Applied Computing Journal https://doi.org/10.52098/acj.202260
ISSN: 2788-9688 Volume 2, Issue 4, pp 227-244, October 2022
Received: 19/12/2022 Revised: 26/12/2022 Accepted: 29/12/2022

Cyber Security Threats, Vulnerability, Challenges with Proposed Solution

Vaman Ashqi Saeed[1], and Renas Rajab Asaad[2]
[1] 1Technical College of Administration, Information Technology Management Department, Duhok, Kurdistan Region of Iraq
[2] Department of Computer Science, Nawroz University, Duhok, Kurdistan Region of Iraq
* Corresponding author: Vaman Ashqi Saeed [1] , vamanatroushi@gmail.com

Abstract

Internet security is one of the most pressing concerns in the twenty-first century when taken into consideration with other online concerns. This is because technological progress, the growth of communications, and the development of the cyber-Internet have all led to a revolution in the way information and data is sent, as well as in e-commerce. Because of this, it was important to find ways to protect information and data on the internet, as well as electronic money accounts and electronic wallets. Information security on the Internet, security of electronic operations, network security, and application security are all included under the umbrella term "cybersecurity." Cybersecurity refers to the measures that are taken to protect data and information stored on all electronic devices that are connected to the Internet from malicious attacks, hacking operations, data theft, and sabotage. All electronic activities and applications require some kind of cyber security, including websites, financial institutions (including banks, banks, and bank accounts), satellite operations (including military missions), and drone management.

***Keywords**:* Cyber Security, Threats, Vulnerability, Attacks.

1. Introduction

Communication through the internet has become an essential component of modern infrastructure. The majority of applications and control mechanisms for infrastructure systems are now able to be run over the internet (Zebari et al., 2018). The tremendous improvements in network and communication technology led to significant advances in communication technology, which in turn led to substantial improvements in communications. Communication for multimedia material, particularly picture content, is becoming increasingly chronic via the internet. This is especially true for image content (Mohammad et al, 2017). Despite this, the openness and accessibility of the Internet pose a significant threat to the confidentiality of multimedia data, which slows down the pace of advancement in the field of communication. Therefore, the general public has to exercise extreme caution with regard to the privacy and safety of their multimedia communication (Ban Al-Omar et al., 2012; Zebari et al., 2021).

Under the concept of cybersecurity, various technologies and practices aimed at maintaining the security of computer systems and the data of their users have been incorporated, especially at the present time, which is witnessing a remarkable increase in the various actions carried out by individuals via electronic networks that use the Internet. Perhaps the most serious challenges facing cybersecurity are the electronic hacking operations carried out by criminal entities, with the aim of obtaining material benefits by stealing people’s data; or public or governmental institutions (Zebari et al., 2019; Yousif & Saini, 2020). Therefore, cyber security is important for many reasons, the most prominent of which are the following: Because it acts as the primary firewall to protect the various confidential data of these parties, cyber security is of utmost importance to a large number of public and private institutions and companies. If it were to fail or be penetrated, the institution or company would be an easy target for criminals. Cybersecurity prevents numerous sorts of sensitive and critical data from being stolen or harmed (Asaad, 2021; Pearson et al., 2011). This protection may be afforded to either the nation as a whole, corporations, or even individual persons. The breach of cyber security might cause significant harm to the reputation of the firm or organization, which would, in turn, have an effect on the volume of transactions carried out in commercial marketplaces. Hacking the cyber security of any party results in a significant and direct threat to a large number of customers' personal data. This is a process that would ruin the customer's relationship with this party and therefore expose the company to the risk of collapse if customers decide to stop cooperating with it because of this breach (Zebari et al., 2017). The purpose of computer or cyber security is to protect information and property from being stolen, corrupted, or destroyed by natural disasters, while at the same time ensuring that information and property can continue to be used effectively and can be accessed by the people for whom they were designed (Clements & Kirkham, 2010).

2. The Importance of Cybersecurity

Every government and every society should make the safeguarding of sensitive data in cyberspace a top priority in order to ensure its continued use. The use of cyber security is required on an individual basis for the purpose of protecting one's personal data, including photos, files, videos, personal accounts, passwords, and bank accounts. On the community level, we gathered data and protected community privacy in order to protect society from social engineering and target social behavior (Asaad, 2021). When it comes to protecting electronic assets, data, and information (including data on employees), servers, and websites at the corporate level and across various types of companies. At the state level, it protects the state's electronic security in addition to defending the state's financial, economic, military, television, and radio networks from electronic attacks, piracy, and interruption (Jubair et al., 2022).

Losses that occur as a direct consequence of cyberattacks cost businesses and whole nations tens of billions of dollars each year. This is a result of the fact that nations are subjected to hundreds of thousands of electronic attacks every single day, in addition to incidents involving the interruption or theft of systems and information, and other forms of electronic attacks (Saini & Yousif, 2021). As a result of this, countries, governments, and large companies have developed new departments that specialize in cyber security, information security, and network security. And in the same way that every nation possesses both military and economic power, and that power is ranked according to which nations are the strongest, the cyber power of the state, as well as its capacity to protect itself and its electronic security, was also invented (Mondal et al., 2020).

3. Research Methodology

3.1 Cyber Security Fields

The specialization of cybersecurity is one of the most sought-after disciplines at the global level and one of the highest jobs globally in terms of wages and salaries. However, in the Arab world, some of the concepts of cybersecurity have not spread as in the major countries, but in the near future, it will become one of the most sought-after disciplines in the labor market (Syed et al., 2020). The cybersecurity specialization is divided into several sections, sub-specialties, and job titles, including:

A. **Network Security**: It is the type that protects the computer network from any penetration or attack, whether from inside or outside the network, through the use of various modern technologies and protocols to prevent malicious programs from reaching this network. Therefore, network security is like a firewall and prevention that protects the electronic network from the access of some untrusted third parties, through the development of various security settings that ensure this purpose.

B. **Application Security:** It is the process of protecting various sensitive information at the level of the application itself that the user is using, and it is represented by a set of security measures that should be taken before entering and using the application, such as the process of requiring the user to set a strong password, setting security questions, or the two-stage authentication process.

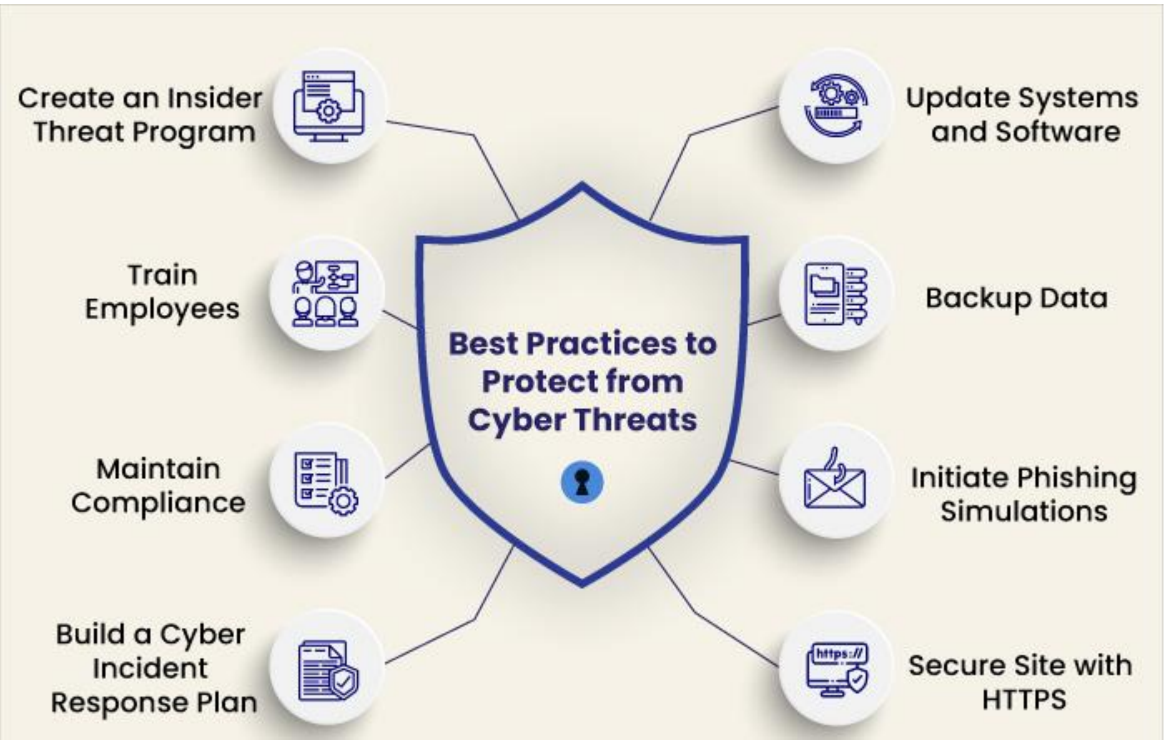

Create an Insider Threat Program
Update Systems and Software
Train Employees
Backup Data
Best Practices to Protect from Cyber Threats
Maintain Compliance
Initiate Phishing Simulations
Build a Cyber Incident Response Plan
Secure Site with HTTPS
https://

Figure 1: Cyber Security Threats Cycle (Clements and Kirkham, 2010)

C. **Network Security**: It is the type that protects the computer network from any penetration or attack, whether from inside or outside the network, through the use of various modern technologies and protocols to prevent malicious programs from reaching this network. Therefore, network security is like a firewall and prevention that protects the electronic network from the access of some untrusted third parties, through the development of various security settings that ensure this purpose.

D. **Application Security:** It is the process of protecting various sensitive information at the level of the application itself that the user is using, and it is represented by a set of security measures that should be taken before entering and using the application, such as the process of requiring the user to set a strong password, setting security questions, or the two-stage authentication process.

E. **Cloud Security:** It is a means of protecting personal information and data, as it is stored in what is known as the electronic cloud, a system found on the Internet such as; (Google Drive), (Microsoft OneDrive) and (Apple iCloud), all of which are highly efficient and capable storage media.

F. **Operational Security:** The process of internal risk management is of different types, and this type is often used by risk management officials in companies and organizations, to ensure that they find an alternative plan in the event that the stored data is exposed to the risk of breach. This type of security includes educating employees and workers in the company or organization to implement the best practices to preserve various data and information, whether personal or commercial.

3.2 Benefits of Cyber-Security

In an open age, the use of sophisticated software to protect against cyberattacks is beneficial for everyone. On an individual level, a cyber security threat might in fact result in a very wide range of negative outcomes, such as the theft of sensitive information like family photographs, extortion attempts, or even the destruction of sensitive material like identification documents. Additionally, because everyone is dependent on important infrastructures like power plants, healthcare facilities, and financial service businesses, it is imperative that these and other institutions be protected in order to ensure the smooth operation of society. In this day and age, everyone can benefit from using modern cybersecurity software. They want to educate the general public about the relevance of cybersecurity, raise attention to newly identified vulnerabilities, and give support for open-source software toolkits (Balani & Varol, 2020).

3.3 Their efforts make the internet a safer place for everyone

Defending society from cyber assaults is important because, in the event that one occurs, it has the potential to damage millions of people, cause state-run organizations to shut down, and prevent residents from receiving services. An example of this would be how the well-known ransomware Sam was used to attacking the city of Atlanta. The hackers requested hush money of $51 million, and the threat was so malevolent that the city lost internet service for five days, which caused many essential citywide operations to stop (Mondal et al., 2020). The city ended up paying $17 million to the hackers, despite the fact that companies face more than 4,000 hacks every day. The use of ransomware alone makes it possible for cyberattacks to take place on a global scale, and the penetration of government organizations by hackers makes it necessary to lay the groundwork for future defenses against cyberattacks on critical infrastructures, such as power plants and power grids. Cyberattacks might be launched against nuclear power facilities, which would result in a catastrophic disaster and the loss of millions of lives. An Iranian nuclear plant was subjected to an attack by a malicious computer virus, which resulted in the destruction of five centrifuges. The spread of these electronic viruses caused the centrifuges to overheat, which may have resulted in an explosion that took the lives of several people (Ghaffari et al., 2019).

According to research conducted by the Brookings Institution, fast advancements in technology have led to the introduction of 5G networks, which have the potential to expose users to enlarged and multi-dimensional cyberattack vulnerabilities. As a result of the proliferation of modern technologies like the Internet of Things, which has led to a significant increase in the number of devices that are connected to the internet, cybercriminals now have access to artificial intelligence and machine learning, which they can use to launch cyberattacks. A program that can effortlessly break into computer systems without the need for any assistance from a human. These automated cyberattacks may be carried out on a large scale, and they cause widespread alarm throughout the world (Balani & Varol, 2020; Zebari et al., 2021). For the purpose of protecting business activity, in recent years, there has been an increase in the number of cyberattacks targeting commercial companies, which has resulted in damages costing millions of dollars for data recovery. As a result of all of these expenses, not only will executives be forced out of their employment, but it is also possible that other employees may be laid off as a consequence of the firm decreasing costs. These companies include Credit bureaus, a global credit rating agency that suffered unauthorized access that influenced numerous customers and for which the costs of recouping from the breach were lately approximated to be $439 million; Yahoo, a web giant whose breach impacted each of its 3 billion account holders; and Target, a retailer that afflicted a data breach that impacted many clients and for whom the costs of recouping from the breach were recently estimated to be one billion dollars. It is estimated that around three hundred and fifty million dollars have been directly spent on the rehabilitation effort (Ghaffari et al., 2019).

Data protection: not only do countries and businesses face cyber-attacks, but individuals also face many risks, and identity theft is a big problem as lawbreakers steal the personal information of the individual and sell it. This also puts the personal safety of the individual and his family in jeopardy, and this has happened many times. In some cases, millions of dollars have indeed been paid to the victim's account, but in other cases, the victim has not been identified.

In some cases, hackers will use extortion and "hush money" to avoid taking further action against the victim's account. Protection (Gupat & Kumar, 2019). With the growing number of dangers posed by cyber security, more new laws can be enacted to protect people from potential assaults. Laws and regulations that protect everyone from potential threats are being established. This suggests that stricter regulations and legislation may soon become a reality; harsh penalties must be imposed on the attackers, and citizens must be made aware of the laws passed and ensure that they follow them. In addition, the government must ensure that the perpetrators of the attack face harsh penalties (Kumari et al., 2019). The United States Bureau of Labor Statistics (BLS) anticipates that jobs for information security specialists will grow by 28% between 2016 and 2026, which is twice as fast as the average growth rate for computer-related occupations. This growth rate is providing new job opportunities as businesses of all sizes scramble to respond to growing threats (Asaad & Abdulnabi, 2022).

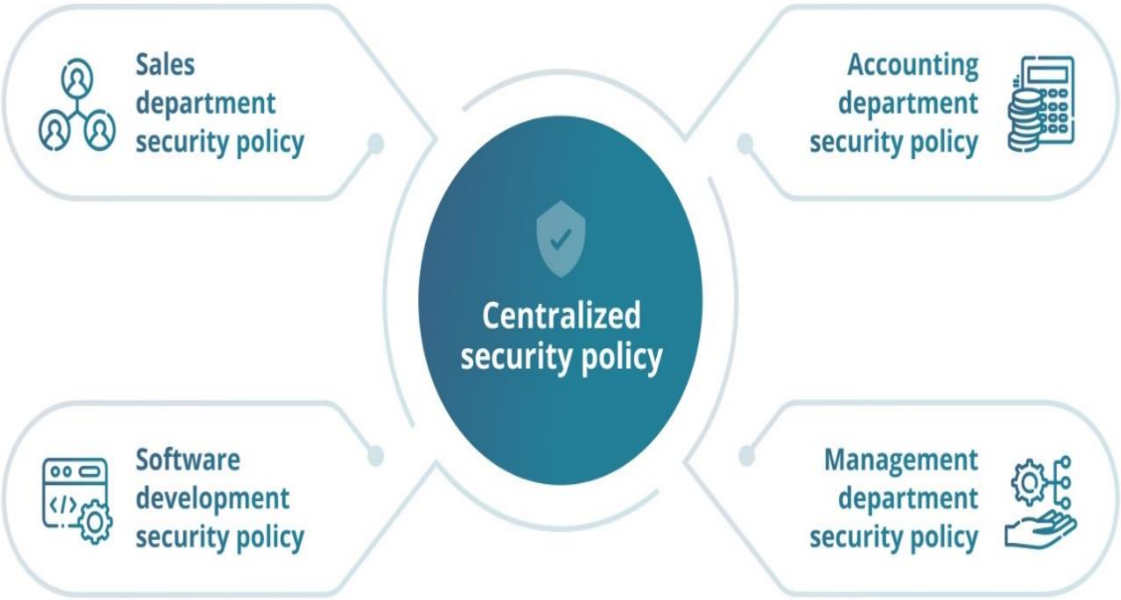

Sales department security policy
Accounting department security policy
Centralized security policy
Software development security policy
Management department security policy

Figure 2: Hierarchy of Cyber Security Policies (Syed et al., 2020)

4. Methodology and Discussing

The protection of systems linked to the internet from harmful assaults is referred to as cybersecurity (Wang & Yi, 2011; Asaad et al. 2017). This protection includes the protection of data, hardware, and software.

4.1 Common Cyber Security Measures

In order to protect their clients, their data, and their cash flow, businesses need to use a variety of cyber security procedures. These precautions should have the goal of preventing dangers from a variety of sources, including the following:

- Attacks that originate on the internet, such as adware or malware;
- Weaknesses that are user-generated, such as readily guessed passwords or lost information;
- flaws and vulnerabilities that are inherent to the system or program;
- Attempts to subvert the functionality of the system or software.

4.2 Essential cyber security measures

The following procedures and tools are not difficult to implement, and when combined, they will provide you with a fundamental degree of security against the most widespread IT-related dangers.

a) Make sure to use robust passwords.

If you want to keep your online activities private, you certainly need to have passwords that are safe. You can make it more difficult for other people to figure out just what your password is by doing a few of the ones that follow: use a mix of equity and lowercase letters, numbers, and symbols; making your password between eight and 12 characters long; attempting to avoid the use of personal data in your password; changing your password on a regular basis; never using the same password for multiple accounts, and utilizing two-factor authentication.

Create a password policy for your organization so that your employees will have a guide to follow when it comes to sticking to the highest possible security standards. For the aim of implementing your password policy, it is recommended that you investigate the availability of a variety of technical choices, such as regularly scheduled password updates. Read the guidance on using passwords to protect your data that is provided by the National Cyber Security Centre (NCSC), which may provide you with more in-depth direction on passwords, and think about various password techniques that could improve the safety of your company (Marqas et al., 2022). This advice is provided by the National Cyber Security Centre (NCSC).

b) Maintain access restrictions on data and computer systems

Make it a point to check that individuals can only access the information and services for which they have been granted permission. For example, you might be in charge of both the physical entrance to the building and the computer network access.

- Restrict what can be copied from the system and saved to storage devices.
- limit what kinds of email attachments can be sent and received.
- Restrict access to unauthorized users • limit access to data or services through application controls.
- Restrict what can be copied from the system and saved to storage devices.

With assistance may do most of these modern operating systems and network software; nevertheless, you will be responsible for managing the registration of users and user authentication mechanisms, such as passwords (Lu et al., 2010).

c) Erect a barrier or a firewall.

The primary function of a computer firewall is to serve as a gatekeeper between an internal network and the internet. They serve as a barrier, limiting the spread of cyber threats such as viruses and malware, which they do by performing the role described above. It is absolutely necessary to appropriately set up firewall devices and to check them on a regular basis in order to guarantee that their software and firmware are up-to-date. If this is not done, the effectiveness of the firewalls may be less than it could be. Studying on firewalls is a great way to increase your knowledge of server security.

d) Make use of a security program

In the event that malicious code finds its way into your network, you should utilize security tools such as anti-spyware, anti-malware, and anti-virus programs to aid you in detecting and deleting the code. These programs may also help you prevent further infections. Check out our in-depth guide to aid you in recognizing spam, malware, and virus attacks, and we will do our best to help you.

e) Regularly update all of your software and operating systems.

The latest versions of software often include important security enhancements that can shield users against previously discovered flaws and vulnerabilities. To avoid becoming a victim of crooks, you must always use the most recent versions of software and hardware on your devices.

f) Keep an eye out for any intrusions.

Monitoring systems and looking for odd behavior on a network may be done with the help of intrusion detectors. A detection system can sound an alarm, such as an email notification if it has reason to believe that there has been a possible violation of security. This alarm is generated based on the kind of behavior that the system has spotted. Learn more about the identification of breaches in cyber security here.

g) Raise awareness

Your staff members have a legal obligation to assist you in maintaining the safety of your company. Make it a point to check that they are aware of their responsibilities, as well as any pertinent rules and procedures, and provide them with regular opportunities for cyber security awareness and training. Learn more about insider dangers in the world of cyber security.

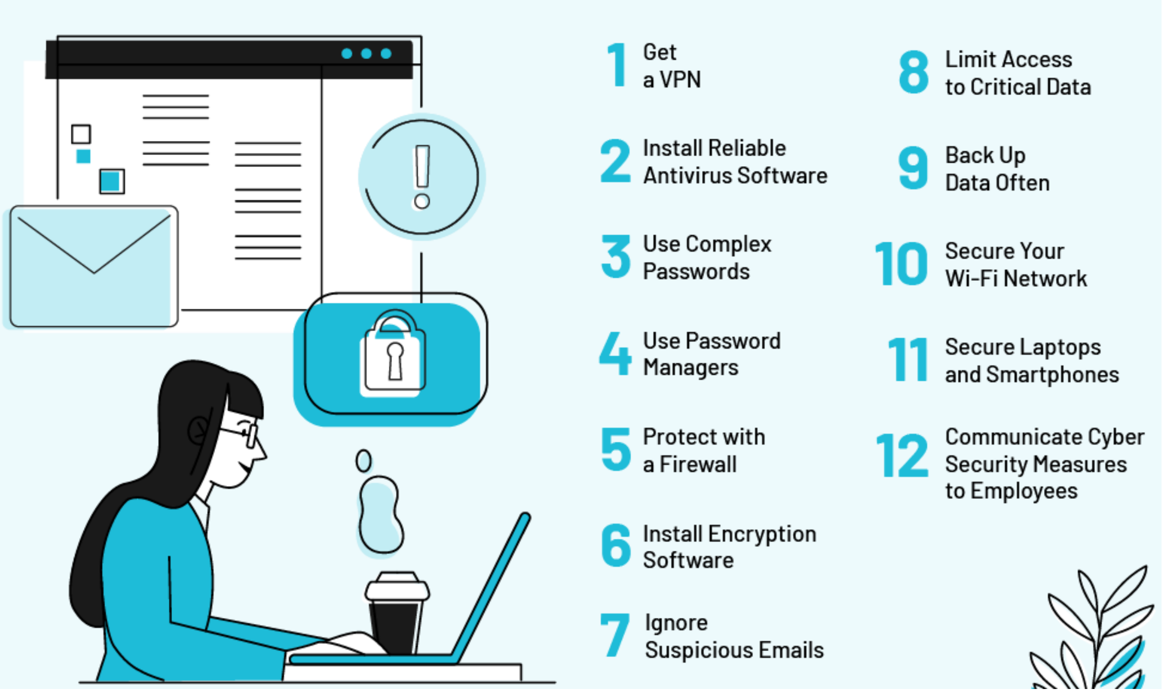
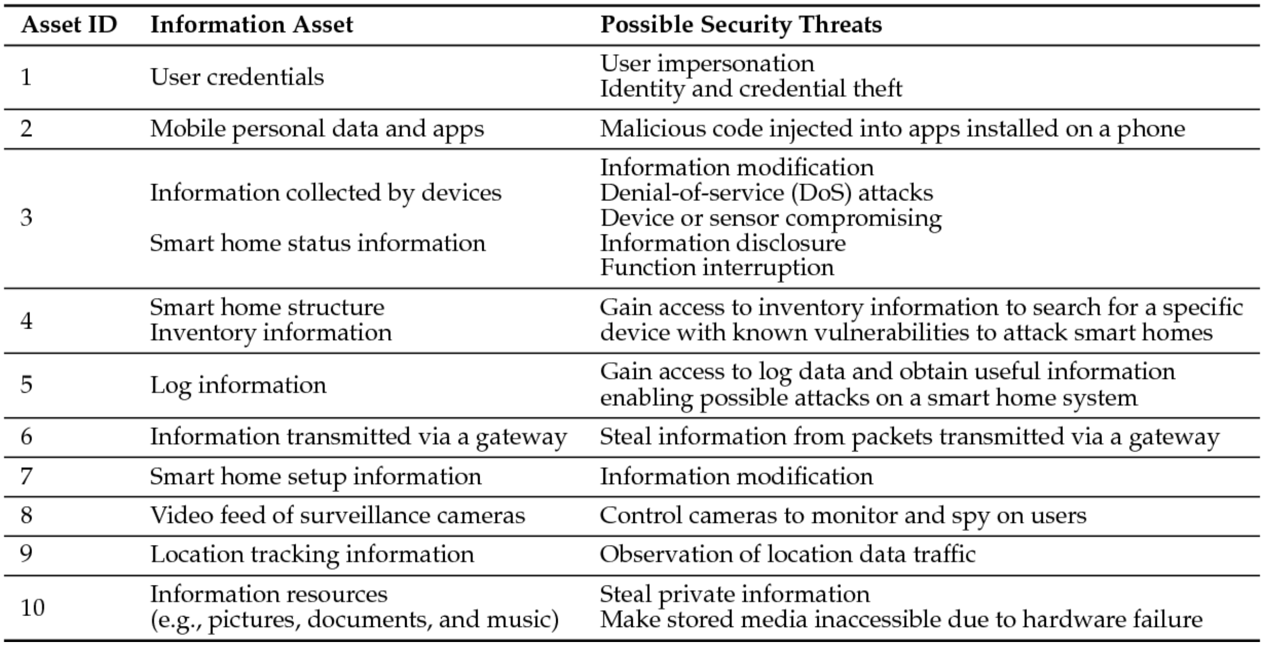

1 Get a VPN
2 Install Reliable Antivirus Software
3 Use Complex Passwords
4 Use Password Managers
5 Protect with a Firewall
6 Install Encryption Software
7 Ignore Suspicious Emails
8 Limit Access to Critical Data
9 Back Up Data Often
10 Secure Your Wi-Fi Network
11 Secure Laptops and Smartphones
12 Communicate Cyber Security Measures to Employees

Figure 3: Cyber Security Measures (Lu et al., 2010)

4.4 The National Cyber Security Centre

The National Cyber Security Center (NCSC) has provided a list of the most important guidelines for maintaining one's privacy and security when using the internet (Asaad et al., 2017). Always keep frequent backups of your most important data and systems. Keep copies separate from the originals in a secure location and ensure that they are functional. To maintain the safety of your devices, it is important to keep your operating system, web browser, and all other software up to date with the latest security patches. In many instances, you have the option of configuring the program to automatically update itself or manually downloading the software updates. On each of your devices, you should install antivirus and anti-malware software and ensure that it is kept up to date. Make sure your passwords are secure and update them frequently. Consider utilizing two-factor authentication for an additional layer of protection as well. Either change your passwords often across all of your online accounts and services, or look into utilizing a trustworthy password management solution. Encrypt any sensitive information, and under no circumstances should you send passwords or other sensitive information in an unencrypted email. Be wary of clicking on links that are supplied to you within emails, social networking websites or applications, or websites that you are not acquainted with in order to protect yourself against phishing and ransomware. Make use of a firewall, and check to see that the firmware on both your internet router and your firewall is up-to-date. If you run a Wi-Fi network, you should make sure that it is encrypted (using a protocol such as WPA2) and that the password is changed on a regular basis. If you need to access your systems while using public Wi-Fi or a network that is not secure, you should make use of a virtual private network, or VPN.

Table 1: Security Vulnerability Assessment (Asaad et al., 2017)



Asset ID	Information Asset	Possible Security Threats
1	User credentials	User impersonation Identity and credential theft
2	Mobile personal data and apps	Malicious code injected into apps installed on a phone
3	Information collected by devices Smart home status information	Information modification Denial-of-service (DoS) attacks Device or sensor compromising Information disclosure Function interruption
4	Smart home structure Inventory information	Gain access to inventory information to search for a specific device with known vulnerabilities to attack smart homes
5	Log information	Gain access to log data and obtain useful information enabling possible attacks on a smart home system
6	Information transmitted via a gateway	Steal information from packets transmitted via a gateway
7	Smart home setup information	Information modification
8	Video feed of surveillance cameras	Control cameras to monitor and spy on users
9	Location tracking information	Observation of location data traffic
10	Information resources (e.g., pictures, documents, and music)	Steal private information Make stored media inaccessible due to hardware failure

5. Existing Works

Several research studies were examined, and their findings are presented in the table below. In this paper. we organized them according to the year of publication, the risks that were addressed by the researcher, and the strategies that were given in each work.

Kushala (Kushala & Shaylaja , 2020) conducted a survey to investigate recent developments in the field of multi-cloud computing security problems. The shift from on-premises computation to cloud technology has introduced a number of new vulnerabilities, not just for end users but also for the businesses that supply these services. The purpose of this study is to discuss the essential characteristics of CC and Multi-Cloud Computing (MCC), together with their security difficulties and potential solutions. Specifically, the paper will focus on security issues. The researcher's contact information includes each danger that has been addressed, the security technique that has been employed, and the type of cloud that has been deployed. Mondal et al., (Mondal et al., 2020) examine the problems and difficulties associated with cloud computing security. It emphasizes the primary difficulties that need to be addressed in order to secure cloud computing, including confidence, validity, privacy, cryptography, key distribution, scalability, data partitioning, and virtual machine security. It also discusses alternative solutions for these concerns. The researchers discuss the difficulties associated with sharing resources in the cloud as a primary cause of weaknesses that should be investigated in further study. Syed et al., (Syed et al., 2020) conducted a review of the security threats, procedures, and controls associated with cloud storage. The purpose of this article is to discuss both the security problems that now exist and the state-of-the-art solutions that have been developed to address those problems. Security and privacy are at the top of the list of issues and requirements in this area because of the significant improvements being made in cloud computing in this particular subject. People can experience severe monetary and information loss as a result of a variety of concerns, including poor data visibility, storage sinks without protected pointers, enormous data spills, and others. The article provides a summary of the security risk, which is broken down into the following categories: lack of control; shared servers; data leakage; API and storage sinks; and shared data. According to the findings of the research, the following best practices are necessary when creating cloud storage: multi-factor authentication, data categorization, security encryption, and evaluation of the cloud framework. In addition, the research report makes use of three more sophisticated procedures when dealing with sensitive data. These include private encryption, encryption while in transit, and ransomware protection.

Balani & Varol, (Balani & Varol, 2020) attempted to depict the difficulties and dangers that come with cloud computing security. In a setting that is based online, data is available to users from any location on the planet. Additionally, customers have concerns regarding the safety of their data while it is stored on the cloud. The purpose of this investigation is to make some recommendations on tactics and procedures that may be used to safeguard data in an online setting. These methods offer the most value for the money, and they are so straightforward that absolutely anybody may use them to protect themselves from potential dangers. According to the findings, a number of different approaches and models have been proposed; however, according to the researchers, none of them have been successful so far since there are no security standards in place for reliable cloud computing. A researcher has suggested that one of their next projects be the investigation of cloud security standards. Ghaffari et al., (Ghaffari et al., 2019) conduct a comprehensive review of the cloud security issues from a people, process, and technology model perspective. The survey attempted a detailed identification of cyber safety problems and provided answers to these threats to classes of persons, processes, and technologies. This was done with the intention of identifying cost-effective, reliable, and practicable security solutions based on the findings of the survey. The researchers examine a selection of pertinent research pertaining to cloud computing. Then, a concept based on the PPT model was proposed for classifying the problems with cloud computing security and the associated solutions. After that, the suggested method is applied to the task of classifying the obstacles that have been presented. Research on the potential dangers posed by cloud computing was carried out by Gupta & Kumar, (Gupta & Kumar, 2019). Using a variety of approaches, the purpose of this research is to investigate potential solutions to the security concerns raised by cloud computing.

6. Results

Figure 4 provides a concise summary of the findings from the preceding section on the dangers that appear most frequently in the articles that were evaluated. According to the statistics presented in this image, the four most prevalent security risks associated with cloud computing are account hijacking, data sanitization, data control, and harmful insiders. Where the data controller is the most important security control since data stored in the cloud is often managed by the service provider, while customers do not have complete control over their own data. Some of the ways to deal with these worries are through encryption, access control, the use of blockchain technology, and service-level agreements between the customer and the service provider.

7. Proposed Solutions

After going over the most significant security flaws and problems, this part is going to go through the most current security fixes (Asaad et al., 2017; Abdulfattah et al., 2018). Strong authentication procedures should be used in order to verify people's identities. It is recommended that businesses adopt an "implicit deny" policy, which stipulates that access to the network can only be allowed through the use of explicit access rights.

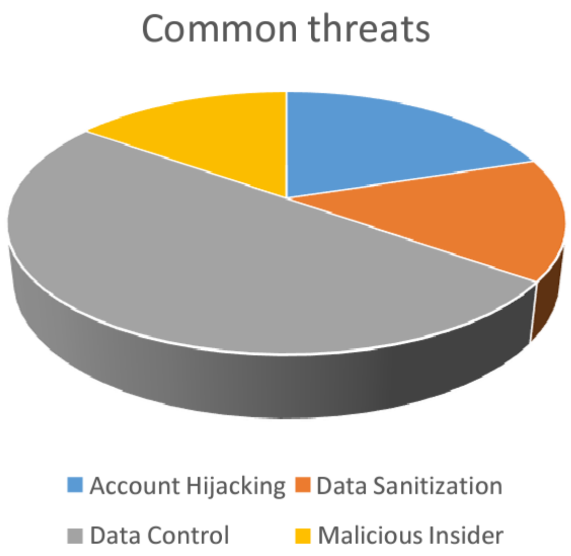


Figure 4: Most common threats mentioned in cloud system

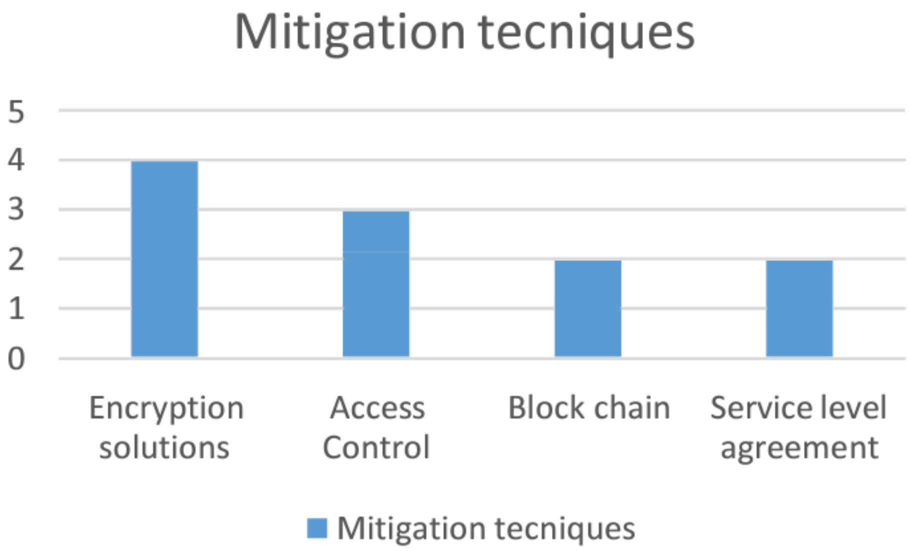


Figure 5: Most common threats mentioned in cloud system

Protection against malware on both integrated and overall computer systems. Embedded systems are designed with the sole purpose of running software that was provided by the original maker. The keying material needed for software validation must be included in the manufacturer's goods in a safe storage facility that must be included as part of this requirement.

Table 2: Addressed Threats and Mitigation Techniques

Author	Addressed threats	Suggested mitigations
Kushala & Shaylaja, (2020)	Control over the data that has been saved, data sanitizing, availability of service, authentication and authorization of confidential computing, and virtualization are all important aspects of information security.	RSA, Cloud Inter-operative Toolkit (CIT), Byzantine Protocol, Optimization Technique, Self-adaptive Technique, DepSky (Byzantine + secret Sharing + cryptography), RAID-like Technique + introduced RACS, ICstore (client-centric distributed protocols), SPORC (fork), HAIL (Proofs + cryptography), and TCCP are some of the protocols that have been developed in recent years.
Mondal et al., (2020)	Trust issues, confidentiality issues, authenticity issues, authentication issues, encryption issues, key management issues, data splitting issues, and multitenancy issues are all problems.	end-to-end encryption that uses a mechanism-based approach, completely holomorphic encryption, a P2P reputation system, a Service Level Agreement, a P2P reputation system, a Secret Sharing method and TMR Technique, Isolation, and a solution that uses two levels of encryption.
Syed et al., (2020)	Accounts Management, Dangerous Insiders, Data Management, Management Console Security, and Multi-tenancy Issues are the five primary types of risks. Multi-tenancy Issues also exist.	Performing an analysis of the cloud framework, using multi-factor identification, pattern discovery, security encryption, personal encryption, in-transit encryption, and ransomware protection.
Balani & Varol, (2020)	Access for privileged users, compliance with regulations, data placement and segregation, recovery and investigation support, and long-term performance are some of the topics covered.	Control of access, provision of increased security at lower expense, and the avoidance and resolution of events are all included.
Ghaffari et al., (2019)	Trust Concerns, Human Resource Matters, Compliance and Legal Matters, Efficiency, Security Systems, Data Protection, Forensics, Multi-tenancy Concerns, Virtualization, Software, Network, and Service-Related Matters, and Monitoring.	A classification of the many threats to information security, which enables managers to locate potential vulnerabilities and select the most effective response.
Gupta & kumar, (2019)	Unauthorized Access, Loss Of data, Malicious Insiders, result Of physical, Financial Fraud, Insecure Application Programming Interfaces, and Multi-Tenancy are some of the most common types of data security vulnerabilities.	Model of two-factor authentication using a fingerprint to prevent unauthorized access.
Kumari et al., (2019)	Account Hijacking, Trust Issues Between Users and Service Providers, Problems with Accessibility and Loss of Data	Access Management, Service Level Agreements (SLA), Encryption, and Integrity Verification are some of the services provided.

The system is able to validate any freshly downloaded program by using a key before it begins to run the software. On the other hand, general purpose platforms are designed to be compatible with software written by a third party.

Antivirus software that is current and receives frequent updates, in addition to host-based intrusion prevention, are both necessary components of this system. Technologies such as Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) should be used to supplement host-based defenses in order to protect the system from both external and internal threats. A minimum of once a year, vulnerability assessments have to be carried out in order to guarantee the safety of the components that are in contact with the perimeter. In some circumstances, the behaviors of users might create possible security holes in the system. As a result of this, awareness campaigns should be implemented to educate the users of the network on the safest ways to utilize the various apps and tools available through the network. It is necessary for devices to be aware of the sources and destinations with which they communicate. This is achieved through the implementation of mutual authentication procedures utilizing either the Transport Layer Security (TLS) or the Internet Protocol Security (IPsec) protocols. In order to ensure the confidentiality of communications, hardware should enable Virtual Private Network, or VPN, designs. To ensure the safety of communications, hardware must implement public key infrastructure (PKI) (Marqas et al., 2022).

Nevertheless, there are a few limitations when it comes to cryptography and key management (Lu et al., 2010). Because current devices do not have sufficient processing power and storage to perform advanced authentication and encryption techniques, communications in a smart grid system will be carried out over multiple channels that have various bandwidths, and connectivity, in which all systems, certificate authorities, and data centers must be connected at all times. Because of the massive volume of data that is exchanged, utilities should only acquire the data that is necessary to accomplish their objectives. When it comes to protecting the smart grid network, control systems and information technology security engineers should share equal responsibility. Because the life cycle of the smart grid will be longer than that of the involved information technology systems, all of the included IT technologies ought to have the capacity to be updated. The architecture of the smart grid has to include security measures. In that case, the security of devices is dependent on the vendor (Author name: Energy Procedia 00 (2011) 000–000 7 details), which may result in a large number of vulnerabilities due to incompatibility concerns. Utilities have to give some thought to utilizing communication businesses that are run by third parties. Allowing the utilities to manage all of the grid communication quickly becomes a burden that the utilities are unable to handle on their own. Companies that are not directly involved in the transaction can provide assistance in addressing the communication and security concerns associated with the data transfer. When interacting among the many stakeholders involved in a smart grid, a strong authentication procedure is required. The protocol needs to be able to function in real-time while adhering to certain limitations, such as having a low communication overhead, minimal processing cost, and a high level of resistance to assaults, particularly denial-of-service attacks.

8. Conclusion

In the current climate of cyberspace, every company is going online as a means of ensuring the continuity of its operations. As part of this process, they are storing their essential resources on web servers, making them freely accessible via the HTTP protocol. Every firm must adhere to some sort of security policy or set of principles in order to ensure the safety of these resources. Regrettably, the majority of security solutions are dependent on signatures and are therefore static (i.e., if a signature is present, it can detect malicious activity; otherwise, it cannot). As a result, there is a requirement for a dynamic solution in order to address the impending vulnerabilities that are appearing on a regular basis. In addition, there is a requirement for a semantic solution that can comprehend the environment in which vulnerabilities exist before attempting to repair them. Everyone may profit from technologically improved cyber defense software in today's interconnected society. On a personal level, a cyber assault can result in a variety of negative outcomes, including the theft of personal information, efforts to extort money, and the loss of essential data such as photographs of one's family. Everyone is reliant on essential infrastructures, such as power plants, hospitals, and organizations that provide financial services. The proper protection of these and other community institutions is very necessary for the continued operation of our society.

Acknowledgment

The research leading to these results has received no Research Project Grant Funding.

References

[1]. Abdulfattah, G. M., Ahmad, M. N., & Asaad, R. R. (2018). A reliable binarization method for offline signature system based on unique signer’s profile. International Journal of Innovative Computing Information and Control, 14(2), 573-586.

[2]. Al-Omar, B., Al-Ali, A. R., Ahmed, R., & Landolsi, T. (2012). Role of information and communication technologies in the smart grid. Journal of Emerging Trends in Computing and Information Sciences, 3(5), 707-716.

[3]. Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. Icontech international journal, 4(2), 28-34. https://doi.org/10.46291/ICONTECHvol4iss2pp28-34

[4]. Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a9987

[5]. Asaad, R. R., & Abdulnabi, N. L. (2022). A Review on Big Data Analytics between Security and Privacy Issue. Academic Journal of Nawroz University, 11(3), 178-184.

[6]. Asaad, R. R., Abdulrahman, S. M., & Hani, A. A. (2017). Advanced Encryption Standard Enhancement with Output Feedback Block Mode Operation. Academic Journal of Nawroz University, 6(3), 1–10. https://doi.org/10.25007/ajnu.v6n3a70

[7]. Asaad, R. R., Abdurahman, S. M., & Hani, A. A. (2017). Partial Image Encryption using RC4 Stream Cipher Approach and Embedded in an Image. Academic Journal of Nawroz University, 6(3), 40–45. https://doi.org/10.25007/ajnu.v6n3a76

[8]. Balani, Z., and Varol, H. (2020). Cloud Computing Security Challenges and Threats. In (pp. 1-4): IEEE

[9]. Clements, S., & Kirkham, H. (2010, July). Cyber-security considerations for the smart grid. In IEEE PES General Meeting (pp. 1-5). IEEE.

[10]. Ghaffari, F., Gharaee, H., and Arabsorkhi, A. (2019). Cloud Security Issues Based on People, Process and Technology Model: A Survey. In (pp. 196-202): IEEE

[11].Gupta, H., & Kumar, D. (2019, May). Security threats in cloud computing. In 2019 International Conference on Intelligent Computing and Control Systems (ICCS) (pp. 1158-1162). IEEE.

[12]. Jubair, M. A., Mostafa, S. A., Zebari, D. A., Hariz, H. M., Abdulsattar, N. F., Hassan, M. H., ... & Alouane, M. T. H. (2022). A QoS Aware Cluster Head Selection and Hybrid Cryptography Routing Protocol for Enhancing Efficiency and Security of VANETs. IEEE Access.

[13]. Kumari, C., Singh, G., Singh, G., & Batth, R. S. (2019, December). Security Issues and Challenges in Cloud Computing: A Mirror Review. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 701-706). IEEE.

[14]. Kushala, M. V., & Shylaja, B. S. (2020, September). Recent trends on security issues in multi-cloud computing: a survey. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 777-781). IEEE.

[15]. Lu, Z., Lu, X., Wang, W., & Wang, C. (2010, October). Review and evaluation of security threats on the communication networks in the smart grid. In 2010-Milcom 2010 Military Communications Conference (pp. 1830-1835). IEEE.

[16]. Marqas, R. B., Almufti, S. M., & Asaad, R. R. (2022). Firebase Efficiency in CSV Data Exchange Through PHP-Based Websites. Academic Journal of Nawroz University, 11(3), 410-414.

[17]. Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[18]. Mondal, A., Paul, S., Goswami, R. T., & Nath, S. (2020). Cloud computing security issues & challenges: A Review. In (pp. 15): IEEE.

[19]. Pearson, I. L. (2011). Smart grid cyber security for Europe. Energy Policy, 39(9), 5211-5218.

[20]. Saini, D. K., & Yousif, J. H. (2021). Vulnerability and Attack Detection Techniques: Intrusion Detection System. In Cybersecurity (pp. 17-26). CRC Press.

[21]. Syed, A., Purushotham, K., and Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. 2020 IEEE International Conference for Innovation in Technology (INOCON), Innovation in Technology (INOCON), 2020 IEEE International Conference For, 1–4. https://doi- org.sdl.idm.oclc.org/10.1109/INOCON50539.2020.9298281

[22]. Wang, X., & Yi, P. (2011). Security framework for wireless communications in smart distribution grid. IEEE Transactions on Smart Grid, 2(4), 809-818.

[23]. Yousif, J. H., & Saini, D. K. (2020). Big Data Analysis on Smart Tools and Techniques. In Cyber Defense Mechanisms (pp. 111-130). CRC Press.

[24]. Zebari, D. A., Haron, H., Zeebaree, D. Q., & Zain, A. M. (2019, August). A simultaneous approach for compression and encryption techniques using deoxyribonucleic acid. In 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA) (pp. 1-6). IEEE.

[25]. Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018, October). Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 312-317). IEEE.

[26]. Zebari, D., Haron, H., & Zeebaree, S. (2017). Security issues in DNA based on data Hiding: A review. International Journal of Applied Engineering Research, 12(24), 0973-4562.

[27]. Zebari, G. M., Zebari, D. A., & Al-zebari, A. (2021). Fundamentals of 5G cellular networks: A review. Journal of Information Technology and Informatics, 1(1), 1-5.

[28]. Zebari, N. A., Zebari, D. A., Zeebaree, D. Q., & Saeed, J. N. (2021). Significant features for steganography techniques using deoxyribonucleic acid: a review. Indonesian Journal of Electrical Engineering and Computer Science, 21(1), 338-347.