SRK INSTITUTE OF TECHNOLOGY

ENIKEPADU, VIJAYAWADA

AI SPYDER CLUB

Artificial Intelligence is a tool, not a threat

August, 2019

Faculty Advisors
Dr. D. Haritha
N. Sudhakar
P. Rani

Co-Ordinators
E. Jahnavi
Siva Sai Babu
Sk. Sabiya
Kundan
T. Nikhitha
Bala Kamal


MACHINE LEARNING
IN
SECURITY

ARTIFICIAL INTELLIGENSE ON SECURITY

17X41A05B4, 17X41A0572

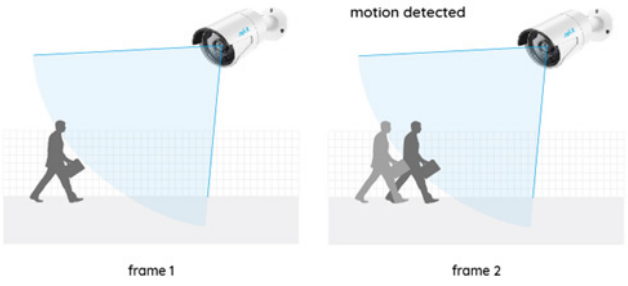
Topic : Security cameras based on Artificial intelligence .

Artificial intelligence (AI) and deep learning technologies in security cameras we can monitor **live** every face by using AI by this process we can provide high security system in restricted areas.

In each and every security cameras provided face recognition to identify culprit in restricted areas AI system can provide end users infinitely more information than traditional security applications ever could.

Motion detection cameras:

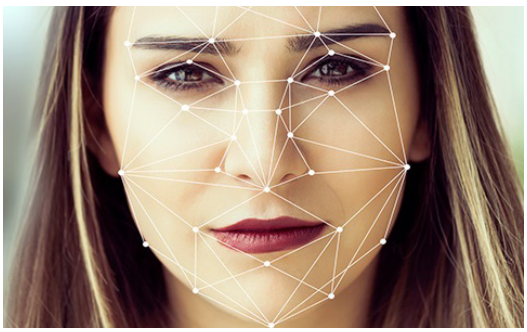
In response to the shortcomings of human guards to watch surveillance monitors long-term, the first solution was to add motion detection to cameras. It was reasoned that an intruder's or perpetrator's motion would send an alert to the remote monitoring officer obviating the need for constant human vigilance The problem was that in an outdoor environment there is constant motion or changes of pixels that comprise the total viewed image on screen. The motion of leaves on trees blowing in the wind, litter along the ground, insects, birds, dogs, shadows, headlights, sunbeams and so forth all comprise motion. This caused hundreds or even thousands of false alerts per day, rendering this solution inoperable except in indoor environments during times of non-operating hours.



Advanced video motion detection:

The next evolution reduced false alerts to a degree but at the cost of complicated and time-consuming manual calibration. Here, changes of a target such as a person or vehicle relative to a fixed background are detected. Where the background changes seasonally or due to other changes, the reliability deteriorates over time. The economics of responding to too many false alerts again proved to be an obstacle and this solution was not sufficient.

Face matching:



The latest facial recognition technology works by using software that can pick a person's face from a crowded image, extract that face from its surroundings and compare it to a database of stored images. To do this, the software uses algorithms that first localise a face and then measure various features of that face for recognition.

This process, known as face matching, consists of several steps. Face detection identifies the extremities of the 'interesting' part of the image and then eye detection marks the centre points of the eye socket, providing fixed reference points for other measurements. Facial landmarks, describing facial elements from the size, shape and locality of a feature to minute details of skin texture, are also identified. These features are mapped into a statistical model that can distinguish between different people and also compensate for reasonable variations in expression and head angle. Biometric templates are generated and compared to those in a database, to provide a final decision, or in most cases a 'likeness score', that indicates the probability of the two matching.

So how does facial recognition work? Technologies vary, but here are the basic steps:

Step 1: A picture of your face is captured from a photo or video. Your face might appear alone or in a crowd. Your image may show you looking straight ahead or nearly in profile.

Step 2: Facial recognition software reads the geometry of your face. Key factors include the distance between your eyes and the distance from forehead to chin. The software identifies facial landmarks one system identifies 68 of them that are key to distinguishing your face. The result: your facial signature.

Step 3: Your facial signature — a mathematical formula is compared to a database of known faces. And consider this: at least 117 million Americans have images of their faces in one or more police databases. According to a May 2018 report, the FBI has had access to 412 million facial images for searches.

Step 4: A determination is made. Your face print may match that of an image in a facial recognition system database.

Who uses facial recognition?

- **U.S. government at airports**. Facial recognition systems can monitor people coming and going in airports. The Department of Homeland Security has used the technology to identify people who have overstayed their visas or may be under criminal investigation. Customs officials at Washington Dulles International Airport made their first arrest using facial recognition in August 2018, catching an impostor trying to enter the country.
- **Mobile phone makers in products**. Apple first used facial recognition to unlock its iPhone X, and continues with the iPhone XS. Face ID authenticates — it makes sure you're you when you access your phone. Apple says the chance of a random face unlocking your phone is about one in 1 million
- **Airlines at departure gates**. You might be accustomed to having an agent scan your boarding pass at the gate to board your flight. At least one airline scans your face.

- **Colleges in the classroom**. Facial recognition software can, in essence, take roll. If you decide to cut class, your professor could know. Don’t even think of sending your brainy roommate to take your test.

NEWS ARTICAL

The Delhi Police will use **cameras equipped with facial recognition** software for the first time to secure the **Red Fort,** where **Prime Minister Narendra modi** will hoist the national flag on Independence Day.

Conclusion :

Artificial intelligence (AI) and deep learning technologies in security cameras we can monitor **live** every face by using AI by this process we can provide high security system in restricted areas.

AI FOR SURVEILLANCE AND SECURITY

CH DIVYA VANI | 17X41A0511

The need for increased monitoring and protection has led to rapid advancements in the sphere of security and surveillance technology today. Statistics reveal that the worldwide expenditure on information security products reached over $114 billion by the last year. New and more innovative solutions are being launched in the market to dabble with the crisis of security at every level. Artificial intelligence for surveillance and security is another one of AI's many life-altering virtues.

How does it work?

AI for video surveillance and security uses machine-based learning and algorithm to monitor and analyze the images, videos, and data recorded from the video surveillance cameras. It is also capable of recognizing and dissecting the movement of human beings, vehicles and a wide array of objects.

AI can make use of machine-based vision to sort the stored data and send alerts on the non-recognition of the system indicating the user of trespassing. The AI software has the ability to keep a record of the surveillance of hundreds and thousands of cameras thereby, challenging and withstanding the ability of us humans to do the same.

Even more interesting is AI's ability to detect threats before they actually happen. With algorithms and deep learning, AI can identify the slightest of changes in the normal behavior of a network and can prevent potential attacks.

Types of Artificial Intelligence Security

There are two types of AI security known:

Rule-based: This is a more generally known form of AI security. In this type, programmers feed the system with pre-designed rules. For example, the video surveillance cameras you see around function on the rule-based AI system.

Behavioral analytics: This is a newer form of AI security. There is no requirement of pre-coded programs as the former rule-based Artificial Intelligence security. Behavioral analytics is a self-learning software in which the artificial intelligence system auto detects, learns and studies normal human behavior and the workings of the environment around him. The system then classifies the data accordingly, and upon detecting any unusual behavior sends out an alarm.

How can Artificial Intelligence Improve Surveillance and Security?

AI has brought forward real-time monitoring of the data acquired along with an intelligent analysis as a solution to curb theft on all grounds. These ideas have been incorporated at a wide array of public places, right from airports to retail stores, to monitor people and detect any unusual activity. AI can be far more reliable and accurate than the human eye thus ensuring that no piece of data or information goes amiss.

AI in the Digital Real

Cybersecurity has been a disturbing issue in today's digital world. Virus attacks deployed by hackers to corrupt and dismantle your systems are a frequent cause of concern. The future of cybersecurity lies in the hands of AI and machine learning, as they are now being used to combat the horror against constant cyber-attacks.

Conclusion

With businesses acknowledging the need to incorporate AI technologies to boost productivity and to secure business processes, the need for AI experts is increasing almost exponentially. However, experts are rare and expensive. MindSync is creating a next-gen ecosystem that is essentially a community of the best AI experts on the planet. Businesses of all sizes can come to the platform and ask the community to create their business solution, as a challenge. This challenge is taken up by relevant AI experts, the best minds in the industry work to create the best solution.

Ch. DIVYA VANI
17X41A0511

ARTIFICIAL INTELLIGENCE IN SECURITY

G.L Krishna Sri | 17X41A0519

Artificial intelligence has, in recent years, developed rapidly, serving as the basis for numerous mainstream applications. From digital assistants to healthcare and from manufacturing to education, AI is widely considered a powerhouse that has yet to unleash its full potential

AI in improvement of cybersecurity :

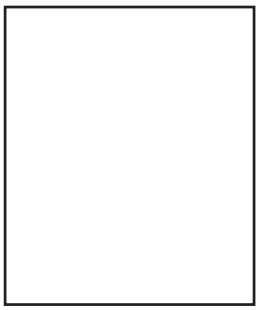
Over the past few years, cybersecurity has emerged as an important aspect for businesses across a wide range of industries, as more and more companies need to have a strong online presence. At the core of cybercrime trends is data – broadly considered as the new currency of an increasingly digital world, data is one of the most important assets for all types of organizations, and safeguarding it is a top priority. In their efforts to keep hackers at bay, cybersecurity experts have developed sophisticated data protection techniques, like data pseudonymization and data encryption. Data pseudonymization is a security process that sees critical data replaced with fictitious information that looks realistic. It is widely used by companies that wish to maintain referential integrity and statistical accuracy of sensitive data to minimize disruption of their operations. Data encryption is another popular technique that makes data impossible to understand for anyone who does not have access to the encryption key, thereby protecting it from intruders.

Recently, artificial intelligence has entered the game. Researchers and cybersecurity experts are harnessing its potential to create solutions that are able to identify and prevent hacker attacks with minimal human input. Using machine learning and AI neural networks has enabled developers to adapt to new attack vectors and better anticipate the next steps of cybercriminals. The expected impact of these applications is so great that 25% of IT leaders considers security the top reason for adopting machine learning within their organizations. Security as a reason is only surpassed by business analytics, which was picked by 33% of respondents, while 16% aim to use machine learning tech for sales and marketing and a further 10% for customer service. AI is not only good for beefing up security, but it is also good for business, as it can reduce the funds and time needed for manual, human-driven detection and intervention by automating the inspection process. It is also believed to be more accurate than humans, responding better to stealthy attacks and insider threats.

AI could be used to build new, more effective malware that will be able to learn and adapt to launch further attacks. Such a development could be devastating for cybersecurity defenses, as traditional protection tools like sandboxes could easily be fooled by a polymorphous AI-powered malware. This could become extremely important in the context of cyber warfare, especially in light of recent allegations for attacks on energy infrastructure by foreign powers. A recent joint report by the FBI and the US Department of Homeland Security has highlighted concerns that hackers associated with Russia were behind a series of attempts to infiltrate and inflict damage on critical infrastructure, including energy and nuclear sectors, the aviation industry, and water facilities. The hackers mostly employed attack vectors like spear phishing emails, credential gathering, and watering hole domains. Using AI could further boost similar attacks and lead to a new era in state-sponsored attacks and cyber espionage.

Last but not least, AI could prove a threat for cybersecurity in a more subtle way. As more and more companies are set to adopt AI-driven and machine learning products as part of their defense strategy, researchers worry that this could lull employees and IT professionals into a false sense of security. Yet lowering our guard in the face of rising cybercrime trends could be a fatal mistake. AI solutions are not 100% foolproof – as no cybersecurity solution alone ever is – so coming up with a comprehensive, multi-faceted strategy should remain a priority for businesses. It is also important that developers allocate enough time to conduct thorough data labeling on potential threats and foster the power of AI to continue learning without supervision.

Yet AI can also become a real headache for cybersecurity professionals around the globe. Just as security firms can use the tech to spot attacks, so can hackers in order to launch more sophisticated attack campaigns. Spear phishing is just one example out of many, as using machine learning tech can allow cybercriminals to craft more convincing messages intended to dupe the victim into giving the attacker access to sensitive information or installing malicious software. AI can even help in matching the style and content of a spear phishing campaign to its targets, as well as enhance the volume and reach of the attacks exponentially. Meanwhile, ransomware attacks are still a hot topic, especially after the WannaCry incident that reportedly cost the British National Health System a whopping £92 million in damages – £20 million during the attack, between May 12 and 19, 2018, and a further £72 million to clean and upgrade its IT networks – and meant that 19,000 healthcare appointments had to be cancelled.



G.L Krishna Sri
17X41A0519

PHISHING DETECTION WITH ML

K.RAHUL CHANDRA | 17X41A0523

Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels.

Typically a victim receives a message that appears to have been sent by a known contact or organization. The message contains malicious software targeting the user's computer or has links to direct victims to malicious websites in order to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Machine learning is the application of artificial intelligence that enables system to automatically learn and improve from experience with out being explicitly programmed

Once the phishing is detected machine learning algorithms is applied on it

Detection approaches

.detection approaches

.offensive defense approach

.Correction approach

.Prevention approach

The types of phishing attacks can be classified into the following categories:

- Vishing refers to phishing done over phone calls. ...
- Smishing. SMS phishing or SMiShing is one of the easiest types of phishing attacks. ...
- Search Engine Phishing. ...
- Spear Phishing. ...
- Whaling.

Detectiom of facing attacks by machine learning

Passive and active warnings

Passive warning- the warning does not block the content area and enables the user to view both the content and the warning

Active warning-The warning blocks the content data which prohibits the user from viewing the content data while the warning is displayed

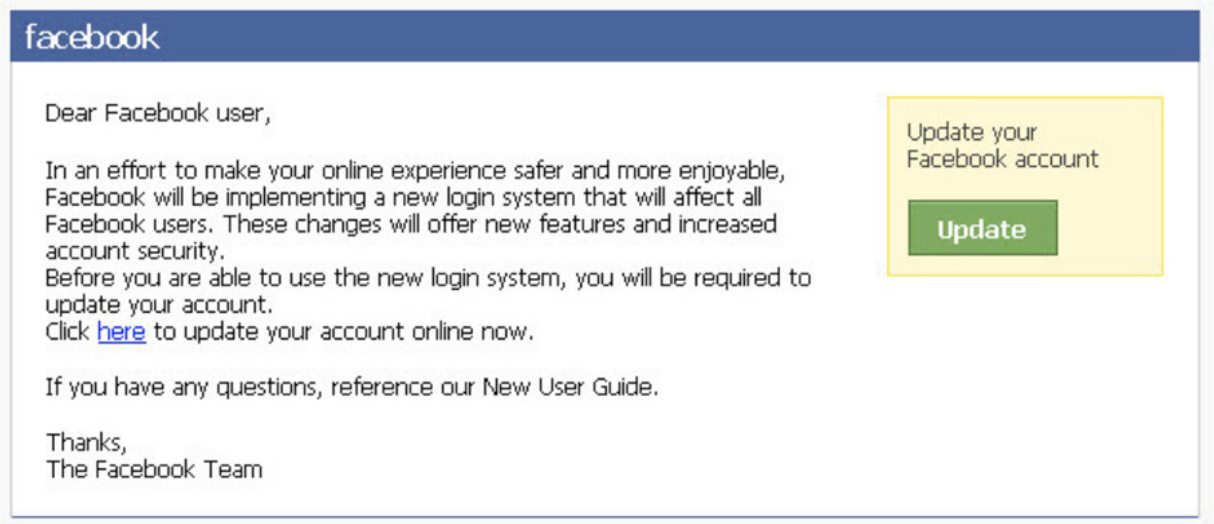
Machine Learning Based Methods

Malicious Domain Detection

Dong et al.18 have investigated a comprehensive list of features that can be extracted from X.509 certificates. With using top 100,000 websites from Alexa top one million web- sites30 as their legitimate examples and phishing URLs downloaded from PhishTank13as phishing examples, precision and recall of 95.5% and 93.7% are attained for the phishing category with a Random Forests classifier. However, these statistics are doubtful when it comes to the current Internet environment, as will be discussed in detail in Section 5.6. Our feature list, in contrast to their work, leverages information from not only certificates, but also several other dimensions of a given website, including server characteristics, DNS responses, network performance and so on.

Email Spam Filtering

Ouyang et al.22 proposed a multi-stage pipelined spam email detection system using machine learning approach, which contains an extensive list of network features. They analyzed their methodology with email data collected in over two years, consisting of over 1.4 million messages, and reported a true positive rate between 12% to 77% using the Decision Tree algorithm. Our work in this thesis differs from their work in several aspects. Firstly, we use an advanced machine learning algorithm, i.e., Random Forests, for the classification purpose. Secondly, we have used a lot of features other than net-work features for the classification purpose.



ARTIFICIAL INTELLIGENCE IN HEALTH CARE

P.KANAKA DURGA | 17X41A0539

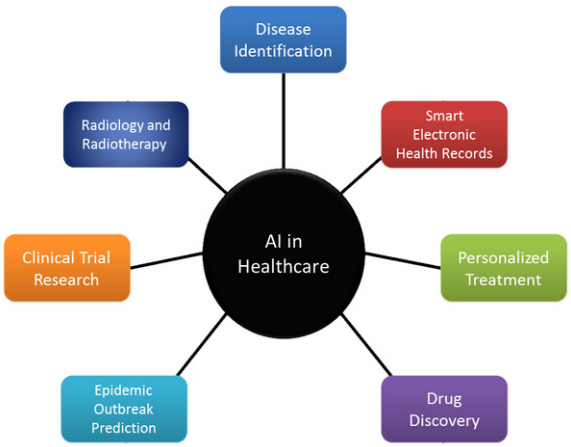
Artificial Intelligence means “To make machines think like humans”. The role of Artificial Intelligence in health care has been a huge talking point in recent months and there’s no sign adoption of this technology slowing down, well ,ever really.AI in health care is the use of complex algorithms and software to estimate human cognition in the analysis of complicated medical data.The need of AI is “AI increases ability for health care professionals to better understand the day-to-day pattern and needs of the people. With this , they are feeling and they are able to provide better feedback, guidance and support for staying healthy.

Uses of AI:

There are mainly six uses of AI in health care.

1. Personal health virtual assistant
2. Advanced analytics and research
3. Personal life coach
4. Healthcare bots
5. Medical imaging analysis and diagnosis assistance
6. Dictation assistance with NLP

Applications of AI in health care:



Challenges of AI in Health Care :

The Challenges and Opportunities Of Implementing AI In Health Care are

- Managing and integrating large data sets
- Interoperability
- Protecting data security and patient privacy
- Getting “Truth” from Machine Learning
- Mass Vs. Individual

Advantages:

- More powerful and more useful computers
- New and improved interfaces
- Solving new problems
- Better handling of information
- Conversion of information into knowledge

Disadvantages:

- Increased costs
- Difficulty with software development
- Few experienced programmers
- Few practical products have reached the market as yet.

Conclusion:

Finally, we can conclude that AI is changing health care and it changes the role of doctors and sometimes it may changes the role of patients also. AI can achieve fast and accurate diagnostics and it will be very helpful to reduce the human errors as well as the cost of treatment also.

P. KANAKA DURGA
17X41A0539

ARTIFICIAL INTELLIGENCE AND SECURITY

S.SAI SONY |17X41A0547

Artificial intelligence is a science field that is interested in finding solutions to complex problems like humans do. A decision mechanism that is similar to a real human decision mechanism is tried to be modelled with some algorithms. Machine learning is a sub domain of **artificial intelligence**.

Security is a broad term, in industry and government there are a myriad of "security" contexts on a variety of levels – from the individual to nation-wide. Artificial intelligence and machine learning technologies are being applied and developed across this spectrum.

The three broken down into three sections:

1. Real-world use cases of artificial intelligence paired with security applications.
2. Potential future applications.
3. Basic glossary of artificial intelligence and security terms.

THE RISKS OF AI IN SECURITY

This Perspective explores the policy implications of the rise of algorithms and artificial intelligence (AI) in two domains of significant importance and public interest: security and employment. These domains are only a sub selection of larger set of affected domains identified by a panel of experts. We drill down on the near-to-medium term trends and implications of AI proliferation in these domains. In brief, we highlight the potential for significant disruption due to AI proliferation on issues of cyber security, justice (criminal and civil), and labour market patterns. Our discussion of the future of work also presents a novel framework for thinking about the susceptibility of occupations to automation. The Perspective ends with a set of AI policy recommendations informed by the trends we highlight.

Artificial Intelligence Changes Everything in the Security Industry

"AI will be to the 21st Century what electricity was to the last…and Data – the oil that drives the generator." Just as nineteenth-century entrepreneurs applied the electricity break-through to cooking food, lighting rooms and powering industrial equipment, today's AI entrepreneurs are doing the same with the deep learning of artificial narrow intelligence (ANI)

In the Deep Learning of AI, we've found that proactive capability we wanted to advance many years ago. We knew if we could determine the pure genomic state of the benign files that make up the Internet, we could detect malicious anomalies and print them before they could hurt us. We just needed technology to catch up with the idea.

PROS AND CONS OF AI FOR SECURITY

To truly keep your organization safe, someone should check every event, but there's no way a human could even begin to prioritize and review such a high daily volume of potential threats. That's where a something artificial intelligence.

AIs use computer algorithms to engage in machine learning to safeguard systems against cyber

security threats. These programs recognize patterns in your system event logs and flag particularly troubling incidents for human review. Cyber security breach detection

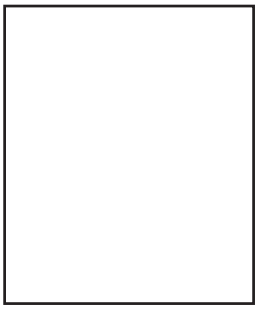
- Incident response
- Situational awareness to shore up a prior to a breach

DRAWBACKS

- AI is not infallible. In the rush to capitalize on the AI hype, programmers and product developers may overlook some of the threat vectors that could do the most damage. In the got-to-get-it-to-market rush, the likelihood of making unintentional errors is high, so rushed AI might not be as successful as promised.
- Plus, the good guys aren't the only ones with AI capabilities. Hackers who gain access to internal systems can corrupt data so infected code is tagged as clean by AI systems. To protect yourself against these vulnerabilities, you may want to supplement internal teams by working with security experts or provide training on how to spot AI-generated security reports. Whatever you do to address weaknesses in AI, just make sure you're always keeping abreast of the latest trends in the industry.

CONCLUSION

AI allows you to automate the detection of threat and combat even without the involvement of the humans.



S. SAI SONY
17X41A0547

AI FOR DATA PROTECTION

T.V.N.C. Nikhita | 17X41A0553

Artificial intelligence (AI) has rapidly developed in recent years. Today, AI tools are used increasingly by both private and public sector organizations around the globe.The capabilities of AI now and in the near future create widespread and substantial benefits for individuals,institutions, and society. AI can help companies limit or monitor who is looking at an individual's data and respond in real-time to prevent inappropriate use or theft of data. Companies are developing AI-based privacy tools, such as privacy bots, which remember privacy preferences and try to make them consistent across various sites, and privacy policy scanners, which attempt to read and simplify privacy policies for users to more easily understand.

AI for Data Protection:

While some scholars have argued that AI poses a threat to data

protection, others have posited that AI can offer opportunities to further bolster it. For example, AI can help companies limit or monitor who is looking at an individual's data and respond in real-time to prevent inappropriate use or theft of data. Companies are

developing AI-based privacy tools, such as privacy bots, which remember privacy preferences and try to make them consistent across various sites, and privacy policy scanners, which attempt to read and simplify privacy policies for users to more easily understand. Polisis, which stands for "privacy policy analysis," is an AI that uses machine learning to "read a privacy policy it's never seen before and extract a readable

summary, displayed in a graphic flow chart, of what kind of data a service collects, where that data could be sent, and whether a user can opt out of that collection or sharing."AI is also being used to alert users of suspicious websites, advertisements,and other malicious activity. Finally, AI is enabling companies to develop technologies that are more protective of user privacy. For example, researchers are attempting to

develop machine learning techniques that evaluate encrypted data, thereby enhancing user privacy.

The Challenge for Data Protection

AI presents challenges as well as benefits. While it is already assisting workers in many professions, AI likely will reduce the need for workers in others. It may introduce bias and new forms of discrimination, especially if the data used in AI development only represents partial segments of the population or reflects existing societal bias. AI will likely challenge traditional notions of urban and residential planning, which have large spaces dedicated to parking lots and garages. AI may also raise important antitrust issues, particularly if the data necessary for its development is concentrated in the hands of a few entities. Each of these important issues

require thoughtful attention, but they are beyond the scope of this article and in most cases they are the subject of other bodies of law. This article focuses exclusively on data protection challenges presented by AI used today and under development for use in the near future.

While data protection laws and regulations attempt to protect sensitive data and similar variables, AI algorithms need to include such data in the analysis to ensure accurate and fair results. For example, when predicting the likelihood of death in pneumonia patients,researchers at Microsoft discovered that a history of asthma resulted in a lower risk of death,

likely because these individuals are likely to seek earlier treatment. Because those protected variables were left in the model, it was easier for researchers to account for them.Resolving the scope of data protection law and principles in the rapidly changing context of AI is not an easy task, but it is essential to protect privacy effectively in this increasingly critical

context and to avoid burdening AI with unnecessary regulatory requirements or with uncertainty about whether or not regulatory requirements apply. Clarifying the application of data protection law is also critical to ensuring that scarce resources are not wasted on

Conclusion

with this i conclude that AI is technology that is leading towards every field including the security side.The proliferation of AI is already yielding significant benefits, but it also raises important issues.Efforts to address those issues within existing data protection frameworks increasingly

demonstrate the limits of those frameworks and their inadequacy both for protecting privacy and for facilitating innovation in an increasingly data-dependent economy. As new AI applications are developed and deployed, we have an opportunity and an increasingly unavoidable need to examine the effectiveness of current data protection laws and to revise

them in light of 21st-century realities.

T.V.N.C. Nikhita
17X41A0553

WHAT IS CYBER SECURITY?

Cybersecurity analysts help prevent attacks through their expertise and knowledge of databases, networks, hardware, firewalls and encryption. **Cybersecurity**analysts may also regulate access to computer files, develop firewalls, perform risk assessments and test data processing systems to verify **security** measures.

How AI helps

AI technologies like machine learning and natural language processing enable analysts to respond to threats with greater confidence and speed

AI for cybersecurity

As cyberattacks grow in volume and complexity, artificial intelligence (AI) is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI provides instant insights to help you fight through the noise of thousands of daily alerts, drastically reducing response times.

Watch the video to hear Kevin Skapinetz, IBM Security vice president of strategy and design, explain how advanced AI can act as an advisor to analysts, helping them quickly identify and connect the dots between threats.

Why Artificial Intelligence in Cyber Security?

Forget those scenes of shiny robots flying around data centres or super-cool disembodied voices discussing advanced concepts. Cyber security has far more basic needs. Through our reliance on ever larger quantities of data, we have created the need for a parallel problem of keeping it all safe. Unfortunately, it is far easier to produce data than it is to protect it.

Where artificial intelligence is really needed?

AI's crucial role right now is to offload work from human cyber security engineers, to handle the depth and detail that humans cannot tackle fast enough or accurately enough. Advances in machine learning technology mean that AI applications can also automatically adapt to changes in threats and spot problems as they arise.

Here are some of the most pressing cyber security needs that AI tools and platforms can help to meet.

The current state of cyber security

Today, companies place an emphasis on the security of their internal network. If hackers manage to infiltrate that layer of their infrastructure, it is only a matter of time before a "small" breach becomes a large-scale attack.

The most common tactic for network protection is a firewall. Firewalls can exist either as a software tool or a hardware device that is physically connected to the network. In either scenario, the firewall's job is to track what network connections are allowed on which ports and block all other requests. Typically, server administrators set and control these firewall policies and adjust them via a change management process.

How artificial intelligence will shape the future?

The majority of legacy cyber security tools require human interaction or configuration at some level. For example, a person from the IT team has to set the firewall policies and backup schedules and then ensure that they are running successfully. The advancement of AI changes the whole equation.

In the future, companies will be able to rely on smart tools to handle the bulk of event monitoring and incident response. The next generation of firewalls will have machine learning technology built into them, allowing the software to recognize patterns in web requests and automatically block those that could be a threat.

The end of passwords (maybe)

Passwords. Can't live without them but they make you crazy. The majority of internet users create their own bespoke passwords for each website or service that they subscribe to online. This system can be frustrating to maintain as well as vulnerable to attack if you rely on simple passwords or use the same one for multiple sites.

There have been improvements in password manager software performance in recent years, most of which aim to simplify and strengthen online security by removing a large portion of the manual effort from the task through algorithms that suggest and store passwords complex enough to reduce your chances of being hacked.

Investing in cyber security solutions and tools is a necessary task for businesses of all sizes. Those with smaller budgets may think they can save money by taking shortcuts, but in fact they are often the prime target for hackers for exactly this reason. Cyber security products prove their worth in the long run by reducing your organization's risk and protecting it from dangerous unknowns.

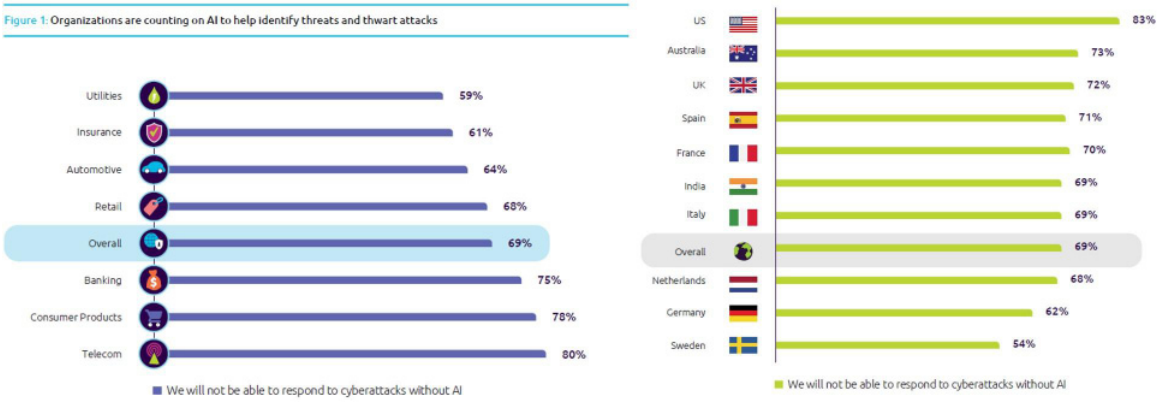
The good news is that thanks to advancements in AI technologies, companies will likely not need to maintain large cyber security teams within their IT department as the future unfolds.

Why AI Is The Future Of Cybersecurity?

- 61% of enterprises say they cannot detect breach attempts today without the use of AI technologies.
- 48% say their budgets for AI in cybersecurity will increase by an average of 29% in Fiscal Year (FY) 2020.
- Breach attempts are proliferating with Cisco reporting that in 2018, they blocked seven trillion threats on behalf of their customers.

These and many other insights are from Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report published this week. You can download the report here (28 pp., PDF, free, no opt-in). Capgemini Research Institute surveyed 850 senior executives from seven industries, including consumer products, retail, banking, insurance, automotive, utilities, and telecom. 20% of the executive respondents are CIOs, and 10% are CISOs. Enterprises headquartered in France, Germany, the UK, the US, Australia, the Netherlands, India, Italy, Spain, and Sweden are included in the report. Please see page 21 of the report for a description of the methodology.

- **69% of enterprises believe AI will be necessary to respond to cyberattacks.** The majority of telecom companies (80%) say they are counting on AI to help identify threats and thwart attacks. Capgemini found the telecom industry has the highest reported incidence of losses exceeding $50M, making AI a priority for thwarting costly breaches in that industry. It's understandable by Consumer Products (78%), and Banking (75%) are 2nd and 3rd given each of these industry's growing reliance on digitally-based business models. U.S.-based enterprises are placing the highest priority on AI-based cybersecurity applications and platforms, 15% higher than the global average when measured on a country basis.



xxxxxxxxxxxxx

11111111111111