Section A-Research Paper
ISSN 2063-5346

Cybersecurity and Human-Machine Interaction - Analysing Modern Threats and Opportunities in AI

Priyal Khapra
priyalkhapra@gmail.com

Article History: Received: 07.04.2023 Revised: 18.05.2023 Accepted: 10.06.2023

Abstract

Several attempts have been made in recent times to use Artificial Intelligence (AI) to secure wide range of cyber applications. To reduce the cybersecurity risks, these threats should be modelled with the use of smart UI design and evaluation and development of threat metrics. In every aspect of daily life, AI has been efficient to build a responsive security model with smart UI, which is missing in existing threat models to deliver efficiency and convenience. As UX and UI are constantly improving and providing more impressive solutions, the existing threat models don't have potential to predict upcoming threats. Hence, it is important to use machine learning models.

This gap can be filled by AI-powered user interface that uses basic principles of effective human-machine interaction interfaces. Developers can improve usability, flexibility, and relevance of interaction to build human and machine interaction with the help of smart UI. Baseline principles are needed to develop threat models to have fascinating UX and UI. Applying AI in designing UI to reduce cyber threats can save time required for critical design and ensure better solutions and applications of threat modelling.

Keywords: *UX, UI, AI, smart UI, human-machine interaction, cybersecurity, cyber threats, artificial intelligence*

1. Introduction

Cybersecurity is beyond social and technical matters and it should get top priority as it has changed the way businesses are conducted and government activities are performed (Veale & Brown, 2020). The over-dependency and complexity of technical system poses a significant threat to security engineers as infrastructure and devices ae connected in social and technical environment they work on. Without the control of system engineer, the use of "Application Program Interface (API)" significantly underrobes the system properties (Kostova et al., 20020). It has created various laws with several provisions to protect cybersecurity data and privacy laws operating since inception with more than 142 nations (Greenleaf & Cottier, 2020).

The provision of several concepts of security and data protection laws like threat modelling will be put into practice effectively and

efficiently when UX is given priority by integrating intelligence in UI. If user experience is perceived to effect highly on user interface design, it could be helpful to security experts to develop smart threat modelling tools to detect vulnerabilities and make users aware of related threats in every human-machine interaction. Human-machine interfaces perform 2-way interaction of records among machines and users to create UX and build a relation with the user (Dong et al., 2018).

It is obvious for the people to be proud of anything they make, no matter how complex or simple it is. Poor designs of human-machine interaction have been considered as variables causing anomalies and exposing the design to cyber criminals. Here are the things to do after following the practices and principles of human-machine interaction to make a user-specific design –

- To consider the aim of the user and obligations
- To consider the mode to process information and make decisions
- To keep the user above things and aware of system condition

Applying baseline principles properly leads to the level of trust on design for the users. For example, a user would not provide payment details if they don't trust a platform. Violation of these principles lead to hacking of the credit card. Table 1 illustrates the difference between effective and poor human-machine interface designs.

Table 1 – Difference between effective and poor human-machine interface

Effective human-machine interface	Poor human-machine interface
Consistent layout as per the operator's model	Represents "Piping and Instrumentation Drawing (PID)"
Depicts the status of the process and values in the form of information instead of numbers	Presents raw data as numbers like pressure, temperature, etc.
Shows "key performance indicators (KPI)" trends	Shows no trends
Low contrast and grey background	3D shadows and bright colors
Consistent color and visual coding	Color coding of vessel and piping elements
Low contrast letters in measurement units	Bright, large texts in measurement units

1.1 Background

UI gives the user the power to control hardware or software applications and interact with the hardware or software of any computing device. UI is available for both software and hardware devices. A remote control is a common example of UI in a hardware device. It has various buttons and a screen to show some basic details. However, the user can use buttons to command the hardware and what to perform. For example, using mouse and keyboard has its own UI to run a program. In the same way, a GUI is used to use a digital camera with on-screen menus. Being user-friendly is the aim of a successful UI, despite the program (Xu & Shah, 2020).

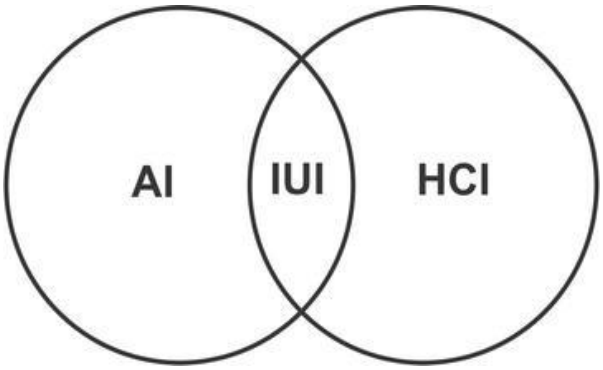
Though the UI is based on interfaces, the UX is centered on the user experience to interact with the system. Interaction is supposed to be bigger than interfaces as it promotes

communication between the device and the user. The users can face interactions with the help of interfaces. The UX has three key dimensions – products, users, and interactions. UX delivers an easy way to analyze interactions and their influences. The experience from the interaction with the product at a specific time is known as UX (Chen et al., 2019). It is a separate perception which comes with the anticipated use or use of a service or platform.

With AI, design focus in UI is known as smart UI design. AI is known to change the status quo and revolutionize industries. AI is widely used to provide details to the designers. An AI or "Intelligent Virtual Assistants (IVA)" is another example of IUI or "AI in UI design". Some of the common IVAs are Cortana, Alexa, and Chatbots. Usually, AI is applicable to UI designs on several channels interfacing between machines and humans, especially when it comes to model cyber threats. Channels like Google, Yahoo, and Bing and other search engines and content recommendation platforms like YouTube, Spotify, and Netflix are some of the common examples of IUI.

Some of the major challenges of IUI are thoughtful interactions and data privacy and they should be considered in design process for cyber threat modeling (Völkel et al., 2020). AI in UI should consider smart capabilities and incorporate AI in human-machine interaction. These interfaces are aimed to improve efficiency of HCI with user models, reasoning, domains, and media like VUI, GUI, and gesture interfaces (Bachmann et al., 2018). IUI is positioned somewhere between HCI and AI. The relationship between HCI and AI is depicted in Figure 1 while considering AI in UI.

Figure 1 – Relation between HCI, AI and IUI

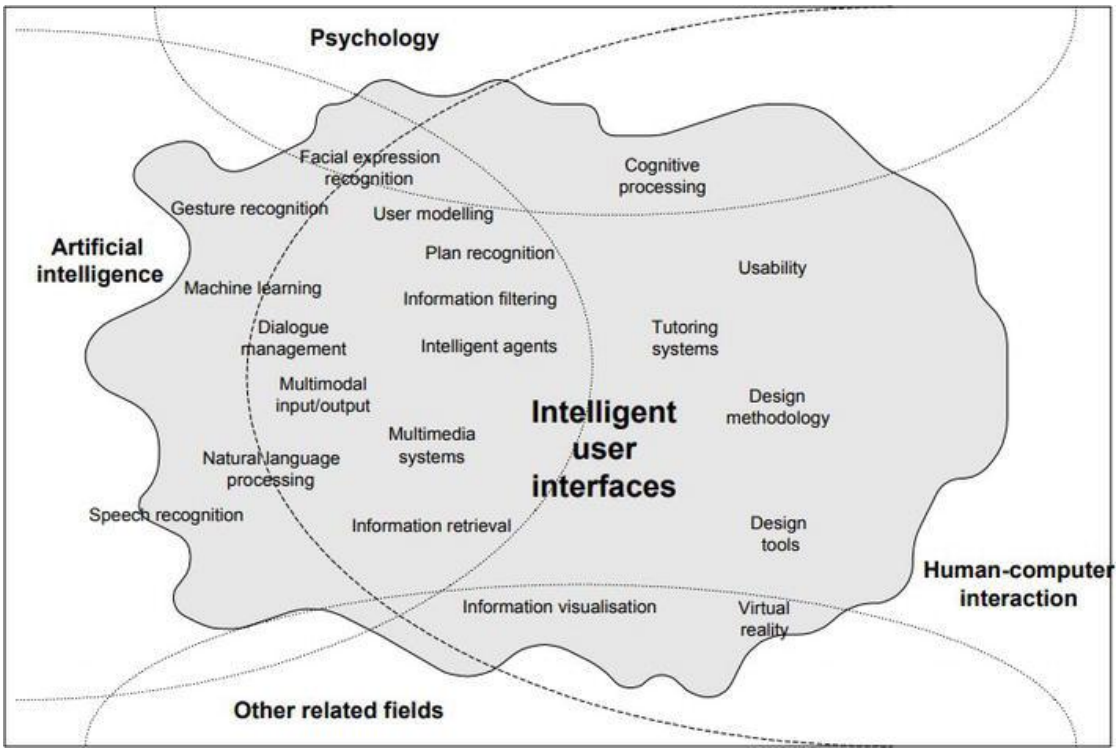


Source – Potluri et al. (2019); Sonntag et al. (2017)

Because of different models from various fields which affect user interfaces significantly, developing AI in UI is similar as disciplines like AI play a vital role in simulation to boost responsiveness. Software engineering enables defining formal language with unified approach of modelling, development Lifecyle and human-machine interaction to avail techniques and user experience to come up with usable interfaces (Cybulski&Horbiński, 2020). Along with it, several fields are there that still play a vital role in developing AI in UI (Figure 2).

ISSN 2063-5346

Figure 2 – Research Areas of Intelligent user interfaces



Source – Ehlert (2003)

2. Literature Reviews

Intelligent UI is supposed to improve human-machine interaction with novel communication approaches and by adapting the interface to the user with AI techniques (Ehlert, 2003). The concepts of IUI are supposed to intersect the domain of HCI and AI in intelligent UI (Eiband et al, 2019). It is known to automate the tasks to engage in threat assessment (Jaquero et al., 2008). Hence, the use of intelligence in UI will bring better control and monitoring of activities to improve cyber security and threat modeling.

Cyberattacks are increasing and getting more complex on regular basis, posing a lot of threat to private and public assets (EC-Council, 2020). Threat modelling techniques are employed in cybersecurity to control attacks over technical asset used by hackers. Threat modeling gives insight to evaluate risks, enable proactiveness, and prioritize mitigation (Gonzalez, 2020). Formal methods are supposed to be deep in evaluation of performance rather than traditional approaches (Akinsola et al., 2020). As cyberthreat is increasing widely, applying AI in cybersecurity is another major improvement in technology used by experts (EC-Council, 2020).

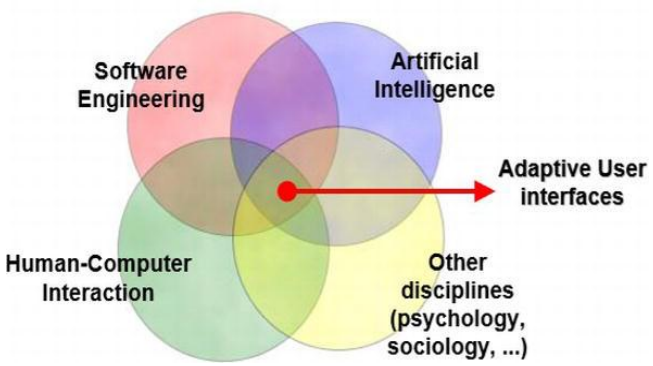
Some of the common examples of AI-based UIs are Alexa, Jarvis, IBM, Netflix, Nest Thermostat, iRobot Roomba, Spotify, etc. (Bader & Kaiser, 2019). When technological advancements are aimed to improve security over cyberthreats, UX should also have high priority in UI design for smooth workflow and high usability. As better system security must not be equivalent to worse user

ISSN 2063-5346

experience, balancing the security of software with user experience is an important factor to enhance UI and UX in cybersecurity, while designing UI on the basis of perception and reducing complexity of interaction in existing infrastructure (Strehlow, 2018).

User experience is affected by poor design of user interface which causes problem for the user to do desired actions (Jaye, 2019). Using AI plays a vital role in intelligent UI design to reduce problems which may take place with human-machine interaction. IUI is supposed to be a subset of research on human-machine interaction in order to use modern and smart technology. Using IUI can significantly improve communication between computers and users. This way, computers can easily understand more communications like hand gestures, body gestures, eye movements, sounds, and other motions (Ganapathy, 2017). Innovative solutions have been designed with this advanced interaction with humans through AI to address the barriers between computer and humans. Conversational AI is a common example. It is a modern platform for commonly-used helpdesk. It can analyze emotion of humans and control frustrations on the system as it routes to various channels to improve customer service (Kleber, 2018). It is possible to provide personalized, adaptive, and responsive services with IUI to ensure meeting specific users' needs even before they realize it. Technologies to offer personalized services can be developed with data mining, big data, and deep learning models to work with smart environments to avoid challenges which may take place due to human-machine interaction.

Figure 3 – Disciplines for developing AI in UI



Source – Jaquero et al. (2008)

Intelligence is applied in UI design to improve UX to enable effectiveness, efficiency, and satisfaction with various approaches. It can be made possible by acting or reasoning as per the set of models like dialog, user, tasks, domain, or speech. As given in Figure 3, various models from various disciplines help in developing AI in UI. AI plays a vital role in simulation of smart techniques to improve communication, unified processes, formal languages, and software engineering notations.

2.1 Research Gap

There have been several studies conducted on using AI techniques in different cybersecurity applications in recent years. Hence, this study adds the applications of AI in human-machine interaction to the existing knowledge and discusses various threats and opportunities for improvements in AI.

2.2 Research Question

- What are the modern threats in AI that organizations should consider?
- What are the opportunities in AI to improve human-machine interaction?

2.3 Research Objectives

- To understand the basic concepts of cybersecurity and modern threats in AI
- To explore the opportunities in AI to improve human-machine interaction

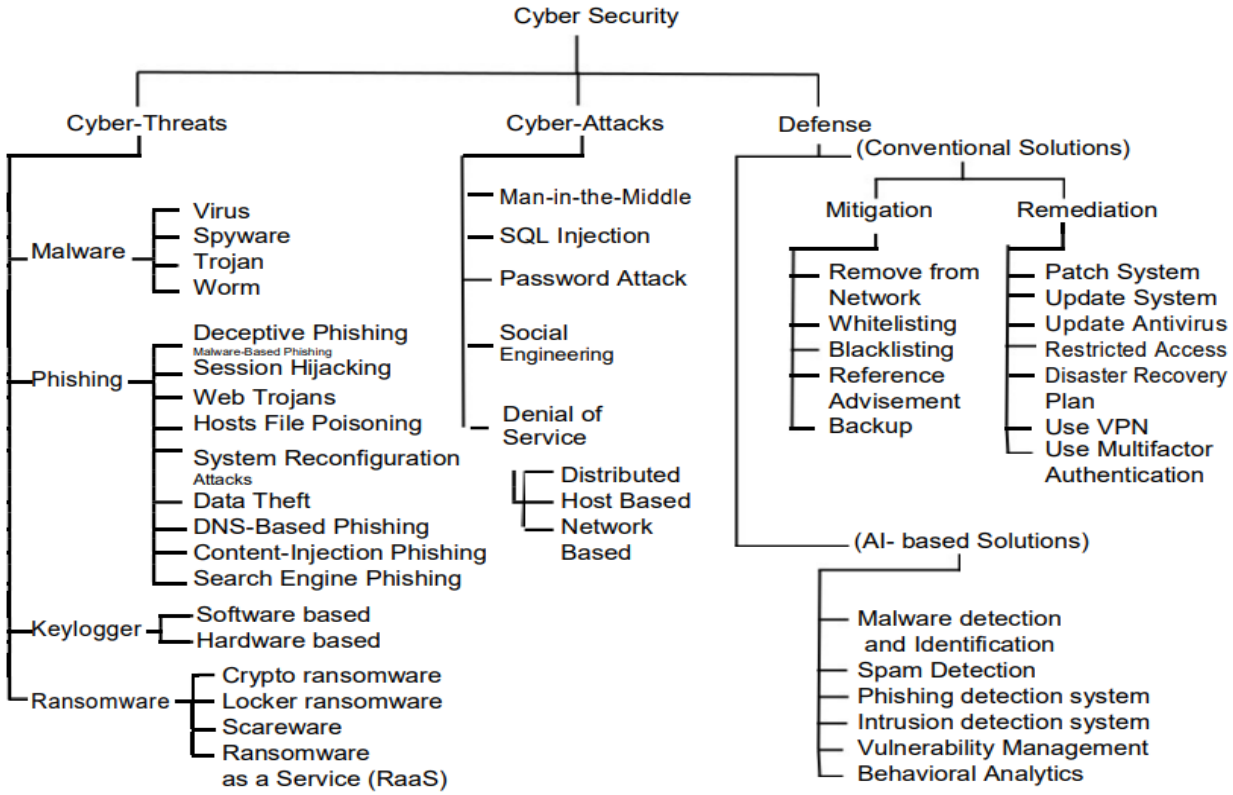
3. Research Methodology

In order to fulfill the above research objectives, this study surveys major AI approaches for cybersecurity applications and modern threats to consider when making AI in human-machine interaction. This study is based on secondary data gathered from various academic platforms like ACM Digital Library, Google Scholar, SpringerLink, IEEE Xplore, Science Direct, etc.

4. Analysis of Study

Cybersecurity is mainly aimed to protect sensitive data and important systems from cyber threats. There are different ways to protect company's infrastructure and data, such as malware detection, intrusion detection, and strict adherence to cybersecurity practices. Ransomware or malware is used to disrupt digital operations, affect information, and gain entry to data. There are different types of cyber threats like hackers, corporate spies, ransomware, etc. (Obotivere&Nwaezeigwe, 2020). The taxonomy of cybersecurity is illustrated in Figure 4. There are different reasons behind cyber-attacks but extreme caution must be maintained as personal and organization's data might be at risk.

Figure 4 – An illustration of Cybersecurity Taxonomy



Source – Chakraborty et al. (2022)

Section A-Research Paper
ISSN 2063-5346

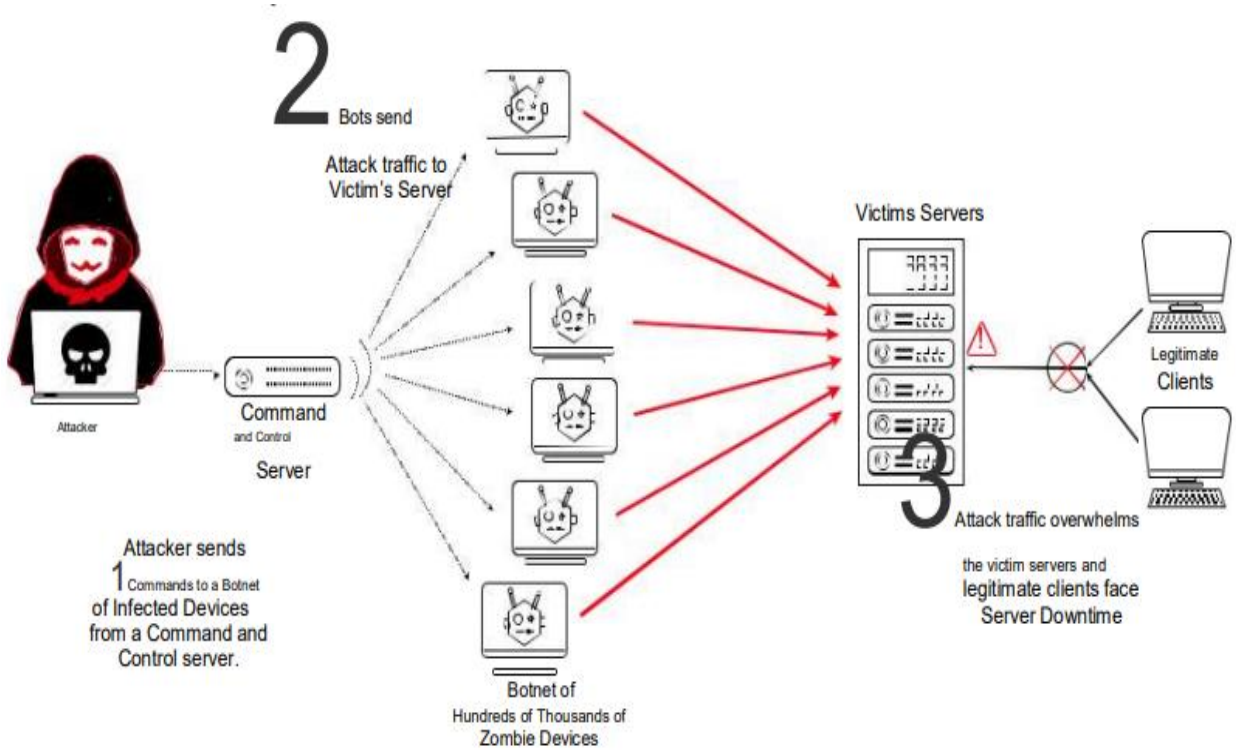
The proliferation of the internet has increased new cybersecurity concerns. Along with the threat to foreign governments and hackers, new challenges have been raised for protecting data from internal threats like insider trading and data breaches. Cybersecurity is an important concern for critical assets, sensitive data and infrastructures. So, there is a significant growth of cybersecurity professionals and they have been very vital to ensure robust and comprehensive defense mechanisms.

4.1. Modern Threats in AI that Organizations should Consider

4.1.1. Distributed Denial of Service (DDoS)

In this type of attack, the attacker uses various systems for flooding the traffic to the targeted system, so that the target cannot access their site or provide service. Volumetric attack is the most common DDoS attack, which floods overwhelming amount of information to the target. A botnet is used by the attacker to infect the systems with malware and control the same without owner's knowledge. Amplification/reflection and flooding attacks are two categories of volume attacks. Traffic is sent for exhausting processing capacity, bandwidth, or other resources in a flooding attack. Reflection/amplification attacks force victims by overloading their network with traffic or refuse access to specific resources with spam messages so that victims have to spend money (Furfaro et al., 2015; Zargar et al., 2013). Figure 5 illustrates the scenario of DDoS attack.

Figure 5 – Scenario of DDoS Attack

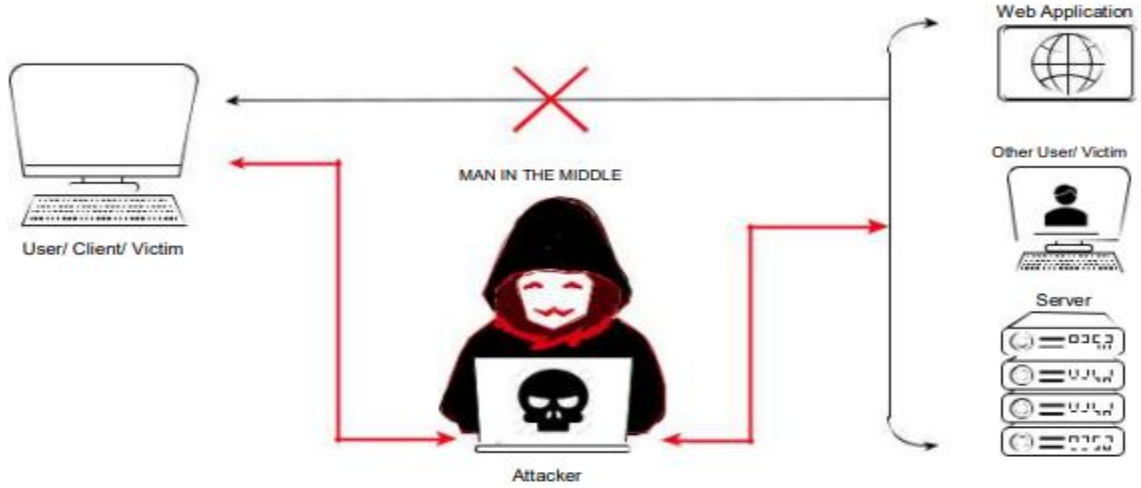


Source - Chakraborty et al. (2022)

4.1.2. Man in the Middle

In this type of attack, the perpetrator discretely alters or relays the communication between two systems by manipulating them in a way that they are communicating with each other. Then, the attacker reads all the messages between them and inject fake messages. The "Man in the Middle" attack acts much like espionage. A party feels that they are talking to another party directly, when an eavesdropper reads the messages of both of them. There are different ways to perform this attack. An attacker may be present between these parties without letting them know and relay messages. For example, they can access network of a telecom company and reroute calls or use public Wi-Fi. They may also access admin access on a remote network to control and intercept traffic among the server and client (Figure 6).

Figure 6 – An Illustration of Man in the Middle Attack



Source - Chakraborty et al. (2022)

4.1.3. SQL Injection

This kind of code injection attack simply targets security loophole in the database. It mainly attacks data-based applications. It is one of the most dangerous and common cyber-attacks. It can steal sensitive data from the database, delete or alter data, and even disrupt the services. It relies on dynamic nature of "Structured Query Language (SQL)" to circumvent access data and input validation that is quite inaccessible. Usually, SQL injection uses completely erroneous or malformed input in the command. For instance, "select password from users" may be sent rather than "inserting user and password of users" to capture the password in account table.

This way, database would perform the query and give the username and attacker can extract a list of usernames from which they extract user password. SQL injection may be useful for changing data in a table with lack of authorization. It may cause loss of availability and confidentiality for that table referencing the same.

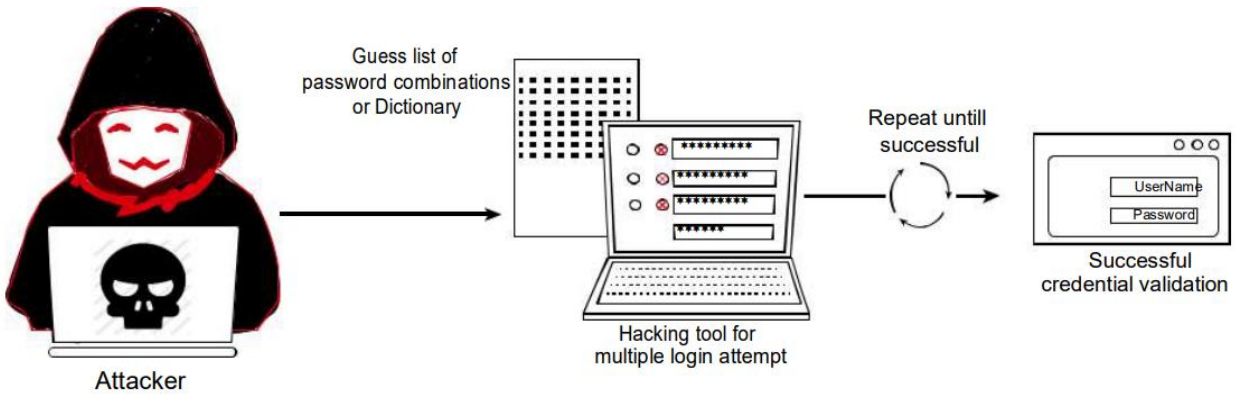
4.1.4. IoT Device Attacks

IoT or Internet of Things refers to a network of objects connected with software, electronic devices, and sensors so that they can exchange and gather data. There are several IoT networks and Intranet and Internet are most widely used. IoT is the new target for attackers. IoT devices are mainly targeted as they lack proper security. They are highly vulnerable to cyber-attacks. Since number of IoT devices keeps growing in this day and age, it is very vital to protect them from being compromised by cybercriminals and malicious actors. "Trusted Platform Module (TPM), Security Standards and IoT Device Software Architecture" are three major aspects of IoT security (Guan et al., 2017).

4.1.5. Password Attack

In this method, an attacker simply steals passwords outright or guesses passwords, mostly by hacking into the system. A "Man in the Middle" attack might be used by an attacker to intercept the password of a victim and using the same for accessing the account (Figure 7). It is very hard to crack a password but hackers can break into the system with modern cracking tactics and programs. Dictionary, brute force, and keylogging are three categories of password attack. In Brute Force, several attempts are made to guess passwords until the attacker gets into the system. In Dictionary, attackers try various combinations of dictionary words until they crack a password. In Keylogging, keystrokes are recorded to gather sensitive data, such as login. Users can use 2-factor authentication or avoid clicking suspected links from unauthorized sources in emails to prevent this kind of attack.

Figure 7 – An Illustration of Password Attack Process



Source - Chakraborty et al. (2022)

4.2. Opportunities in AI to Improve Human-Machine Interaction

Network security is the most common way to prevent cyberattacks, such as intrusion detection, firewall, encryption methods and using antivirus software. Though network security is helpful, it is not a solution in itself. A system cannot be 100% secure as vulnerabilities are always there for attackers to use. Cloud security is also used to protect

data in cloud like Microsoft Azure, Google Drive, or Amazon Web Services. When it comes to store huge amount of data in cloud, data security is usually provided with encryption. It can be made possible with public key infrastructure or similar technology.

A cybersecurity strategy must be created with policies, procedures, and techniques to mitigate the effect of security breaches. It consists of steps to reduce risks from data breaches, cyber-attacks and malicious program. There are various components of cybersecurity strategy. Risk assessment is one of those components to find out the chance that an event may take place and its possible consequences. Different types of vulnerabilities and threats are often considered by the risk assessment strategy. For example, IT department may find out whether company website might be hacked or if password is weak. They can develop mitigation strategies accordingly to reduce the impact or risk of cybersecurity events. Mitigation strategies can reduce the risks of those events. Encryption, patching, and security measures are widely used to mitigate risks.

Zero Trust policy is one of several policies, which is ideal for companies to build better control over various aspects of digital security in the company. It helps companies to handle access to sensitive data by looking at history or resources. With Zero Trust policy, one can maintain privacy and mitigate data breaches. It is applicable to data management and applications, mobile apps and apps owned by the company, email, cloud, storage services, infrastructure providers, or terminals of companies.

This policy is ideal for employees and companies to secure privacy of the users. It can create secure digital identity and make opportunities for access, when required. This policy refers to the method to ensure data security in which end user can access application or any other computer without assuming any trust. It is an approach to secure data for the end user to access any other system of the user or application without trust relationship. It can be made possible with "penetration of trusted computing" model which needs all devices and users to meet specific needs before getting connected to network sources. Zero trust approach is widely used to understand cybersecurity to create trustless computing protocols for connecting IoT.

5. Results

There are certain strategies to prevent cyber threats. This section discusses some of the effective measures based on the findings of this study.

- **Antivirus software and firewall**–A firewall is a hardware or software program which prevents infection of the computer system due to malicious programs or viruses. Firewalls are basically barriers between the network and the internet to provide better control to organizations over outgoing and incoming traffic. Antivirus software identifies and blocks any threats. It usually scans for virus on the devices or network and removes any potential malware. There are two ways modern antivirus can access systems. One way is

Section A-Research Paper
ISSN 2063-5346

doing a quick system scan through files and avoiding any possible harm to avoid any damage. It is the way to ensure that the system is safe. Full system scan is another method. The antivirus scans each and every file and removes any possible threat like malware or virus. However, it takes several hours as it scans all the files.

- **Verified extensions** – Using known browser extension can help prevent malicious and phishing attacks to steal data. It prevents the risk of adware and malware. For example, a Firefox extension "HTTPS Everywhere" can improve online security by forcing browser to use only websites with SSL encryption. Similarly, "Privacy Badger" prevents third-party sites from tracking online activity of the users automatically and "AdBlock Plus" removes ads while browsing.
- **VPNs** –It is highly effective for data protection. The data is encrypted and routed using an encrypted tunnel to prevent hackers. Some VPNs also have a kill switch to prevent all the traffic when connection is lost. It helps avoid any leakage of data using P2P connections in some cases. VPN locks the data and secures while passing through servers. So, hackers and ISPs cannot access data and browsing history. Final destination also remains secret of the outgoing traffic. In addition, IP address or computer is hidden behind the address offered by the VPN server to browse online anonymously.
- **Unique and strong passwords** – It is the obvious but most important tip to make it harder for anyone to guess the right password on various apps or websites. A strong password consists of both lowercase and uppercase letters, symbols, numbers, etc. in a unique fashion. One can use password manager to organize passwords to avoid forgetting the passwords for different apps or websites.
- **Security updates and patches** – It is not recommended to avoid security updates. These updates have security patches to prevent recent attacks on the device.

6. Conclusion

AI is capable enough to catch and prevent cyber threats using limited resources. Cyber-attacks are evolving rapidly in this day and age. Hence, humans might find it hard to stay ahead with latest technologies. However, AI can train itself with machine learning to analyze the threat quickly and provide best security without much effort and time. Analysts can focus on results with deep analysis and devise latest techniques to prevent cybercrime with machine learning. AI is not a complete solution. Even though AI techniques are getting more cost-effective in cybersecurity, they don't provide complete security. AI has its limitations. It is up to the human users to follow cybersecurity practices. Proper human training and supervision is needed for AI to improve results.

References

1. Potluri, V., Grindeland, T., Froehlich, J. E., &Mankoff, J. (2019). Ai-assisted ui design for blind and low-vision creators. In *the ASSETS'19 Workshop: AI Fairness for People with Disabilities*.

2. Sonntag, D., Zillner, S., van der Smagt, P., &Lörincz, A. (2017). Overview of the CPS for smart factories project: Deep learning, knowledge acquisition, anomaly detection and intelligent user interfaces. *Industrial Internet of Things: Cybermanufacturing Systems*, 487-504.
3. Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1-22.
4. Kostova, B., Gürses, S., &Troncoso, C. (2020). Privacy engineering meets software engineering. on the challenges of engineering privacy bydesign. *arXiv preprint arXiv:2007.08613*.
5. Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws.
6. Dong, W., Wang, Y., Zhou, Y., Bai, Y., Ju, Z., Guo, J., ... & Huang, Y. (2018). Soft human–machine interfaces: design, sensing and stimulation. *International Journal of Intelligent Robotics and Applications*, *2*, 313-338.
7. Xu, C., & Shah, S. (2020). Evaluating the User Experience. *Teaching with Digital Tools and Apps*.
8. Chen, W., Feng, G., Zhang, C., Liu, P., Ren, W., Cao, N., & Ding, J. (2019). Development and application of big data platform for garlic industry chain. *Computers, Materials & Continua*, *58*(1), 229.
9. Völkel, S. T., Schneegass, C., Eiband, M., &Buschek, D. (2020, March). What is" intelligent" in intelligent user interfaces? a meta-analysis of 25 years of IUI. In *Proceedings of the 25th international conference on intelligent user interfaces* (pp. 477-487).
10. Bachmann, D., Weichert, F., &Rinkenauer, G. (2018). Review of three-dimensional human-computer interaction with focus on the leap motion controller. *Sensors*, *18*(7), 2194.
11. Cybulski, P., &Horbiński, T. (2020). User experience in using graphical user interfaces of web maps. *ISPRS International Journal of Geo-Information*, *9*(7), 412.
12. Ehlert, P. (2003). Intelligent user interfaces: introduction and survey. *Delft University of Technology*.
13. Akinsola, J. E., Moruf, A., &Ayomikun, A. (2020). Performance evaluation of software using formal methods. *Global Journal of Computer Science and Technology*, *20*(C1), 17-23.
14. Gonzalez, C. (2020). 6 Threat Modeling Methodologies: Prioritize & Mitigate Threats. Retrieved from https://www.exabeam.com/information-security/threat-modeling/.
15. Eiband, M., Völkel, S. T., Buschek, D., Cook, S., & Hussmann, H. (2019, March). When people and algorithms meet: User-reported problems in intelligent everyday applications. In *Proceedings of the 24th international conference on intelligent user interfaces* (pp. 96-106).
16. Jaquero, V. L., Montero, F., Molina, J. P., &Gonz´ lez, P. (2008). Intelligent user interfaces: Past, present and future. In *Engineering the User Interface: From Research to Practice* (pp. 1-12). London: Springer London.

17. EC-Council (2020). How To Use Artificial Intelligence for Threat Intelligence.
18. Bader, V., & Kaiser, S. (2019). Algorithmic decision-making? The user interface and its role for human involvement in decisions supported by artificial intelligence. *Organization*, *26*(5), 655-672.
19. Strehlow, R. (2018). *Cyber Security Requires an Important Ingredient*. Strong UX.
20. Jaye, H. (2019). *What Is A User Interface, And What Are The Elements That Comprise one?*.UI Design.
21. Ganapathy B. (2017). How Artificial Intelligence is transforming Human-Computer Interaction, and its implications for Design.*LinkedIn*. Retrieved 31 January 2023, from https://www.linkedin.com/pulse/how-artificial-intelligence-transforming-interaction-its-ganapathy/.
22. Kleber, S. (2018). ways AI is getting more emotional. *Harvard Business Review*, *31*.
23. Jaquero, V. L., Montero, F., Molina, J. P., &Gonz´ lez, P. (2008). Intelligent user interfaces: Past, present and future. In *Engineering the User Interface: From Research to Practice* (pp. 1-12). London: Springer London.
24. Chakraborty, A., Biswas, A., & Khan, A. K. (2022). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *arXiv preprint arXiv:2209.13454*.
25. Obotivere, B. A., &Nwaezeigwe, A. O. (2020). Cyber Security Threats on the Internet and Possible Solutions. *IJARCCE*, *9*(9), 92-97.
26. Furfaro, A., Malena, G., Molina, L., & Parise, A. (2015, March). A simulation model for the analysis of DDOS amplification attacks. In *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)* (pp. 267-272). IEEE.
27. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, *15*(4), 2046-2069.
28. Guan, Z., Li, J., Wu, L., Zhang, Y., Wu, J., & Du, X. (2017). Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. *IEEE Internet of Things Journal*, *4*(6), 1934-1944.