INTRODUCTION TO ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Abstract

In today's technologically advanced and network-connected world, being able to comprehend and use cyber security efficiently is essential. Without security in place, systems, critical files, data, and other significant virtual objects are at risk. The network's cyber security risk assessment, which determines risk using the AHP approach and security status, is assessed in conjunction with the network unit's relevance. This method might be able to identify the main network threats and the degree of security of every network unit based on experimental findings. Threat hackers would now have easier access to a wider attack surface due to the enhanced connection. Blackouts that were common in the past have been caused by cyberattacks that used esls.

Keywords: Cyber security, Electronic shelf labels

Authors

Ashima
Department of CSE
Rayat Bahra University
Mohali-140103, Punjab.
ashimamockoul@gmail.com,

Sukhjinder Kaur
Department of CSE
Rayat Bahra University
Mohali-140103, Punjab.
skaur29100@gmail.com

Poonam Kukana
Department of CSE,
UIE, Chandigarh University
Mohali-140413, Punjab.
poonamkukana@gmail.com

Chiman Saini
Department of CSE
World Collage of Technology
and Management, Farukh Nagar
Gurgoan-122506, Haryana, India.
Chimansaini1994@gmail.com

I. INTRODUCTION

Artificial Intelligence (AI) is rapidly transforming a variety of industries by enhancing capabilities through data analysis, automation, and innovative applications.

Here are some key areas in which AI is making significant strides:

1. **Generative AI and Creativity**
   - **Generative AI Models:** Technologies like GPT-4, DALL-E, and Midjourney create text, images, music, and even 3D models, enabling applications in content creation, entertainment, and design.
   - **Text-to-Anything:** Advanced multimodal AI systems are integrating text, image, audio, and video generation into single platforms, allowing more seamless and context-aware media creation.

2. **AI in Healthcare**
   - **Diagnostics and Drug Discovery:** AI helps diagnose diseases faster, develop new drugs, and predict patient outcomes. For example, algorithms can identify tumors in medical imaging or model potential drugs at a much faster rate.
   - **Personalized Medicine:** AI can analyze patient data to recommend customized treatments, increasing the effectiveness and reducing side effects.

3. **AI-Powered Autonomous Systems**
   - **Self-Driving Vehicles:** AI is improving autonomous vehicles, helping them to safely navigate complex environments. This includes not only cars but also drones and robots for delivery and industrial applications.
   - **Robotics:** Advanced robotics use AI for more flexible manufacturing, warehousing, and even personal assistance in healthcare or home automation.

4. **Natural Language Processing (NLP) and Conversational AI**
   - **Virtual Assistants and Chatbots:** AI-driven virtual assistants can handle customer service inquiries, streamline operations, and improve user experience. They're becoming more intuitive, handling complex queries and conversational context.
   - **Language Translation:** Real-time AI translators are improving cross-lingual communication, which is particularly valuable in globalized business and education settings.

5. **AI in Cybersecurity**
   - **Threat Detection and Prevention:** AI-driven systems can detect patterns in network traffic to identify and mitigate cybersecurity threats in real time.
   - **Automated Incident Response:** AI systems are increasingly used to respond to threats autonomously, protecting critical infrastructure and sensitive data.

6. **Sustainable AI and Green Computing**
   - **Energy-Efficient AI Models:** As AI models become more computationally intensive, there's a push toward energy-efficient hardware and algorithms that reduce carbon footprints.

- **Climate Prediction and Environmental Management:** AI assists in predicting climate trends and managing resources, such as optimizing energy consumption in smart cities.

7. **Explainable AI and Ethical Considerations**
   - **Transparency and Fairness:** As AI is embedded in decision-making processes, there's an increased focus on explainable AI (XAI) to ensure algorithms are transparent, fair, and free from biases.
   - **AI Ethics and Regulations:** Governments and organizations are establishing ethical guidelines and regulations to address issues related to privacy, bias, and the impact of AI on employment.

AI's ongoing development promises continued transformation across multiple sectors, influencing our daily lives, and requiring us to address ethical, practical, and technical challenges as we harness its potential.

1. Introduction to Cyber Security

In effective cyber security strategies, numerous protection levels are distributed between computers, networks, programs, and data that want to maintain security from attacks. Successful prevention or recovery from cyber-attacks requires cooperation between all systems, people and resources. Combined threat management systems and cyber systems can accelerate three important security measures, inspections and modifications. People's consumers must know and follow the principles of basic information security, such as using powerful passwords, investments and data storage by e-mail. Learn more about basic laws and cyber security concepts.

Processes -The government must have a strategy to work with frequent and successful cyber-attacks. Familiar outline can be accompanied. He explains how to decide to occur, protect the company, recognize risks, cope, and record successful results.

Technology -technology is important for providing the ability of people to protect yourself from cyber-attacks. The three main goals at the most risk is the final strategy, including computers, smartphones and routers. System; Firewalls Cloud. Next Generation, DNS filter, malware protection, viral vaccine software and email safety results are some examples of general technologies that are discarded to protect these products. One of the approaches to cyber definitions is that it is associated with network or collection of workstations. The system to protect something is sometimes called safety. From this, the terms "safety" and "cyber" are made to explain the process of protecting user data after events or hostile attacks, which can indicate Kazak safety. This is a period of time canceled after the Internet began to develop rapidly. The advantage of cyber security is that all users or groups can protect confidential information from hackers. At present, this is paying attention to hacking. At this stage, despite the fact that he is afraid of hacking, he used ethical hacks to introduce cyber security to all buildings.

2. Types of Cyber Security

a. Network Security: Network security is the process of defending a computer network against assaults or intrusions. It makes use of firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs). The primary goal of network security is to safeguard a network's infrastructure, which consists of servers, routers, switches, and other network equipment. Among the crucial elements of network security are:

- Tools for network management and monitoring
- Systems for authentication and access control
- Methods for encrypting and decrypting data; firewall technology
- Routine security audits

b. Application Security: Application security refers to the measures used to safeguard software applications against online threats. It includes checking the application for errors, analyzing the code, and identifying security flaws. Application security can be used at various stages of the software development life cycle, from planning to deployment. Code review and vulnerability scanning are crucial components of application security, as is the implementation of secure coding techniques.

- The use of safe authorization and authentication procedures
- Frequent updates and security testing

c. Information Security: Information security is the process of safeguarding digital data, including that stored in databases, files, and other repositories. Information security ensures the availability, confidentiality, and integrity of data by protecting it from unauthorized access, disclosure, alteration, and destruction. It has several security features, such as access control, encryption, and backups. Important aspects of information security include:

- Using biometric verification, two-factor authentication, or passwords as access control methods
- Sensitive information is encrypted both in transit and at rest.
- Monitoring and recording system and network activities
- Putting disaster recovery and business continuity plans into action
- Performing routine backups of important data

d. Cloud Security: Protecting data and systems hosted on cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud is what it is. Cloud security uses a combination of technical and administrative measures to protect the data stored in the cloud as well as the cloud infrastructure. Essential components of cloud security:

- Utilizing virtual private networks and secure cloud configurations
- The use of controls for identity and access management
- Frequent security audits and compliance checks;
- Data encryption both in transit and at rest

e. Internet of Things (IoT) Security: The Internet of Things (IoT) is the term used to describe the network of linked devices, which includes wearables, smartphones, and smart homes. IoT security means safeguarding the devices as well as the network that

connects them. The more IoT devices there are, the higher the potential of cyberattacks. The use of secure communication protocols and frequent software patches and updates are two important aspects of IoT security.

- Using robust authentication and access control procedures
- Encrypting and verifying the integrity of data
- Conducting frequent vulnerability assessments
- Penetration tests

f. Identity and Access Management (IAM): Identity and access management, or IAM, is the process of controlling user identities and resource access within a company. Access control, authorization, and user authentication are among the security aspects that IAM integrates. Important aspects of IAM:

- Using robust authentication techniques,
- Including two-factor authentication or biometric verification;
- Putting role-based access restriction into place
- Frequent compliance inspections and security audits
- Putting password standards into place and updating them frequently

3. Cyber Attack

A cyber-attack is an effort by hackers, cybercriminals, or other online adversaries to obtain access to a computer network or system, usually with the goal of altering, stealing, destroying, or revealing data.

Cyber-attacks can target governments, corporations, and even private citizens. In order to obtain sensitive and crucial company resources, such payment information, customer data, or intellectual property (IP), hackers usually target corporations or other organizations.

Some common types of cyber-attacks are:

a. Malware: It is a type of program designed to compromise a system or get an unauthorized authority to use it. Social web engineering This tactic is used by adversaries to fool you into divulging private information. They have the authority to request improved access to your protected data or a monetary settlement. Some of the previously listed elements can be combined with social engineering to increase your likelihood of clicking on links, spreading malware, or endorsing malicious causes.

b. Denial of Service (DoS): A hostile, targeted attack called a denial-of-service (DoS) attack floods a network with fake requests in an attempt to disrupt corporate operations. A denial-of-service attack stops users from performing routine and necessary actions, such as using a compromised machine or network to access websites, online accounts, email, or other services. Denial-of-service attacks cost the organization money, time, and other resources to restore critical business services, even though most of them don't result in data loss and can typically be prevented without paying a ransom.

c. Phishing: Phishing is the practice of disseminating fraudulent emails that appear to be from reliable sources. A relevant data exchange involving login credentials and credit card information is the aim. This type of hack is the worst.

d. Spoofing: Cybercriminals utilize it as a strategy to impersonate a reliable or well-known source. By doing this, the adversary gains access to the target's devices or systems and can engage with them with the ultimate goal of infecting the device with malware or other harmful software, extorting money, or stealing data. Spoofing can happen in a number of ways, including:

- Spoofing domains
- Spoofing emails
- Spoofing the Address Resolution Protocol (ARP)

e. Identity-based Attacks: Identity-motivated attacks are extremely hard to spot. It is often quite difficult to discern between the behavior of the hacker and the typical behavior of the legitimate user whose credentials have been stolen and who is impersonating that user using standard security procedures and techniques.

f. Code Injection Attacks: It consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action.

g. Supply Chain Attacks: Supply chain attacks are cyberattacking that target a trustworthy third-party vendor that offers software or services that are necessary to the supply chain. Software supply chain attacks introduce harmful code into an application to infect all users, whereas hardware supply chain attacks impact physical components for the same purpose. Software supply chains are particularly vulnerable since modern software is not built from scratch but rather incorporates many off-the-shelf components, such as third-party APIs, open-source code, and proprietary code from software manufacturers.

h. Social Engineering Attacks: Social engineering is a practice used by attackers to coerce victims into performing a desired action by using psychological tricks. Attackers can obtain sensitive information by using strong motivators like love, money, fear, and status. They can then use this information to either extort the organization or utilize it as a competitive advantage.

i. IoT-based Attacks: An internet of things (IoT) assault is any hack that targets an IoT device or network. Once the hacker has gained access to the device, they can take control of it, steal data, or join a network of compromised devices to launch DoS or DDoS attacks. According to cybersecurity experts, as the number of connected devices is expected to grow rapidly, so too will IoT attacks. Furthermore, the introduction of 5G networks, which will promote the use of connected devices, may lead to a rise in attacks.

j. AI-powered Attacks: As AI and ML technologies have advanced, so too have the amount of use cases for these technologies. Just as cybersecurity professionals employ AI and ML to protect their online spaces, attackers use these technologies to breach a network or steal sensitive information.

4. Goals of Cyber Attack

a. Confidentiality: Limiting who has access to your sensitive information and making sure that no information is shared with unapproved parties. This jeopardizes secrecy if your key is confidential and will not be shared with anybody. The following are some ways to safeguard confidentiality:

Data encryption, two- or multi-factor authentication, and biometric validation.

b. Integrity: Make sure that every piece of information you provide is true, trustworthy, and doesn't change as you go along. Techniques for ensuring integrity include the following:

- The records cannot be accessed by unauthorized individuals, which is also against privacy. As a result, controls for operator contact will be present to ensure the devices function properly.
- It is necessary to have readily available backups that can be restored promptly.
- Version supervisory must be close by to check the change log.

c. Firewalls: A firewall is a piece of hardware or software that helps stop hackers, worms, and viruses from trying to access your computer through the Internet. A firewall confirms every communication that enters or leaves the internet. To stop any kind of virus or trojan from infiltrating the system, this interface is used to first confirm connectivity. Thus, firewalls are crucial for detecting malware.

d. Anti-virus Software: A computer program known as antivirus software finds, eliminates, and takes action against malicious software, such as viruses and worms. The auto-update feature of the majority of antivirus products enables the program to download new virus profiles so that it may begin scanning for them as soon as they are found. Antivirus software is the most basic requirement for any machine.

e. Availability: Every time an operator accesses a resource for statistics, there shouldn't be any Denial of Service (doS) alerts. All supporting paperwork has to be available. When an attacker gets control of a website, for example, the actions that follow will make it harder to get.

5. Inspecting Cyber Security Risks

Despite being a common network, the power grid does not represent data or information; it merely represents electricity. The electrical market and the "internet" are transformed by astute energy, which uses a large amount of renewable energy. The terms "user-side vitality and power," "data transformation," and "transmission" refer to many essentially minor facts that need to be merged. Single data has a lower value density than large data. high worth. By cleverly connecting large, small data volumes, Upiot provides a pervasive view of information and data. Upiot is currently in the planning stages The most important features of its Upiot Cyber Security Development Center are its support network and accessibility. To assess the risk of cyber security, a cyber security evaluation model needs to be developed. This indicates that the asset's worth, risk, and susceptibility all have an impact on Uplot's cyber security risk. The risk rises in direct proportion to the asset's value and the degree of vulnerability. Asset (a) and risk (r) are two elements of upiot cybersecurity. Tva can be used

to express risk (r). This is therefore a representation of the network unit's risk (r). Network I in (nu). Given that each node in the network has a different impact on network risk, the weighted sum of all the network's total risk (r) can be described using unit risks.

6. Electronic Shelf Label

Retailers display product prices on shelves using electronic shelf label (ESL) devices. A central server can manage these systems, and they can be automatically updated or changed. These systems are commonly found on the front edge of retail shelving.

Either liquid crystal display (LCD) or electronic paper (E-paper) with ESL tag modules can be used by the client to examine the current product pricing. Because it offers clear, full-graphic images, just needs electricity for updates, and doesn't require power to keep images, e-paper is popular among eSL students. Unlike static placards, a communication network from the central server allows the price display to be automatically updated anytime a product price changes. Reliability, battery life, speed, and application range are all requirements for wireless communication. Infrared, radio, and even visible light communication are examples of wireless communication methods. In the ESL sector, radio frequency communication is currently very popular.

The majority of retailers who sell their products in physical storefronts utilize electronic shelf labels, which are commonly affixed to the front edge of retail shelves and show the product's price. Depending on the type of ESL, further details may be supplied to guarantee accuracy in the results, such as stock levels, expiration dates, or product specifics. Paper labels have been replaced by electronic shelf labels (esls), which are tiny, battery-operated electronic paper (e-paper) screens that display product and price information at the shelf edge. In order to create a dynamic price automation network and achieve accurate outcomes, ESLs wirelessly connect to a central hub.

7. Examining and Estimation

According to our data, noncompliance with cyber and network security requirements is linked to specific personality traits like impulsivity, risk-taking, and a failure to consider the long-term effects of decisions. Future studies should concentrate on creating a set of assessments that combine cognitive functions and personality characteristics associated with network and cyber security behaviors into a unified framework. This battery of tests should examine the previously mentioned cognitive abilities, such as impulsivity, risk-taking, and taking future consequences into account, in order to produce results based on esls.

Here, we also demonstrate how pro-security behavior may be increased by employing specific psychological techniques, such as rewarding and punishing security-related conduct, employing inventive polymorphic security alarms, and using psychological techniques to raise awareness of the repercussions of activities. Furthermore, there are cognitive training techniques that help the general public become less impulsive, risk-taking, and procrastinating, such as working memory training and supplementary technical lectures.

Next, the probability of an IoT device being attacked is computed. We estimated that the likelihood of this attack in our fictitious scenario was 70%. According to the experts' study, this chance might alter. The susceptibility, attack, and interdependence layers are the three

areas that attackers can choose to target. Therefore, the Internet of Things system's ability to support economic, social, and environmental elements will have an impact on the company's success. Other tactics might be created to reduce the possibility of this damage by detecting it earlier using ESL, given the suggested IoT system security.

As mentioned before, a number of human mistakes can compromise security and computer systems. These errors include sharing passwords, sharing too much on social media, visiting dubious websites, using unapproved external media, clicking links at random, using weak passwords, opening attachments from dubious sources, sending private information over mobile networks, and not physically protecting personal information. However, phishing emails and password sharing have been the subject of a lot of human error study. Future studies should examine the effects of individual traits and environmental factors (e.g., emotional state, work urgency, or multitasking) on other types of cyber security failures, such as the use of weak or identical passwords.

II. CONCLUSION

AI and Cyber Security are the two most powerful domains of tomorrow. As AI permeates every domain like healthcare, autonomous systems, natural language processing or sustainability; its synthesis with cyber security is essential. AI-Fuelled Weapons, Combat Emphasis on AI Systems, AI systems can be deployed to enhance automation, precision, and threat detection in real-time. However, the emergence of AI also brings in new challenges to security in adversary attacks, AI-powered threats, and ethical dilemmas. Cyber security, as we have covered, must advance in step with AI developments to protect critical infrastructure, sensitive data, and systems from corruption. Phishing, identity-based attacks, and IoT vulnerabilities are on the rise, and so must defenses against them, bolstered by intelligent, adaptive security architectures. Furthermore, human elements e.g., lust for biological data, unawareness to target attacks, risk-taking behaviour, etc. — are still a major consideration element of cyber incident, requiring further education, behavioural manipulation, and ethics awareness. Researchers, practitioners, and policymakers should work to promote interdisciplinary collaboration, invest in AI ethics and transparency, and foster cognitive and technological resilience. Together, by steering the course of AI growth hand in hand and being the proactive in the cyber security movement, we can safeguard for the prosperous future smart, connection world; preserve privacy, trust, and innovation.

REFERENCES

[1] Ullah, S., Zahilah, R. Curve25519 based lightweight end-to-endencryption in resource constrained autonomous 8-bit iotdevices. Cybersecur 4, 11 (2021). Https://doi.org/10.1186/s42400-021-00078-6.

[2] P. A., B. Seth and G. Ramachandran, "Analysis of Current smartwearable Trends using Internet of Medical Things," 2023 thirdinternational Conference on Artificial Intelligence and Smart Energy(ICAIS), Coimbatore, India, 2023, pp. 19-22, doi:10.1109/ICAIS56108.2023.10073832.

[3] P. A., G. V. Reddy "Artificial Intelligence Techniques for the wirelesswearable Smart Healthcare Prediction System Applications," 2023Second International Conference on Electronics and renewablesystems (ICEARS), Tuticorin, India, 2023, pp. 879-884, doi:10.1109/ICEARS56392.2023.10085051.

[4] Manzil, H.H.R., Manohar Naik, S. Android malware categorydetection using a novel feature vector-based machine learningmodel. Cybersecurity 6, 6 (2023). Https://doi.org/10.1186/s42400-023-00139-y.

[5] Wang, H., Singhal, A. & Liu, P. Tackling imbalanced data incybersecurity with transfer learning: a case with ROP payloaddetection. Cybersecurity 6, 2 (2023). Https://doi.org/10.1186/s42400-022-00135-8.

[6] Renganathan, V., Yurtsever, E., Ahmed, Q. Et al. Valet attack onprivacy: a cybersecurity threat in automotive Bluetooth infotainmentsystems. Cybersecurity 5, 30 (2022). Https://doi.org/10.1186/s42400-022-00132-x.

[7] Wohwe Sambo, D., Yenke, B.O., Förster, A. Et al. A new fuzzy logicapproach for reliable communications in wireless underground sensornetworks. Wireless Netw 28, 3275–3292 (2022).https://doi.org/10.1007/s11276-022-03008-7.

[8] Rahaman, S.M.A., Azharuddin, M. A cluster based charging schedulefor wireless rechargeable sensor networks using gravitational searchalgorithm. Wireless Netw 28, 3323–3336 (2022).https://doi.org/10.1007/s11276-022-03049-y.

[9] Kumar, Naween, Dash, Dinesh, & Kumar, Mukesh. (2021). Anefficient on-demand charging schedule method in rechargeable sensornetworks. Journal of Ambient Intelligence and humanizedcomputing, 12(7), 8041–8058

[10] Vishnu P Parandhaman, Analysis Techniques Artificial intelligence fordetection of Cyber Security Risks in acommunication and Information Security (2023)