what are the emerging and future technologies that we will have to worry the most about from a security perspective?

Aaron Hernandez
Professor Saltuk Karahan
11/20/22
CYSE 426

Aaron Hernandez

Professor Saltuk Karahan

11/20/22

CYSE 426

What is technology and what will technology look like in the next decade? As technological advancements continue to alter our everyday life the question remains what prevents that technology from become a problem rather than a solution. Throughout this paper I will be answering the question: What are the emerging and future technologies that we will have to worry the most about from a security perspective? To answer this question, I will look at the history of technology and its security issues. I will also be using 8 scholarly sources to analyze the questions and conclude.

The first emerging technology I will be analyzing for security issues is cloud computing. Cloud computing is defined as the use of network connection to a remote server host over the internet which manages, stores, and process data instead of using local devices such as your local pc. Some of the emerging organization that provide this service are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). These are the top three largest cloud computing companies as of 2022. In the next section we will be looking at the history of cloud computing.

Cloud computing was first introduced in 1963 when a project funded by the “Defense Advanced Research Projects Agency” granted MIT a 2 million dollar grant for project MAC

(Foote, 2022). The goal for the project was to develop technology which allow two or more people to concurrently use a computer and its process power at the same time. At the time they were able to produce a reel of magnetic tape for memory which was able to be use simultaneously by two individuals at the same time (Foote, 2022). As cloud computing became more popular more and more organizations began to develop the idea. Salesforce was one of the first organizations to introduce the idea of sharing software over the internet in 1999 (Foote, 2022). 7 years later Amazon launched their Amazon Web Service which was revolutionary at the time. This service provided storage, computation, and human intelligence along with many other services. In the coming years companies like Apple, Oracle, IBM, and CloudBolt launched their own versions of cloud computing. Cloud computing is relatively young technology that hasn't been thoroughly developed and for that reason there are many security risks. In the next section I will be analyzing some of these security risks.

Some of the major security issues with cloud computing are its use of software as a service (SaaS) and finally infrastructure as a service (IaaS) (Hashizume,2013). These are all types of cloud computing services which have security issues that have not been patched or solved resulting in vulnerability. IaaS is a security issue for cloud computing because the virtual machine which creates the connection between the cloud and the user is a huge vulnerability. The virtual machines unlike the cloud servers have their set of security protocols which can be changed by the user. This creates more vulnerabilities for hackers to take advantage of and infiltrate. This creates security risks for both the user and the cloud servers. This issue is compounded when considering that multiple vms are ran from one computer. So let's say one vm was corrupted it could potentially corrupt all the vms on that computer. Software as a service

provides software such as email, video conferencing, and other application on demand over the network (Hashizume,2013). Unlike IaaS users have less control over security control over SaaS. Since SaaS are applications that are provided over the web browser it inherits the security vulnerabilities of web browsers (Hashizume,2013). Another major issue of SaaS is that organizational data is transferred over plain text and stored in the cloud (Hashizume,2013). This creates a massive vulnerability which intruders can take advantage of and it's the responsibility of the cloud computing provider to secure this information. Although there are data transfer protocols some of these are not as effective due to the cloud computing system.

The second emerging technology which rises some concern for both government and private organizations is the internet of things (IoT). The internet of things is defined as any technology, software, and processor that can connect and interchange data over the network. Some examples of these types of devices can be smartphones, vehicles, smart lights, electronic planting systems, etc. All these devices can collect information and sharing it with other devices or data collection centers. Essentially the Internet of things is physical devices that are equipped with software and sensors that can be connected over the network and work together to collect and transfer data.

The history of the Internet of Things as we know it begins in 1962. It initially started as part of the Defense Advanced Research Projects Agency like Cloud Computing. It later evolved into Advanced Research Projects Agency Network in 1969 ((*A brief history of the internet of things* 2022)). In the 1980s the first introduction of commercial use of the Internet of Things was opened and supported by the public. Some of the first things interconnected were satellites and

landlines which provided basic communication for the Internet of Things. In 1993 the introduction of global position systems helped push the Internet of Things even further (*A brief history of the internet of things* 2022). This is because not only was the GPS supported by the 24 government satellites, but also private and commercial businesses started to launch their satellites into orbit (*A brief history of the internet of things* 2022). In the 2000s IoT made its largest impact on business with the introduction of FRID. FRID tags could be placed on any item which made keeping inventory easier. The next few years saw the growth of the IoT with some smart cities relying on this concept to effectively handle its need. Some implementations of this were real-time traffic monitoring, air quality, smart buildings, smart public light, and smart transportation (*A brief history of the internet of things* 2022).

Although the IoT can make life easier it also comes with its vulnerability and security issues. In section, I will review and explain some of the security challenges that come with the Internet of Things. One of the main threats of the IoT is unauthorized access to the networks. Since these sensors and devices transfer and share the information over a wide area network it can leave the information vulnerable to attacks. One example of this vulnerability being exploited is an attack that occurred in 2016 on Verizon's shipping containers which contained thousands of dollars of company merchandise (Kumar). A group of hackers was able to take advantage of a SQL vulnerability and track Verizon's shipping container. This information was later sold to another group that tracked the shipping container to the Indian Sea where they boarded the vessel and stole thousands of dollars of merchandise. This is only one example of the vulnerabilities of the IoT. Another security issue with IoT is the denial-of-service attacks (Kumar). Since some of these sensors are used to monitor and manage traffic conditions, they

could potentially be vulnerable to these types of attacks. In some cases, DDoS attacks have been used to gain control of traffic lights. This could be a vulnerability that could cause atrophic damages. Since the traffic light system automatically changes the algorithm to manage traffic flow it could potentially be used to cause harm if taken advantage of. Finally, another security concern relating to IoT is data leaking. Data leaking is defined as the unauthorized transmission of data from an organization to an outside source (Kumar). This can cause issues with both privacy and security concerns. One example of this vulnerability being exploited is Wyze smart cameras back in 2019. The Wyze company produces in-home cameras that monitor and record both video and voice. They are marketed as in-home security systems that be easily set up. In 2019 that had one of the largest security breaches which resulted in 2.4 million users' information being gathered by a hacker group. this information included private emails, names, ages, dates of birth, gender, etc. These types of attacks were only possible because of the IoT vulnerability and technology. While IoT is a relatively young technology it still has its security concerns and vulnerabilities which have not been solved.

The third emerging technology that rises some concern from a security standpoint is blockchains. Blockchains are defined as shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network (*IBM Blockchain*). Blockchains are a new technology that recently made their way into organizations. Some of the most popular companies that are currently using blockchains are Coinbase Global, Monex Group, SOS LTD, Silvergate Capital Corporations, and many other companies. In the next section, we will be looking at the history of blockchains to grasp an understanding of how they were created and their current uses.

The idea of blockchains was first introduced in 1991 by Stuart Haber and W Scott Stornetta (Poposki & Soussou). Later in 1998, the idea became reality when CS Nick Szabo created a bit gold which was one of the first decentralized digital currencies. In 2009 the first introduction of public use blockchain transactions was introduced by Satoshi Nakamoto (Poposki & Soussou). Satoshi created Bitcoin which is currently one of the largest cryptocurrencies to date. It is currently worth between Ten and Twenty million dollars. There are currently 21 million bitcoins in existence and each one has its who individual node on the blockchain. A node is a point at which lines or pathways intersect connecting to a centralized point. Essentially a blockchain is created up of thousands or millions of nodes that contain information such as transaction date, user information, updated information, and its private key which is essential to the blockchain. Blockchains are currently being studied and developed by government agencies, financial institutions, distribution businesses, private organizations, and many other entities. This is because they see value in blockchain technology and see how it could streamline transactions. Blockchains are no longer just being used in cryptocurrency but instead being developed for many other purposes.

Although Blockchains are currently being used in society they still have not been thoroughly combed for security issues. In this section, I will be analyzing some of the security issues that have arisen. One of the vulnerabilities of blockchains is Sybil's attacks (Li et al., 2017). A Sybil attack can use one singular node to operate as many fake identities as possible. The goal of this attack is to gain most of the influence in the blockchain. Once this majority

influence is gained the attack can then use that power to refuse to transmit nodes or receive blocks (Li et al., 2017). This essentially disrupts the entire blockchain creating a standstill until those unauthorized nodes are removed. Another security concern with blockchains is endpoint vulnerabilities (Li et al., 2017). In this type of attack, an attacker monitors a blockchain user's activity on their devices such as computers or phones. Once the attacker gains access to that device they can steal the blockchain key which grants them access to any node that the user has access to. The final security issue I will analyze is phishing scams (Li et al., 2017). Even if blockchain technology can patch both the security concerns above and the others human error will always be an issue. Since this technology is based on a peer-to-peer platform it places trust that humans will due their diligence to stay safe. In a phishing attack, an attacker sends a legitimate-looking email to a user. Once the user clicks the email, they essentially send the attack all the information they need. The emails are disgusting behind legitimate emails which are explaining to the user that they may need to change their password or username because there are security concerns regarding their account. An example of this attack occurred recently in October 2022. A hacker named Monkey Drainer was able to send phishing emails around and eventually gained access to two or three accounts. Once they gained access, they were able to drain the account accumulating 3.4 million dollars. Monkey Drainer had stolen 700 ether which was roughly worth one million dollars. Then he was able to gain another cryptocurrency called Bored Ape which was worth 2.4 million dollars in less than 24 hours.

The final emerging technology that rises some concern for security experts is Artificial intelligence. Artificial intelligence is defined as the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech

recognition, decision-making, and translation between languages (*Artificial Intelligence, 2018*). Artificial intelligence is currently being used throughout organizations to automate tasks such as back-end IT and factory floor operations. It is also being used in the cybersecurity industry to monitor attacks and vulnerabilities. Artificial intelligence is a young and emerging technology that is constantly being developed. In the next section, I will review a bit of history regarding artificial intelligence.

Artificial intelligence has been around since the 1900s. The first AI program was developed in 1955 called the logic theorist (Kaplan, 2019). The logic theorist program was able to think at the human level. It could solve mathematical problems and create theories through analysis. Since the program was massive success research groups and colleges began to develop the idea of AI even further. Some of the most popular research groups were Dartmouth and MIT (Kaplan, 2019). In 1982 the autonomous car was created and built by Carnegie Mellon (Kaplan, 2019). Finally, the first publicly available AI software was released in 1997. The software had the ability of speech recognition combined with a computer it could use speech to launch programs along with also controlling most of the functions of the computer (Kaplan, 2019). Currently, AI is part of our everyday life which we might not realize. Some of the AI that we interact with every day included Siri, Google, Alexa, and much more technology. AI is constantly being developed but it also had its own security risk. In the next section, I will be looking at some of these security risks.

One of the biggest threats to Artificial intelligence is system manipulation (Kaplan, 2019). This attack is done by feeding the AI false information and tricking the system into

thinking something is wrong. This can be a catastrophic failure for AI because it could change the AI's behavior. AI unlike humans can't see when something is wrong with the code instead, they continue to run the code as long as they can. This leads into the next security threat which is transfer learning attacks. This type of attack completely changes the behavior of the AI by replacing some of the pre training algorithms. This can change how the AI process and adapts to all the information that it analyzes. Finally, a last concern for AI is its large dataset. Since the AI is constantly processing and saving information that data becomes a threat for those individuals whose data is kept.

In conclusion emerging and future technology has massive security risks. One common factor for this risk come because the technology has not been fully developed and tested. Although these four technologies are currently being used in the public, they still have massive vulnerabilities that both a user and organization have to be aware of. These are only four of the technologies that i have gone over but some honorable mention are 5G, Quantum Computing, Nanotechnology, and robotics. These are all technologies that are being developed and tested by the government and private organizations for the future and present use. These technologies are thought to be the future and therefore their weaknesses should be a focus although we may not always discover ever vulnerability.

.

References

Hashizume, K., Rosado, D.G., Fernández-Medina, E. *et al.* An analysis of security issues for cloud computing. *J Internet Serv Appl* 4, 5 . https://doi.org/10.1186/1869-0238-4-5

Poposki, L., & Soussou, G. (n.d.). *Rief history of Blockchain - Patterson Belknap Webb & Tyler*. Retrieved November 21, 2022, from https://www.pbwt.com/content/uploads/2018/05/010051804-Patterson.pdf

Kumar, J. S. (n.d.). *A survey on internet of things: Security and privacy issues*. Retrieved November 21, 2022, from https://course.ccs.neu.edu/cs7680su18/resources/pxc3894454.pdf

Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.

Siyal, A.A.; Junejo, A.Z.; Zawish, M.; Ahmed, K.; Khalil, A.; Soursou, G. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography* 2019, *3*, 3. https://doi.org/10.3390/cryptography3010003

Artificial Intelligence. Artificial Intelligence - an overview | ScienceDirect Topics. (n.d.). Retrieved November 20, 2022, from https://www.sciencedirect.com/topics/social-sciences/artificial-intelligence#:~:text=Artificial%20intelligence%20is%20the%20theory,making%2C%20and%20translation%20between%20languages.

Foote, K. D. (2022, November 17). *A brief history of cloud computing*. DATAVERSITY. Retrieved November 20, 2022, from https://www.dataversity.net/brief-history-cloud-computing/#

What is blockchain technology? - IBM Blockchain. IBM. (n.d.). Retrieved November 20, 2022, from https://www.ibm.com/topics/what-is-blockchain#:~:text=Blockchain%20defined%3A%20Blockchain%20is%20a,patents%2C%20copyrights%2C%20branding).

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017, August 23). *A survey on the security of Blockchain Systems*. Future Generation Computer Systems. Retrieved November 20, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S0167739X17318332#preview-section-cited-by

Haenlein, M., & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925