

Project: Summarising and Analysing Research Papers

Learner Name: Trivendra Sharma

Learner Email: trivendra846@gmail.com

Topic: Engineering: Artificial Intelligence in Cyber Security

Research Paper:

https://r.search.yahoo.com/_ylt=AwrX_NccRdxmpwQA2dq7HAX.;_ylu=Y29sbwNzZzMEcG9zAzIEdnRpZAMEc2VjA3Ny/RV=2/RE=1726921245/RO=10/RU=https%3a%2f%2fwww.researchgate.net%2fpublication%2f353419449_Artificial_Intelligence_in_Cyber_Security/RK=2/RS=TXrRp3pl21EF08.jV05ejmBLx38-

Initial Prompt

Description : Summarise the key findings of this research paper

Generated Summary: Artificial Intelligence in Cyber Security. Rammanohar Das and Raghav Sandhane 2021 J. Phys.: Conf. Ser. 1964 042072. View the article online for updates and enhancements. This paper provides a concise overview of AI implementations of various cybersecurity using artificial technologies. We may infer that valuable applications already exist after the review of current artificial intelligence software. Virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield. In January 2010, the Information Network of the Greater Manchester Police triggered apre-emptive disconnection of the Police Central Database for three days. Cyber incidents are particularlyhazardous with Network Centric Warfare (NCW) Cyber defence alterations are urgently needed. Use of artificial intelligence techniques and knowledge-intensive tools would be vital in newoffensive methods. This paper presents the areas of technology and science with artificial intelligence. In the third chapter, we will delve into the established cyber protection AI implementations. The fourth segment explores the possibilities and introduces new smart devices. Researchers used four databases: Scopus, Web of Science, ACM digital library also IEEE Xplore. A set of keywords matching the topics were searched for in these databases. The search results which we got were limited to the papers published in the last four years. This study brings together the effect of multiple areas, AI usage in the Security domain, methods implemented, and methods that were put forth. It is used to develop an overall architecture for future research in this specific domain. It was "on the horizon" that devices/software/structures could be built cleverer than humans. The issue is that as time progresses, the time frame is going further. We saw a variety of machines, for example, playing really good chess. In the 1960s, N. Chomski 's research in computational linguistics, has been anticipated to address the issue of Natural Language Processing early. It hasn't yet occurred, even though certain unique programs such as Google's AI linguistics indicated initial success. In this article, we apply the right line, propose the application of particular AI methods in cyber defense issues and respond to the cyber defense issue. Industries and private sector companies have already adopted AI programs. Many government departments utilize the tool. AI checks for behavioral anomalies that hackers are expected to display. Artificial intelligence is human-controlled and may still, therefore,

be vanquished. As hackers adjust to the Artificial Intelligence systems, new defensive measures will have to be adopted. The game of cat and mouse will proceed, but AI is a positive strengthening in the fight to secure data. NSL works with the machine learning stage Tensor Flow and is designed to work for qualified besides incompetent machine learning professionals. NSL can work with monitored, semi-supervised, or unsupervised representations. AI is what brought us speech recognition apps (assume Siri), a search app from Google, and facial recognition tools from Facebook. Many manufacturers of payment cards often use AI to aid in stopping trillions of dollars in recorded fraud. But what about the application of AI to Information Security? Artificial intelligence is rapidly a field of emphasis inside the computer safety community. We will analyze advancements in security tools for AI and how the technology impacts institutions, cybercriminal. Cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyberprotection either. You need to be able to detect, identify and respond instantly to the threats 24/7/365. Artificial Intelligence may respond to cyber threats, which would require many minutes, hours, days, months, or even years to recognize by human beings. Capgemini Research Institute examined the position of information protection besides their study "Reinventing Cyber Protection with AI" 75 percent of survey respondents say that AI enables their organization to respond to infringements more quickly. Three in five firms say that using AI makes cyber analysts more accurate and more efficient. Allerin CEO and founder Naveen Joshi shares in an article for Forbes that there are numerous ways AI systems can ensure the sustainability of cybersecurity operations. Some of those features include: Developing precise, biometric password-based log-in technique. AI frameworks-based information protection technologies — besides those aren't cheap. Be vigilant not to fail to invest with the organization's human aspect. New SaaS (Security-as-a-service) technologies available that make AI cyber defence technologies more cost-efficient for business. It is partially because access to the advanced AI technologies besides machine learning strategies is cruising as costs of producing and applying these developments decline. The danger to information security, including artificial intelligence, falls in the context of adversarial AI. Accenture defines adversarial AI as something that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder" IBM's Dublin labs are additionally dynamic in the project and have made the IBM Adversarial Robustness Toolbox (ART) ill-disposed AI index. Several methods are so prominent that they are no longer considered as a part of artificial intelligence. We do not cover machine vision, robotics, and comprehension of natural languages that we find in particular AI applications. Neural networks are a type of computer network. They can be used to make decisions about how to solve problems. They are also used to identify threats to the network. The fast mobility, whether implemented in hardware or used in graphical chipsets, causes the prominence of deep learning in computer security. The use of FPGAs (field gate arrays) is a great way to rapidly build and adapt neural networks. A current plastic understanding must be filled before it is used. The artificial

intelligence shell must be endorsed by knowledge base software and can be lengthened by interactive query programs. In general, a device contains an artificial intelligence shell and has usability to add Understanding to the repository of information. For security preparation, the instance of a cyber security device specialist is one. Initial stuff on the deployment of professional detection techniques is underway. Intelligent agents are software applications. They may have the capacity to prepare, organize and evaluate. Simulators were used to protect cooperation agents from the attacks of DDoS. Search is embedded in the application stack and is not seen as an AI function. Dynamic analysis programming is used primarily to address optimal security concerns. Check on besides- or trees is commonly used in the applications of gamers. Learning strengthens the information structure through the extension, reorganization, or enhancement of the knowledge base. Learning challenges range widely from basic parametric learning to complex types of abstract teaching. Multiple AI approaches can be used on cybersecurity quickly. Uncontrolled learning may be a function of self-organized neural networks. Genetic analytics, in addition to fuzzy logic, was used in mentioned threat detection methods. New concepts of information processing in the management of circumstances and decision-making in the future would be exciting. Some people are tempted that the AI's main goal – artificial cognition – can be accomplished in the mid-20th century. In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cybersecurity. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that perpetrators will exploit a new form of artificial intelligence as long as it is accessible. The latest technology in the understanding, interpretation, and management of information would significantly improve systems' cybersecurity capabilities. A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. Summarize the key findings of the paper. the detection of DOS attacks. Innovations in Hybrid Intelligent Systems {--} Proceeding. Summarize the key findings of the paper. dia - Social and Behavioral Sciences, 46, 5646–5655. A real-time intrusion detection system based on learning program behavior. Summarize the key findings of the paper. s of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07) Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013). A model-based software technology proposal. MODELSWARD 2013 - Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development. Pati, N., & Anand, P. (2017) Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322. HAL Id : hal-01534315 HTTP Botnet Detection.using Adaptive Learning Rate Multilayer Feed-forward Neural Network. Aarthi, J. Design Of Advanced Encryption Standard (AES) Based Rijndael Algorithm. Expert Systems with Applications, 36(3 PART 1), 4321–4330.

Iteration 2

Description: Provide a concise summary of the methodology used in this research.

Generated Summary:

Artificial Intelligence in Cyber Security. Rammanohar Das and Raghav Sandhane 2021 J. Phys.: Conf. Ser. 1964 042072View the article online for updates and enhancements. This paper provides a concise overview of AI implementations of various cybersecurity using artificial technologies. We may infer that valuable applications already exist after the review of current artificial intelligence software. Virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield. In January 2010, the Information Network of the Greater Manchester Police triggered a pre-emptive disconnection of the Police Central Database for three days. Cyber incidents are particularly hazardous with Network Centric Warfare (NCW), and cyber defence alterations are urgently needed. Use of artificial intelligence techniques and knowledge-intensive tools would be vital in new offensive methods. This paper presents the areas of technology and science with artificial intelligence. In the third chapter, we will delve into the established cyber protection AI implementations. The fourth segment explores the possibilities and introduces the new smart devices. Researchers used four databases: Scopus, Web of Science, ACM digital library also IEEE Xplore. A set of keywords matching the topics were searched for in these databases. The search results which we got were limited only to the papers published in the last four years. This study brings together the effect of multiple areas, AI usage in the Security domain, methods implemented, and methods that were put forth. It is used to develop an overall architecture for future research in this specific domain. It was "on the horizon" that devices/software/structures could be built cleverer than humans. As time progresses, the time frame is going further. We saw a variety of machines, for example, playing really good chess, overcome sensibly complex problems. AI can be regarded, in general, as an aspect of intellect, and broadly the creation of intelligent devices. In the 1960s, N. Chomsky's research in computational linguistics, has been anticipated to address the issue of Natural Language Processing early. Industries and private sector companies have already adopted AI programs. Many government departments utilize the tool. AI could save both tax dollars as well as national secrets. Artificial intelligence is human-controlled and may still, therefore, be vanquished. Google introduced a graphical data learning model for TensorFlow machine learning. The game of cat and mouse will proceed, but AI is a positive strengthening in the fight to secure data. NSL works with the machine learning stage Tensor Flow. NSL may render machine vision models, execute NLP, and run projections from interactive databases such as medical reports or graphs. AI is what brought us speech recognition apps (assume Siri), a search app from Google, and facial recognition tools from Facebook. Many manufacturers of payment cards often use AI to aid in stopping trillions of dollars in recorded fraud. But what about the application of AI to Information Security? Artificial intelligence is rapidly a field of emphasis inside the computer safety community. We will analyze advancements in security tools for AI and how the technology impacts institutions,

cybercriminal. Cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyberprotection either. You need to be able to detect, identify and respond instantly to the threats 24/7/365. Artificial Intelligence may respond to cyber threats, which would require many minutes, hours, days, months, or even years to recognize by human beings. Capgemini Research Institute examined the position of information protection besides their study "Reinventing Cyber Protection with AI" 75 percent of the survey respondents say that AI enables their organization to respond to infringements more quickly. Sixty-nine percent of organizations agree that AI is required. Three in five firms say that using AI makes cyber analysts more accurate and more efficient. It's not anything that can be achieved immediately that incorporates artificial intelligence technologies with the current information defence networks. Allierin CEO and founder Naveen Joshi shares in an article for Forbes that there are numerous ways AI systems can ensure the sustainability of cybersecurity operations. There are many advantages of using artificial intelligence in knowledge security. But there are risks to keep in mind too. One of the big difficulties is that it appears to take more time and funds than traditional non-AI computer protection solutions. The application of AI in information defence is generating new challenges to physical protection. Access to the advanced AI technologies is cruising as costs of producing and applying these developments decline. This ensures that computer attackers can build increasingly sophisticated and efficient malicious apps. The danger to information security, including artificial intelligence, falls in the context of adversarial AI. Accenture defines adversarial AI as something that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder" IBM's Dublin labs are additionally dynamic in the project and have made the IBM Adversarial Robustness Toolbox (ART) ill-disposed AI index. We have divided approaches and architectures into multiple categories. These categories include artificial neural, expert systems, smart agents, quest, computer education, data gathering, and constraint resolution. We do not cover machine vision, robotics, and comprehension of natural languages. Neural networks have a parallel distributed learning and decision-making capability. These are ideal for identification of learning patterns, grouping, a compilation of threat responses. They may be applied in applications or electronics. Cognitive nets are rocketing machine learning that more effectively imitate artificial neurons and offer greater possibilities for application. The use of FPGAs (field gate arrays) is a great way to build and adapt neural networks to changes in risks. A current plastic understanding must be filled before it is used. The artificial intelligence shell must be endorsed by knowledge base software and can be lengthened by interactive query programs. In general, a device contains an artificial intelligence shell and has usability to add Understanding to the repository of information. For security preparation, the instance of a cyber security device specialist is one. Intelligent agents are software applications. They may have the capacity to prepare, organize and evaluate. When all regulatory and contractual problems have been addressed, a 'cyber police force' composed of mobile smart officers would, in practice, be feasible. A broad variety of search techniques is

created that takes detailed focus on specific search problems into consideration. The search is embedded in the application stack and is not seen as an AI function. 5.5 Learning strengthens the information structure through the extension, reorganization, or enhancement of the knowledge base. It is one of the most important artificial intelligence topics being studied intensively. Multiple AI approaches can be used on cybersecurity quickly, and urgent cybersecurity challenges need smarter solutions than they are actually applied. For instance, genetic analytics, in addition to fuzzy logic, was used in mentioned threat detection methods. New concepts of information processing in the management of circumstances and decision-making in the future would be exciting. Some people are tempted that the AI's main goal – artificial cognition – can be accomplished in the mid-20th century. In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Publications reviews indicate that studies into artificial neural networks offer the findings of AI most widely relevant to cybersecurity. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that perpetrators will exploit a new form of artificial intelligence as long as it is accessible. The latest technology in the understanding, interpretation, and management of information would significantly improve systems' cybersecurity capabilities. Provide a concise summary of the methodology used in this research. the detection of DOS attacks. SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. Provide a concise summary of the methodology used in this research. dia - Social and Behavioral Sciences, 46, 5646–5655. provide a concise summary of the methodology used in this research. s of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07). 44/2008(June 2014). 20(2), 224–234. Provide a concise summary of the methodology used in this research. e/. Provide a brief description of the goals of the research. Provide a short description of how the research was carried out. The Conficker computer worm was first discovered in 2009. The Conficker worm is one of the most destructive computer viruses. The worm is thought to have been created by the Chinese government. It is believed to be the most powerful worm in the world. Provide a concise summary of the methodology used in this research. Sadiku, M. N. O., Fagbohunge, O. I., & Musa, S. M. (2020). Artificial Intelligence in CyberSecurity. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. Aarthi, J. Design Of Advanced Encryption Standard (AES) Based Rijindael Algorithm. The method of rule-based techniques and neural networks. Expert Systems with Applications, 36(3 PART 1), 4321–4330.

Final Prompt

Description: Summaries and Analyze Insights from the research paper

Generated Summary :

Summary of the Research Paper

Rammanohar Das and Raghav Sandhane 2021 J. Phys.: Conf. Ser. 1964 042072. Summaries and Analyze Insights from the research paper. This paper provides a

concise overview of AI implementations of various cybersecurity using artificial technologies. It evaluates the prospects for expanding the cybersecurity capabilities by enhancing the defence vehicle. Virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield. In January 2010, the Information Network of the Greater Manchester Police triggered apre-emptive disconnection of the Police Central Database for three days. Cyber incidents are particularlyhazardous with Network Centric Warfare (NCW), and cyber defence alterations are urgently needed. Use of artificial intelligence techniques and knowledge-intensive tools would be vital in newoffensive methods. This is a forum for automated technologies of intelligence [4]. The latter part of this paper presents the areas of technology and science with artificial intelligence. In the third chapter, we will delve into the established cyber protection AI implementations. The fourth segment explores the possibilities and introduces new smart devices. Researchers used four databases:Scopus, Web of Science, ACM digital library also IEEE Xplore. A set of keywords matching the topics were searched for in these databases. The search results which we got were limited only to the papers published in the last four years. This study brings together the effect of multiple areas, AI usage in the Security domain, methods implemented, and methods that were put forth. It is used to develop an overall architecture for future research in this specific domain. It was "on the horizon" that devices/software/structures could be built cleverer than humans. The issue is that as time progresses, the time frame is going further. We saw a variety of machines, for example, playing really good chess. AI can be regarded, in general, as an aspect of intellect, and broadly thecreation of intelligent devices. In this article, we apply the right line, propose the application of particular AI methods in cyber defense issues and respond to the responses. Industries and private sector companies have already adopted AI programs. Many government departments utilize the tool. AI could save both tax dollars aswell as national secrets. Artificial intelligence is human-controlled and may still, therefore, be vanquished. Google introduced a graphical data learning model for TensorFlow machine learning. The game of cat and mouse will proceed, but AI is a positivestrengthening in the fight to secure data. NSL works with the machine learning stage Tensor Flow. NSL may render machine visionmodels, execute NLP, and run projections from interactive databases such as medical reports. Google Cloud launched other organized data approaches, such as linked sheets in Big Query. In several other AI news, Google AI, formally known as Google Research, open-sourced SM3, a compiler for large-scale speech recognition models. Artificial intelligence is rapidly a field of emphasis inside the computer safety community. We will analyze advancements in security tools for AI and how the technology impacts institutions, cybercriminal. Cybercrime isn't necessarily pursuing a fixed timetable and shouldn't suit your susceptibility to cyber protections either. You need to be able to detect, identify and respond instantly to the threats 24/7/365. Artificial Intelligence may respond to cyber threats, which would require many minutes, hours, days,months, or even years to recognize by human beings. Capgemini Research Institute examined the position of information protection besides their study "Reinventing Cyber Protection with AI" 75

percent of respondents say that AI enables their organization to respond to infringements more quickly. Sixty-nine percent of organizations agree that AI is required. Three in five firms say that using AI makes cyber analysts more accurate and more efficient. It's not anything that can be achieved immediately that incorporates artificial intelligence technologies successfully with the current information defence networks. Allierin CEO and founder Naveen Joshi shares in an article for Forbes that there are numerous ways AI systems can ensure the sustainability of cybersecurity operations. AI frameworks-based information protection technologies — besides those aren't cheap. Be vigilant not to fail to invest with the organization's human aspect. Lots of big position players now use AI. The application of AI in information defence is generating new challenges to physical protection. It is partially because access to the advanced AI technologies is declining. This ensures that computer attackers can build increasingly sophisticated apps. The danger to information security, including artificial intelligence, falls in the context of adversarial AI, a word used for sinister purposes to apply to the growth also utilization of AI. Accenture defines adversarial AI as something that "causes machine learning algorithms to misunderstand inputs" IBM's Dublin labs are additionally dynamic in the project and have made the IBM Adversarial Robustness Toolbox (ART) ill-disposed AI index. We have divided approaches and architectures into multiple categories. These categories include artificial neural, expert systems, smart agents, quest, computer education, data gathering, and constraint resolution. We do not cover machine vision, robotics, and comprehension of natural languages. Neural networks are a type of computer network. They can be used to make decisions and identify threats. They are also used to detect malware and viruses. The fast mobility, whether implemented in hardware or used in graphical chipsets, causes the prominence of deep learning in computer security. The use of FPGAs (field gate arrays) is a great way to build and adapt neural networks to changes in risks. A current plastic understanding must be filled before it is used. The artificial intelligence shell must be endorsed by knowledge base software and can be lengthened by interactive query programs. A device contains an artificial intelligence shell and has usability to add Understanding to the repository of information. For security preparation, the instance of a cyber security device specialist is one. Initial stuff on the deployment of professional detection techniques is underway. Intelligent agents are software applications. They may have the capacity to prepare, organize and evaluate. When all regulatory and contractual problems have been addressed, a 'cyber police force' composed of mobile smart officers would be feasible. A broad variety of search techniques is created that takes detailed focus on specific search problems into consideration. The search is embedded in the application stack and is not seen as an AI function. 5.5 Learning strengthens the information structure through the extension, reorganization, or enhancement of the knowledge base. Learning challenges range widely from basic parametric learning, to complex types of abstract teaching. Uncontrolled learning may be a function of self-organized neural networks. For instance, genetic analytics, in addition to fuzzy logic, was used in mentioned threat detection methods. Multiple AI approaches can be used quickly to

solve cybersecurity challenges. New concepts of information processing in the management of circumstances and decision-making in the future would be exciting. Some people are tempted that the AI's main goal – artificial cognition – can be accomplished in the mid-20th century. In a scenario where malicious intelligence and cyber threats are rising exponentially, sophisticated cybersecurity strategies cannot be ignored. Security against large-scale threats, with very minimal resources, has been demonstrated from experience in DDoS prevention. Too fast general artificial intelligence has advanced cannot be known, but a possibility remains that perpetrators will exploit a new form of artificial intelligence. The latest technology in the understanding, interpretation, and management of information, particularly in the area of computer learning, would significantly improve systems' cyber security capabilities. Research paper. the detection of DOS attacks. SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks, 229–234. A Distributed Intrusion Detection Prototype using Security Agents. Summaries and Analyze Insights from the research paper. dia - Social and Behavioral Sciences, 46, 5646–5655. A real-time intrusion detection system based on learning program behavior. Summaries and Analyze Insights from the 2nd International Workshop on Hybrid Artificial Intelligence Systems. Kotenko, I., & Ulanov, A. (2007) Multi-agent framework for simulation of adaptive cooperative defense against internet attacks. Kotkas, V., Penjam, J., Kalja, A., & Tyugu, E. (2013) A model-based software technology proposal. Pati, N., & Anand, P. (2017) Machine Learning in Cyber Defence. International Journal of Computer Sciences and Engineering, 5(12), 317–322. HAL Id : hal-01534315 HTTP Botnet Detection using Adaptive Learning Rate Multilayer Feed-forward Neural Network. Summaries and Analyze Insights from the research paper. Aarthi, J. Design Of Advanced Encryption Standard (AES) Based Rijindael Algorithm. Expert Systems with Applications, 36(3 PART 1), 4321–4330