Figure 1: Source (FREEPIK)

ADVANCEMEMTS IN CYBERSECURITY

A look at the present and the into the future

ABSTRACT

In this research paper, we dive into some of the existing and upcoming technologies involved in the world of cybersecurity and analyze some practical applications of cybersecurity along with some ethical dilemmas.

Bagga & Harden

Advancements in Cybersecurity

Gracy Bagga

Garrett Harden

June 5, 2025

Saskatchewan Polytechnic

Table of Contents

Abstract

In today’s digital world, we use technology quite literally in all aspects of our lives. As a result of this reliance on the Internet and the Internet of Things (IoT), there is a significant need to safeguard our digital assets. This is why cybersecurity has become essential. To protect against the growing risks posed by malicious actors, every individual must have at least a basic understanding of cybersecurity, regardless of one's professional experience.

Thus, in this paper, we seek to offer clear and thorough insights into cybersecurity. Important cybersecurity technologies such as encryption, zero trust architecture, and blockchain-based security have been explained via real-world examples. By comparing complex concepts with relatable analogies, our intention is to captivate readers from all walks of life.

The study also looks at real-world uses for cybersecurity, showing how it affects almost every part of our lives, frequently even without our knowledge. Additionally, common cybersecurity problems and their fixes have been discussed. These practical applications help emphasize the importance of defensive mechanisms in the cyber world.

Further, ethical dilemmas in cybersecurity have also been discussed. And then, this report concludes by looking at new developments and future trends in cybersecurity. Some of them are blockchain's growing influence and quantum-safe encryption. Such developments are crucial to enter the next stage of cybersecurity and to stay future proof.

Introduction

In today's world, securing a product or service is equally important as its development. Cybercriminals often try to exploit vulnerabilities in softwares in order to jeopardize the confidentiality and integrity of user information. Such activities not only threaten a product's operation capabilities but also decrease user confidence in the product.

These cyberattacks can result in swift but extensive real-world consequences. In the 2016 cyberattack on Ukraine's power grid, attackers targeted the transmission of electricity and left almost one-fifth of the population without power. In fact, the ongoing confrontation between Russia and Ukraine has seen the re-surfacing of similar attacks. This highlights the continuous use of cyberwarfare as a strategic tactic (Cerf, 2024). More recently on March 10, 2025, millions of users were compromised in a matter of a few hours, when a hacker group launched a planned attack on X (Satter, 2025). These events highlight the dynamic nature and scale of cyber threats.

Therefore, it has become critically important to protect our assets wherever the internet is involved. Some of the cybersecurity measures are firewalls, encryption, endpoint security, antivirus software, and others. To identify any malware activities in real-time, network traffic is continuously administered. To thwart social engineering efforts, user and staff training, via social media ad campaigns or specially designed crash courses, is also essential.

Strong cybersecurity can ensure data privacy and security. This improves operational integrity and builds user confidence. Subsequently, investors' trust is strengthened which drives sustainable business growth and long-term revenue performance (Accenture, 2025).

Chapter 1: Technology Concepts and Reasoning

There is an increased demand to stay updated with the various technologies involved in cybersecurity, thanks to the rapidly evolving digital market. Considering the multitude of threats that are faced in the modern cyber scene, they cannot be singularly protected by a single line of defense.

Thus, to achieve a successful defense plan, an integration of several methodologies is often required so that there is a complete security perimeter around our assets. This could be analogous to how multiple defense systems were used to create “the Great Wall of China” which protected China for hundreds of years. In the following sections, we will explore fundamental cybersecurity technologies, beginning with firewalls.

Firewalls

Consider thinking about a military checkpoint to comprehend the purpose of firewalls in cybersecurity. Individuals must provide identity, be tracked, and be granted authority before they may access a secure military base. Likewise, a firewall serves as a checkpoint between two networks, usually the external internet and an internal network such as a company's infrastructure - their WANs or LANs. Based on pre-established safety guidelines (pre-coded logic flow), firewalls examine every incoming and outgoing network traffic and permit or prohibit it as necessary.

However, just as a military checkpoint alone cannot protect an entire base, where additional defense mechanisms such as surveillance systems, perimeter fencing, and access controls are required, a firewall by itself cannot protect against every possible threat. It works

well against unauthorized access through network traffic, but it is unable to stop strikes that get past the network perimeter, including malware sent via USB drives, phishing emails, or dangerous websites that users visit, among many others.

In essence, firewalls are coded to monitor and filter network traffic across various layers, such as application-layer interactions, transactions, outbound requests, and connection protocols. For increased protection, sophisticated systems may employ several firewall levels. However, despite all the above-mentioned benefits, firewalls do come with some limitations attached as well. Ransomware, viruses, worms, spyware, adware, trojans, phishing attempts, and pharming schemes are often designed so that they can easily bypass firewalls. These demand extra security measures including email filtering, endpoint security, anti-malware programs, and user awareness training (FortinetFirewall, 2025).

Anti-Virus / Anti-Malware Software

Anti-virus and anti-malware software are essential endpoint technologies that are designed to secure the devices at the user level. These softwares are installed directly on end-user devices, including laptops, desktops, and servers, to prevent malware from entering internally . Those internal attacks are often carried out through USB devices, software installations, file transfers, and other local access methods. While firewalls are deployed at the network's permitter access level, these softwares protect users from local attacks.

A useful analogy is airport security. At every terminal, security checks are performed before a passenger may board a flight. To find any prohibited or possibly hazardous materials, people are inspected, and their belongings are investigated. Further examination is carried out if an object is found to be questionable. Likewise, anti-virus/anti-malware software looks for

indications of malicious activity in all incoming and existing files and apps. To protect the system from adverse effects, the program notifies the user, isolates the file, and may even remove it if a threat is detected.

Key functions of these softwares include the following (Sophos, n.d.):

1. **Virus detection:** This process usually uses signature-based detection. All files entering the device and all applications being installed are scanned. The file characteristics and applications' behaviours are compared with a database of known threats. This comparison allows the opportunity to match file/program characteristics with those of known malware.
2. **Malware prevention:** These provide security in real-time continuous monitoring. Files are regularly scanned, programs' functionalities are observed, and network activities are monitored to thwart threats before any damage is done.
3. **Virus containment and removal:** The program quarantines or deletes compromised files as soon as it finds them to stop the infection from spreading throughout the network or system.
4. **Continuous Monitoring and Scanning:** Users may plan entire system scans to find latent or previously overlooked malware that was delivered through indirect or delayed pathways, even while real-time scanning guards against imminent threats.

Anti-virus softwares provided by TotalAV, McAfee, Norton, and Avast are some of the most popular ones. These are an essential component in a complete cybersecurity architecture, especially for endpoint security.

Encryption

The process of encryption is essentially of converting a readable data (plain text) into a format that is encoded and is unreadable. It is done with the help of encryption algorithms and a key to decode. The ciphertext can only be decrypted and returned to its original form by authorized individuals who possess the appropriate key. This guarantees that private data continues to remain private even if it is intercepted.

A simple analogy can be of adventure movies such as Jumanji where riddles are used as a form of encoded message. A person who already has decoded the riddle can act as the Key for the next person or the individual can try to use brute force and try different permutations and combinations to try and tackle the situation. Brute Force is usually the best buddy for hackers. Although hackers may try to use cryptanalysis or brute force to unlock encrypted information, it is important to understand that a well-designed encryption renders unauthorized decryption practically impossible.

Consider encoding the word "Hello" as "H1e1lll1o1", a very primitive kind of substitution, to provide a simple example. This example illustrates the fundamental idea, even if it is simplistic and risky by modern standards: the original message can only be recovered by someone who is aware of the encoding rule (remove the 1s).

Encryption is a fundamental cybersecurity technology that protects data while it's in transit and at rest. Some popular encryption techniques are as follows (FortinetEncryption, 2025):

1. **Symmetric encryption:** This encryption algorithm encrypts and decrypts data using a single shared secret key. It is perfect for sending large amounts of data and is

computationally efficient. However, since both parties need to have the key beforehand, safe key sharing is difficult. DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are examples of symmetric algorithms.

2. **Asymmetric encryption:** Contrary to symmetric encryption, two keys are involved in this encryption. A private key is used for decrypting data, and a public key is then used for encrypting it. Since the public key may be shared freely, secure key sharing is no longer necessary. Secure online communication (like HTTPS) makes extensive use of it.
3. **RSA (Rivest-Shamir-Adleman):** Though this algorithm is built on the principles of asymmetric encryption, there is one key difference. The difference is that the functionality of the private and public keys is interchangeable. If a private key is used for encryption, the public key can be used for decryption. Similarly, the opposite pair can also be used.
4. **End-to-End encryption:** In this algorithm, no middleman is involved. Data is encrypted on the sender's device and decrypted only on the receiver’s device. As a result, this prevents any third party, not even the service provider, from accessing the data. Currently, E2EE is recognized as the most secure way of encryption, with WhatsApp being its notable user.

To summarize, it must be noted that while some companies like to use already tested algorithms, others prefer to develop their own robust encryption algorithms from scratch. At the same time, some companies may opt to combine two or more existing algorithms. In the end, there is no perfect way to perform encryption. It all boils down to what the use case is.

Network Intrusion Detection (NID)

As the name suggests, the Network Intrusion Detection (NID) devices target unauthorized activities in network traffic. All the data coming in and leaving the network is monitored and scanned. If any possible intrusion is detected, the system administrators are notified immediately so that the damages can be contained. NIDs are preventive in nature, meaning they do not necessarily revoke access, they rather alert the system administrators.

Intrusion Detection Systems (IDS), which are software programs installed in business infrastructures to identify suspicious behaviours and security breaches, are the foundation of NID. To continuously monitor and analyze network data for abnormalities or known threat signatures, intrusion detection systems (IDS) are usually placed at strategic locations (FortinetIDS, 2025).

A variety of IDS solutions are available that can be employed based on the use case. In some cases, even a combination of some of them is utilized to secure the fortress. Some of these technologies have been discussed below (FortinetIDS, 2025):

1. **NIDS (Network-based IDS):** Network-based intrusion detection systems, or NIDS, keep an eye on network activity throughout the whole infrastructure to identify threats from the external networks instantly.
2. **HIDS (Host-based IDS):** Installed on specific devices, HIDS (Host-based IDS) keeps an eye on internal operations and identifies threats that could evade NIDS.
3. **SIDS (Signature-based IDS):** SIDS (Signature-based IDS) identifies known risks by comparing traffic anomalies to a database of harmful signatures.

4. **VMIDS (Virtual Machine IDS):** VMIDS (Virtual Machine IDS) keeps watch on virtual networks and searches for irregularities in virtual machines that conventional IDS solutions could miss.

Artificial Intelligence and Machine Learning (AI/ML)

With the extensive integration of Artificial Intelligence (AI) across various fields, the application of AI in cybersecurity has shown great potential. The Machine Learning (ML) subset of AI is its key strength in this field as it allows systems to learn from data and get better over time without the need for explicit programming.

Large volumes of historical threat data may be used to train machine learning models in cybersecurity to simulate the actions of human analysts. Following that, these models can assess firewall integrity, monitor network traffic, evaluate file behaviour, and identify anomalies instantly. Signature-based threat detection is one of the most successful use cases, in which machine learning models identify patterns in files or network activity that match the signatures of known threats. That being said, Signature databases are also used in traditional systems, but machine learning offers a significant advantage: flexibility. The system maintains its internal datasets and improves its detection logic when it comes across new suspicious behaviours while in operation. The accuracy and responsiveness of threat detection are greatly improved by this dynamic learning process (Miller, 2024).

Furthermore, AI has become crucial for phishing detection as well. Machine learning algorithms can identify phishing trends by examining the text of incoming emails. This allows them to automatically flag or quarantine emails before they are viewed by the user, which lowers the possibility of human errors. Moreover, AI also makes post-incident operations more efficient.

After a cyberattack, it can automatically create incident reports, saving analysts a significant amount of time. This frees up cybersecurity experts to work on more complex tasks like improving model accuracy, honing firewall rules, and strengthening the overall security (SailPoint, 2025).

Zero Trust Architecture

Zero Trust Architecture (ZTA), as its name implies, is founded on the concept of "never trust, always verify." It is constantly assumed that any attempt to access the system might be dangerous. Thus, all internal and external activities must be constantly monitored.

It is important to note that the cyber attack surface has significantly increased in modern times due to the increased usage of the Internet of Things, such as desktops, smartphones, etcetera. Thus, stricter and more proactive security methods are required to protect ourselves.

Zero Trust Architecture, which was first introduced in 2010, assumes that every endpoint is susceptible to compromise to enforce a proactive security posture. As a result, ZTA involves the utilization of a mix of technologies. They are as follows (PaloaltoZTA, 2025):

1. Identity and Access Management (IAM)
2. Multi-factor Authentication (MFA)
3. Micro-segmentation
4. Encryption
5. Real-time monitoring

The key concepts of Zero Trust Architecture comprise 3 principles of zero trust, 5 pillars of zero trust, and Zero Trust Network Access (ZTNA). These key concepts are discussed below:

The 3 Principles of Zero Trust

The following are the three principles of zero trust architecture (IBMZeroTrust, 2024):

Continuous monitoring and validation

Considering the impression that an attack might happen at any time, network activity is continuously monitored. Users and devices need to re-authenticate consistently, not just when they connect for the first time.

The principle of least privilege

The concept is that the users are given highly contextual and temporary access, enough for them to perform their tasks. When access is no longer required, it is revoked immediately. A common implementation would be RBAC – Role-Based Access Control.

Assume breach

This principle basically presumes that there are going to be hacking attempts. It is recommended that businesses do periodic internal penetration testing to proactively detect and patch vulnerabilities.

The 5 Pillars of Zero Trust

The following are the 5 pillars of the zero-trust principle (IBMZeroTrust, 2024) :

Identity

Each user entering the network must be registered and authenticated. Access tokens are issued and periodically verified. Common tools used for identification are Identity and Access Management systems (IAM), Multi-factor authentication (MFA), or Single Sign-Ons (SSO).

Devices

Each device on the network must be fully registered and be compliant with the Zero Trust policies. A clear inventory of all the hardware accessing the network is a must for this purpose. No access must be issued to any random device trying to access the network.

Networks

Instead of utilizing traditional network segmentation, micro-segmentation is employed. Resources are shared among smaller chunks of the network called the subnetworks. This allows the opportunity to contain the blast radius should there ever be a breach.

Applications and workloads

In the zero-trust architecture, Applications and APIs are presumed untrustworthy. Instead of one-time validations during an application's initial access or when an API is called, a continuous authentication model is put into use to ensure continuous authentication.

Data

Encryption is the key to this pillar. All the data, whether it be at rest or in transit or in use must be always encrypted.

Zero Trust Network Access (ZTNA) :

One of the key technologies in ZTA is Zero Trust Network Access (ZTNA). Because ZTNA only allows access to resources that a user is permitted to use, it is more secure even if it enables remote access in a manner like that of a VPN. The attack surface is much decreased since it does not grant access to the full network. The most common use case for ZTNA is Work from Home employees. Many service providers such as CISCO and FortiClient offer such services (IBMZeroTrust, 2024).

Blockchain

Blockchain-based cybersecurity is a relatively new concept. It is primarily utilized in financial institutions as of now. Cryptocurrencies like Bitcoin and Ethereum continue to be the top contenders in this race when compared to traditional banking security.

Blockchain security is based on two fundamental principles of decentralization and cryptography. Its basic structure follows the principles of a linked list in programming. In such a linked data structure, each data block called a transaction in this instance, is cryptographically (meaning data is encoded) connected to the one before it by using a unique set of rules. As a result, once a transaction is recorded, it cannot be tampered with without impacting the entire network, creating a tamper-proof chain of blocks. Data integrity is consequently strengthened by this block styled data (think of it as a chain-link fence) which also makes unauthorized alterations nearly impossible.

Utilizing the concept of Cryptography, all transactions are encoded using cryptographic hash functions. These hash functions are extremely difficult to reverse-engineer. Any small alteration can result in a completely different hash function, alerting a cyber security guard of a potential breach. For authorized parties to be able to decode the data, a private key is issued for decryption. Only parties with such keys can create or alter data. This is often seen in cryptocurrency transactions when a user goes to deposit or withdraw Bitcoin money to their conventional accounts.

Furthermore, Blockchain also uses the concept of decentralization. The concept of decentralization involves dispersing the data among several nodes. This is a stark comparison to the traditional allocation of data to a central server. Thus, this breakdown of the network

minimizes the risk of failure of a single point in the network, and it also makes it incredibly hard for hackers to gain access to the entire network. Consequent to this dispersed node architecture, Decentralization allows an opportunity to minimize the radius of breach if there is ever one. Moreover, decentralization also prevents insider attacks as a breach from inside would demand a coordinated effort of several insiders, which practically makes it quite a daunting task (Pehar, 2024).

Let us analyze the pros and cons of blockchain cybersecurity in the following table (Herzberg, 2017) :

	Pros	Cons
1.	**Decentralisation**: Storing data across several nodes, as opposed to a central network, ensuring network resilience.	**Data Loss**: Risk of data being irrecoverable in case the user loses the private key of decryption.
2.	**Data Integrity**: All transactions are digitally stamped making transaction tracking easy.	**Storage Limitations**: One data block can contain at most 1 Mb of data with a blockchain allowing only 7 transactions per second.
3.	**Confidentiality**: Network users' confidentiality is ensured due to public key cryptography to authenticate users and encrypt transactions.	**Operational Expenses**: High Operational Costs due to high computational abilities requirements.

Chapter 2: Practical Applications

Our dependence on smart appliances keeps on increasing exponentially with each passing year. With increased exposure to cyber attacks, cybersecurity has become a key factor in the development of new softwares. The reason this is important is because a special emphasis on cybersecurity ensures protection of user data and digital assets. Here are some significant real-world uses for cybersecurity in daily life:

1. **Protecting Personal Information:** To prevent unauthorized access, user's personal information must always be handled securely. In our daily lives, we often come across scenarios when we must submit online forms. They could be some registration forms, billing forms when doing a checkout on an e-business website, or using login credentials to sign in. Thus, these interactions with online forms can result in data breaches and these breaches can result in identity theft, extortion, and impersonation. To prevent these crimes, modern systems use secure communication protocols like HTTPS for all databases read/write operations and encryptions (like hashing sensitive data) (GGCybersecurityApplications, 2025).
2. **Safe Internet browsing:** Malicious websites that mislead users that their device is infected or claim that they have "won a prize" are frequently encountered by users. These are quite common malware and phishing campaigns. As a result, multiple technologies such as firewalls, secure DNS filtering, anti-malware software, and browser-based threat detection are often used to provide users with a secure and smooth internet experience (GGCybersecurityApplications, 2025).

3. **Internet of Things:** The increased household reliance on smart appliances has made IoT cybersecurity quite important. These Wi-Fi connected devices are prone to cyber attacks if not adequately protected. To block unauthorized access and ensure a smooth user experience, companies often employ secure cyber practices such as regularly issuing firmware updates and equipping devices with device-level encryption. Further, users are also urged to create strong passwords and update them on a frequent basis, be it quarterly or annually (GGCybersecurityApplications, 2025).
4. **Email Security:** Phishing is one of the most common cyber attacks. Cybercriminals often create convincing emails. Such emails can trick users into downloading corrupted files or clicking on links that can potentially install malware on their devices. To thwart such threats, modern email security systems use technologies such as Spam filters and sender verification systems. These technologies help identify suspicious behaviour, prevent harmful content from entering your system, and reduce the risk of data breaches (GGCybersecurityApplications, 2025).
5. **Secure Work-from-Home Environments:** Since the COVID-19 epidemic, working remotely has become quite common. Although WFM provides users flexibility, it also puts enterprises and people at risk for cyber threats since personal home networks usually lack enterprise-grade security. The attack surface may be significantly decreased and organizational integrity preserved by putting secure procedures into place, such as employing VPNs, working only on company-issued devices, turning on endpoint protection, and implementing stringent access restrictions (GGCybersecurityApplications, 2025).

Although the examples above illustrate important domains in which cybersecurity is essential, the fundamental idea is universal: technology is insufficient on its own. It is essential to raise cybersecurity awareness because most successful cyberattacks often target human flaws and not technological flaws. Even basic awareness courses can enable people to identify dangers. The ecosystem becomes more robust once the users become more aware.

Chapter 3: Existing Problems and Solutions

The current cyber-security landscape is turbulent at best. With the ever-growing power and presence of AI technologies, both cyber-threats and cyber-security are entering currently unknown territory. In an article on the World Economic Forum website, the current threats in cyber-security are broken down into six key concerns: supply chain concerns, geopolitical tensions, AI adoption risks, generative AI and cybercrime, regulatory challenges, and a cyber talent shortage (Joshi, 2025).

Cyber-security is a concern at all levels and in every aspect of an organization these days. If attackers are not able to damage an organization directly, that does not mean that the organization is completely secure. Shipment tracking and scheduling are handled by virtual systems just as much as inventory and financial information are. As stated in the article, The cyber threats to watch in 2025, and other cybersecurity news to know this month, “54% of large organizations cite supply chain challenges as the biggest barrier to cyber resilience, driven by complexity and lack of visibility into suppliers' security” (Joshi, 2025). Transparency among business partners, particularly between suppliers and consumers, is just one change that will have to be implemented into common business practices as more and more of the world is moved into digital spaces.

The relationships between countries always have an impact on international security. As the world becomes more and more globalized, new challenges are arising in every field of business. The geopolitical state of the world has always affected these international relations and will continue to do so. The current conflicts of the world are no different, many malicious actors are coming out of the woodwork these days, trying to damage and interrupt the economy and

livelihoods of rival nations and organizations. In the article mentioned earlier, it is stated that "[a]lmost 60% of organizations say geopolitical issues affect their cybersecurity strategy, with CEOs concerned about cyber espionage and IP theft, and cyber leaders focused on disruption of operations" (Joshi, 2025). When two nations desire to bring each other down, there are no fields of battle that will not be tread on. If political rivalries result in the disruption of the global economy, then these conflicts do indeed hurt us all and will need to soon become something of the past.

With how new AI technologies are, many organizations will find themselves ill-prepared to implement and utilize these powerful tools. Those businesses who, for one reason or another, are not able to adapt their operations to the growing use of AI technologies in every field of work and area of life will find themselves falling behind in the extreme-paced economic climate that we find ourselves in today. This is majorly important, as "[d]espite growing reliance on AI for cybersecurity, many organizations lack processes to properly assess the security of AI tools before deployment, creating a gap in managing associated risks" (Joshi, 2025). Going forward, risk management and change management will have to keep up with technology's ever-increasing pace of development if we want to remain the masters of these tools that we use.

To continue slightly from my previous point, the abilities of AI technologies are currently being both overstated and underestimated. Without a doubt, AI technologies will change every aspect of our daily lives at some point, but most likely that time is still ways away. Regardless, people are acting as quickly as they can to get ahead of the curve and not be left behind in the wake of increasing AI technology. In the meantime, though, "[a]lmost three-quarters of organizations report rising cyber risks, with generative AI fuelling more sophisticated social engineering and ransomware attacks; 42% saw an uptick in phishing incidents" (Joshi, 2025). So,

just as much as AI is increasing work efficiency in the white market, AI is also increasing the efficiency of malicious black-market businesses that seek to consume the assets of those who cannot defend themselves. It will be the duty of every citizen to be vigilant to malicious market activities.

Chapter 4: Ethical Dilemmas

One of the biggest concerns of modern technology is that of privacy. Since the internet has become commonplace and the need for surveillance has continued to increase year after year, so too have the concerns of people who fear being caught in the crossfire of modern surveillance. This is expressed well by an article written for the Pew Research Center which starts, "[i]n an era where every click, tap or keystroke leaves a digital trail, Americans remain uneasy and uncertain about their personal data and feel they have little control over how it's used" (Mcclain, Faverio, Anderson, & Park, 2023). In this part of the paper, I will discuss how emerging technologies are presenting new and increasing concerns in the tech field.

A big source of concern for the common citizen is the lack of transparency from organizations regarding how collected data is used. As the previously mentioned article goes on to say, "[t]he public increasingly says they don't understand what companies are doing with their data. Some 67% say they understand little to nothing about what companies are doing with their personal data, up from 59%" (Mcclain, Faverio, Anderson, & Park, 2023). There is a good reason for this concern. Between inappropriate personal data finding its way into AI training models and the ever-increasing exposure to the world the common child is experiencing—raising concerns from parents about their safety—the concern is reasonable. As stated in the article, "[w]e've studied Americans' views on data privacy for years. The topic remains in the national spotlight today, and it's particularly relevant given the policy debates ranging from regulating AI to protecting kids on social media. But these are far from abstract concepts. They play out in the day-to-day lives of Americans in the passwords they choose, the privacy policies they agree to and the tactics they take – or not – to secure their personal information" (Mcclain, Faverio,

Anderson, & Park, 2023). It strikes me that it would be unreasonable to expect every individual who uses the internet, regardless of interest or knowledge, to be completely safe and secure with their private information given the natural inclination towards trust most people experience. The first step to making data collection more ethical is to implement basic policies that incentivize the transparency of organizations' data collection and handling for those whose data is being collected and in an easily understandable format for those affected.

A major contributor to the ethical dilemmas that are currently being faced in the tech industry is the rapid development and adoption of Large Language Model technologies in every industry. The mass deployment of a still rapidly developing technology presents many ethical and practical concerns that are being felt by the common citizen. As the Pew article states, "[a]s AI raises new frontiers in how people's data is being used, unease is high. Among those who've heard about AI, 70% have little to no trust in companies to make responsible decisions about how they use it in their products. And about eight-in-ten of those familiar with AI say its use by companies will lead to people's personal information being used in ways they won't be comfortable with (81%) or that weren't originally intended (80%)" (Mcclain, Faverio, Anderson, & Park, 2023). This should be a major point of focus when drafting the above-mentioned basic policies for data transparency since information collected for AI training models will not only be used for marketing but will be integrated into the language models that are being developed right now, and that same model with the private information integrated within it could be used for decades to come. People should have a right to know if these AI models have been trained on data collected from them, as well as what this data is and what the intended purpose of the AI model using said data is. Without data transparency, there can be no trust between organizations and their clients or users.

Chapter 5: Future Advancements

Like any other technical development, enhanced cybersecurity technologies are being employed by both the Samaritan side and the Nemesis side. For instance, while Artificial Intelligence (AI) can detect phishing or social engineering attacks and filter spam, it can also be used by attackers to create more realistic phishing emails. Similarly, people talk about using Machine Learning's adaptive behaviour as a defense; however, it must be considered that attackers can also use it to repeatedly try to find and exploit vulnerabilities more precisely.

It is important to recognize that subject to our increased dependence on IoT devices, and the internet in general, the cyber threat landscape keeps on evolving rapidly. Thus, to remain ahead of any future dangers, it is crucial to invest in research and development of emerging cyber technologies.

We will discuss the future of cybersecurity below – what the future entails, how we can include upcoming technologies, and make better use of existing technologies.

AI-Driven Adaptive Authentication

In the future, beyond spotting harmful software or phishing emails, AI and ML will play a key role in adaptive authentication. This method, sometimes also referred to as biometric-based security or behavioural authentication, tracks a user's actions in real-time while they attempt to authenticate. Access is allowed if the behaviour is consistent with the user's past patterns such as login location, IP address involved, etcetera. However, further verification (such as multi-factor authentication) will be triggered if an abnormality is detected.

The best use case for such measures would be corporate settings where access patterns are predictable and any deviations might be signs of a potential breach (Effect, 2025).

Zero Trust Architecture Expansion

The wider adoption of Zero Trust Architecture (ZTA) is still a work in progress, even though it is already gaining traction. The ZTA concept has become increasingly crucial in the hyperconnected worlds of today. Many businesses are still not utilizing ZTA to its full potential. An article by Ec-Council University cites a report by Cisco which notes that “nearly 86.5% of organizations have begun embracing zero-trust security, but many still have a long way to go” (University, 2025).

In the upcoming years, raising awareness and streamlining ZTA implementation frameworks will be essential. As the core technologies of ZTA such as micro-segmentation, continuous monitoring, and others keep on improving, ZTA will keep becoming more commercialized and it will become easier to adopt it at the retail level.

Blockchain Advancements

Blockchain will continue to prove to be a technology for safe and unchangeable transactions in the financial sector due to its fundamental cores of decentralization and encryption. In fact, amid growing geopolitical tensions and worries about conventional currencies in 2025, investors have been observed increasingly using cryptocurrencies as hedges along with assets such as gold and silver. This can be proved by a jump in bitcoin valuation from CAD 105,766 on April 9, 2025, to CAD 154,768 on May 22, 2025. Crypto assets are being widely adopted by financial enterprises because of this.

According to Globe and Mail, “In 2025, Bitcoin has seen some serious institutional buy-in. Strategy (formerly MicroStrategy) (MSTR)now holds over 538,000 BTC, nearly $47 billion worth. Metaplanet (JP:3350) is close behind, aiming to hit 21,000 BTC by 2026. Even the State of Wisconsin’s pension fund put $160 million into spot Bitcoin ETFs.” (Tipranks, 2025).

Strong blockchain-based security infrastructure becomes increasingly crucial as the popularity of cryptocurrencies grows. For high-value financial systems to manage higher transaction volumes and guarantee data integrity, blockchain technology must advance and corporations must keep exploring the path of blockchain-based cybersecurity.

Quantum Computing and Post-Quantum Cryptography

Nowadays, quantum computing is no longer a distant dream. Quantum businesses like PsiQuantum are receiving active investment from IT behemoths like Nvidia. As per a report by Reuters on May 18, 2025, “Nvidia (NVDA.O), opens new tab is in advanced talks to invest in quantum computing startup PsiQuantum, The Information reported on Sunday.” (Reuters, 2025).

The reason we need to worry about this topic is because traditional encryption techniques like RSA and ECC could potentially be compromised by quantum computers, bringing secure communications from today at a serious security risk. Unless cybersecurity experts dive into quantum-safe encryption standards beforehand, this poses an impending security threat. Henceforth, to maintain resilience in the context of future quantum threats, governments and organizations must initiate the transition to Post-Quantum Cryptography as soon as possible (University, 2025).

In essence, cyber threats will continue to evolve with the advancements in technology; however, the defense of our cyber assets depends on our ability to quickly adjust our course

depending on the demands of the situation and potentially develop new solutions to the new problems.

Conclusion

To wrap things up, it is clear that cybersecurity is no longer a niche concern but rather it is something that touches nearly every part of our daily lives. The tech we use, the systems businesses rely on, and even the choices governments make all affect how we understand and manage security in digital spaces. As we have seen, the core concepts behind these technologies are not always simple but taking the time to understand how and why they work the way that they do is a big part of staying prepared in a world that does not seem to be slowing down any time soon.

Throughout this paper, we have talked about some of the real-world ways cybersecurity affects us, from how companies try to protect supply chains, to how AI is being used both to defend and to attack. These are not just hypothetical issues anymore. They are problems we are facing today, and they are only going to become more common as technology continues to grow. While there are solutions out there, the reality is that many organizations are still behind where they should be. Whether it is not having enough skilled workers or not fully understanding the tools they are using, there is plenty of catching up still to do.

Maybe the most important point is that every risk we take with new technology comes with real ethical concerns. People have a right to demand transparency towards the use of their personal data. They deserve to feel safe using the technology that surrounds them. To become future proof, we are going to need to ask better questions and demand clearer answers. We must ensure the tools that we are building today will serve everyone and not just those in control of the data. There is still a lot of work to be done, but if we can keep these ideas in focus, we have a real chance at building something awesome.

References

Accenture. (2025). *What is cybersecurity?* Retrieved from Accenture: https://www.accenture.com/ca-en/insights/cyber-security-index

Cerf, E. (2024, 05 17). *Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world*. Retrieved from News: https://news.ucsc.edu/2024/05/ukraine-cybersecurity/

Effect, F. (2025, 02 03). *What is the future of cybersecurity?* Retrieved from Field Effect: https://fieldeffect.com/blog/what-is-the-future-of-cyber-security

FortinetEncryption. (2025). *What Is Encryption?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/encryption

FortinetFirewall. (2025). *Firewall Definition*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/what-does-a-firewall-do#:~:text=Basically%2C%20a%20firewall%20is%20a,to%20a%20more%20secure%20environment.

FortinetIDS. (2025). *What Is An Intrusion Detection System (IDS)?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

GGCybersecurityApplications. (2025, 04 08). *Applications of Cybersecurity*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/applications-of-cybersecurity/

Herzberg, C. (2017, 09 17). *Cybersecurity via blockchain: the pros and cons*. Retrieved from Technology Record: https://www.technologyrecord.com/article/cybersecurity-via-blockchain-the-pros-and-cons

IBMZeroTrust. (2024, 06 20). *What is zero trust?* Retrieved from IBM: https://www.ibm.com/think/topics/zero-trust

Joshi, A. (2025, 03 21). *The cyber threats to watch in 2025, and other cybersecurity news to know this month*. Retrieved from World Economic Forum: https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/

Mcclain, C., Faverio, M., Anderson, M., & Park, E. (2023, 10 18). *How Americans View Data Privacy*. Retrieved from Pew Research Center: https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Miller, S. (2024, 10 10). *The future of machine learning in cybersecurity*. Retrieved from Infosec: https://www.infosecinstitute.com/resources/machine-learning-and-ai/the-future-of-machine-learning-in-cybersecurity/

PaloaltoZTA. (2025). *What is Zero Trust Architecture (ZTA)?* Retrieved from Paloalto Networks: https://www.paloaltonetworks.ca/cyberpedia/what-is-a-zero-trust-architecture

Pehar, D. (2024, 01 17). *How Blockchain Revolutionizes Data Integrity And Cybersecurity*. Retrieved from Forbes: https://www.forbes.com/councils/forbestechcouncil/2024/01/17/how-blockchain-revolutionizes-data-integrity-and-cybersecurity/

Reuters. (2025, 05 18). *Nvidia in advanced talks to invest in PsiQuantum, The Information reports*. Retrieved from Reuters: https://www.reuters.com/business/nvidia-advanced-talks-invest-psiquantum-information-reports-2025-05-19/

SailPoint. (2025, 05 19). *Machine learning (ML) in cybersecurity*. Retrieved from SailPoint: https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity

Satter, R. (2025, 03 10). *Musk blames X outage on cyberattack*. Retrieved from Reuters: https://www.reuters.com/technology/social-media-platform-x-down-thousands-users-downdetector-shows-2025-03-10/

Sophos. (n.d.). *What is antivirus software?* Retrieved from Sophos: https://www.sophos.com/en-us/cybersecurity-explained/antivirus

Tipranks, T. (2025, 05 01). *Can Bitcoin Really Hedge Inflation in 2025?* Retrieved from The Globe And Mail: https://www.theglobeandmail.com/investing/markets/stocks/MSTR/pressreleases/32152484/can-bitcoin-really-hedge-inflation-in-2025/

University, E.-C. (2025). *Emerging Technologies Driving the Future of Cybersecurity in 2025*. Retrieved from EC-Council University: https://www.eccu.edu/blog/emerging-technologies-driving-the-future-of-cybersecurity-in-2025/