Karshi Multidisciplinary International Scientific Journal

Vol. 1(1) (2024), 96–106

FRAMEWORK, TOOLS AND CHALLENGES IN CYBER SECURITY

F. Basholli, D.A. Juraev and Kh. Egamberdiev

Communicated by Ebrahim Eldesoky Elsayed

Abstract: In recent years, the Internet has become an integral element of the daily lifestyle of people throughout the human society, and online crime, on the other hand, has increased along with the increase in Internet activity. Cyber security has advanced greatly in recent years to keep up with the rapid changes taking place in cyberspace. Cybersecurity refers to the methods a country or organization can use to protect products and information in cyberspace, where two decades ago, the term "cybersecurity" was unknown to the general public. Cyber security is not only a problem that affects individuals, but it is more important for organizations, public and private institutions. Recently everything has been digitized, using a variety of technologies such as the Cloud, smartphones and the Internet of Things and where cyber attacks are raising concerns about privacy, security and finance. Cybersecurity is a set of technologies, processes and practices aimed at preventing attacks, protecting against damage and illegal access to networks, computers, programs and data. The main purpose of this article is to conduct an examination of the types of cyber security within the framework of a security framework, the tools, methods and difficulties for more cyber security. In conclusion, we will understand that cyber security protects data and the integrity of IT assets that are part of or connected to an organization's network and aims to protect these assets from all threat actors throughout the life cycle of a cyber attack.

Keywords and phrases: The Cauchy problem, regularization, factorization, regular solution, fundamental solution.

MSC 2010 Classifications: Primary 68M25; Secondary 68M12.

1 Introduction

The Internet is one of the most important inventions that continues to have a significant impact on our lives. Today, the Internet has broken all barriers and transformed the way we communicate, work, shop, connect with friends, listen to music, watch movies, order food, pay bills, play games and greet friends on their birthdays and anniversaries. Our world is becoming increasingly networked, where digitized information is supporting key services and infrastructures. Nations, states, organizations and end-users are all concerned about the threats they are experiencing in maintaining the confidentiality, integrity and availability of digitized information, where in a digital world that is progressively permeating every area of our daily lives, both public and private, security is a must. The attacks have caused damage to unprepared citizens, businesses and organizations, even putting their operations at risk. In the field of information technology, cyber security plays a critical role and when we come across a scam or attack, cyber security is the first thing that comes to mind. The number of networked devices has expanded at a rapid pace, exceeding about 50 billion by the end of 2023, resulting in an increase in the number of vulnerable devices, thus protecting data online has become a concern. large [13]-[19]. The stages followed by a cyber attacker can be summarized (Figure-1):

• Discovery that includes scanning the environment or gathering information from social media and any other source.

• Weaponization, which includes creating a digital arsenal – turning discovered vulnerabilities into potential threats.

• Attack launch - sending malicious material/malware to infiltrate target systems.

• Processing the findings - placing the malware code, activating it by exploiting the victim's weaknesses.

• Installing malware on the system.

• Command and control takeover where attackers create a remote command channel to manipulate the victim.

• Actions according to the Objectives where the attacker seeks to achieve the goals - extraction of data, disruption of services until the fulfillment of the main objective of the attack.

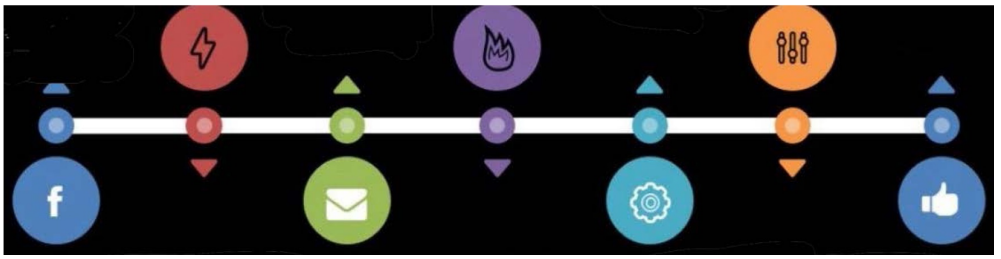

Figure 1. The stages followed by a cyber attacker.

2 Cyber security framework

Data is the most valuable asset, especially the security of digital data has become a priority around the world, where data breaches and security flaws can endanger the global economy. Developing a cyber security framework to help mitigate cyber risks is linked to a country's national and economic security. Security of vital systems and data is currently a problem for businesses of all sizes, industries, educational institutions and in context for all public structures. A public or private organization needs a strategic, well-thought-out cyber security plan to protect critical infrastructure and information systems to address these issues and comply with national cyber security frameworks. When used correctly, a cybersecurity framework allows IT security leaders to more effectively manage their companies' cyber threats. A company can use an existing cybersecurity framework or create one from scratch to meet its specific requirements. Various cybersecurity groups, including government institutions, produce these frameworks to serve as guidance for organizations looking to improve their cybersecurity. By cyber security framework we must understand a set of documents that define the best practices of an organization to manage cyber security risk and such frameworks reduce the exposure to the vulnerability of digital data available to a company or organization. Each cybersecurity framework will describe in detail how to implement a five-step cybersecurity approach. The Cyber Security Framework is a set of rules that private sector firms can use to detect, identify and respond to cyber threats, cyber security frameworks have the potential and are becoming legal instruments in the implementation of security legislation by defining guidelines for to help businesses prevent and recover from cyber attacks [5]-[7]-[28]. The cybersecurity framework should be considered by businesses of all sizes, regardless of the stages of development they are in, with flexibility in mind. This framework can be customized to be used by any organization of public or private structure thinking about a customized and integrated option. The main roles of cyber security, now accepted by banks, energy, water businesses, telecommunications companies and a wider community include [3]- [15]:

• Identification: To manage cybersecurity risk to systems, assets, data and capabilities, companies must first understand their environments.

• Detection: Organizations should establish the necessary procedures to detect cyber security incidents as soon as possible.

• Protection: Organizations must create and deploy appropriate controls to limit or cope with the consequences of potential cyber security incidents.

• Response (counteraction): Businesses must be able to build response plans to mitigate the effects of cyber attacks.

• Recovery: Businesses must design and implement effective strategies for restoring capabilities or services that have been damaged as a result of cyber security incidents.

Figure 2 shows schematically the five main functions of the security framework.

Figure 2. The five main functions of cyber security framework.

2.1 The core of the framework

It provides a list of the necessary cyber security exercises needed for the training of managers, their assistants and specialists who manage telecommunication systems in achieving results. Core helps organizations manage and reduce their cybersecurity risks in a way that complements existing security and addresses future risk management processes. The core is a collection of desirable cyber security activities and the results to be achieved, linked with informative references also gathered from the experience and mistakes of others [22]-[30]. The core of the framework should be intuitive and serve as a protective layer to allow IT systems service teams to communicate and collaborate using a simple and not necessarily technical language. As part of the Cyber Security Framework, we can identify three main components shown in figure 3.

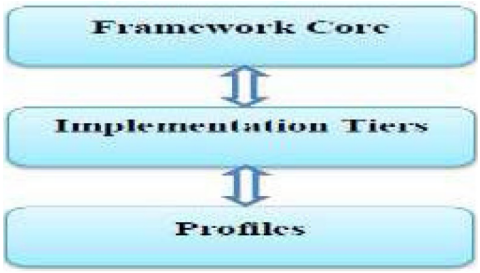

Figure 3. The cyber security framework components.

2.2 Levels of implementation

It helps organizations by determining how to approach cyber security risk management at several levels by defining the right details and programming the right measures for cyber security, it is often used as a specialized tool to discuss the intentions of the system attacker, the risk that present, the necessity of the security mission and the budget that must be spent, keeping in every case the criteria provided by the security framework. The levels vary in several degrees, from the partial first level to an increasing level of attack severity, integrating broader decisions and the extent to which the company provides and receives information on cyber security from third parties. Levels do not always correspond to maturity levels, but in any case organizations must determine the target level, ensuring that it meets business objectives and minimizes cyber security risk to acceptable levels.

2.3 Profiles

Profiles are the unique arrangement of an organization's requirements, goals, and organizational assets in relation to desired outcomes within the framework of the security framework. Profiles are primarily used to identify and categorize "open doors" for improving an organization's

cybersecurity. Profiles are the unique alignment of goals and objectives, risk prediction and resources that the Security Framework provides for achieving the desired results. By comparing an "actual" profile with an "objective" profile, opportunities can be discovered to strengthen the cybersecurity posture so that it can best serve the organization, institution, enterprise, etc.

3 Cyber cecurity tools

Protecting hardware, software and data from hackers is called cyber security. These protect against cyber attacks aimed at financial gain, changing or destroying sensitive data, etc. Cyber attacks have the ability to bring an entire country to its knees. As a result, protecting these networks is not an option, but a requirement [35]. It is important for every firm to be informed of potentially dangerous security attacks and to keep them safe, and many different components of cyber defense must be considered. There are many cyber security technologies that can perform a privacy audit on all software and detect and avoid and remove the latest risks [9]. These cyber security solutions help you control file access and conduct further investigations. Here are six critical technologies and services that every company should evaluate and consider effective in order to provide the best possible cyber protection.

3.1 Firewalls

Firewall, as we all know, is at the heart of security technologies and has become one of the most critical security tools. Its job is to keep unauthorized users away from accessing a private network. It can take the form of hardware, software or a hybrid of the two. Unauthorized Internet users are prevented from accessing private networks connected to the Internet through firewalls [16]. The firewall filters all messages entering and leaving the intranet. Every message is examined by the firewall, and those that do not meet the security standard are blocked.

3.2 Antivirus software

Antivirus software is a program that prevents, detects and removes viruses and other malware from personal computers, networks and IT systems. Trojan horses, worms, keyloggers, browser hijackers, rootkits, spyware, botnets, adware and ransomware are among the threats and viruses that this antivirus software protects us from. Most antivirus programs include an automatic update capability that allows the system to scan for new viruses and threats in real time. It also offers other services such as email scanning to ensure that emails do not have harmful attachments.

3.3 PKI services

Data protection through public key (PKI). This program enables you to distribute and identify public encryption keys. It allows individuals and computers to communicate data over the Internet securely while also verifying the identity of the other party. We can also exchange sensitive information without PKI, but in that case, there would be no assurance of authentication of the other party. People associate [10] PKI with SSL or TLS. It is the technology that encrypts the communication on the server and is responsible for the HTTPS that we can see in the address bar of our browser. PKI solves many cybersecurity problems and deserves a place in the organization's security stack.

3.4 Software as a cyber security tool

Without a solid cybersecurity staff, no firm can avoid today's cyber risks and security challenges. Hackers are constantly looking for security flaws in order to exploit them and put companies at risk. Albania is ranked among the countries most attacked by cybercriminals in the last three years. When it comes to protecting sensitive and private data held by businesses and individuals, cybersecurity software plays a critical role.

3.5 Network security monitoring tools

Network security monitoring solutions make network administration and monitoring easier while also helping to audit security compliance. Antivirus applications, firewalls, and intrusion detection systems are examples of network security solutions that sit at the edge of the network and work together to help ensure its safety and security. There are also network security utility tools used in penetration testing, such as packet analyzers and port scanners, which allow system administrators and security professionals to identify vulnerabilities that threat actors can use to exploit. your network with DDoS attacks and more.

3.6 Managed detection and response (MDR) service

To breach an organization's security, today's cybercriminals and hackers use the most modern techniques and tools. As a result, it is imperative that all firms employ more robust cyber security protections. Threat intelligence, threat intelligence, security monitoring, incident analysis and incident response are all part of the advanced security solution. It is a service that is designed to help organizations (with limited resources) become more aware of risks and increase their ability to recognize and respond to threats. MDR also uses Artificial Intelligence (AI) and machine learning to research, automatically detect risks and orchestrate responses to achieve faster results.

3.7 Penetration testing

Penetration testing, often known as pen testing, is a method of assessing a company's security systems and the security of its IT infrastructure by safely exploiting vulnerabilities. These flaws can be found in the operation of the system, the services and applications that are offered, as well as in incorrect configurations and insecure behavior of the end user. Cyber security professionals will perform penetration testing using the same tools and processes used by criminal hackers [27]. A pen test simulates the type of attacks that criminal hackers might launch against a company, such as password cracking, code injection, and phishing. This test can examine servers, online applications, network devices, endpoints, wireless networks, mobile devices, and other potential vulnerabilities using manual or automated technologies. Once the pen test has been successfully completed, the pen testers will report their results to us and may be able to help us by recommending system fixes.

3.8 Web vulnerability scanning tools

Web vulnerability and scanning tools are automated programs that analyze your organization's web applications for security flaws including SQL injection, command injection, path traversal, cross-site scripting, and insecure server configuration. Your web vulnerability scanning tools should provide you with a detailed post-scan report that includes a list of vulnerabilities, detailed explanations of the risks and vulnerabilities, and remediation recommendations.

3.9 Staff training

Staff training is not a "cyber security tool", but it is one of the most effective types of defense against cyber attacks to have knowledgeable staff who understand cyber security. There are now many training options available that can teach employees about cybersecurity best practices. Any company can use these training tools to teach their employees about cybersecurity and their role in it. All cyber thieves know this and are constantly improving their methods and level of expertise to penetrate security in public and private institutions and companies operating in various fields. It has become critical for businesses to invest in training tools and services. If they fail to do this, they risk putting the company in a situation where hackers can simply target their security system and it would cost the organization a lot in terms of security [4].

4 Cyber security challenges

Cyber security is becoming a critical part of the country's overall national security and economic plans. The key to overcoming cybersecurity challenges is to stay ahead of the game by adopting proactive measures before adversaries [27] exploit the system. It serves a crucial role in protecting our privacy in these days of digitization, when hackers are becoming more and more sophisticated. We hear about threats like ransomware, phishing, vulnerability exploitation, IoT-based attacks, and so on every day. Cloud infrastructure is powered by the Internet, making it vulnerable to a variety of attacks and data breaches. Easy Jet is the most prominent case, where hackers gained access to the travel data of 9 million customers by taking phone numbers, email addresses, personal correspondence, contracts and agreements with all advertising firms, etc., causing not only issues reputational or [24] monetary loss but there is also the possibility that companies will go bankrupt after paying the fines. As a result, security analysts face numerous issues related to cyber security, such as securing classified government data, securing private company servers, and so on. Ransomware, phishing attacks, malware attacks, and other cybersecurity concerns [33] arise in various forms.

4.1 IoT threats

The Internet of Things (IoT) is a term that refers to a network of connected devices. It is a network of interconnected physical devices that can be accessed through the Internet. Connected physical devices are given a unique identifier (UID) and can communicate data over a network without the need for human or human-computer contact. Consumers and organizations are particularly vulnerable to cyberattacks due to the firmware and software running on IoT devices. By 2024, IoT [26] is predicted to have 11.6 billion IoT devices in the market. IoT devices are computing, digital and mechanical devices that can send data themselves through the Internet, where as an example we can bring desktops, laptops, mobile phones, smart security devices, etc. As the popularity of IoT devices grows at an unprecedented rate, so do the cybersecurity challenges. When IoT devices are built, they are not designed with cybersecurity and commercial considerations in mind. To help manage risk, every firm should work with cybersecurity experts [18] to ensure the security of their password rules, session handling, user authentication, multi-factor authentication, and security procedures. Compromise of sensitive user data can occur when IoT devices are attacked. Securing IoT devices is one of the biggest challenges in Cyber Security, as access to these devices can open doors to other malicious attacks [14]-[34].

4.2 Evolution of ransomware

Ransomware is a type of software that encrypts data on the victim's computer and demands payment from the victim so that the data can be released. The victim's access rights are restored after a successful payment. IT experts and all executives fear ransomware [2]. Ransomware attacks have grown in popularity in recent years and in 2023, they were one of the most important Cyber Security threats worldwide. Ransomware attacks are dangerous for individual users, but they are much more dangerous for organizations that cannot access the data they need to run their day-to-day operations. In most ransomware attacks, attackers refuse to release data even after receiving payment, instead trying to extort more money.

4.3 Blockchain and cryptocurrency attacks

The most important invention in the age of computing is Blockchain technology. We now have a real digital medium for the exchange of "monetary" values. Blockchain is a technology that allows the creation of cryptocurrencies such as Bitcoin. Blockchain is a massive worldwide platform that allows two or more parties to conduct business or conduct transactions for a third party by creating trust. It is difficult to say what Blockchain technology will bring in the future in terms of cyber security. Professionals in the field of cyber security make positive assessments about Blockchain technology, while developing applications in the context of cyber security [31]-[17] and it is expected that there will be a healthy development as well as complementary

synergy in the existing cyber security. Organizations must be aware of the challenges that may accompany these technologies in the future so that no gap is created for intruders.

4.4 Expanding artificial intelligence and machine learning

It is a branch of computer science concerned with building intelligent machines that function and react in the same way as humans. Machine learning and artificial intelligence technologies have proven to be extremely useful for significant progress in a number of fields [8], but they also have drawbacks. Speech recognition, learning, planning, problem solving and other artificial intelligence operations are just a few examples. Thus, the ability to protect an environment when a malicious attack is launched is impact mitigation and one of the key benefits of incorporating artificial intelligence into cybersecurity. Illegal individuals can use these technologies to carry out cyber attacks and represent a threat to enterprises, businesses. These algorithms can be used to find high-value targets in a vast dataset. Attacks in machine learning and artificial intelligence are a major concern today. Due to the lack of knowledge in this area of cyber security, a sophisticated attack can be very difficult to handle. Artificial intelligence reacts quickly to hostile attacks when they threaten a company's operations. After much research and modeling, artificial intelligence can identify anomalies in behavior patterns that can be used as a defensive tool, but unfortunately, hackers, phishers and thieves can use the same techniques to carry out a cyber attack.

4.5 BYOD policies

For its employees, most companies offer a Bring-Your-Own-Device policy. Having such systems creates a host of problems in terms of cyber security. To begin with, if the device has an outdated or pirated software version, it is already a prime target for hackers. Hackers can easily get confidential corporate data because the method is used for personal and professional purposes. Second, if their security is hacked, these devices make it easier to access your private network. Thus, organizations must abandon BYOD policies and provide secure devices for employees to face the major challenges of computer security and network compromisers.

4.6 Risks in the cloud

Cloud services are used by most people today for personal and professional purposes. Due to the inflexibility and costs associated with older data centers, businesses are migrating their critical data [6] to the cloud. Moving data to the cloud requires proper configuration and security procedures, or else you risk slipping into a trap. Cloud service providers only provide their platform in protecting a company's infrastructure against theft and cloud destruction is the firm's responsibility. Firewalls, multi-factor authentication, Virtual Private Networks (VPNs) and other cloud security solutions are available today, and organizations must implement procedures and technologies to protect against external and internal threats.

4.7 The technical skills gap

Thieves can simply clone identities for any scam and hackers can exploit any vulnerability even now in 2024, the problem will only get worse if there isn't an equal amount of resources and skills to deal with these problems. Companies must invest in training existing staff and acquire new resources to assess the network for risks and avoid cyber attacks, where companies can lose millions of dollars. Navigating potential threats, personnel education and experience in this field are essential. The IT manager's job is to provide guidance and training to enable employees to understand their position in the firm's security. Specialists should describe in the company that manage the strong and weak points, as well as apply alternative ways to actively train the staff, familiarizing them with security flaws, and this training should focus on the roles of employees in the security policy. of the company. Today, companies are investing extensively in making the system more secure, deploying new advanced technologies that require technically skilled, highly qualified and practical human resources.

4.8 Obsolete hardware

Not all cyber security threats take the form of software attacks. As software developers become more aware of the dangers of software vulnerabilities, they regularly provide updates. However, these new updates may not be compatible with the device hardware. This is what distinguishes obsolete hardware, where the hardware is not advanced enough to run the latest versions of software. This causes such outdated devices to be stuck with an older version of software, making them highly vulnerable to cyber attacks.

4.9 Biometric authentication

Biometric authentication is increasingly being used as a last resort cyber security solution. While some see biometrics as a new and effective tool to improve company security, others see it as a potential threat. Biometric identification can take many forms, from simple fingerprint scanning to more advanced ones such as voice, iris (pupil of the eye) or face recognition [29]. Many people think that biometric systems are almost impossible because the data they collect is impossible to guess and is unique to each user and recommend instead one-factor authentication in a system or a multi-factor authentication add-on as a solution. Biometric systems, on the other hand, have the disadvantage that biometric information, such as user identification and password, can still be stolen or copied, which is a serious issue, but unlike a password, users cannot modify the baby's scans. than the eye (iris) or get a new face and this is an advantage that creates new challenges for cyber security for professionals in the future.

4.10 5G technology

Applications of 5G technology will have great benefits, including improved performance and speed in data processing and increased efficiency. One of the most likely and well-known benefits of 5G technology is that it will enable even more IoT devices to connect to the Internet and support more connectivity between them [32]. This would allow consumers to connect or monitor their IoT devices remotely over the Internet, meaning that cyber attacks will always be possible. As a result, IoT devices and sensors will increasingly require complex authentication to prevent unwanted access, however potential risks cannot be avoided. To avoid widespread service disruptions, malicious exploitation of IoT devices, and millions, if not billions of dollars in losses, it is now inevitable to leave 5G security issues unaddressed. The 5G standard will result in a greater security risk in a wider and more diverse attack surface due to the massive number of devices expected to be connected and used in the cloud. To understand a healthy and strong communication future, the industry must focus on the current security in 5G technology.

4.11 Risks of mobile applications

Mobile app development has become a critical component of any company's success. As we are seeing that mobile applications are becoming more popular among consumers, making it even more vital for developers to make these applications secure. Security in mobile applications is critical, as it may be the data contained within the application that is compromised if appropriate security measures are not implemented during application development. Moreover, the increasing use of mobile applications has resulted in increased sensitivity, where hackers nowadays are interested in obtaining personal information from consumers for their own benefit. As a result, when developing apps for Android and iOS platforms, developers are showing more caution. Various platforms are available for developing applications through mobile, but none of them can guarantee complete security from viruses. Currently, many Android applications have been found to be infected with malware or have faulty code that thieves can exploit. App developers have been known to skip or undertake minimal testing on their apps, where the lack of testing could, in turn, lead to a data breach. The source code of a mobile application may incorporate code from third-party libraries. We advise you to use any library only after you have tested it thoroughly, as some libraries can be dangerous. Without decryption, we can change the transmitted data into a form that no one else can read. Hackers often infect a mobile app through vulnerable source code. Therefore, it's important to follow mobile app security best practices when writing code.

4.12 Evolution of bluetooth

People have been using Bluetooth technology to connect their devices and transfer data in an easy way. Bluetooth has a number of advantages and benefits, but they do not come without risk. authorization, authentication and optional encryption are all part of Bluetooth security. The act of verifying the identity of one Bluetooth device to another is known as authentication. Granting or denying Bluetooth, access to related resources or services from the requesting device is known as authorization. Encryption is the process of converting data into a secret code that cannot be read by eavesdroppers. Bluetooth [21] connections, like any other Internet connection, have significant drawbacks. This is especially true these days, when data hackers lurk around every corner, waiting to prey on unwary smartphone users. Bluetooth eavesdropping is a technique in which a hacker gains access to your Bluetooth-enabled phone and uses it to make spam calls and send text messages without your knowledge. Via Bluetooth hackers will use your phone to create a malicious phone book contact and then use that contact to send malicious text messages to your phone. And because your phone is already trusted by the contact, the messages will automatically open, stealing your data in the process. Currently viruses and worms are very common these days for smartphone users to unknowingly download apps that contain malware and other harmful files. Sometimes you misspell a URL and end up on a phishing page or download an app and it brings with it harmful malware. These viruses can open your Bluetooth and attack your shared files. In this case the hacker gains access to your Smartphone by connecting to your network, then proceeds to copy personal data from your phone's applications.

4.13 Evolution of recommendation systems

Users are increasingly using recommender systems to be exposed to the entire digital world through their behaviors, preferences, and interests [22]. An internet engine recommends a system that, based on data analysis, proposes products, services and information to users. The recommendation can be based on a variety of criteria, including user history and the behavior of similar users. To arrive at a recommendation [23], collaborative filtering utilizes data from the client and other users who share similar characteristics. Filtering based on content or product attributes you prefer to know as content-based filtering. The goal behind content-based filtering is to classify products with specific keywords, learn what the customer likes, search for those terms in the database, and then recommend similar things. When service providers collect more and more personal information, the public's privacy is at risk [25]. Malicious users seeking to deviate from the suggestions may aim to offer the service. Commercial recommender systems are often required to process large amounts of real-time data these days. Using cryptographic techniques to ensure privacy will be a major problem taking things a step further by relying heavily on a user's friends to generate recommendations. However, this would require the service provider to create/maintain a social network for all its customers, which may not be a simple task [1]. Another issue is the flaws in security models that are usually based on half-sincere attackers [20]. To acquire these functions in reality, service providers need to track user behavior, and most existing solutions are only concerned with protecting rating vectors [12] for users. Existing privacy protection technologies, such as anti-tracking techniques, can be integrated to give consumers more privacy protection which, unfortunately, may not be that simple. Finally, we can take basic steps to protect our devices and data against cyber threats by using the most up-to-date hardware and software for our digital needs. We will also need to take more advanced precautions, such as deploying a firewall to add an extra layer of security [11].

5 Conclusion

With the rapid advancement of technology, our lives are becoming more and more digitized. People now live in a cyber world where all data and information is stored digitally and online. The focus on cyber security is often an attempt to characterize the problem and determine the true level of threat. All individuals, professionals, legislators and more broadly all decision makers are concerned about cyber security. Cyberspace has no borders, a nation's cyberspace is a component of the global cyberspace and cannot be isolated in defining its boundaries and it is not easy to maintain cyber security, at a time when attacks are becoming more innovative every

day. Cyber security is a technology that is designed to protect data and information systems and the state or process of protecting and recovering networks, devices and programs from any type of cyber attack is known as cyber security.

Acknowledgment

The authors express their sincere gratitude to the reviewers and editors for their useful comments.

References

[1] A. Jeckmans, A. Peter, P. Hartel, Efficient privacy-enhanced familiarity based recommender system, *Proceedings of the 18th European Symposium on Research in Computer Security, ESORICS 2013, Lecture Notes in Computer Science*, **8134**, 400–417 (2013).

[2] S. Bag, S. Ruj and K. Sakurai, TBitcoin block withholding attack: Analysis and mitigation, *IEEE Transactions on Information Forensics and Security*, **8:12**, 1967–1978 (2017).

[3] F. Basholli, B. Mema, D. Hyka, A. Basholli, A. Daberdini, Analysis of security challenges in SCADA systems, a technical review on automated real-time systems, *8th Advanced Engineering Days*, 8–22 (2023).

[4] A. Basholli, B. Mema, F. Basholli, D. Hyka, D. Salillari, The role of education in cyber hygiene, *7th Advanced Engineering Days*, 178–181 (2023).

[5] F. Basholli, D. Hyka, A. Basholli, A. Daberdini, B. Mema, Analysis of cyber-attacks through simulation, *7th Advanced Engineering Days*, 120–122 (2023).

[6] F. Basholli, R. Mezini, A. Basholli, Security in the components of information systems, *7th Advanced Engineering Days*, 185–187 (2023).

[7] B. Genge, P. Haller, I. Kiss, A framework for designing resilient distributed intrusion detection systems for critical infrastructures, *International Journal of Critical Infrastructure Protection*, **15**, 3–11 (2016).

[8] J. Wayman, A. Jain, D. Maltoni, D. Maio, *Biometric Systems: Technology Design and Performance Evaluation*, Springer, Verlag (2005).

[9] B. Komar, R. Beekelaar, J. Wettern, *Firewalls for Dummies*, 1–17 (2001).

[10] C. Weissman, *Security Penetration Testing Guideline*, Handbook for the Computer Security Certification of Trusted Systems, Center for Secure Information Technology, Naval Research Laboratory (1993).

[11] A. Daberdini, B. Basholli, N. Metaj, E. Skenderaj, Cyber security in mail with Fortiweb and Fortinet for companies and institutions, *5th Advanced Engineering Days*, 81–83 (2022).

[12] A. Sfakianakis, Ch. Douligeris, L. Marinos, ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends, European Network and Information Security Agency (2019).

[13] F. Setiadi, P.H. Putra, Y.G. Sucahyo, Z.A. Hasibuan, Determining components of national cyber security framework using Grounded Theory, *Second Int. Conf. Informatics Comput.*, 1–6 (2017).

[14] M. Harizaj, I. Bisha, F. Basholli, IoT integration in electric car chargers'Infrastructure, *6th Advanced Engineering Days*, 152–155 (2023).

[15] D. Hyka, A. Hyra, F. Basholli,B. Mema, A. Basholli, Data security in public and private administration: Challenges, trends, and effective protection in the era of digitalization, *7th Advanced Engineering Days*, 125–127 (2023).

[16] I. Ijaz, Design and implementation of PKI (for multi domain environment), *Inter. Journal of Com. Theory and Eng.* **4:4**, 505–509 (2012).

[17] B. Mema, F. Basholli, Internet of things in the development of future businesses in Albania, *Advanced Engineering Science*, **3**, 196–205 (2023).

[18] N. Scaife, P. Traynor, K. Butler, Making sense of the ransomware mess planning a sensible path forward, *IEEE Potentials*, **36:6**, 28–31 (2017).

[19] N. Akhtar, A model based research material recommendation system for individual users, *Transactions on Machine Learning and Artificial Intelligence*, **5:2**, 1–8 (2017).

[20] N. Akhtar, Inverse conductivity problem in the infinite slab, *International Journal of Computer Applications*, **81:14**, 23–30 (2013).

[21] N. Akhtar, D. Agarwal, A Literature Review of Empirical Studies of Recommendation Systems, *International Journal of Applied Information Systems*, **10:2**, 6–14 (2015).

[22] N. Akhtar, D. Agarwal, An influential recommendation system usage for general users, *Foundation of Computer Science*, **5:7**, 5–9 (2016).

[23] N. Akhtar, D. Agarwal, A survey of imperfection of existing recommender system for academic fraternity, *IOSR Journal of Computer Engineering* , **20:3**, 8–15 (2018).

[24] B. Pranggono, A. Arabo, COVID-19 pandemic cybersecurity issues, *Internet Technology Letters*, **4:8**, 1–6 (2020).

[25] Q. Tang, J. Wang, Privacy preserving context-aware recommender systems: Analysis and new solutions, *Computer Security - ESORICS 2015*, **9327**, 101–119 (2015).

[26] R. Doshi, N. Apthorpe, N. Feamster, Machine learning DDoS detection for consumer internet of things devices, *IEEE Security and Privacy Workshops*, 29–35 (2018).

[27] R. Trifonov, G. Manolov, R. Yoshinov, G. Pavlova, A survey of artificial intelligence for enhancing the information security, *International Journal of Development Research*, **7:11**, 16866–16872 (2017).

[28] T. Chmielecki, P. Cholda, P. Pacyna, P. Potrawka, N. Rapacz, R. Stankiewicz, et al., Enterpriseoriented cybersecurity management, *Computer Science and Information Systems (FedCSIS) 2014 Federated Conference*, 863–870 (2014).

[29] A. Tudzarov, T. Janevski, Design of 5G mobile architecture, *International Journal of Communication Networks and Information Security*, **3:2**, 804–810 (2011).

[30] Yu. Nugraha, S. Member, I. Brown, A.S. Sastrosubroto, An adaptive wideband Delphi method to study state cyber-defence requirements, *IEEE Transactions On Emerging Topics in Computing*, **4:1**, 47–59 (2016).

[31] Yu. Perwej, A. Chaturved, Machine recognition of hand written characters using neural networks, *International Journal of Computer Applications*, **14:2**, 6–9 (2011).

[32] Yu. Perwej, K. Haq, U. Jaleel, Sh. Saxena, Some drastic improvements found in the analysis of routing protocol for the bluetooth technology using scatternet, *Special Issue on The International Conference on Computing, Communications and Information Technology Applications (CCITA-2010), Ubiquitous Computing and Communication Journal (UBICC)*, **5**, 86–95 (2010).

[33] Yu. Perwej, M.K. Omer, O.E. Sheta, H.A.M. Harb, M.S. Adrees, The future of internet of things (IoT) and its empowering technology, *International Journal of Engineering Science and Computing*, **9:3**, 20192–20203 (2019).

[34] Z.A. Soomro, M.H. Shah, J. Ahmed, Information security management needs more holistie approach: A literature review, *International Journal of Information Management*, **36:2**, 215–225 (2016).

[35] Z. Trabelsi, K. Hayawi, A. Braiki, S. Mathew, *Network Attacks and Defenses: A Hands-on Approach*, Boca Raton, Florida:CRC Press (2013).

Author information

F. Basholli, Department of Engineering, Albanian University, Tirana, 1001, ALBANIA.
E-mail: fatmir.basholli@albanianuniversity.edu.al; fatmirbashalli@gmail.com

D.A. Juraev, Department of Scientific Research, Innovation and Training of Scientific and Pedagogical Staff, University of Economics and Pedagogy, Karshi, 180100, UZBEKISTAN.
E-mail: juraevdavron12@gmail.com

Kh. Egamberdiev, Department of Computer Systems, University of Economics and Pedagogy, Karshi, 180100, UZBEKISTAN.
E-mail: ehojiakbar1984@gmail.com

Received: 01.02.024
Accepted: 31.03.2024
Published: 30.06.2024