Original Research Article

Cybersecurityin Autonomous Systems: Threats, Vulnerabilities, and Defense Mechanisms

Seyed Milad Kashefi Pour Dezfuli*

Department of Research and Development, UOP, USA

Citation S.M.K.P. Dezfuli. Cybersecurityin Autonomous Systems: Threats, Vulnerabilities, and Defense Mechanisms. *J. Eng. Ind. Res.* **2025**, 6 (2):179-194.

https://doi.org/10.48309/jeires.2025.512281.1180

Article info:
Submitted: 2025-03-13
Revised: 2025-03-23
Accepted: 2024-04-14
ID: JEIRES-2503-1180

Keywords:
Autonomous systems; Cybersecurity; Threats; Vulnerabilities; Defense mechanisms; Intrusion detection.

ABSTRACT

There is the rapid evolution of autonomous systems, including autonomous vehicles, drones, and smart infrastructure, that has revolutionized industries through enhanced efficiency, precision, and scalability. It has, however, been accompanied by significant cybersecurity risks. Autonomous systems are susceptible to all types of cyber-attacks because of their connectivity to networks, including data tampering, sensor spoofing, denial-of-service attacks, and unauthorized access to control systems. These vulnerabilities stem from the integration of complex software architectures, communications networks, and sensor suites that offer a number of attack surfaces to malicious agents. This study provides a comprehensive assessment of the primary cybersecurity threats and vulnerabilities in autonomous systems, with an emphasis on their ability to affect safety, privacy, and operational integrity. Moreover, it analyzes state-of-the-art protection methods, including intrusion detection systems, encryption protocols, anomaly-based monitoring, and machine learning-based threat prevention methods. By presenting real case studies and current research advances, this study advocates for the urgent need for secure, adaptive, and multi-level security architectures for safeguarding autonomous systems against new and rising cyber threats. The findings stress the importance of coordination among cybersecurity researchers, system engineers, and policy makers to ensure the secure and dependable introduction of autonomous technologies into mission-critical applications.

Introduction

The increasing number and variety of devices connected to the Internet is a welcome development for cyber attackers, as they can easily exploit devices like printers and cameras that were never designed to prevent sophisticated attacks [1]. As a result, companies and individuals alike need to rethink how secure their networks are. With the increasing number of incidents, there is also a greater need for a way to categorize the risks facing businesses and customers. Vulnerabilities, exploits, and threats are three of the most common terms used when discussing cyberattacks. Mistakes

*Corresponding Author: Seyed Milad Kashefi Pour Dezfuli (skash009@fiu.edu)

happen all the time, even in the design and coding stages of technology [2]. What remains of these mistakes is called a bug. Bugs are not inherently harmful, except in terms of the potential functionality of the technology, but some can be exploited by malicious actors, which are called vulnerabilities. Vulnerabilities allow software to be used to perform tasks such as gathering information about existing defense mechanisms against cyberattacks that are incompatible with their original intent. Once a bug is identified as a vulnerability, it is registered as a CVE, or Common Vulnerability and Threat, by MITRE, and is assigned a CVSS score, which indicates the potential risk that the vulnerability poses to an organization. The list of these CVEs is used as a reference for vulnerability scanners. In general, a vulnerability scanner scans the environment and compares it to a database or list of known vulnerabilities. The more information the scanner has, the more accurate it will be. After the team has prepared a vulnerability report, developers can use penetration testing as a tool to discover the weaknesses location, so that the problem can be fixed and similar mistakes can be prevented in the future. If the scanning process is used consistently and repeatedly, commonalities between vulnerabilities will be identified and a better understanding of the system will be achieved [3].

Examples of security vulnerabilities

Security vulnerability is a weakness, flaw, or error found in a security system that may be used by a threat actor to compromise a secure network. There are many security vulnerabilities, some of the most common of which are described below:

Authentication breach

If authentication credentials are compromised, sessions and user identities may be controlled by malicious individuals who can impersonate the original users.

SQL injection

As one of the most common types of security vulnerabilities, SQL injection attacks attempt to gain access to the contents of a database by injecting malicious code into it. A successful SQL injection attack can allow attackers to steal sensitive data, impersonate others, and engage in a range of other malicious activities [4].

Cross-site scripting

Cross-Site Scripting, or XSS, also involves injecting malicious code into a website and is somewhat similar to SQL injection in this regard. However, XSS attacks target users of the website rather than the website itself, putting the user's sensitive information at risk of being stolen.

Cross-site request forgery

Cross-Site Request Forgery, or CSRF, attacks seek to trick authenticated users into performing an action they did not intend to perform. Using CSRF in conjunction with social engineering can trick users into providing sensitive information to malicious parties [5].

Security misconfiguration

Any component of a security system that can be exploited by attackers due to configuration errors can be considered a security misconfiguration (Figure 1).

What is an exploit?

In an attacker's playbook, an exploit is the next step after finding vulnerability. Exploits are tools that allow hackers to exploit a vulnerability for malicious activity and include pieces of software, a sequence of commands, or even open source exploit kits. A threat is a hypothetical event in which an attacker exploits a vulnerability. Given the usual practice of hackers to carry out their actions, threats typically include at least one exploit. A hacker, after assessing the situation, may use multiple exploits simultaneously to achieve the best result. Although we are constantly hearing about new cyberattacks or threats in the world, these terms can provide more context to the

steps and risks that cyber professionals face on a daily basis [6].

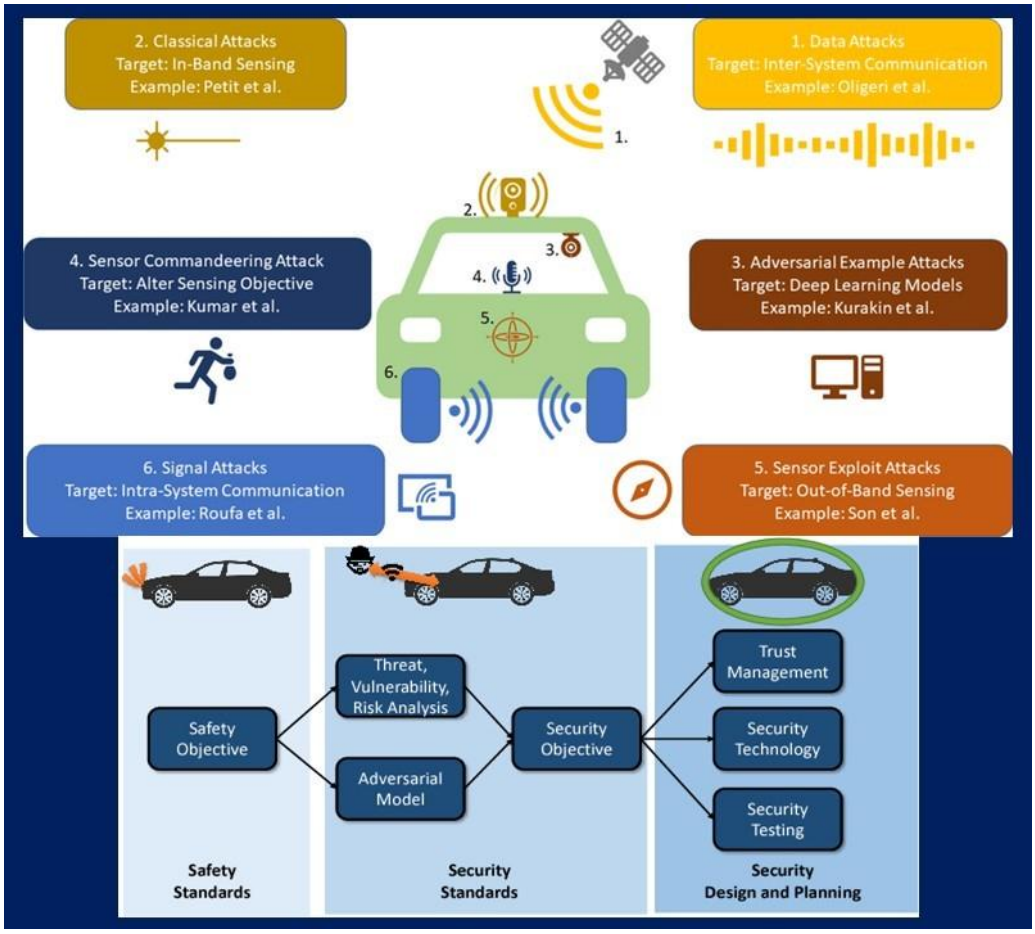

Figure 1: Examples of security vulnerabilities.

The cybersecurity importance

Cybersecurity is a vital pillar of digital life in the 21st century. The growth of technology and constant connectivity to the Internet has provided us with countless possibilities, but at the same time it has created a wide platform for cyber threats and attacks. The importance of cybersecurity is tangible not only for organizations and governments, but also for every individual who uses digital technology.

Protecting personal and private data

In the digital world, personal information is like our identity. This information includes: national ID, banking information, medical data and even daily activities on social networks. If this information is disclosed, people may face identity theft, financial abuse or damage to their reputation. Cybersecurity helps prevent such incidents [7].

Protecting critical infrastructure

Critical infrastructure such as energy systems, transportation networks, healthcare centers and banks are the main targets of cyber-attacks. Any security flaws in these systems can have serious consequences such as widespread disruptions, reduced public access to vital services and even risks to life. Cybersecurity ensures that these infrastructures remain resilient to attacks [8].

Preventing financial losses

Cyberattacks can cause huge financial losses. For example:

Ransomware

Hackers lock down an organization's systems and demand a large ransom to unlock them.

Data theft

Sensitive information may be sold or used for fraud [9].

Lost revenue

A security breach may cause a business to shut down or reduce sales. According to reports, the cost of cybercrime has reached billions of dollars per year in recent years and this trend continues to increase [10].

Maintaining trust and reputation

One of the most important assets of any organization is the trust of customers and shareholders. Any cybersecurity breach can severely affect this trust and damage the organization's reputation. Organizations that are unable to manage cybersecurity may lose their customers and business [11].

Preventing global threats

Cybersecurity is not just an individual or organizational issue, but a global challenge. Cybercrime is often carried out by transnational organized groups that can threaten national security. Cyber espionage, cyber warfare, and targeted attacks are among the tools that governments should invest in to counter them.

Supporting innovation and digital growth

Cybersecurity helps technological advances. When individuals and organizations are confident in the safety of their information and systems, they will have a greater incentive to invest in innovation, digitize processes, and use new technologies [12].

Legal and regulatory requirements

Governments and regulatory bodies around the world have set laws and standards to ensure compliance with information security. Organizations that fail to meet these requirements may face heavy fines or operational restrictions [13].

Why is cybersecurity a necessity?

In today's world, cybersecurity is no longer an option or preference, but a necessity. The dramatic increase in dependence on technology and the Internet in all areas of life, from personal to professional and national, requires that cybersecurity be considered a critical priority [14]. Here are the reasons why cybersecurity is necessary:

Increase in cyber-attacks and their sophistication

Hackers and cybercriminals are developing more advanced and sophisticated techniques to penetrate networks and systems every day. These threats include: phishing, ransomware, cyber espionage and social engineering, which can affect all aspects of digital life. Cybersecurity provides a strong barrier against these threats [15].

Protection of information and privacy

Personal information such as passwords, bank card numbers, medical records and financial data are among the most valuable assets of individuals. A breach of this information can have serious consequences such as identity theft, financial abuse or privacy disclosure. Cybersecurity ensures that this data is not accessible to unauthorized persons.

Protecting businesses and the digital economy

Businesses are increasingly relying on digital technologies. A security breach can lead to loss of customers, loss of public trust, financial losses, and even the complete shutdown of a company. For this reason, implementing cybersecurity measures protects businesses

from attacks and provides a safe platform for economic growth [16].

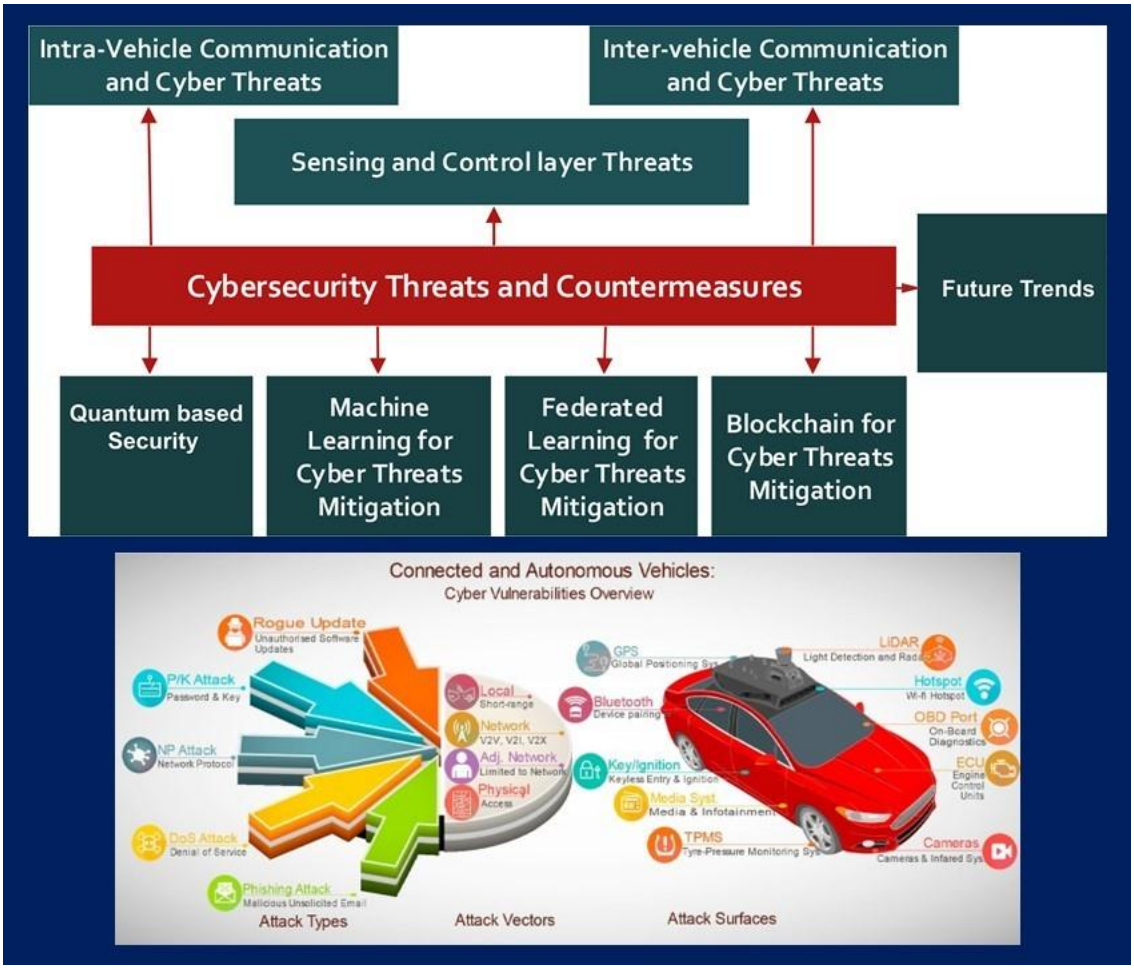

Figure 2: Vital role in the era of the Internet of Things (IoT).

Preventing national security threats

Governments also face serious cyber threats. Cyberattacks can target critical national systems such as the power grid, transportation infrastructure, and government databases. Such attacks may jeopardize public security, national sovereignty, and international relations. Cybersecurity is an essential part of national defense (Figure 2).

Vital role in the era of the Internet of Things (IoT)

With the proliferation of internet-connected devices, from smartwatches to car systems and smart homes, the space for cyberattacks has increased. Many of these devices are vulnerable and can be exploited. Cybersecurity ensures that these technologies make our lives easier rather than posing a threat [17].

Preventing financial and social crises

Cyberattacks can have profound effects on societies. For example:

Ransomware: Locking sensitive data or systems by demanding large sums of money.

Disinformation: Information attacks that influence public opinion.

Financial theft: Illegal transfer of funds or digital assets [18].

Building trust in cyberspace

Cyberspace will be safe and trustworthy when users are confident that their information and activities are protected. This trust is the basis of

digital interactions, e-commerce and the use of new technologies. Cybersecurity strengthens this trust at all levels [19].

Supporting innovation and emerging technologies

Cybersecurity is the foundation and pillar of new innovations such as artificial intelligence, machine learning, and big data. Without ensuring security in these areas, technological advances may face serious threats and innovative opportunities may be missed. Cybersecurity is not only essential for protecting personal information and digital assets, but also serves as a vital infrastructure for digital life, the global economy, and national security. As technology continues to evolve, cybersecurity will play an increasingly important role in mitigating vulnerabilities and creating a secure environment for future advancements.

Types of cyber threats

Cyber threats come in many forms and aim to infiltrate systems, steal data, disrupt services, or gain unauthorized access to digital resources. Understanding the types of cyber threats is the first step in preventing them. Here are the most important types of cyber threats:

Malware

Malware is a type of malicious software designed to damage or gain unauthorized access to computer systems. Common types of malware include:

A) Viruses: Programs that attach themselves to other files or programs and spread [20].
B) Worms: Software that spreads on systems and networks without requiring user intervention.
C) Ransomware: Software that locks system data and demands money to restore it.
D) Spyware: Software that collects sensitive information from users without their knowledge.

Phishing

Phishing is one of the most common methods of cyberattacks, which includes sending fake messages to trick users into revealing sensitive information such as usernames, passwords, or financial information.

A) Spear Phishing: Attacks that target specific individuals or organizations.
B) Phishing via phone (Vishing) and SMS (Smishing): Versions of phishing that use phones or SMS for attacks.

Social engineering attacks

These attacks use psychological and human deception methods instead of technical techniques. The goal is to provoke the victim to provide sensitive information or access resources.

A) Pretexting: Creating fake scenarios to gain trust [21].
B) Baiting: Offering attractive promises such as free files to trick the victim into downloading malicious files.

DDoS (distributed denial of service) attacks

In this type of attack, a large volume of fake traffic is sent to a system or website, so that its resources are busy and access is disrupted by legitimate users. DDoS attacks are usually carried out to disrupt services or as part of a wider hacking program [22].

Data breaches

In this type of attack, hackers gain access to sensitive data of an organization and steal information such as user profiles, financial information or confidential business data. This information may be used to sell on illegal markets.

Insider threats

Sometimes cyber threats occur from within the organization, such that employees, contractors, or individuals with internal access to resources attempt to misuse or steal information. These threats may be intentional or unintentional, such as employees clicking on infected links [23].

Hacking

These attacks include: unauthorized access to systems, networks, or accounts to change, steal, or delete data.

A) Targeted Hacking: Attacks that target a specific organization or individual.

B) Backdoors: Covert methods that hackers use to bypass security measures [24].

Cyber espionage

This type of attack includes: intrusion into government systems, companies, or organizations with the aim of accessing sensitive information or confidential secrets. These threats are usually carried out by governments or organized groups.

IoT malware

Internet-connected devices such as security cameras, smart refrigerators, or thermostats often lack strong security measures, and hackers use these weaknesses to infiltrate and disrupt or steal information [25].

Supply chain threats

this type of attack involves: infiltrating an organization's business partners or suppliers. Hackers use weaknesses in the supply chain to gain unauthorized access to the target's data or infrastructure.

Zero-day attacks

In these attacks, hackers exploit unknown vulnerabilities in software or systems before developers can provide a solution for it [26].

Mobile threats

With the expansion of smartphone usage, cyber threats such as malicious apps, data theft, and SMS phishing have increased dramatically. Cyber threats are becoming more sophisticated and dangerous over time. Understanding the types of these threats and their risks is the initial step in protecting personal, business, and infrastructure information. Therefore, investing in cybersecurity and raising user awareness is an inevitable necessity.

Cyber security solutions

With the increase in cyber threats, adopting effective solutions to protect data, systems, and networks is of great importance. Below are the most important cybersecurity solutions that individuals and organizations can use to protect their digital assets:

Identity and access management (IAM)

Managing access to digital resources is an important part of cybersecurity. The following measures are useful in this regard:

Use multi-factor authentication (MFA) to increase account security [27].

Define access levels based on user needs and the principle of least privilege.

Disable unnecessary or outdated user accounts.

Use security software

Security software can provide a primary layer of protection against threats:

A) Antivirus and anti-malware: Identify and remove malware.

B) Firewalls: Protect the network from unauthorized traffic [28].

C) Intrusion detection and prevention systems (IDS/IPS): Identify and stop suspicious activities.

Encryption

Data encryption is an effective way to protect sensitive information from unauthorized access:

- ✓ Use end-to-end encryption for communications.
- ✓ Store sensitive information such as passwords using strong encryption algorithms.
- ✓ Ensure data security when transferred between systems or servers [29].

Regular updates and patches

Old and vulnerable systems are the main targets of cyber-attacks. Therefore,

- ✓ Software and operating systems must be updated regularly.
- ✓ Quickly install security patches to prevent vulnerabilities exploitation.

Data backup

Regular backups of sensitive information can be very useful in attacks or data loss:

- ✓ Backup in secure environments separate from the main network.
- ✓ Regularly test data recovery to ensure the accuracy of backups [30].

User training and awareness

Many cyber threats occur through human error. Training employees and users includes the following:

- ✓ Recognizing phishing emails and messages.
- ✓ Avoid downloading files or clicking on suspicious links.
- ✓ Create and manage strong passwords and change them regularly.

Continuous monitoring of systems and networks

Continuous monitoring of the network and systems helps to identify unusual activities early:

- ✓ Use monitoring tools to analyze unusual behaviors.
- ✓ Set up reporting and immediate alerts in the event of attacks.

Implement strict security policies

Organizations should define a set of security policies and processes:

- ✓ Require periodic password changes.
- ✓ Restrict the use of personal devices in work environments.
- ✓ Control remote access carefully.

IoT security

With the expansion of Internet-connected devices, it is essential to adopt security measures in this area:

- ✓ Change default device settings such as passwords.
- ✓ Use separate networks for IoT devices.
- ✓ Keep IoT device software up to date [31].

Penetration testing

Conducting security tests helps organizations identify and correct weaknesses in their systems and networks before they are deployed.

Implementing advanced authentication systems

- ✓ Using Biometric Authentication, such as fingerprints or facial scans.
- ✓ Implementing security tokens and smart cards to increase access security.

Cooperating with security centers and using the services of experts

Organizations can use the services of cybersecurity companies:

- ✓ Advice to develop a cybersecurity strategy.
- ✓ Using a Security Operations Center (SOC) to monitor and respond to threats.

Security in software development

Organizations that produce software must include security in the development process:

- ✓ Implementing Develops standards to integrate security into the development lifecycle.
- ✓ Security review of application codes and fixing vulnerabilities.

Using block chain in cybersecurity

Block chain can play an effective role in protecting data and increasing network security by providing a distributed and immutable system. Implementing cybersecurity solutions not only helps protect digital assets, but also plays an important role in reducing risks and improving trust in new technologies.

These solutions should be used comprehensively and continuously, and upgraded as cyber threats evolve [32].

Cybersecurity challenges

Cybersecurity is one of the most important areas in protecting information and systems, but its effective implementation is accompanied by numerous challenges. These challenges can arise from the complexity of the technology, lack of awareness, or the speed of evolution of cyber threats. Below are the most important cybersecurity challenges:

The growing number of sophisticated threats

Cyber threats are rapidly increasing in number and complexity. New techniques such as advanced social engineering attacks, zero-day attacks, and artificial intelligence-based malware have made it more difficult to predict and counter these threats [33].

Lack of skilled personnel

The lack of skilled professionals in the field of cybersecurity is one of the biggest challenges. Organizations face difficulty in finding trained personnel to manage and analyze cyber-attacks, which can increase the time to respond to attacks (Figure 3).

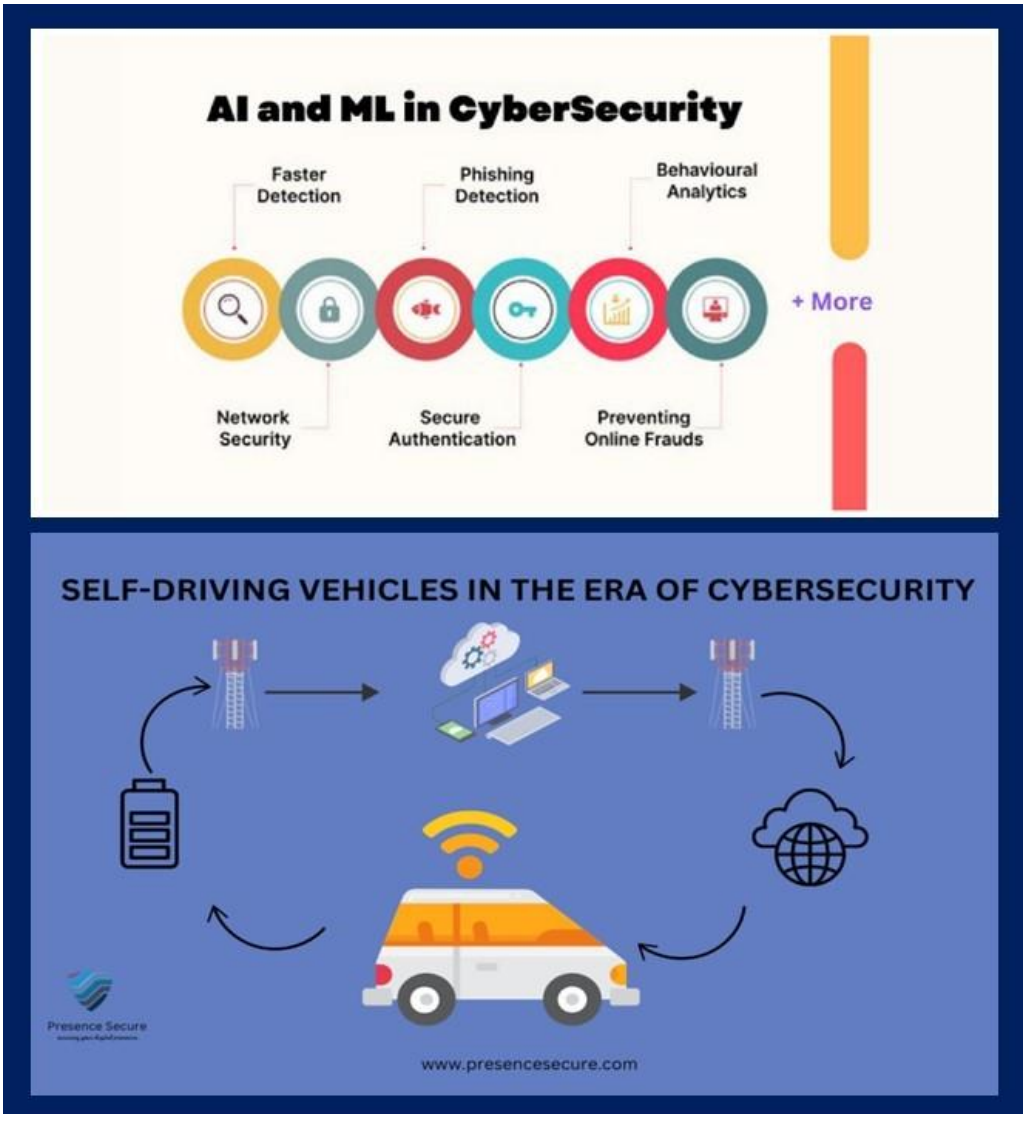

Figure 3: Cybersecurity challenges.

Complexity of systems and infrastructure

Many organizations use complex systems and networks that include: old, new, and hybrid technologies. Managing security in such environments is difficult because:

- ✓ Legacy systems may lack updates and support.
- ✓ Coordination between different components requires a lot of effort and resources.

Insider threats

Employees or people with inside access are one of the main sources of cyber risks. These threats may be caused by human errors, lack of adequate training, or even deliberate actions to steal data.

The speed of development of emerging technologies

New technologies such as the Internet of Things (IoT), block chain, big data, and artificial intelligence create new opportunities, but also bring many security challenges. These technologies are often deployed before thorough security review [34].

Budget constraints

Many organizations, especially small and medium-sized companies, do not have sufficient financial resources to implement comprehensive security strategies. This can make them vulnerable to attacks.

Lack of user awareness and training

Many cyberattacks succeed through human errors, such as clicking on phishing links or downloading malicious files. User awareness of cyber threats is the biggest security weakness in most organizations [35].

Compliance with changing laws and regulations

Laws and regulations related to privacy and information security, such as GDPR in Europe and CCPA in California, are changing and developing rapidly. Organizations must allocate significant resources to comply with these standards and avoid heavy fines.

Targeted attacks

Targeted cyberattacks, known as APT (Advanced Persistent Threat), are carried out by highly professional groups, often with significant financial support. These attacks often target governments and large organizations and are difficult to counter.

Difficulty in monitoring and responding promptly

Identifying threats in a timely manner and responding appropriately is a major challenge. Inefficient tools or lack of transparent processes make organizations highly vulnerable to attacks [36].

Supply chain threats

Many organizations depend on external suppliers, partners, and technologies. Supply chain intrusion can be an effective attack route for hackers. Recent examples of these types of attacks, such as the attack on Solar Winds, illustrate these risks.

Internet of things (IoT) security challenges

With the rapid growth of IoT devices, organizations are faced with a large amount of insecure data and connected devices with various vulnerabilities. These devices often lack adequate security standards.

Impact of AI and machine learning technologies

Although AI technologies are very effective in identifying cyber threats, hackers also use these technologies to create intelligent malware or carry out advanced attacks.

Lack of security in the cloud

Transferring data and services to the cloud can improve security and accessibility, but this space is also a target for cyber-attacks. Threats such as intrusion into user accounts and data breaches can cause serious problems [37].

Challenges of managing big data

The large volume of data generated by organizations makes it difficult to manage their security. Secure storage, transfer and processing of data is one of the main concerns of cybersecurity. Cybersecurity challenges continue to increase and evolve. Organizations must mitigate these challenges by using new technologies, creating a security-based organizational culture, and improving user education. It is also essential to use expert personnel and advanced methods to deal with these challenges. Cybersecurity, as one of the most important aspects of the digital world, plays a fundamental role in protecting privacy, information, and infrastructure. Given the rapid growth of technology and threats, organizations and individuals must continuously invest in cybersecurity and protect their assets using best practices. Only through awareness, education, and the use of new technologies can we deal with cybersecurity challenges [38].

Discussion

Cybersecurity mesh is of high signficance as a new approach to protecting data and networks. This architecture creates a powerful defensive shield against cyber-attacks by creating multiple layers of security at every point of the network. In today's complex and dynamic world where cyber threats are constantly evolving, cyber security mesh with high flexibility, rapid threat identification, and reduction of potential losses is proposed as a comprehensive and efficient solution to protect the information of organizations and individuals. Given the increasing number of cyber-attacks and the importance of data in the digital age, implementing a cybersecurity mesh has become an inevitable necessity [39]. The capacity of hard drives continues to increase at a slow pace. Recently, we have seen the launch of several models with a capacity of 30 terabytes. On the other hand, the capacity of solid-state drives (SSDs) is increasing at a very high rate. As we've seen with drives like the 61.44TB Solidigm D5-P5336, hard drives are losing ground. The 122.88TB generation is already available and several vendors have begun shipping them. Many networking experts believe that we will likely see the widespread availability of 122.88TB drives in 2025. We will also see the 245.76TB generation in the near future, which will enter the market faster than many expect. Implementing a cybersecurity network is a complex, multi-step process that requires careful planning and collaboration across all parts of the organization. The initial step is to carefully assess the organization's current cybersecurity posture [40]. This assessment includes: identifying digital assets, assessing existing threats, and examining the weaknesses of current systems. After that, a comprehensive security architecture is designed based on the cybersecurity network, in which each device, application, and data have an independent security layer. Then, the infrastructure necessary to implement this architecture, including security tools, management and monitoring software, and the required hardware, is prepared and configured. In the next step, clear and precise security policies are developed and implemented for access control, data encryption, and incident management. Training employees on the importance of cybersecurity and methods for dealing with threats is also of great importance. Finally, a continuous monitoring and management system is created to evaluate the performance of the security system and identify potential weaknesses. It is worth noting that implementing a cybersecurity network is a dynamic process that requires constant updating and adaptation to technological changes and new threats. More precisely, when implementing the above plan, it is important to pay attention to the following key points:

Setting specific goals

Before starting, define specific goals for implementing the cybersecurity network.

Involve all parts of the organization

All parts of the organization should participate in the implementation process.

Select the right tools

Select security tools according to the needs of the organization.

Train employees

Train employees on the importance of cybersecurity and how to use security tools [41].

Continuous monitoring and evaluation

Continuously monitor and evaluate the security system.

Flexibility

The security system must be able to adapt to changes. By following these points, organizations can implement a strong and efficient security system based on cybersecurity network and protect their digital assets from cyber threats. Security agency warns businesses that the level of cyber threat increases with the emergence of geopolitical tensions. Security agency warns businesses that the level of cyber threat increases with the emergence of geopolitical tensions. The UK's security agency has told organizations to take steps to bolster their defenses in the event of a surge in cyber threats due to software flaws or geopolitical tensions. The National Cyber Security Centre (NCSC) is not the only one warning companies to take action. Last week, the US Cybersecurity and Infrastructure Security Agency (CISA) also warned all organizations to take immediate steps to mitigate critical cyber threats in response to last week's cyber-attacks on Ukrainian government websites and IT systems. The advice comes amid growing fears of a Russian invasion of Ukraine. CISA issued the warning after Microsoft discovered a malware known as "WhisperGate" on several Ukrainian systems. CISA reminded American businesses of Not Petya, a ransomware that targeted Ukrainian organizations in 2017 through a malicious update to a popular accounting software package, but also infected the IT networks of American and European businesses. The attack cost American and European companies billions of dollars, according to White House estimates. Raf Pilling, a senior security researcher at Secure Works Threat Intelligence, believes that American and European organizations could fall victim to Whisper Gate in a similar way. While it's unlikely that organizations outside of Ukraine would be directly targeted, customers could potentially be exposed to collateral damage through service providers or business partners in Ukraine, Pilling said [2]. Organizations need to be very vigilant and back up business-critical systems and data, perform recovery processes before they are needed and ensure that backups are not affected by ransomware-style or malware-wiping attacks. So, what should businesses and government agencies potentially affected in the UK and elsewhere do to reduce the risk of collateral damage? The UK's NCSC says organizations need to balance cyber risks with defense, noting that there may be times when the cyber threat to an organization is higher than usual. The NCSC says: "Drivers for increased risk include: increased adversary capability due to new flaws in popular software, or something more specific to a particular organization, sector or even country, due to hackerism or geopolitical tensions." The NCSC's answer is to control what you can. Because you cannot control the level of the threat, that means patching systems, checking configurations and protecting the network against password attacks. The NCSC says: "It is rare for an organization to be able to influence the level of threat. Therefore, measures are usually focused on reducing your vulnerability to an attack in the first place and reducing the impact of a successful attack. CISA, NCSC has provided a list of essential cybersecurity measures that are important in any situation, but are especially important during periods of increased cyber threat and are especially important to implement. This is because organizations are unlikely to be able to quickly implement sweeping changes when the threat level increases.

Conclusion

According to Forbes and BlackBerry research, 76% of companies have prioritized AI and

machine learning in their IT budgets, so they can analyze large volumes of data to identify and mitigate cyber threats. As a result, AI is an essential tool for both cybercriminals and the fight against cybercrime. Another capability of AI is the design of adversarial malware samples that are specifically designed to deceive AI. By generating such examples, experts can create the necessary security measures to protect AI models and systems from adversarial attacks. These measures can lead to strengthening the defenses and robustness of AI against sophisticated attacks by adversaries and cybercriminals. AI can analyze and examine user behavior to make it harder for cybercriminals to use password-smashing techniques, consider possible password combinations, create new password models that are harder to crack, and design stronger authentication systems. These AI capabilities can help increase cybersecurity. AI can identify vulnerabilities in software systems and provide recommendations to fix them, and in this regard, it can be more powerful than antiviruses. Since it reduces the time and effort required to identify and fix security flaws and improves the overall security posture of systems and applications with its optimal performance compared to old tools. On the other hand, AI can detect suspicious behavior that indicates network intrusion and respond appropriately to protect critical infrastructure. In other words, AI enables continuous automated monitoring, which is essential for modern cybersecurity. One of the dangers of language-generating AI is the ability to create very convincing phishing emails, messages, or phone calls. This is a major alarm for individuals in organizations and even governments. Because attackers can use phishing to trick users into committing malicious actions and revealing sensitive information. The complexity of generative AI enhances the effectiveness of social engineering and makes it harder to resist it. Raising a society with high cyber and media literacy and awareness of the principles of social engineering to prevent being deceived by modern technological tools is one of the needs of humanity today. Generative AI can produce very realistic deep fake content in image, video, and audio formats. Using this AI capability, abusers can manipulate public opinion by spreading false information and even forge people's identities. Deepfake can have severe consequences such as damaging reputations, political abuses, and ultimately irreparable damage to public trust. Attackers can bypass traditional security tools such as antiviruses by designing malware with a complex system and carry out complex attacks by designing and producing malware that is constantly developing and evolving and evades detection. The use of generative AI in cybersecurity has raised concerns about the violation of individuals' privacy and biased decision-making of this tool. In other words, generative AI is capable of threatening the security of users in cyberspace. It is necessary to create legal frameworks around the liability of this new technological tool and update them simultaneously with the advances in AI, to increase its obligations by creating the necessary norms and regulations.

Orcid

Seyed Milad Kashefi Pour Dezfuli: 0000-0001-9567-5817

Reference

[1]. F. Jameel, Z. Chang, J. Huang, T. Ristaniemi, Internet of autonomous vehicles: architecture, features, and socio-technological challenges, *IEEE Wireless Communications*, **2019**, *26*, 21-29. [Crossref], [Google Scholar], [Publisher]
[2]. E. Yağdereli, C. Gemci, A.Z. Aktaş, A study on cyber-security of autonomous and unmanned vehicles, *The Journal of Defense Modeling and Simulation*, **2015**, *12*, 369-381. [Crossref], [Google Scholar], [Publisher]
[3]. S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber threats facing autonomous and connected vehicles: Future challenges, *IEEE Transactions on Intelligent Transportation Systems*, **2017**, *18*, 2898-2915. [Crossref], [Google Scholar], [Publisher]
[4]. V.K. Kukkala, S.V. Thiruloga, S. Pasricha, Roadmap for cybersecurity in autonomous vehicles, *IEEE Consumer Electronics Magazine*,

2022, *11*, 13-23. [Crossref], [Google Scholar], [Publisher]
[5]. J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, *IEEE Transactions on Intelligent transportation systems*, **2014**, *16*, 546-556. [Crossref], [Google Scholar], [Publisher]
[6]. M. Chowdhury, M. Islam, Z. Khan, Security of connected and automated vehicles, *arXiv Preprint Arxiv:2012.13464*, **2020**. [Crossref], [Google Scholar], [Publisher]
[7]. F. Jahan, W. Sun, Q. Niyaz, M. Alam, Security modeling of autonomous systems: A survey, *ACM Computing Surveys (CSUR)*, **2019**, *52*, 1-34. [Crossref], [Google Scholar], [Publisher]
[8]. A. Khadka, P. Karypidis, A. Lytos, G. Efstathopoulos, A benchmarking framework for cyber-attacks on autonomous vehicles, *Transportation Research Procedia*, **2021**, *52*, 323-330. [Crossref], [Google Scholar], [Publisher]
[9]. K. Kim, J.S. Kim, S. Jeong, J.H. Park, H.K. Kim, Cybersecurity for autonomous vehicles: Review of attacks and defense, *Computers & security*, **2021**, *103*, 102150. [Crossref], [Google Scholar], [Publisher]
[10]. X. Sun, F.R. Yu, P. Zhang, A survey on cyber-security of connected and autonomous vehicles (CAVs), *IEEE Transactions on Intelligent Transportation Systems*, **2021**, *23*, 6240-6259. [Crossref], [Google Scholar], [Publisher]
[11]. C. Gao, G. Wang, W. Shi, Z. Wang, Y. Chen, Autonomous driving security: State of the art and challenges, *IEEE Internet of Things Journal*, **2021**, *9*, 7572-7595. [Crossref], [Google Scholar], [Publisher]
[12]. M.C. Chow, M. Ma, Z. Pan, Attack models and countermeasures for autonomous vehicles, *Intelligent Technologies for Internet of Vehicles*, **2021**, 375-401. [Crossref], [Google Scholar], [Publisher]
[13]. H.P.D. Nguyen, D.D. Nguyen, Drone application in smart cities: The general overview of security vulnerabilities and countermeasures for data communication, *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, **2021**, 185-210. [Crossref], [Google Scholar], [Publisher]
[14]. J.P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations, *International Journal of Information Security*, **2022**, *21*, 115-158. [Crossref], [Google Scholar], [Publisher]
[15]. P. Ranaweera, A. Jurcut, M. Liyanage, MEC-enabled 5G use cases: A survey on security vulnerabilities and countermeasures, *ACM Computing Surveys (CSUR)*, **2021**, *54*, 1-37. [Crossref], [Google Scholar], [Publisher]
[16]. T. Campisi, A. Severino, M.A. Al-Rashid, G. Pau, The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities, *Infrastructures*, **2021**, *6*, 100. [Crossref], [Google Scholar], [Publisher]
[17]. M.A. Ribeiro, D. Gursoy, O.H. Chi, Customer acceptance of autonomous vehicles in travel and tourism, *Journal of Travel Research*, **2022**, *61*, 620-636. [Crossref], [Google Scholar], [Publisher]
[18]. E.V. Brovarone, J. Scudellari, L. Staricco, Planning the transition to autonomous driving: A policy pathway towards urban liveability, *Cities*, **2021**, *108*, 102996. [Crossref], [Google Scholar], [Publisher]
[19]. A. Aldakkhelallah, M. Simic, Autonomous vehicles in intelligent transportation systems, Human Centred Intelligent Systems: Proceedings of KES-HCIS 2021 Conference, Springer, 2021, pp. 185-198. [Crossref], [Google Scholar], [Publisher]
[20]. A. Ahmadpour, Investigating the economic feasibility of using a fuel cell for a chlor-alkali unit of a petrochemical company, *Eurasian Journal of Chemical, Medicinal and Petroleum Research*, **2024**, *4*, 42-55. [Google Scholar], [Publisher]
[21]. A. Ahmadpour, synthetic wastewater Treatment of methanol to propylene conversion unit by membrane bioreactor system, *Eurasian Journal of Chemical, Medicinal and Petroleum Research*, **2024**, *3*, 140-151. [Google Scholar], [Publisher]
[22]. A. Algarni, V. Thayananthan, Improvement of 5G transportation services with SDN-based security solutions and beyond 5G, *Electronics*, **2021**, *10*, 2490. [Crossref], [Google Scholar], [Publisher]

[23]. R.A. Shaikh, V. Thayananthan, Risk-based decision methods for vehicular networks, *Electronics*, **2019**, *8*, 627. [Crossref], [Google Scholar], [Publisher]
[24]. V. Thayananthan, J. Yazdani, Secure Cyber-Physical Systems for improving transportation facilities in Smart cities and industry 4.0, *Secure Cyber-Physical Systems for Smart Cities*, **2019**, 1-26. [Crossref], [Google Scholar], [Publisher]
[25]. A. Gupta, S.K. Gupta, Flying through the secure fog: a complete study on UAV-fog in heterogeneous networks, *International Journal of Communication Systems*, **2022**, *35*, e5237. [Crossref], [Google Scholar], [Publisher]
[26]. D. Sharma, S.K. Gupta, A. Rashid, S. Gupta, M. Rashid, A. Srivastava, A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique, *Transactions on Emerging Telecommunications Technologies*, **2021**, *32*, e4114. [Crossref], [Google Scholar], [Publisher]
[27]. S. Kumar, M.K. Chaube, S.N. Nenavath, S.K. Gupta, S.K. Tetarave, Privacy preservation and security challenges: a new frontier multimodal machine learning research, *International Journal of Sensor Networks*, **2022**, *39*, 227-245. [Crossref], [Google Scholar], [Publisher]
[28]. A. Alharbi, A. Alotaibi, L. Alghofaili, M. Alsalamah, N. Alwasil, S. Elkhediri, Security in social-media: awareness of phishing attacks techniques and countermeasures, *2022 2nd International Conference on Computing and Information Technology (ICCIT), IEEE*, **2022**, 10-16. [Crossref], [Google Scholar], [Publisher]
[29]. J. Chen, A.J. Gallo, S. Yan, T. Parisini, S.Y.R. Hui, Cyber-attack detection and countermeasure for distributed electric springs for smart grid applications, *IEEE Access*, **2022**, *10*, 13182-13192. [Crossref], [Google Scholar], [Publisher]
[30]. D. An, F. Zhang, Q. Yang, C. Zhang, Data integrity attack in dynamic state estimation of smart grid: Attack model and countermeasures, *IEEE Transactions on Automation Science and Engineering*, **2022**, *19*, 1631-1644. [Crossref], [Google Scholar], [Publisher]
[31]. A. Bahalul Haque, B. Bhushan, A. Nawar, K.R. Talha, S.J. Ayesha, Attacks and countermeasures in IoT based smart healthcare applications, Recent advances in internet of things and machine learning: Real-world applications, **2022**, 67-90. [Crossref], [Google Scholar], [Publisher]
[32]. M.N. Ahangar, Q.Z. Ahmed, F.A. Khan, M. Hafeez, A survey of autonomous vehicles: Enabling communication technologies and challenges, *Sensors*, **2021**, *21*, 706. [Crossref], [Google Scholar], [Publisher]
[33]. H. Bangui, M. Ge, B. Buhnova, L. Hong Trang, Towards faster big data analytics for anti-jamming applications in vehicular ad-hoc network, *Transactions on Emerging Telecommunications Technologies*, **2021**, *32*, e4280. [Crossref], [Google Scholar], [Publisher]
[34]. H. Bangui, M. Ge, B. Buhnova, Improving big data clustering for jamming detection in smart mobility, *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35*, 2020, 78-91. [Crossref], [Google Scholar], [Publisher]
[35]. A. Samimi, Risk Management in EPC Projects, *Eurasian Journal of Chemical, Medicinal and Petroleum Research* 3, **2024**, 191-201. [Crossref], [Google Scholar], [Publisher]
[36]. J. Renn, Einstein's invention of Brownian motion, *Annalen der Physik*, **2005**, *517*, 23-37. [Crossref], [Google Scholar], [Publisher]
[37]. S. Bokhari, S. Hamrioui, M. Aider, Cybersecurity strategy under uncertainties for an IoE environment, *Journal of Network and Computer Applications*, **2022**, *205*, 103426. [Crossref], [Google Scholar], [Publisher]
[38]. N.R. Potlapally, S. Ravi, A. Raghunathan, N.K. Jha, Analyzing the energy consumption of security protocols, *Proceedings of the 2003 International Symposium on Low Power Electronics and Design*, **2003**, 30-35. [Crossref], [Google Scholar], [Publisher]
[39]. S.A. Oussous, F.Z. Hamza, S. Beloualid, A.E. Allali, A. Bajit, A. Tamtaoui, Green smart city intelligent and cyber-security-based iot transportation solutions for combating the Pandemic COVID-19, *Computational Intelligence Techniques for Green Smart Cities*, **2022**, 129-146. [Crossref], [Google Scholar], [Publisher]
[40]. D. Said, M. Elloumi, L. Khoukhi, Cyber-attack on P2P energy transaction between connected electric vehicles: A false data injection detection-based machine learning

model, *IEEE access*, **2022**, *10*, 63640-63647. [Crossref], [Google Scholar], [Publisher]
[41]. S. Srivastava, A. Tiwari, P.K. Srivastava, Review on quantum safe algorithms based on Symmetric Key and Asymmetric Key Encryption methods, *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE*, **2022**, 905-908. [Crossref], [Google Scholar], [Publisher]