**IT Technologies**

***A picture containing text, room, gambling house, vector graphics

Description automatically generated*Cyber Security**

***A person using a computer

Description automatically generated with low confidence Emre Altunsu***

***Current and Future Applications***

In contemporary times, protecting our personal data has become a prevalent concern in many aspects of life. The application of cyber security brought on by the need to preserve confidentiality has further compelled advancement in related fields. Instances of mass and targeted fraud, intrusion, spam, and cyber harassment have led to unthinkable losses in revenue, trust, and reputation for many large-scale organizations. As a result, large corporations have diverted a large scale of resources into mitigating such issues. The lead organization providing affordable, manageable, and fundamental security services for the past 20 years is IBM Security. IBM’s services have branched out in recent years, leading other organizations to form comparable products and services directed toward individual systems. Some examples include Norton Security, Malwarebytes and AVG, all of which provide basic support in malware prevention, data protection and restoration, ensuring users are not only protected from malicious activity, but to also provide assurance in events of large-scale data loss. Although present day services provide extensive cyber security coverage, the ‘potency’ of cyber-attacks are increasing exponentially to the point that implemented systems are becoming obsolete. Phishing schemes, APT attacks, spyware, targeted hacks have become more common throughout recent years, more notably since the start of the coronavirus pandemic beginning in early 2020. Intuitive solutions in countering malicious threats are being drafted and implemented each day. Artificial intelligence and machine learning advancements have improved in the early detection/prediction of current vulnerabilities and potential future threats. Implementing a ‘zero trust policy’ in many organizations have additionally reduced the risk of data breaches and network intrusion, as many as 70% of large-scale organizations have introduced this policy indefinitely to protect employees, client confidentiality as well as internal workplace data.

Further, a sizable portion of cyber security software developers and engineers are looking to introduce adaptive security processes in conjunction with various cyber security software’s, widely used in professional environments. The ‘Adaptive’ approach to cyber security involves the analysis of common behavioral tendencies of the user and cross checking with previously encountered threats in order for a highly sophisticated and complex architecturally relevant algorithm to be formed. This algorithm is highly reflective of Artificial intelligence in that it can predict potential threats and either execute required procedures in order mitigate the problem or provide a detailed report to relevant technical staff in which they can effectively compile a viable solution. Based on Paloaltos Networks list for Cybersecurity Automation, the correlation of data is critical in providing rapid solutions in identifying ‘unknown threats’ inclusive of previously unidentified; infected host systems. The concept of cyber security through automated systems and/or artificial intelligence has been up for further study due to potential flaws within secondary backchecking, target accuracy and most notably, unintentional data wiping which can prove extremely troublesome in elaborate/multi component database systems.

Although implementing previously mentioned cyber security systems/services are highly valued in both individual and cooperate settings, a deficiency in available technologies and knowledge is apparent. Applications in cybersecurity via intelligent systems require both skilled expertise understanding machine learning capabilities, programming recognizable features including the reasoning aspects of A.I such as problem solving, resource manipulation with reference to the target cybersecurity requirements and desired outcomes. A wider understanding around elements such as embedded hardware authentication (EHA) is vital in adding further user authentication abilities in respects to providing priority access for designated personnel and in software maintenance. Overall, contemporary technologies in cybersecurity applications are critical in ensuring data privacy, security, and authentication. Emerging technologies such as artificial intelligence, cloud-based systems/servers and various authentical techniques further extend cybersecurity capabilities by highlighting potential flaws or areas for improvement within pre-existing cybersecurity products and services

***What is the impact?***

Recent advancements in cybersecurity technologies have demonstrated that the majority of individuals who utilize computer systems; whether it be in a personal or organizational sense, heavily depend upon cybersecurity services and software. Recent developments in implementing automated cybersecurity systems have been showing extremely promising results. These automated systems will increase the users or organizations abilities to detect potential or immediate threats, identify its severity or potential impact on specific operations and quarantine them without the need for human intervention. This can heavily reduce the need for a cumbersome and time-consuming process with addition to increased workplace efficiency. Furthermore, current cybersecurity systems require increased maintenance and resource diversion. Replacing outdated systems with a self-contained and automated variant will undoubtably improve resource management capabilities and heavily alleviate workloads for technical support/analyst units.

Advanced technological developments in cybersecurity will considerably shift standard workplace practices and improve overall security and safety for many individuals. Large corporations such as Apple, Samsung and Windows follow a strict set of business rules, practices, and arrangements with respect to slight differences. The listed corporations store countless quantities of data some of which are extremely confidential. For this reason, companies heavily rely on various forms of cybersecurity including software, firewalls, and physical embedded hardware authentication elements. Although currently described as ‘sufficient’, cybersecurity threats are becoming more prevalent in recent years. Introducing improved forms of cybersecurity can substantially reduce the risk of data breaches or damaging leaks. Automated cybersecurity systems are being implemented in many industry settings, filtering through large server computers, network properties and cloud servers to identify threats and vanquish each with tactical precision.

Many current employment positions require a basic understanding of computer systems and internal functionalities. However, all most all businesses operate with a technical support team who are the most prone to be impacted by workplace change. Introducing automated or self-operating cybersecurity systems may lead to reduced work hours, less application acceptance or in potential cases permeate discharging of technical support members. Although, potential job prospects may be opened in the programming and maintenance operations for the automated cybersecurity systems.

***How will this affect you?***

On a regular basis, I utilize various forms of cybersecurity including: user authentication services, ISP, and IP hiders such as Nord VPN and smaller scale web browser extensions including Malwarebytes and privacy.com. The future of cybersecurity provides a sense of safety in that I feel assured that my confidential information and data remains safe in years to come. The use of automated cybersecurity systems and further improvements in threat detection will surely improve my digital as well as my physical wellbeing and safety. Although extremely confronting to some extent, having my files, passwords, confidential data, and search history monitored automatedly can elevate some stress when it comes to protecting personal information.

Improvements to the cybersecurity functionalities within my computer system will undoubtably prove to be a useful asset in a professional sense. Being able to keep track of potentially malicious websites, files or unauthorized access can improve your confidence when using the internet or your computing device in general. According to ZDNET, each year approximately “261 billion data records [are] being lost or stolen” every year. Having advanced forms of user authentication, password management and malware identification software can heavily reduce your chances of losing valuable and confidential information, also protecting your computer from being accessed by malicious hackers’ intent on ruining your digital status.

Friends and family are extremely important to me as they provide me with comfort and support in times of grief, sadness, or general discontent. Majority of my family is over the age of 40 and have difficulties understanding basic computer functionalities. Recently, one of grandparents fell victim to a fraud scheme which involved a scammer entering their computer and stealing their personal documentation. The lack of cybersecurity on their computer was a key factor in this occurring. The promising developments put forth by developers including automated file filtration systems and authentication services etc., provide hope to struggling elderly or inexperienced individuals in that they confidently use the internet without being afraid of potential scams, data loss or invasion of privacy