Fundamentals of artificial intelligence

Group Assignment 1

Title- Applications of AI in data security

Group members ID

1.Hamza Shehabu ………………………………..ru0098/12

2.Hawi Guta………………………………………..ru5092/12

3.Kaleab Erdachew………………………………..

4.Kibru Abebe

Contents

[Introduction 3](#_Toc120712908)

[Advantages of AI in data security 4](#_Toc120712909)

[Disadvantages of AI in cyber security 6](#_Toc120712910)

[How Artificial intelligence works in data security. 7](#_Toc120712911)

[AI-Powered Data Security Solutions 7](#_Toc120712912)

[Main Challenges of AI 8](#_Toc120712913)

[Trending technologies of AI in security 9](#_Toc120712914)

[Conclusion 12](#_Toc120712915)

# Introduction

Information security, taking into account the increasingly widely implemented and used computer systems, occupies an important place in the monumdern world. Everyone, whether an individual or a company, wants to reduce the threat of theft, deletion, or alteration of their information. Including in the automated system, cyber security plays an important role.

According to an IDC study, "organizations will spend $ 101.6 billion by 2020 on cyber security software, services and hardware." Leading organizations integrate dozens of security products, but nevertheless fear being vulnerable to attacks. This indicates that even after increasing security spending, security breaches show no signs of stopping or slowing down. The introduction of advanced technologies in the field of cyber security takes time, which allows attacks to be detected in detail and resolved faster than cyber security specialists, such technology can be artificial intelligence. AI is a technology that, among other things, can detect threats and automatically take the necessary actions to eliminate and prevent them.

As a result of the information revolution, a fundamentally new type of society is being created, with its own laws and principles of functioning, as well as risks and threats. This type of society, called the "information society", is characterized by a violation of linearity, continuity, stability and predictability of social development, which fundamentally distinguishes it from all previous types of society that existed in the history of our civilization. This society, created by the domination of information and its total influence on the consciousness and behavior of individuals, has the highest potential for scientific and technological development, but, at the same time, contains an equally high potential of threat to the security of society

In this document we will try to show you some of the essential applications of Artificial intelligence in data security and how they work under the influence of today’s computer threats .and also we try to show some basic needs of AI in the data security system like authentication systems, threat identification systems and we also try to cover the advantage and disadvantages of using AI in cyber security.

# Advantages of AI in data security

1. AI learns more over time-As the name suggests, [AI technology](https://www.engati.com/blog/explainable-ai) is intelligent, and it uses its ability to improve network security over time. It uses machine learning and deep learning to learn a business network’s behavior over time. It recognizes patterns on the network and clusters them. It then proceeds to detect any deviations or security incidents from the norm before responding to them. The patterns that artificial neural networks learn over time can help to improve security in the future. Potential threats with similar traits to those recorded get blocked early enough. The fact that AI keeps learning makes it difficult for hackers to beat its intelligence.
2. AI identifies unknown Threats- A human being may not be able to identify all the threats a company faces. Every year, hackers launch hundreds of millions of attacks with different motives. Unknown threats can cause massive damage to a network. Worse still is the impact they can have before you detect, identify, and prevent them. As attackers try new tactics from sophisticated [social engineering](https://www.engati.com/blog/social-engineering) to malware attacks, it is necessary to use modern solutions to prevent them. AI has proven to be one of the best technologies in mapping and stopping unknown threats from ravaging a company.
3. AI can handle a lot of data- A lot of activity happens on a company’s network. An average mid-sized company itself has huge traffic. That means there’s a lot of data transferred between customers and the business daily. This data needs protection from malicious people and software. But then, cyber security personnel cannot check all the traffic for possible threats. AI is the best solution that will help you detect any threats masked as normal activity. Its automated nature allows it to skim through massive chunks of data and traffic. Technology that uses AI, such as residential proxy, can help you to transfer data. It can also detect and identify any threats hidden in the sea of chaotic traffic.
4. Better vulnerability management- Vulnerability management is key to securing a company’s network. As mentioned earlier, an average company deals with many threats daily. It needs to detect, identify and prevent them to be safe. Analyzing and assessing the existing security measures through AI research can help in vulnerability management. With the use of tool Analyzing threat becomes much easier for the companies.

AI helps you assess systems quicker than cyber security personnel, thereby increasing your problem solving ability manifold. It identifies weak points in computer systems and business networks and helps businesses focus on important security tasks. That makes it possible to manage vulnerability and secure business systems in time.

1. Fast detection and response time- Threat detection is the beginning of protecting your company’s network. It would be best if you detected things like untrusted data quickly. It will save you from the irreversible damage to your network. The best way to detect and respond to threats in time is by integrating AI with cyber security. AI scans your entire system and checks for any possible threats. Unlike humans, AI will identify threats extremely early and simplify your security tasks.
2. Securing Authentication- Most websites have a user account feature where one logs in to access services or buy products. Some have contact forms that visitors need to fill with sensitive information. As a company, you need an extra security layer to run such a site because it involves personal data and sensitive information. The additional security layer will ensure that your visitors are safe while browsing your network.

# Disadvantages of AI in cyber security

1. HACKERS USE AI AS WELL- When it comes to maturity in technology, hackers are the best at it. These individuals sitting behind computer screens logging data and doing advanced analytics to identify any loophole or vulnerability they can use to their benefits. The use of AI as far as cybersecurity is concerned is a double-edged sword. It is actually a race of who can develop a better algorithm that caters better to the data which is circulating online. In this sense, the use of AI is a big threat to security. Another issue is that while a company is analyzing and learning from data to discover threats, a hacker is concurrently analyzing the company’s cyber-defense mechanisms and policies to find “open doors’ that will take it into the system to complete the intended attack.
2. Data Confidentiality- AI algorithms are associated with the analysis with large volumes of data, a key requirement for the developed algorithms to produce accurate outputs. The data a company deals with contains normal traffic related to daily transactions and activities, but also sensitive information related to the clients [including their biometrics and personal information](https://insidetelecom.com/Artificial%20Intelligence/the-use-of-ai-as-a-biometric-age-verification-tool). What happens to our data when it goes to the AI-agent though is another thing. [Protecting the data is key when AI is used for cybersecurity reasons](https://insidetelecom.com/Cybersecurity/how-to-protect-your-data-in-2022). The secrecy of the clients’ data should not be compromised for any reason.
3. Increasing need for data- The field of cybersecurity is constantly evolving with ingenious attacks and threats emerging every now and then. The increasingly dynamic environment with threats emerging and evolving will lead to a surge in the required volumes of data, which can potentially not be readily available to have a fast response to the attack itself. Whether it is the ability of AI to keep track of the exponential growth in data or the availability of data for the AI-algorithm to produce results is a big disadvantage of this approach for cybersecurity.
4. High adoption barrier: Artificial Intelligence still requires a lot of human resources and computing power, compared to typical antiviruses. You can simply install a ready software rather than spend time and money on building a custom AI solution. The good news, however, is that AI becoming increasingly more available and even small businesses can afford to build a security neural network.
5. Resources—companies need to invest a lot of time and money in resources like computing power, memory, and data to build and maintain AI systems.

# How Artificial intelligence works in data security.

Incorporating the advanced technology in cyber security is the need of the hour that can detect the attacks in depth and tackle the attacks precisely faster than the human cyber security engineers. Artificial intelligence is the technology that can spot the threats and take the desired action in an automated fashion.

# AI-Powered Data Security Solutions

AI-driven security tools are capable of reducing the risks and even manage many of the threats to data security. They can do this either by themselves through automation and detection or by providing security teams and Security Operation Centers with enhanced capabilities.

* **Security Information and Event Management —**a security tool that uses rules and statistical correlations to actionable information on security and helps security teams deal with events across the entire organizational environment. With the information provided by SIEM, SOC staffs are more equipped to deal with data security threats in real-time.
* **User and Entity Behavior Analytics**—a tool that uses AI to collect, track and analyze data from computer activities to indicate suspicious behaviors. it learns patterns of legitimate access usage and uses these patterns to detect complex attacks like insider threats by recognizing behaviors that indicate malicious intent and jeopardize valuable data.
* **Security, Orchestration, Automation, and Response** —a cyber-security solution used by organizations for data collection and alerts on threats. it can detect threats and automatically deal with low-level threats quickly and efficiently.

# Main Challenges of AI

Not withstanding all the indisputable benefits AI brings to the[cyber security industry](https://en.wikipedia.org/wiki/Computer_security), it should in no way be considered a panacea. AI isn’t necessarily the all-powerful solution to end cyber attacks all together. In fact, it poses challenges, too.

First all, it’s important to keep in mind that AI techs are not invincible. Some tasks performed by Ai can be manipulated if hackers manage to access them. For example, an AI-enabled program could be tricked into labeling malicious software or dangerous user behavior as safe or normal, or the other way around.

Biometric authentication, which is highly popular among users, can also prove to be dangerous. Biometric information in the wrong hands can be used for surveillance or other infringements of users’ privacy.

And unlike passwords, there is no way you can make any changes to your biometric data. This brings users to another problem. [AI technology](https://thenextscoop.com/using-ai-in-business/) has enabled us to collect and process more data than ever before. As a result, it will probably cause further deterioration of digital privacy and security.

Another challenge that AI poses is how expensive it actually is to implement. Since a good deal of AI is still in its nascent stage of its development and is experimental, the cost associated with it may be too high for many businesses.

And what if criminals tap into the power of AI solutions? This will enable hackers to carry out bigger and more sophisticated attacks very quickly. Like network monitoring and learning patterns of user behavior, criminals can also apply machine learning to determine why certain cyber attacks have ended in failure and devise more powerful and effective attack models.

AI also can be used to create malware that resembles trusted software. It can be used to learn more about the target network’s patterns and execute dangerous attacks without ever being detected.

Hackers can also use AI for more powerful attacks with deep learning.

# Trending technologies of AI in security

1) Biometrics

Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

2) Rise of Automotive Hacking

Modern vehicles nowadays come packed with automated software creating seamless connectivity for drivers in cruise control, engine timing, door lock, airbags and advanced systems for driver assistance. These vehicles use Bluetooth and Wi-Fi technologies to communicate that also opens them to several vulnerabilities or[threats](https://www.simplilearn.com/steps-to-eliminate-cyber-security-threat-article) from hackers. Gaining control of the vehicle or using microphones for eavesdropping is expected to rise in 2023 with more use of automated vehicles. Self-driving or autonomous vehicles use an even further complex mechanism that requires strict cybersecurity measures.

3) Mobile is the New Target

Cybersecurity trends provide a considerable increase [(50 percent)](https://www.darkreading.com/cloud/mobile-banking-malware-up-50--in-first-half-of-2019/d/d-id/1336834) for mobile banking malware or attacks in 2019, making our handheld devices a potential prospect for hackers. All our photos, financial transactions, emails, and messages possess more threats to individuals. Smartphone's virus or malware may capture the attention of cybersecurity trends in 2023.

Some of today’s well-known companies that are highly focused on developing AI based cyber security systems are as follows-

1. Crowd Strike

The AI approach adopted by Crowd Strike monitors all activity on an endpoint, profiling each user’s activity and watching all of the system processes that get run on any normal day. This establishes a baseline of regular activity. The system continues to monitor all processes and raises an alert if a user suddenly does something different or if a previously un encountered system process starts up. This is a flag that draws extra activity tracking procedures into play.

The secret weapon of the Crowd Strike Falcon system is an AI-based detection system, known as user and entity behavior analytics (UEBA). The UEBA concept is one of the major innovations that has thrust the system security industry forward, escaping the flawed AV detection model that had started to let too many new viruses onto devices.

1. [Cynet](https://www.cynet.com/)

Cynet deploys AI in its network threat detection systems that examine threats and act on them automatically. The ethos at Cynet is to make advanced threat protection as straightforward as running any system monitoring package.

The Cynet network protection suite is written to provide accessible threat protection to organizations that do not have specialist cyber security personnel. That said, the system is not just for understaffed small enterprises. The service’s customer base includes large multinationals with tens of thousands of employees, including organizations with a high cost of security failure, such as banks.

**Threat detection** extends to the placement of decoys masquerading as real endpoints, files, and servers that aim to attract attackers away from genuine network resources.

3. [Fire Eye](https://www.fireeye.com/)

Fire Eye is much older than the two previous companies examined in this list. It was founded in 2004 and specialized in threat research and recovery consultancy services. This is a labor- intensive field of work and didn’t make the company any money.

# Conclusion

An overview of the state of the artificial intelligence segment in information security allows us to draw the following conclusions: Artificial intelligence makes a significant contribution to the fight against modern information threats. In particular, in most cases, the introduction of AI technologies in the information security of the organization reduces the time to identify problems and respond to incidents, as well as the costs of personnel management. Operators have noted an increase in the efficiency of detecting unknown threats, as well as in the speed of analysis and detection of malicious activity on endpoints and applications.

References

1, [www.insidetelecom.com/AItrending](http://www.insidetelecom.com/AItrending)

2.severality innovative software development

3.Engatiteam/techcorner.com