Horizon | Journal of Humanity and Artificial Intelligence

FUTURE OF CYBERSECURITY

Matthew N. O. Sadiku
Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX USA

Uwakwe C. Chukwu
Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA

Janet O. Sadiku
Juliana King University, Houston, TX, USA

Abstract

Cyber attacks have grown in the last few years and have targeted all kinds of sectors. Cybersecurity is the umbrella term used to describe efforts to protect computer networks from unauthorized access. As we increasingly rely on technology and the Internet for business, communication, and personal use, the importance of cybersecurity has become more apparent than ever. The field of cybersecurity will continue to evolve as technology continues to advance exponentially. This paper attempts to predict the future of cybersecurity.

Keywords: cyber attacks, cyber threats, cybersecurity, future of cybersecurity.

INTRODUCTION

The technology is evolving at an alarming rate to reshape our daily lives. Technology has now become an integral part of our day to day life. It has the potential to improve every aspect of our lives. Smartphones, computers, laptops, and tablets keep surrounding us, 24/7. As the world's reliance on technology grows, so does the need for cybersecurity. The threat of cybercrime and cyberattacks is on the rise, and the consequences of a security breach can be devastating for individuals and businesses alike. It is important to stay ahead of the latest cybersecurity trends to keep your organization and personal data safe. By implementing a high-quality security system, you can slash the vulnerabilities and combat your business from cybersecurity threats [1].

Cybersecurity is all about cyber assets. It is crucial for the constant evolution of the digital world. Although the future of cybersecurity is difficult to predict, as the market is continuously changing in response to cybercriminals' shifting activities and the new attacks they are creating, one can confidently say that the future of cybersecurity is an ever-evolving field. With the rise of digital technology, cybersecurity threats have become more prevalent and damaging to individuals, businesses, organizations, and governments. Figure 1 showS the influences of the technical, organizational, and political spheres on the Cybersecurity situation [2].

In order to predict the future of cybersecurity, it is important to first have an understanding of its current state and the technologies that will determine its future. These technologies include artificial intelligence, machine learning, cloud computing, Internet of things, blockchain, 5G, etc. These are emerging technologies influencing cybersecurity. Some of them are shown in Figure 2 [3]. By implementing these emerging security technologies, businesses can reduce the risk of suffering a major cyber-attack [4].

OVERFVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 3, cybersecurity involves multiple issues related to people, process, and technology [5].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [6].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [7].

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [8]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating

with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 4 [9].

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [10]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

FUTURE OF ARTIFICIAL INTELLIGENCE.

The future of cybersecurity is artificial intelligence (AI). The role of artificial intelligence in future cybersecurity cannot be underestimated. Increased use of AI and machine learning (ML) is one trend that is likely to shape the future of cybersecurity. AI and ML are redefining every aspect of cybersecurity today. They are essential to securing the perimeters of any enterprise. AI provides a unique set of tools and techniques to prevent, detect, and respond to cyberattacks. AI will be necessary to respond to cyberattacks. Today, it is difficult to detect breach attempts today without the use of AI technologies. As a result, US-based businesses are placing the highest priority on AI-based cybersecurity applications and platforms. Enterprise executives are concentrating their budgets and time on detecting cyber threats using AI because AI lowers the cost to detect and respond to breaches [11]. Artificial intelligence is not limited to chatbots; it can automate tasks, study data, and make decisions for humans in just a few moments. Cybersecurity professionals believe that AI will be able to detect potential threats and flag problems faster than humans can realize, greatly helping overall security measures. AI also the ability to learn from past experiences.

The use of AI has some drawbacks. AI requires significant amounts of data and computational power and is not feasible for all organizations. There is always the risk that AI may make mistakes or be manipulated by attackers, leading to false positives or missed threats.

FUTURE OF AUTOMATION

The future of cybersecurity is autonomous bots. Automated tasks could include source code analysis, network traffic analysis, and endpoint detection. Automation is becoming more widely used in cybersecurity to improve incident response time and simplify compliance. It will play a vital role in the cyber workplace. Automation in incident response refers to the use of technology to automate various tasks and processes involved in incident response. This can help organizations to quickly and efficiently respond to security incidents, reducing the time it takes to contain and remediate an incident, and ultimately reducing the damage caused by an attack. This may include automating the detection of security incidents, the collection of data, the analysis of that data, and the execution of incident response procedures. Automated incident response systems can quickly detect and respond to potential threats, reducing the time it takes to respond to a cyber attack. Automation can also be used to simplify compliance with regulations [12].

FUTURE OF COLLABORATION

The future of cybersecurity is collaboration. In other words, the future of cybersecurity demands collaboration. A major trend in cybersecurity is the increasing focus on collaboration between organizations. There is no security concept that will have a greater impact on the overall cyber landscape than collaboration. In the past, organizations have often been reluctant to share information about cyber threats, for fear of revealing their own vulnerabilities. Industries will find stronger defenses in partnerships, and the shared knowledge will benefit clients. The economies of scale achieved through open security collaboration can revolutionize the way organization do cybersecurity. Collaboration is

cheaper and more effective means of security than the alternative. The transition in the attitudes around sharing information risk can be extended to other aspects of cybersecurity. If organizations have already accepted sharing critically important security event information with partners, what is holding them back from participating more openly in the security community? There is a lot to gain by working openly and collaboratively in the cybersecurity space. A lot is to benefit when many organizations subscribe to security services that shared lessons learned. We should focus on collaboration if we want to protect not only our own boundaries, but the economies and ecosystems of our nations. The some national governments are taking collaborative approach to uplift their country's cyber security posture [13,14].

FUTURE OF CLOUD COMPUTING

Cloud computing is an emerging model of storing and processing data that relies on remote servers. It allows you to transfer data and other computing services over the Internet. As more organizations move their data and applications to the cloud, protecting them from cyber threats will become a priority. Cloud computing is one of the most effective ways to mitigate cyber risk. This is because it offers several compelling benefits [15]:

- ✓ It speeds up deployment times by allowing companies to build and launch new apps without having to invest in the infrastructure needed to support them.
- ✓ Cloud computing cuts costs by removing hardware or software maintenance from the equation. It lowers operational costs and frees up valuable resources for other business initiatives.
- ✓ It allows companies to scale their operations easily by adding more server capacity as necessary.
- ✓ It opens up new channels for revenue generation by letting them sell services directly to customers.
- ✓ Cloud computing allows companies to access specialized expertise through third-party providers like data scientists and AI experts. This can help them boost their competitive edge and stay ahead of the curve in an increasingly competitive industry landscape.

One of the major security concerns with cloud computing is the risk of unauthorized access to sensitive information. There are also compliance and regulatory considerations that organizations need to be aware of when using cloud computing. Cloud environments will continue to remain as the new digital advancement as well as a battlefront.

FUTURE OF INTERNET OF THINGS

The Internet of things (IoT) has brought countless benefits to our lives. The rise of the IoT has a major impact on the future of cybersecurity. IoT devices are becoming increasingly common, and are often used to control critical systems and infrastructure. Our lives are made easier by the birth of smart devices, from Alexa to Google Home. However, many IoT devices have poor security features, and can be easily compromised by cyber criminals. As a result, organizations will need to implement better security measures to protect against IoT-related cyber threats [3].

FUTURE OF BLOCKCHAIN

The future of cybersecurity is blockchain. Blockchain technology is best known for its use in cryptocurrencies like Bitcoin or Ethereum. As an advantage for cybersecurity, blockchain can be used to generate a secure and tamper-proof record of transactions and data exchanges. Smart contracts are another cybersecurity blockchain tool. Blockchain technology is expected to play a critical role in providing secure and reliable data transmission for both individuals and organizations in the incoming years. One of the main benefits of blockchain is that it creates better user privacy, eliminates human error, adds transparency to business interactions, and eliminates the need for costly third-party verification. As a result, a decentralized system is created which is less vulnerable to data breaches by hackers [16].

FUTURE OF CYBERSECURITY WORKFORCE

The future of work is changing. As cybercrime increases, the consequences of a security breach can be devastating for individuals and businesses alike. This has led to a growing demand for qualified professionals in cybersecurity, which has made cybersecurity one of the industries that is growing the fastest right now. Cybersecurity faces a critical skills gap across a wide range of areas, including cloud security, OT security, and data analytics. Research shows that people, process, place, and technology transformation are the foundation upon which successful digital workplace ecosystems are created. A cybersecurity professional is anyone who can help companies and organizations protect themselves from online threats. Cybersecurity professionals may work in a variety of roles, including IT specialists, engineers, network administrators, and IT consultants. The cybersecurity skills shortage has been growing for some time, and so have the number and complexity of attacks; using machine learning to augment the few available skilled people can help ease this. Figure 5 shows a typical workforce of the future [17].

FUTURE OF INDUSTRY

Cyberattacks are rampant across all industries. As a result, cybersecurity has risen to the top of corporate agendas, as businesses continue to grapple with cyberattacks. Cyber has become foundational to business. Year after year, the industry changes, while Cyber threats evolve and the tools that defend against them mirror those change. Government institutions, public organizations, and technology companies are reexamining their approach to protective measures in security and privacy. The future of cybersecurity depends on the following industries [15]:

1. *Healthcare:* Healthcare is one of the most important industries in the world. It touches all aspects of life, from medical procedures to medical devices and pharmaceuticals. Since healthcare suffers from many threats, from cyberattacks to data breaches, it is crucial that healthcare organizations take cybersecurity seriously. In the future of healthcare, data will be more widely shared, collected, and analyzed. Healthcare organizations will be positioned to create new value from this previously unavailable information. The future of healthcare will be characterized by lots of devices, lots of data, and lots of sharing [18].
2. *Vehicular Communications*: Transportation has long been a target for cyberattacks, with vehicles and infrastructure increasingly vulnerable to hacking. As a result, the transportation industry is investing heavily in cybersecurity technology to keep up with the threat. Self-driving vehicles are extremely vulnerable to cyberattacks. Vehicles are physical objects driven by people, with all their accompanying human flaws.

With intelligent vehicles, there is a promise of saving tens of thousands of lives each year in the US alone. Cybersecurity will be nearly as important as crash testing for the new age of self-driving cars. Figure 6 shows a typical autonomous vehicle [19].

3. *Banking:* Cybersecurity is important in banking due to the highly sensitive nature of financial transactions. To keep pace with these threats, banks are investing heavily in cybersecurity solutions.
4. *Manufacturing:* There are cybersecurity threats that come with the manufacturing industry. Manufacturers need to guard against hackers who may try to steal information or cause physical damage.
5. *Government:* Cybersecurity has a major impact on national security, compelling governments to take steps to protect their critical infrastructure from cyber-attacks. Governments are also investing in R&D to stay ahead of the latest cyber threats, and to develop new technologies to better protect against these threats. Some governments have employed that zero-trust principle: Don't assume that anything or anyone should be trusted, i.e. never trust, always verify. The principle relies on the entire technology infrastructure being designed to check and recheck the identity and security posture of each entity and to continuously monitor the activities involving each entity. Everyone attempting to obtain entry must present identification.

CONCLUSION

The future of cybersecurity is complex and is always changing. It is set to be a constant battle between those who would protect information and those who would steal it. Properly done, cybersecurity is a mile wide and many miles deep. As a relatively new field, cybersecurity has been on the rise and will continue to be so. Cybersecurity became the fastest growing startup sector which aims at protecting our "new world" by providing tools and consultancies to help companies test their resilience and identify vulnerabilities. The demand for cybersecurity professionals is on the rise. A future-proof career in cybersecurity is an incredibly lucrative and the future is bright. There is also a growing need for cybersecurity education in schools and universities. More information about the future of cybersecurity can be found in the books in [20-23] and the following related periodicals:

- ✓ *Journal of Cybersecurity*
- ✓ *Security Magazine*
- ✓ *Cyber Defense Magazine*

REFERENCES

1. B. Shewmake, "Research: Delinea reveals cloud automation is key to future-proofing cybersecurity," March 2022,

   https://www.prnewswire.com/news-releases/research-delinea-reveals-cloud-automation-is-key-to-future-proofing-cybersecurity-301508687.html

2. R. Koch, "On the future of cybersecurity," March 2017

   https://www.researchgate.net/publication/315378408_On_the_Future_of_Cybersecurity

3. A. Banafa, "The future of cybersecurity: Predictions and trends," April 2023,

   https://www.bbvaopenmind.com/en/technology/digital-world/future-of-cybersecurity-predictions-trends/#:~:text=One%20of%20the%20biggest%20trends,may%20indicate%20a%20potential%20threat.

4. "The future of cyber security: Overview of new technologies,"

   https://myturn.careers/blog/the-future-of-cyber-security-overview-of-new-technologies/#:~:text=The%20future%20promises%20advanced%20security,present%20their%20own%20unique%20challenges.

5. "Eliminating the complexity in cybersecurity with artificial intelligence,"

   https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/

6. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

7. M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

8. "FCC Small Biz Cyber Planning Guide,"

   https://transition.fcc.gov/cyber/cyberplanner.pdf

9. "The 8 most common cybersecurity attacks to be aware of,"

   https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

10. Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

11. L. Columbus, "Why AI is the future of cybersecurity,"

    https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/?sh=4c5dd0117eb6

12. "2023: A look into the future of cybersecurity,"

    https://taks3.com/2023-a-look-into-the-future-of-cybersecurity/

13. K. Ford, "The future of cybersecurity is collaboration,"

    https://www.cybergrx.com/resources/the-future-of-cybersecurity-is-collaboration#:~:text=There%20is%20no%20single%20tool,organization%20do%20cybersecurity%20and%20privacy.

14. "Collaboration is the future of cybersecurity," October 2018,

    https://www.thinkcsc.com/collaboration-is-the-future-of-cybersecurity/

15. "The future of cybersecurity: Career growth,"

    https://www.knowledgehut.com/blog/security/future-of-cybersecurity

16. "The future of cyber security: Overview of new technologies,"

    https://myturn.careers/blog/the-future-of-cyber-security-overview-of-new-technologies/#:~:text=The%20future%20promises%20advanced%20security,present%20their%20own%20unique%20challenges.

17. "The future of cybersecurity job market 2023,"

    https://myturn.careers/blog/future-of-cybersecurity-job-market/

18. "The future of cybersecurity in health care,"

    https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cybersecurity-healthcare.html

19. "Autonomous vehicles pose new challenges to future of cybersecurity,"

    https://www.ttnews.com/articles/autonomous-vehicles-pose-new-challenges-future-cybersecurity

20. M. M. Ghonge et al. (eds.), *Cyber Security and Digital Forensics: Challenges and Future Trends*. Wiley, 2022.

21. C. Morillo, *The Future of Security.* O'Reilly Media, 2022.

22. M. Miller et al., *Modern Cybersecurity: Tales from the Near-Distant Future.* Independently published, 2021.

23. P. Quade, *The Digital Big Bang: The Hard Stuff, the Soft Stuff, and the Future of Cybersecurity*. Wiley, 2019.

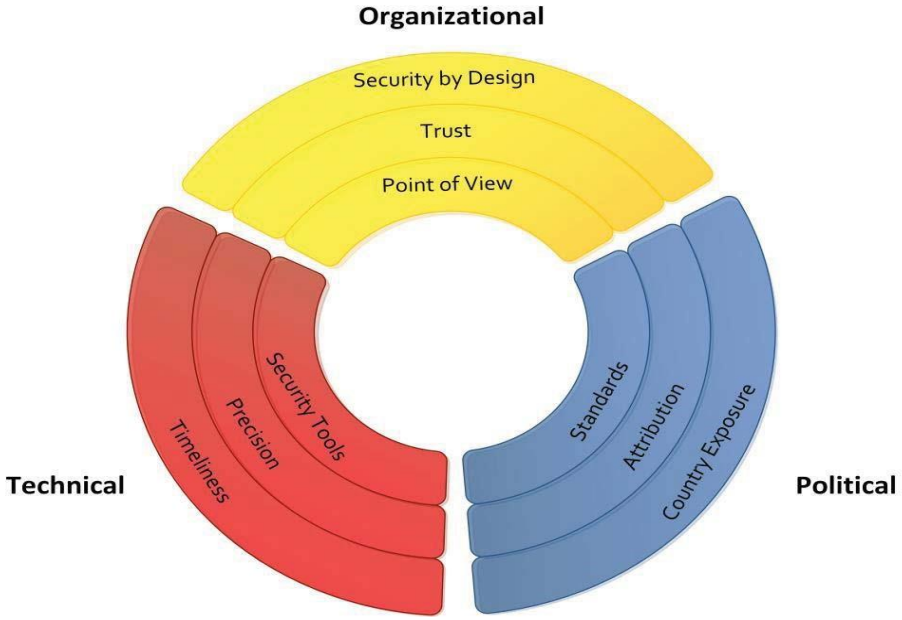


Figure 1. The influences of the technical, organizational, and political spheres on the cybersecurity situation [2].



Figure 2. Some emerging technologies influencing cybersecurity and its future [3].



Figure 3. Cybersecurity involves multiple issues related to people, process, and technology [5].

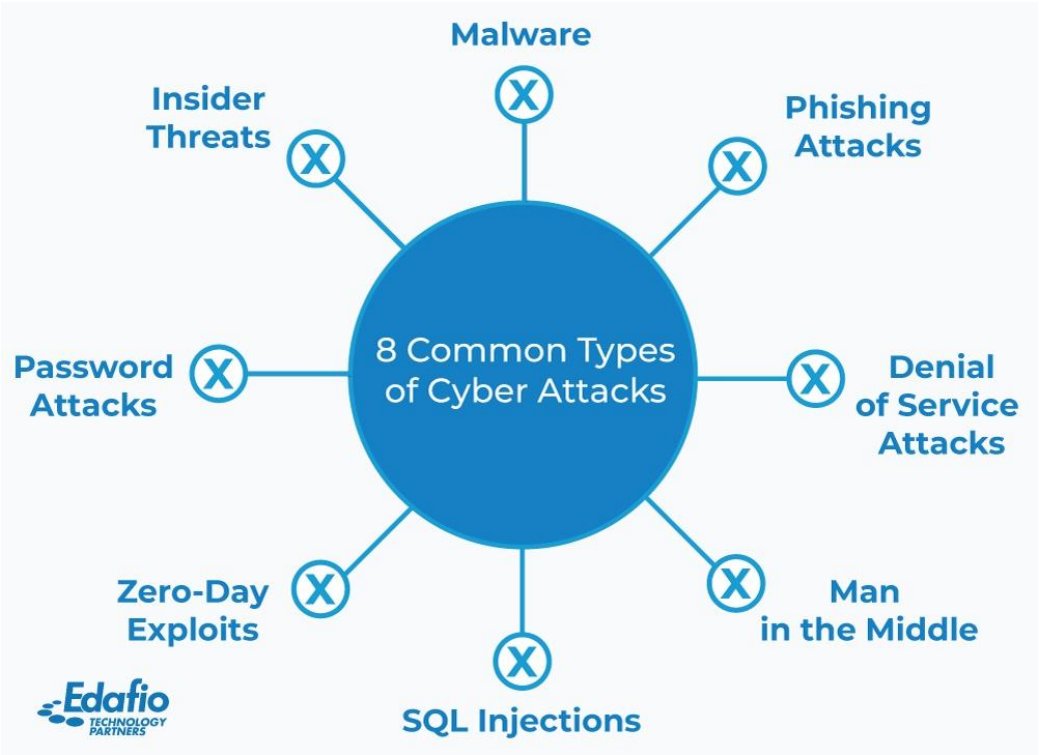


Figure 4. Common types of cyber attacks [9].



Figure 5. A typical workforce of the future [14].

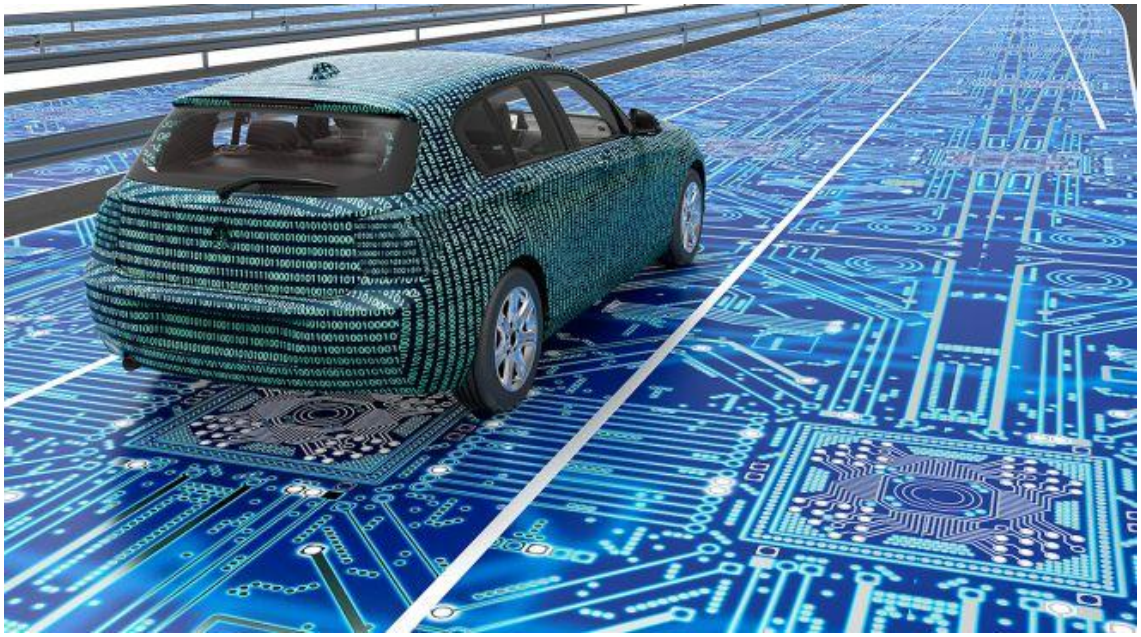


Figure 6. A typical autonomous vehicle [19].