78	9	8	0	500

Using the aforementioned table, we can see what typical pieces of data are shared on social media. Eighty-two percent of respondents said that they could easily find personal information about them on social media. Only eight percent of those who fill out surveys provide any kind of financial information in their profile. Almost 80% of Facebook users actively include lifestyle-related information, and 34% also list professional/work-related information. Respondents provide just a bare minimum of information on their religious and political affiliation (8%). The poll results show that over two-thirds of respondents are seldom involved in spreading rumours and sharing private information within their close circle of friends and acquaintances.

Table 8: Privacy controls settings used in Social Networking Sites

Sr.	Particulars	Never	Rarely	Sometim es	Often	Always	Total
		1	2	3	4	5	
1	Lock profile so only people I know can view it.	355	105	19	14	7	500
2	Limit post to only be viewable by selected friends.	15	21	6	73	385	500
3	Provide some fake or inaccurate information	382	36	8	32	38	500
4	Not to allow search engines to directly link	482	11	5	2	0	500

	to your timeline.						
5	Control who can post on timeline and who can see timeline	147	114	24	131	84	500
6	Take no action/accept the default privacy settings	8	9	6	143	334	500

According to the results, the vast majority of survey takers (71%!) are clueless when it comes to their profile's privacy settings and have not restricted access to friends and family. Women seem to spend more time than men do online, maybe because socialising and exchanging knowledge are more natural female activities. For instance, women are more likely than men to restrict who may see a post by selecting friends (48% vs. 29%). Researchers concluded that some proportion of these respondents (8%) disclosed such information (mainly the profile image) to the general public based on the findings in the aforementioned table and the results for supplying fraudulent or misleading information.

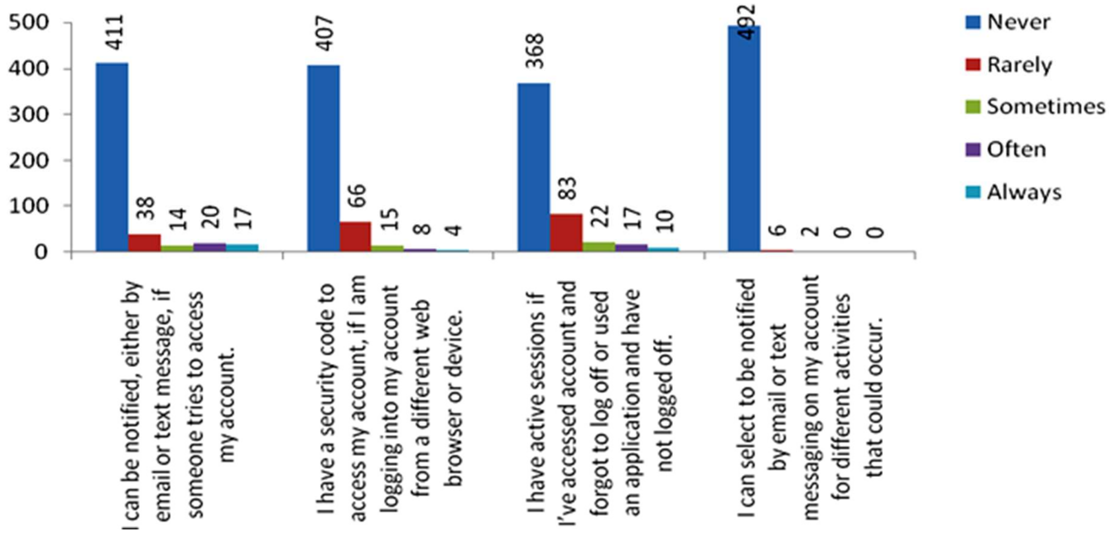
It's disheartening that most people questioned had no idea that search engines may see their Facebook timeline. Only 3% of those who took the poll almost never let search engines connect directly to their timeline. Inadequate privacy settings for restricting who may post on timeline and who can access timeline puts 62% of survey respondents susceptible to having their personal information revealed. The bulk of respondents (82%) did not realize the possible harm of not managing the timeline, while only 17% properly identified to manage who may publish on timeline and who can view timeline. Most poll takers obviously didn't adjust their privacy settings. Almost two-thirds of respondents had their privacy settings left at their default.

Table 9: Security control settings used in Social Networking Sites

Sr.	Particulars	Never	Rarely	Sometimes	Often	Always	Total
		1	2	3	4		
1	I can be notified, either by email or text message, if someone tries to access my	411	38	14	20	17	500

	account.						
2	I have a security code to access my account, if I am logging into my account from a different web browser or device.	407	66	15	8	4	500
3	I have active sessions if I've accessed account and forgot to log off or used an application and have not logged off.	368	83	22	17	10	500
4	I can select to be notified by email or text messaging on my account for different activities that could occur.	492	6	2	0	0	500

Fig. 4 Security control settings used in Social Networking Sites



The goal of this table is to see how long respondents think it will take before they realise their account has been compromised. Note that 82% of survey respondents did not use any security settings that would alert them through email or text message if their account was compromised. Whether they try to access their account from a browser or device other than the one they normally use, this subsequent message will tell you if they need to change their security settings. Perhaps this is because 81% of those who took part in our poll said they had never changed their profile's default browser or device for further protection.

According to the poll, the vast majority (74%) of people don't even realize they're still connected into an account or an application even if they haven't closed the tab or exited the programme. This suggests that the majority of users are oblivious to the security of their accounts (3/4). Although social media businesses are improving their response to user security concerns, consumers must take some of the onus for their own safety. Nobody in the poll was aware that they could set preferences to be alerted by email or text message if certain events occurred in their account. Only 2% of users had the option to be alerted by email or text message whenever there was activity on their account, while 98% claimed they did not.

5. CONCLUSION

Artificial intelligence is expanding, and researchers are digging further into the field. This demonstrates the enormous technical progress being made in the methods utilized to guarantee cybersecurity support. These steps demonstrate the technology's influence on preventative measures for cybercrime. With the exponential growth of both hostile intelligence and cyber threats, it is no longer possible to disregard the need for advanced cybersecurity tactics. Experience in DDoS protection has also shown that security may be achieved against large-scale attacks with relatively low resources, provided that clever ways are applied. Research into artificial neural networks seems to provide the most applicable AI discoveries for cyber security, according to a survey of scholarly articles. Cybersecurity applications of neural networks persist. The demand for advanced cyber-security measures remains for many domains where neural networks aren't the best fit technology. Decision analysis, context comprehension, and data management are all examples of such specialized areas. The creation of more intelligent machines is the most intriguing prospect here. It is unknown how quickly general artificial intelligence has progressed, but it is possible that offenders will use a new kind of AI so long as it is available. It's not immediately clear. Furthermore, state-of-the-art tools for data analysis, interpretation, and administration, especially in the field of machine learning, would greatly enhance the security of systems.

REFERENCES

1. Choithani, T., Chowdhury, A., Patel, S. et al. A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. Ann. Data. Sci. (2022).

2. Naik, B., Mehta, A., Yagnik, H. et al. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex Intell. Syst. 8, 1763–1780 (2022).

3. Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1,

4. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics 2022, 11, 198.

5. Mohammad Wazid, Ashok Kumar Das, Vinay Chamola, Youngho Park, Uniting cyber security and machine learning: Advantages, challenges and future research, ICT Express, Volume 8, Issue 3, 2022, Pages 313-321, ISSN 2405-9595,

6. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the Next-Generation Networks and Internet of Things. IEEE Trans. Ind. Inform. **2020**, 16, 3515–3520.

7. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory **2020**, 101, 102031.

8. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. Futur. Gener. Comput. Syst. **2022**, 127, 286–296.

9. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. Sustain. Cities Soc. **2021**, 75, 103311.

10. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. IEEE Trans. Ind. Inform. **2020**, 16, 4166–4176.

11. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and multidirectional data aggregation for edge computing-enhanced IoT. J. Syst. Archit. **2020**, 106, 101713

12. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener. Comput. Syst. **2018**, 82, 761–768.

13. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans. Ind. Inform. **2020**, 16, 2716–2725.

14. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access **2020**, 8, 34564–34584.

15. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. Electronics **2020**, 9, 2152.