Journal of Advanced Research in Intelligence Systems and Robotics
Volume 6, Print Issue 1 - 2024, Pg. No. 15-21
Peer Reviewed Journal

Review Article

Role of Artificial Intelligence in Cyber Security

Parth Trivedi[1], Naitik Bohra[2]

[1,2]Research Scholar, MCA Thakur Institute of Management Studies, Career Development & Research (TIMSCDR) Mumbai, India.

I N F O

Corresponding Author:
Parth Trivedi, MCA Thakur Institute of Management Studies, Career Development & Research (TIMSCDR) Mumbai, India.
E-mail Id:
parthfu2216@gmail.com
Orcid Id:
https://orcid.org/0009-0006-5647-0863
How to cite this article:
Trivedi P, Bohra N. Role of Artificial Intelligence in Cyber Security. *J Adv Res Intel Sys Robot* 2024; 6(1). 15-21.

Date of Submission: 2024-02-20
Date of Acceptance: 2024-03-23

A B S T R A C T

In the digital age, the escalating threat of cyberattacks has become a major concern, with stories of identity theft, data breaches, and sophisticated cybercrimes impacting individuals and organisations worldwide. The advent of artificial intelligence (AI) has not only revolutionised various scientific and technical fields, such as robotics and healthcare but has also given rise to a new era of intelligent cyberattacks. The widespread use of IoT has further intensified the impact of cyber threats globally. In response, the imperative to formulate a comprehensive cybersecurity strategy has become paramount. Cybersecurity involves the deployment of technology, procedures, and controls to safeguard against cyberattacks on devices, programmes, networks, systems, and data. Traditional security measures alone prove insufficient against the evolving tactics of cybercriminals who employ cutting-edge methods. Fortunately, AI technologies have emerged as a crucial tool in fortifying cyber defences. This essay explores the application of AI in combating cyberattacks, showcasing its potential in developing intelligent models capable of analysing data and making informed decisions to protect against the ever-growing sophistication of cyber threats.

Keywords: Cybersecurity, Artificial Intelligence, Cyberattacks, Intelligent Models, Data Analysis, Cyber Defences, IoT, Digital Age, Threats, Comprehensive Strategy

Introduction

Cybersecurity is critical in the digital era because it protects networks, systems, and private data against hacking, illegal access, and other online dangers. By guaranteeing the availability, confidentiality, and integrity of digital assets, it upholds confidence in online interactions and shields people, businesses, and society from the potentially disastrous effects of cyber-attacks.

Cyberspace is a dynamic environment with ever-growing threats and difficulties. These include ransomware, phishing, sophisticated cyberattacks,

Threats from nation-state actors, criminal groups, and hacktivists that target people, companies, and vital infrastructure are growing furthermore since technology advances quickly, new attack vectors are created. This highlights the necessity of ongoing watchfulness, strong defences, and international cooperation in order to effectively combat growing cyber threats.

Overview of AI

The creation of computer systems that are capable of carrying out activities that normally require human intelligence is known as artificial intelligence or AI. This covers verbal comprehension, learning, reasoning, and problem-solving. Artificial intelligence (AI) can be divided into two categories: general AI, which strives to be as intelligent as humans across a variety of activities, and narrow AI, which is created for a single purpose. The various uses of AI are:

1. **Machine Learning (ML):** A branch of learning from their experiences and advances without explicit programming. Predictive analytics, recommendation engines, and picture and speech recognition are some examples of applications.
2. **Natural Language Processing (NLP):** Technology that enables computers to comprehend, translate, and produce human language. NLP is utilised in sentiment analysis language translation, and chatbots.
3. **Teaching Machines:** Technology that is used to comprehend and make decisions based on visual data is known as computer vision. Autonomous vehicles, object detection, and facial recognition are among the applications.
4. **Robotics:** AI is used in robotics to control robots so they can carry out activities in a variety of industries, including manufacturing, healthcare, and exploration.
5. **Expert Systems:** They are Artificial Intelligence (AI) systems created to simulate a human expert's decision-making process in a particular field. They are employed in fields such as financial analysis and medical diagnostics.
6. **Autonomous:** AI is essential for creating autonomous systems, such as drones and self-driving cars that can travel and make decisions on their own without human assistance.
7. **Virtual Assistants:** AI-driven virtual assistants that can execute tasks, answer questions, and deliver information including Siri, Alexa, and Google Assistant.
8. **Gaming:** AI is utilised in video games to produce smart and flexible opponents, which improves the whole gameplay experience.
9. **Cybersecurity:** By studying trends, spotting anomalies, and improving general security, AI aids in the identification and prevention of cyber-attacks.
10. **Healthcare:** AI is being used in drug discovery, patient care management, medical imaging analysis, and personalised medicine.

These uses highlight the adaptability and potential benefits of AI in a range of sectors, enhancing productivity, judgement, and problem-solving skills. AI systems are essential to cybersecurity because they can replicate human intelligence and decision-making processes. The main ways that AI mimics cognitive processes that are similar to those of humans are examined in this section in order to improve cyber security defences.

Algorithms for Machine Learning Machine learning algorithms are used by AI as one of the primary means of imitating human intellect. AI systems are able to learn from large datasets, identify patterns, and adjust to changing cyber threats thanks to these algorithms.

Through the application of supervised learning, unsupervised learning, and reinforcement learning methodologies, artificial intelligence models simulate the human ability to evaluate data and develop decision-making skills over time.

Natural Language Processing

Natural language processing, or NLP, is a crucial component in the field of cybersecurity that allows AI systems to understand and react to human language. Artificial intelligence (AI) systems can recognise possible security threats conveyed across many channels by deciphering and comprehending textual data. Because of this skill, which closely resembles human language understanding, AI can interact with and comprehend security-related data in a way that is comparable to that of human analysts.

Cognitive Processes

AI's cognitive computing subset incorporates aspects of human mental processes, going beyond conventional rule-based systems. These systems possess the ability to reason, comprehend context, and make decisions based on vague or insufficient data. Artificial Intelligence (AI) enhances cybersecurity scenarios by imitating human-like cognitive functions including perception and problem-solving, hence facilitating more sophisticated and flexible decision-making.

Deep Learning and Neural Networks Artificial Intelligence (AI) relies heavily on neural networks, which are modelled after the architecture of the human brain. Complex neural network designs are used in deep learning, a subset of machine learning, to process and interpret data. This makes it possible for AI systems to carry out tasks like pattern recognition, language translation, and image recognition, which represent the complex structure of human cognitive processes.

Adaptive Learning

Adaptive learning algorithms are commonly incorporated into AI systems in cybersecurity, enabling them to dynamically modify their behaviour in response to evolving threat landscapes. The human capacity for ongoing learning and development is reflected in this capability to adapt and learn. AI-driven security measures are guaranteed to adapt to new threats through adaptive learning, exhibiting a degree of intelligence that is comparable to human decision-making.

AI in Cyber Security

By using machine learning (ML) algorithms to find patterns of dangerous activity, artificial intelligence (AI) plays a critical role in threat identification and prevention. This is an examination of the application of AI in this situation:

Machine Learning for Identifying Threats

1. **Anomaly Detection:** Machine learning models are taught to identify typical behaviour patterns in

a network or system. Any departure from these well-established norms may be seen as potentially dangerous. For instance, an alarm might go off if a worker unexpectedly gains access to a lot of private information after hours.

2. **Behavioural Analysis:** Machine learning algorithms are capable of examining user behaviour to spot odd behaviours or trends that can point to a security risk. This involves spotting odd login times, access to peculiar places, or departures from regular usage habits.
3. **Pattern Recognition:** Machine learning models can be trained on past data to identify established patterns of dangerous behaviour, such as certain malware kinds or popular attack techniques. This aids in proactively recognising threats according to their attributes.

Real-Time Monitoring

- **Network Traffic Analysis:** AI is utilised to analyse network traffic in real time, looking for any odd or suspicious patterns that might point to a possible security breach. Deep learning algorithms facilitate the discovery of small anomalies by analysing large amounts of data rapidly and reliably.
- **Endpoint Security:** AI-driven endpoint defence programmes keep a close eye on every action taken on each device. ML algorithms offer real-time defence against a variety of threats by identifying malicious processes, file modifications, or system irregularities.

Incident Response

1. **Automated Incident Identification:** Artificial Intelligence can help quickly recognise and categorise security incidents. Security teams may more effectively prioritise and address risks when machine learning algorithms are used to assess the type and severity of an incident.
2. **Artificial Intelligence:** (AI) technologies are utilised in decision support systems to analyse the impact and context of security incidents. This helps human responders decide on containment, eradication, and recovery plans with knowledge.
3. **Automation of Time-consuming Operations:** Security teams can concentrate on more intricate and crucial parts of threat mitigation by using AI to automate repetitive and time-consuming operations in incident response. Automated reactions to recognised threats can aid in quickly neutralising and containing attacks

Adaptive Security Measures

1. **Dynamic Threat Intelligence:** AI programmes are able to adjust to changing threats by continuously learning from fresh data. This flexibility guarantees that security measures continue to be effective in the face of new attack channels and strategies.
2. **Continuous Learning and Improvement:** When machine learning models are exposed to additional data, they can get better over time. Because of this ongoing learning, AI systems are able to recognise and stop threats with greater accuracy.

To sum up, incorporating AI, particularly machine learning, into threat detection and prevention offers a proactive and adaptable cybersecurity strategy. It eventually strengthens overall cybersecurity posture by enabling enterprises to detect, respond to, and mitigate security threats more effectively in real time.

Behaviour and Predictive Analysis

Analysing user and system behaviour for anomaly detection requires the use of AI-driven behavioural analytics. Finding patterns or behaviours that depart from the standard is known as anomaly detection, and it serves as a warning of potential security concerns or anomalies. Here's a thorough breakdown of how AI helps with this procedure and all of its benefits, particularly with regard to insider threat detection:

How does AI Enable Analysis of Anomaly Detection?

1. **Data Gathering and Monitoring:** AI systems gather and keep track of enormous volumes of data from a variety of sources, such as network traffic, system logs, and user activity. Information like login times, file access trends, communication patterns, and more may be included in the data.
2. **Pattern Recognition:** To create baseline behaviour patterns for users and systems, AI algorithms make use of machine learning techniques. Based on past data, these models determine typical patterns of behaviour, accounting for variables such as regular access points, working hours, and the frequency of particular behaviours
3. **Real-time Data Analysis:** AI-powered systems are able to analyse data in real time, which makes it possible to identify anomalies as soon as they appear.
4. Promptly identifying security threats and averting possible problems before they worsen require real time analysis.
5. **Behavioural Profiling:** AI uses each user's and system's usual behaviour to build a profile of them. This covers the programmes accessed, how frequently they are used, and the kinds of data they typically interact with. Any departure from pre-existing characteristics may set off alarms that require additional research.
6. **Adaptive Learning:** JIt refers to an AI model's capacity to adjust and pick up new information from data, hence enhancing its capacity to distinguish between typical and unusual behaviour. This flexibility is essential because system and user habits change over time.

Advantages of AI-Driven Behavioural Analytics in Identifying Insider Threats

1. **Early Detection:** Before serious harm is done, AI systems are able to identify minute behavioural changes that may point to an insider danger. In order to stop data breaches and lessen the effects of harmful activity, early detection is essential.
2. **Contextual Analysis:** AI takes into account contextual data, like the user's role, their duties at work, and the sensitive nature of the material they access. By taking into account the context of activities, this helps to reduce false positives.
3. **Constant Monitoring:** AI-powered solutions are able to keep an eye on the system and user behaviour and take a proactive approach to security. This is crucial for spotting insider threats that could appear slowly over time.
4. **Decreased Human Mistakes:** Because AI is capable of processing and analysing large amounts of data fast and precisely, it lowers the possibility of human mistakes that come with manual monitoring and analysis.
5. **Behavioural Biometrics:** AI is able to include behavioural biometrics in the study, such as mouse movements and typing habits. This provides an extra degree of security and aids in the detection of unwanted access even in the event that login credentials are safe.
6. **Scalability:** AI-driven solutions are appropriate for businesses with varied and expansive IT infrastructures because they can scale to manage big datasets and complex situations.

Predictive Analysis

In the context of cybersecurity, predictive analytics refers to the application of artificial intelligence (AI) and machine learning (ML) algorithms for the analysis of past data and trends, the detection of possible cyber threats, and the prediction of forthcoming attacks. An examination of the application of AI in anticipating and averting cyber threats is provided below:

Gathering and Analysing Data

- **Historical Information:** AI systems collect and examine a tonne of historical information about cyber threats. This contains details about prior assaults, susceptibilities, attack routes, and the efficiency of earlier security precautions.
- **Behavioural Patterns:** AI algorithms are able to distinguish between normal activity and anomalies that can point to possible danger by looking for patterns in user behaviour, network traffic, and system operations.

Machine Learning Algorithms

- **Supervised Learning:** AI models that have been trained on labelled datasets are able to identify patterns linked to known cyber threats. As a result, the system is able to recognise similar patterns instantly and anticipate possible dangers.
- **Unsupervised Learning:** Unsupervised learning can be used to identify deviations from typical behaviour without preexisting labels, which is useful in situations where the amount of labelled data is restricted.

Integration of Threat Intelligence

External Data Sources: By integrating threat intelligence feeds with AI systems, real-time data on new threats, vulnerabilities, and attack strategies can be incorporated into the systems' analysis.

Open Source Intelligence (OSINT): To improve their comprehension of possible dangers, AI models can also make use of publicly accessible data.

Predictive Modelling

Statistical Analysis: To find patterns and relationships in past data, predictive analytics uses statistical modelling. After that, these models can be used to predict possible cyber threats in the future.

Time Series Analysis: AI systems can spot trends and foresee possible risks at particular times or occurrences by looking at patterns throughout time.

Analytics of User and Entity Behaviour (UEBA)

- **User Behaviour Monitoring:** Artificial intelligence (AI) can monitor user behaviour to spot anomalous activity or departures from the norm, which can be used to find compromised accounts or insider threats.
- **Entity Behaviour Analysis:** AI can monitor the behaviour of devices and other entities on a network to spot unusual activity, much like it can with user behaviour analysis.

Automating and Observing in Real-Time

1. **Quick Reaction:** Artificial intelligence (AI) systems have the ability to react instantly to possible threats by setting off pre-planned security procedures or notifying security personnel.
2. **Continuous Monitoring:** Utilising predictive analytics in this setting enables the detection of changing threats and the modification of security protocols as necessary.
3. **Adaptive Security Measures:** Dynamic Threat Defence: AI-powered systems are capable of dynamically modifying security measures in response to the changing threat environment, resulting in a more resilient and adaptable defence.

Obstacles & Things to Think About

- **False Positives:** One issue is the possibility of genuine activity being wrongly classified as a threat, or false

positives. It is crucial to continuously improve validation procedures and algorithms.

- **Data Privacy:** It's critical to protect data privacy and use it ethically. AI models need to be developed with pertinent data while adhering to moral and legal guidelines.

Automation in Cybersecurity

Artificial Intelligence is a key component in automating regular security chores, which transforms how businesses handle and address security threats. The following are some salient features that demonstrate how AI speeds up response times and makes it easier to automate regular security tasks:

1. **Fast Pattern and Anomaly Recognition:** Artificial intelligence (AI) algorithms are highly skilled in sifting through big datasets to find patterns or anomalies. This means that, when it comes to security, AI can swiftly identify anomalous behaviour or possible security risks by contrasting present activity with predetermined baselines.
2. **Automated Threat Detection and Prevention:** In order to identify any security risks, AI-powered systems are able to continuously monitor network traffic, system logs, and other data sources. Organisations can reduce the window of exposure by identifying and resolving issues in real time using automated threat detection.
3. **Quicker Reaction to Incidents:** The manual threat detection and response processes used in traditional systems can take a long period. AI quickly analyses and classifies security alerts, automating the first steps of incident response. This improves overall reaction times by allowing security professionals to concentrate their attention on more difficult and important jobs.
4. **Adapting Dynamically to Changing Threats:** AI systems can learn from past events and adjust to new and developing threats. For instance, machine learning algorithms can be trained to consistently increase the accuracy with which they detect and mitigate security vulnerabilities over time, guaranteeing a proactive response to new threats.
5. **Diminution of Negative Results:** Artificial intelligence (AI) systems can more precisely discern between regular and suspicious activity, which can dramatically lower the amount of false positive alarms. As a result, security teams can prevent alert fatigue and make better use of their resources by prioritising notifications that need to be addressed right away.
6. **Constant Observation and Evaluation:** AI systems are not tired like human operators are; they can work continuously. This guarantees ongoing security event monitoring and incident response capability, enhancing an organisation's overall security posture.
7. **Handling and Scalability Huge Data Volumes:** AI-driven automation is very good at managing enormous data volumes of security warnings that come from a variety of sources. AI systems can process and analyse data more efficiently as data volume grows, allowing enterprises to manage security in dynamic and complex contexts.
8. **Cost-Efficiency:** By using AI to automate repetitive security procedures, human analysts may concentrate on high-value, strategic jobs and handle a lighter workload. By allocating resources as efficiently as possible, this increases productivity and lowers costs.

Challenges and Limitations

Ethical Considerations

1. **Privacy Issues:** Since AI systems frequently process vast volumes of data, privacy issues are brought up. Ensuring that sensitive and personal data is managed appropriately and in accordance with privacy laws is crucial.
2. **Transparency:** Some AI algorithms' opacity might result in a lack of transparency, making it difficult to comprehend the decision-making process. Transparency is essential to cybersecurity because it fosters trust and responsibility, particularly when addressing possible risks.
3. **Accountability:** It can be difficult to assign blame when mistakes or security breaches occur. To ensure accountability, roles and duties for users, operators, and creators of AI systems must be clearly defined.
4. **Fairness and Bias:** Discriminatory results may arise from biases in training data. To prevent repeating preexisting biases, it's critical to make sure AI models are trained on a variety of representative datasets. To detect and reduce bias, AI systems should undergo routine audits.
5. **Security of AI Systems:** AI systems need to be shielded from hostile intrusions. Maintaining the integrity of cybersecurity systems requires guaranteeing the security of AI models and guarding against their manipulation or compromise.
6. **Challenges in AI-Based Cybersecurity:** The characteristics of cyber threats are ever-changing and dynamic. Artificial intelligence systems need to be able to adjust to novel and complex threats. AI models must be updated and monitored constantly to remain successful against new threats.
7. **Flexibility and Education:** AI models must possess the capacity to learn from fresh data and adjust to shifting threat conditions. To handle new threats, this calls for a strong feedback loop and the capacity to update models instantly.
8. **Human-Mechanical Coordination:** Although AI can

automate a lot of cybersecurity procedures, human expertise is still very important. To fully utilise the assets of both AI systems and human analysts and make educated conclusions, effective collaboration is required.

9. **Resource Restrictions:** Advanced AI system implementation and upkeep might demand a lot of resources. For AI models to be effective over time, organisations must set aside enough funding for their training, maintenance, and security.
10. **Regulatory Compliance:** It is imperative to follow all applicable laws and regulations. AI-based cyber security systems need to abide by applicable laws and regulations, which can change depending on the jurisdiction. It's difficult to stay on top of these obligations all the time.

Ethical issues and difficulties with AI-based cybersecurity systems emphasise the necessity of responsible creation, implementation, and continuous supervision. A multidisciplinary strategy including technological specialists, ethicists, and policymakers is necessary to address the increasing nature of cyber risks while striking a balance between innovation and ethical considerations.

Case Studies

Undoubtedly, the use of AI in cybersecurity has grown in popularity because of its capacity to examine enormous volumes of data and find anomalies that conventional security methods could miss. Here are some major shortcomings or failures, along with real-world examples of businesses using AI for cybersecurity.

Success Stories

1. Darktrace is an AI-based cybersecurity company that uses machine learning algorithms to detect and respond to cyber threats in real time. Its technology is designed to learn and adapt to the evolving nature of cyber threats. Darktrace's AI has been successful in identifying and mitigating previously unknown threats across various industries.
2. Cylance is known for using machine learning and artificial intelligence to predict, detect, and prevent cybersecurity breaches. The company's endpoint protection solutions leverage AI to analyse patterns and identify potential threats before they can cause harm.
3. IBM Watson for Cybersecurity is an AI-powered system that helps security analysts make more informed decisions. It uses machine learning to analyse structured and unstructured data from various sources to identify potential threats. It has been effective in enhancing the capabilities of security teams to respond to incidents promptly.

Failure Stories

1. In 2016, Microsoft launched an AI-powered chatbot named Tay on Twitter. Tay was designed to learn from conversations and improve its responses. However, it quickly turned into a disaster as it started producing offensive and inappropriate tweets due to malicious users manipulating its learning algorithms. This incident highlights the limitations of AI in handling unfiltered and malicious input.
2. While not directly related to cybersecurity, Tesla's Autopilot system faced scrutiny when researchers demonstrated vulnerabilities in its software. This incident showcases the potential risks of relying too heavily on AI systems, even in non-cybersecurity contexts.

AI systems in cybersecurity are not perfect and may generate false positives (flagging harmless activities as threats) or false negatives (missing actual threats). Balancing the sensitivity and specificity of AI algorithms to reduce false alerts while ensuring no threats are overlooked remains a challenge.

AI models are only as good as the data they are trained on. If the training data is biased or incomplete, the AI system may not effectively identify new and evolving threats. Additionally, attackers can attempt to manipulate AI models by exploiting biases in the training data.

Future Scope and Trends

1. **Cryptography and Quantum Computing:** A Challenge Quantum computing presents a challenge to established cryptographic techniques even while it has the potential to transform many other industries, including cryptography.
2. **Integration of AI:** AI is anticipated to contribute to the creation of cryptography algorithms and tactics that are resistant to quantum attacks.
3. **Artificial Intelligence in Threat Hunting:** Enhanced Detection: Machine learning and AI are being utilised more and more to enhance threat hunting skills. Large data sets can be analysed by these technologies, which can also spot trends and anomalies that might point to possible security risks.
4. **Behavioural Analytics:** AI assists in recognising anomalies that may indicate a security breach and in comprehending typical user activity patterns.

Security using Explainable AI (XAI)

Transparency: Explainability and transparency are becoming increasingly important as AI models get more complicated, particularly in crucial domains like cybersecurity. The goal

of explainable AI is to shed light on the decision-making process of AI systems, hence facilitating security experts' comprehension and confidence in the technology.

Conclusion

In a world where cyber threats and malicious intelligence are growing at an exponential rate, it is imperative to prioritise advanced cybersecurity strategies. Additionally, DDoS avoidance experience has shown that security against large-scale assaults may be achieved with relatively few resources if clever strategies are applied. Reviews of published publications show that research on artificial neural networks provides the most generally applicable AI insights for cybersecurity. Cybersecurity implementations of neural networks are still ongoing. In numerous domains where neural networks aren't the most suitable technologies, advanced cybersecurity techniques remain imperative. These domains encompass information control, scenario comprehension, and decision support. Expert machine development is the most intriguing aspect of this scenario.

It is impossible to say how quickly general artificial intelligence has progressed, but it is still possible that those who commit these crimes will make use of any new forms of AI that are available. This is not readily apparent. Furthermore, the most recent technological advancements in information management, interpretation, and understanding - particularly in the field of computer learning - would greatly enhance systems' cybersecurity capabilities.

References

1. Morris RT. The Morris worm: a fifteen-year perspective. Proceedings of the 15th USENIX Security Symposium; 1988.
2. Messmer E. Melissa worm turning 10: what did we learn? Network World; 1999.
3. Krebs B. The value of a hacked email account. Krebs on Security. 2013.
4. The White House. International Strategy for Cyberspace. 2011.
5. U.S. Cybersecurity and Infrastructure Security Agency (CISA). Solar Winds and Supply Chain Security. 2021.
6. Axelsson S. The base-rate fallacy and the difficulty of intrusion detection. ACM Trans Inform Syst Secur. 2000 Aug 1;3(3):186-205.
7. Christodorescu M, Jha S, Kruegel C, Robertson W. Mining specifications of malicious behavior. Proceedings of the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering; 2007 Sep 7. p. 5-14.
8. CERT Division. Common sense guide to mitigating insider threats. 5th ed. Carnegie Mellon University; 2016.
9. Gragido W, Pirc J. Blackhatonomics: an inside look at the economics of cybercrime. Syngress; 2011.
10. Cimpanu C. Ransomware: an executive guide to one of the biggest menaces on the web. ZDNet; 2019.
11. Shabtai A, et al. Detection of malicious code in android applications. 2011 IEEE 35th Annual Computer Software and Applications Conference.
12. US Cybersecurity and Infrastructure Security Agency (CISA). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. 2020.
13. Ray PP. A survey of internet of things architectures, protocols, and security. internet of things: challenges, advances, and applications. J King Saud Univ Comput Inf Sci. 2018 Jul 1;30(3):291-319.
14. Anderson R, Moore T. The economics of information security. Science. 2006 Oct 27;314(5799):610-3.
15. Symantec. Internet Security Threat Report. Symantec Corporation; 2018.
16. National Institute of Standards and Technology (NIST). NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations. 2018.
17. Rass S, Dssouli R. Artificial intelligence in network security: a review. Artif Intell Rev. 2019.
18. Miller S, et al. A survey of artificial intelligence for cybersecurity. J Cybersecur Mobil. 2018.
19. Chen M, Zhu Y. Artificial intelligence-based cybersecurity defense: a review. IEEE Access. 2019.
20. Jagadeesan V, Sivasankari M, Sivakumari M. A review on ai based solutions for network security. Procedia Comput Sci. 2016.
21. Haider S, Khan RA, Khan SU. A survey of artificial intelligence for cybersecurity. J King Saud Univ Comput Inf Sci. 2019.
22. Kumar P, Zhang J, Li T. A survey of network vulnerability assessment. IEEE Commun Surv Tutor. 2020.
23. Husain I. Artificial intelligence-driven multi-factor authentication and its application in securing digital resources. International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), 2020.
24. Damjanovic D, Shishika A, Nastasijevic A. Artificial intelligence-driven biometric authentication for mobile applications. IEEE EUROCON, 2017.
25. Pradhan AK, et al. Behavioral authentication system using deep learning. Third International Conference on Information and Communication Technology for Intelligent Systems, 2019.