جامعة جدة
University of Jeddah

All-in-one App

Submission for Computing Ethics (CCCY 112)

7-12-2021

College of Computer Science and Engineering

Submitted by :

Ruba Khalid Alsualmi

ID No : 2110618

Aryam Abdul Rahman Mahjoub

ID No : 2111406

Introduction

After the mobile phone is used in every step we take,and technology has become a way to facilitate our lives and make them more flexible.Applications have become a necessary component of our daily lives in order to save time and effort.The application is made by Saudi hands and we use a variety of methods to maintain a high level of confidentiality in the All-in-One.The application provides many services to meet the wishes of employees, citizens .or visitors, saving time and effort, and obtaining information faster and easily

Where among the services provided by the application is the user's access to his health information and the identification of the nearest care center for the beneficiaries as the location where vital health services are provided, in conducting your own transactions in the government and private sectors easily and easily, tracking daily expenses and knowing the **.**amount of money available in each of the bank accounts

1. Communication channel is secure for secure communication of the data

Secure channel: It is a method of transferring important data that is not intended to be tampered with or spied on

A secure communication channel consists of three basic components. The first is the idea that information shared between or among users should not be visible to third parties. The second condition is the difficulty of hacking the channel by guessing passwords or exploiting flaws in the code. Last but not least, your connection connection should be uninterrupted and .available at all times, with no vulnerabilities to exploit

The secure communication of personal, confidential and private data requires protection that ensures the confidentiality, integrity and availability of information.The All-in-One application has technology that guarantees the highest levels of security and privacy across .data transmission channels

There are many ways to secure data and create a secure communication channel for secure data exchange:

Data encryption

It is one of the means of maintaining data security and establishing a secure connection. It is a communication system in which messages on your device are encrypted and not decrypted until they reach the intended recipient.This ensures that any attacker who intercepts the traffic cannot read the contents of the message, nor can anyone access the central servers where the data is stored.

Why do we need encryption in an all-in-one app?

Privacy: Encryption helps protect your privacy across the Internet and apps, by turning personal information into messages intended for specific individuals, but not for anyone else.

Cybercriminals often steal personal information of users of various internet sites for financial gain.
Security: We use encryption to protect users' personal data because it enables the secure protection of user data
Spyware Prevention: We use encryption to protect the contents of files safely in a way that protects them from spyware, and if one of our devices is stolen,These files will not be able to be opened by thieves.

How does encryption work in an all-in-one app?

Encryption involves converting plain text that is readable to a human being into unintelligible text, which is known as ciphertext.This often entails altering readable data such that it appears at random. The usage of an encryption key, which is a set of mathematical values agreed upon by both the sender and the receiver, is required for encryption. The data is decrypted and returned to readable plain text by the recipient using the key.When the appropriate receiver receives the message, the information is decrypted and returned to its original state.

Firewall

A system of software or hardware that stands as a guard between the internal network and the traffic of external sources such as the Internet in order to prevent a malicious attack.

How does the firewall work?

Firewalls create a barrier between secured networks and vulnerable networks and control them, whether they are trusted or untrusted networks, such as the Internet. By using a firewall that contains specific code, this will isolate and protect your computer and devices from the Internet while scanning The data that must be executed from the firewall, then determines which data must be allowed to pass through or even block the connection completely. Incoming traffic is analyzed based on predefined security rules where data is carefully filtered from unsafe or malicious sources to prevent any occurrence expected attack.

Why do we need firewalls in an all-in-one application?

Firewalls, especially Next Generation Firewalls (NGWF), focus a hardware or software-based network security system capable of detecting and preventing complex attacks by filtering network traffic that depends on packet contents.Prevents malware and application layer attacks.Combined with an Integrated Intrusion Prevention System (IPS), these next-generation firewalls are able to respond quickly and seamlessly to detect and combat attacks across the entire network.Firewalls can work according to pre-set policies to better protect our network and can perform quick assessments to detect and close suspicious activities, such as malware.The network layer or packet filters check packets at a low level of the TCP/IP protocol stack and do not allow packets to flow through the firewall unless they meet the defined rule set, which is based on IP addresses and ports.

Router

A device that connects two or more networks and transmits network packets containing many types of data - such as files, connections, and simple correspondence such as web interactions - to their addresses from their source until they reach their destination.

Why do we need a router in an all-in-one application?

The router is the first line of security from network snooping. Enabling the highest level of security on the router turns things like a firewall on, which is the best way to keep your computer system and your information safe from attack

How does the router work in an all-in-one application?

A router is a device that connects two or more networks and communicates with them directly through one of its ports. Every network has its own set of addresses. A network address is stored on the router port. When one of the router ports receives a data packet, it reads the information in the packet, specifically the address destination, and then searches for an equivalent in its routing table, or decides to route the packet towards its destination, and determines its path to an appropriate neighboring network or the appropriate next router, or delivers it to its final destination, depending on the routing policy followed.

Virtual private networks (VPN)

A virtual private network (VPN) is a network that allows you to create a private network (Private Network) between a group of devices that are not physically connected to a local network, through the use of the Internet, the VPN protocol uses a set of encryption tools to create private internal networks between A group of devices without the need to connect these devices.

Why do we need a VPN in an all-in-one application?

It is one of the best solutions that encrypts your connection to the Internet or other computers by making a fake "tunnel" that encrypts what data passes through, and this means that no one is able to intercept the user's data or activities on the Internet.

How does a VPN work in an all-in-one application?

A VPN encrypts all data sent over the Internet from a computer, turns it to a certain sort of data packet, and sends it to a VPN server that can decrypt it using numeric keys, ensuring that no one but those keys can read the data sent.
When the VPN user receives a response from the intended destination, the response is sent to the VPN server, which encrypts the data and delivers it back to the VPN user's computer or phone, where the application identifies it.
VPN and decoder are both available. The VPN server masks the user's IP address and location, making it impossible for others to listen in on their conversations.

Intrusion detection system (IDS)

They are devices or programs that monitor the work of the computer network, waiting for anything suspicious and any violation of network management policies, or monitoring any modification, addition or deletion of files on the host machine.

Why is the use of an intrusion detection system important in an all-in-one application?

By recognizing and alerting us to suspect network traffic, we can improve the security of network devices and vital network data. To preserve current data, internal and external network data transmissions, our network requires excellent security.Cyber attacks are getting more sophisticated and regular, so it is important to have a comprehensive and adaptive intrusion detection system in place.An intrusion detection system can help us manage crucial network data in addition to boosting network security.Every day, our network creates a large amount of data, and an intrusion detection system can assist us in distinguishing between vital activities and less important data. When it comes to intrusion detection, this can save us time, minimize manual effort, and reduce human mistake.

How does the intrusion detection system work in an all-in-one application?

An intrusion detection system can be made up of several components: a sensor that generates security events, a control panel that monitors events and alerts and controls sensors, and a generic engine that records entries for events received through sensors in a database and uses a system of rules it makes to generate alerts of the security events that have been received.

A data detection system (IDS) is used to monitor network traffic and match traffic patterns to known threats after the data has been collected. The intrusion prevention system can assess if odd activity is a cyber attack using this strategy, which is also known as pattern correlation. The intrusion detection system will send an alert to the specified technicians or IT administrators as soon as suspicious or malicious behavior is identified. IDS alarms allow us to immediately start debugging and identifying the main causes of issues, as well as detect and halt malicious agents in their tracks.

2. User authentication is secure enough to stop unauthorized login attempts

We will be using Multi-Factor Authentication (MFA) in our all-in-one application.

Multi-factor authentication helps establish the identity of the provider by using information that only the provider knows, usually a name and password.

The MFA requires one or more validators and generates a new token each time an authentication request is submitted, which helps reduce cyberattacks.

The use of multi-factor authentication in an "all-in-one" application is more effective for **achieving Zero Trust and is the most reliable approach to cybersecurity because:**

- easy to use
- Protects against the impersonation of users

Provides high data protection

In our all-in-one application, we will use the three types of authentication where we will use defined authentication for the password, followed by ownership authentication where a security code will be sent to an email or mobile number, and biometric authentication where the user is asked to enter a sample voice pattern, electronic signature, or sign language gestures.

There are three main parts to multi-factor authentication:

First : Application-level multi-factor authentication that relies on user knowledge:

We will use password authentication, which is the most common authentication that requires only the user name and password to access so that when the user wants to register for the first time in the application, a list will appear with two options: New registration or login. If the user chooses to log in, a page will appear asking him to enter a named User, password, e-mail, or mobile number. The user must create a password that contains 8 characters or more of different letters and symbols. But if the user chooses to log in, he will be shown entering the user name or personal identification number and password, in addition to a list of them (user name and password, fingerprint, security code, smart card and password, voice pattern sample, hand gestures, electronic signature) where he can The user chooses the authentication that he wants to compare the selected authentication with the data recorded in the system. If the user chooses an authentication that is not registered in the system, the user will be asked to choose another authentication.

Suggestions for some secure passwords:
- by bydingels,tee2d is an abbreviation for the sentence (My hobby is reading novels, but I don't have time to read), where we delete the first three letters of each word.
- Study * stress = extreme fatigue Create a mathematical equation
- Iwoudlice2tricorinramen is an abbreviation for a sentence (I would like to try korean ramen) where the word is intentionally misspelled.

Secondly : User-level multi-factor authentication that depends on user ownership:
We will use OTP authentication, whether by sending the security code to the e-mail or by text message to the phone number. After the user has completed filling the first page, he will send a security code consisting of 6 numbers and letters to the email or the entered mobile phone, to verify the user's ownership.

Third : Network-wide multi-factor authentication that depends on dynamic characteristics or user behavior:
We will use biometric authentication. This method of authentication relies on sensing biometric features such as voice patterns, signature patterns, and gestures. So that after the user completes entering the security code, a list will appear for him (voice pattern, electronic signature, gesture gestures) and he will choose the appropriate attribute for him. If he chooses the audio mode, the application will ask the user to record audio of no more than 30 seconds. If the user chooses the electronic signature, a white page will appear asking him to sign and confirm the signature again. If the user chooses sign gestures, an image will appear with some sign language movements, and the user will be asked to choose from 8 to 16 different gestures and record the movements in the form of video or sequential images.

MFA protects user data from being accessed by an unauthorized third party.
By requesting additional verification information from users such as a one-time security code request. If we assume that the ransom virus has penetrated the device of one of the users of the application, the ransom program is malicious, as the attacker surreptitiously installs it on the victim's system. In addition to encrypting files and data. To decrypt and restore user access, the attacker demands a ransom from the victim. But when using MFA; The attacker does not have the additional information (PIN, OTP, ...) required to access the victim's data, making it out of the system and preventing a possible attack. Therefore, multi-factor authentication has a high level of security because it has one or more user identity verification factors.

3. Privacy of users is not compromised

Data security versus data privacy

Although data protection and privacy are both vital,they are not synonymous.
The first is concerned with policies and other procedures.

Data privacy is concerned with determining who has access to information, whereas data protection is concerned with enforcing those restrictions.The policies that data protection instruments and processes follow are defined by data privacy.Users are in charge of their privacy, while corporations ensure that it is protected.

Another significant distinction between privacy and security is who is normally in charge. Users can typically decide how much data is shared and with whom for privacy reasons.This distinction is reflected in compliance regulations, which are designed to assist corporations comply with users' privacy requests.

User information entered by the user to use the application:

User data and information means all and any of the following:

a- Personal data used in registration such as name, date of birth, health status and education degree.

b-Information about the user's current position and movements.

c- Contact data information and updates related to usage.

All-in-one user right :

- Any user who has previously provided us with personal information has the full right to:
- Access to information.
- Getting information.
- Correct or modify information.
- Withdrawal of agreement and deletion of information.

How does an all-in-one app protect users privacy?

1-We use top-of-the-line encryption technologies such as Transport Encryption (SSL/TLS) to secure usernames, passwords, API keys and any other important data sent from a device to the server. This is especially important because many users use unsecured public WiFi networks to access apps and the app supports sending fully encrypted SMS text messages. As the data is encrypted, and no one but the user and the bank that deals with it can understand it. Encryption protects the data even if it is stolen.Without the encryption key, the hacker will not be able to decrypt it.

2- We can assist users in protecting any personal information handled by the All-in-One app if their device is infected with a virus or malware, or if their devices are lost. One possibility is encryption. To protect sensitive user data such as passwords and keys, several platforms use their own storage systems.

3- Continuing to work on its security, updating security libraries, pushing updates to users, and using users' feedback to discover security vulnerabilities and work to fix them

4- Take security measures to protect the server used for the application

5- We do not keep user data that we do not need and prefer to avoid because it may increase security risks.

6- When logging in to accounts, we impose complex passwords and do not accept weak or duplicate passwords, and to increase security, the application prevents any screen capture process.

7- At every stage of the application development, it is tested and the test is not postponed, as it is harsh tests that simulate reality and challenge the attack.

8- We use high-level authentication, where when the user enters the password, he also enters the finger to ensure that he is the user who benefits from the application, as security attacks occur due to weak authentication.
9- Our employees are trained on the privacy policy and dealing, and they are aware of the penalties for disclosing user privacy.

Examples of the data in the All-in-One application and how we work to protect it:

Sharia is our basic principle to protect the user's personal data and preserve his rights, as the principles of Sharia stipulate that it is forbidden to disclose secrets except in the case of the consent of the owner of the secret.

Financial data:

Financial data is definitely at the top of the list. This is a kind of privacy in which all the customer's financial information is collected and we work hard to protect it
Where according to the financial privacy rule, which stipulates mandatory principles for the collection of financial data, as the user has notice about the information collected about him and how this data is used and how to protect it
And Gram Leach Billy's law on the basis of guarantees, as we have a security plan to protect the user's personal data
We use two-factor authentication, where it identifies the real account holders, where we need a password and a personal identification number, where when the user enters it wrong twice, we ask him the third time for the account number, and if it is entered in a wrong way, we stop his account and ask him to review the bank

Health records:

Each personal statement related to an individual's health condition, whether physical, mental, psychological, or related to his health services. In the All-in-One application, we provide a set of services such as locating the nearest health care center and setting an appointment for a consultation.
Patients and their guardians enjoy privacy rights laws under HIPAA law for the purpose of protecting medical records and securing the content of health information that is stored on servers, where they have the right to file a privacy complaint and the right to access and modify health information and that the user has knowledge of the data accessed and has the right to refuse or accept and Data encryption related to the Ministry of Health, which means that only the user can access his data, and user data is constantly updated .

Educational records:

The Family Education Rights and Privacy Act (FERPA) governs pupils' educational records and was passed in 1974. It gives parents the right to examine and change their children's records, as well as the option of not disclosing those records. FERPA offers parents access to their children's educational records, as well as the ability to request amendments and some control over the material disclosed from the records. Before revealing educational records, schools must get student consent, with a few exceptions.

The all-in-one application maintains the privacy of the educational records of the user and his children, and the information will not be used except in cases of extreme necessity in accordance with the controls regulated by the approved regulations for that.

Location data

The all-in-one policy describes how we deal with geographic information. The geolocation feature contributes to determining the places near the user in the case of determining his destination and displaying driving directions. When the user registers for the application, we ask him to specify his geographical location and we can also know it from the website of the device and the user has the right to share his location or refuse his participation and in the event that participation is refused,he won't be able to use the services available in that location because the user's location will be kept totally confidential.

User responsibility to protect privacy:

In order to protect user information, we recommend the following:
1- Immediately contacting the technical support of the application when the user believes that another person has been able to obtain access information to his account in the application or any other confidential information.
2- Not to give out any confidential information over the phone or the Internet unless the identity of the person or party receiving the information is known.
3- Not to share the login information (username and password) with others, and not to allow others to use the user account in the application and to create and remember unique and complex passwords.
4- Using the application through a secure electronic device, closing unused Internet-connected applications, and ensuring that the antivirus program is always up-to-date.

4. All-in-one-app follows the relevant CITC (Communications and Information Technology Commission) and Saudi NCA (National Cybersecurity Authority) policies

The Communications and Information Technology Commission contains:

First the privacy policy:
It describes how to manage the personal data of users, by collecting and using it when the user logs in to the application, and the ability to communicate with the authority when there is any inquiry about personal data.

Undoubtedly, the information collected or stored is only for use within CITC, and personal information collected by CITC such as name, nickname, and IP address of devices. However, the user can, at any time, request a copy of his data, with the possibility of requesting an amendment or deletion of his information. In addition to the authority’s keenness to provide the best services and ensure the confidentiality of users’ data, by preventing unauthorized access to it, its leakage, tampering, or misuse in any way, in addition to not viewing it and not disclosing it except to authorized persons only, and that When specific controls are available.

Thus, when we use the CITC's privacy policies in our all-in-one application, they maintain the privacy of users' data and help us protect their rights. CITC processes the personal data of users in a systematic manner so that the results of the processing are fair without causing harm to the users.

Second, the comprehensive service policy:
It is the provision of basic communication services to all members of society, specifically to areas where these services are not available. These services include data transmission at rates that allow access to the Internet, by creating a competitive environment of technology neutrality.

That is, to allow the participation of nearly 100% of the population of the Arab Kingdom of Saudi Arabia in the specific communications and information technology service, and to use it to a degree that suits families or individuals with a specific quality. Therefore, when we use the comprehensive service policy in the all-in-one application, the Communications Authority ensures the service of all users of the application, even for those in rural or island areas, at reasonable prices for everyone, i.e. ensuring the expansion of the scope of services provided to the latest thing in technology.

In fact, people who do not have a network or the Internet can download the all-in-one application to provide an unlimited network and Internet in their smartphones, just by choosing the type of package that suits them monthly, which helps the application to provide unique features that are not provided by the applications else. This feature is optional and not mandatory for all users.

The Cyber Security Authority contains:

First on the policy of enhancing cyber security:
A Network Security Policy (NSP) is a set of documents that outline the policy for acceptable and unacceptable use of an organization's IT assets. Indeed the need to constantly develop and update these documents by the developments of technology and the needs of employees. In addition to monitoring the system and recording all login attempts. Also, users can access network servers through MFA-based processes, such as passwords, biometrics, and security tokens. The NSP includes the Computer Use Policy, the Internal Access Policy, the External Access Policy, and the Acceptable Use Policy (AUP).

This all-in-one application complies with the guidelines for the expectations of network security and resources, these expectations are from the founders and developers of this application. Besides they should all familiarize themselves with the Acceptable Use Policies (AUP), which define the rules and practices to be followed for network access. This helps users to know the cybersecurity laws of network usage and what is usable with network resources and what is not. It aims to reduce risks and security attacks for users of the application. When establishing an NSP, it is necessary to understand what information and services are available, what should be protected, how to protect it, and what the potential for damages is, as well as the appropriate action when data or information is breached.

AlgoSec helps manage all-in-one application network security policy by providing network policy management tools and solutions, to ensure continuity of connectivity, and we use them to complete our tasks and save time and effort. AlgoSec works on the IT infrastructure in an all-in-one application, and AlgoSec facilitates and automates the network security policy to make the application more flexible, secure, and compliant at all times. AlgoSec automatically generates a network map of the application network and can intelligently assign and understand the NSP across cross-network ownership. So that it can automatically detect cyber risks, and develop a quick plan and automatically implement it to change the security of the network.

Second, on the cybersecurity resilience policy:
Cyber resilience is the systemic ability to respond to cyber-attacks and ways to recover from them. Electronic resilience provides rapid online adaptation to known and unknown crises and challenges, and helps protect and reduce cyber-attacks, and ensures the continuity and prosperity of the organization even if it is under attack.

Electronic flexibility has three main components:
1) Management and Protection: It is to ensure the ability to identify, assess and manage risks related to the application and information network systems, protect the system and data from electronic attacks and prevent the access of unauthorized persons. Moreover, electronic flexibility provides a good strategy that enables us to track users as they enter the application, by using strong user identity access management and using advanced authentication methods with it.
2) Discovery: It relies on constantly monitoring networks and information systems, to detect cybersecurity incidents and possible deviations before any major damages occur, in addition to finding any security holes that may be exploited, and in addition to making smart decisions based on deep analyzes.
3) Adaptation: It helps us in the quick management when the application is exposed to a cyber-attack incident and ensures the continuity of our application, and its return as soon as possible to work and with high efficiency. Adaptation requires the integration and deployment of new services available in the application, in addition to its rapid ability to link data using machine learning and mathematical models, and make data-driven decision making.

However because day by day the security landscape is changing, whether it is because of hackers, sudden disasters, or changes in enterprise standards. Without a doubt, the cybersecurity approach depends on being flexible and the ability to quickly adapt to continuous changes. Therefore, when we use the cybersecurity flexibility method, the all-in-one application will give the best way for its longevity and continuity with high efficiency.

5. Relevant intellectual property rights are not violated

Legal outputs that protect the rights and intellectual property of individuals, groups and institutions of all kinds, including: trademarks, copyrights, graphics, designs, models, specifications, concepts, processes, technologies, databases, trade names, trade secrets and others.

1-Trademark intellectual property right:

According to the new Gulf Trademarks Law in force in the Kingdom of Saudi Arabia as of September 27, 2016 a trademark or service mark include any term, name, symbol, device, or combination of words, names, symbols, and devices used or intended to be used to identify and distinguish the goods/services.

Why is trademark protection important in an all-in-one application?

The application logo and application name will be saved by the trademark of the intellectual property rights to prevent any other person from violating these rights and using the names and marks for his own account, as it serves as the identity and as it makes it easier for our customers to distinguish us. And its role is not limited to here, but also helps to increase our confidence in our services by users significantly.
A trademark is registered until it has the legal effect that helps protect it as well
It proves ownership of this person who owns the trademark, so the law stressed the need to register
The trademark so that its owner can obtain full protection for that distinctive trademark. The brand embodies the wisdom and work of the production company and is an important intellectual property; It is an intangible property that is always produced profit.Because the brand has the function of renewal (the brand is valid for 10 years and can be renewed when it expires), it has the function of adding value.

Trademark Protection in All-in-One App from Infringement:

Under Saudi Trademark Law, well-known trademarks are recognized even if they are not registered. In many cases, Saudi courts have recognized the protection of well-known, unregistered trademarks.
Infringement may sometimes occur accidentally or intentionally for financial gain where the trademark is imitated or infringed using a third-party trademark in a way that misleads or confuses people as to your association with it is a violation of our trademark policy.

2-Intellectual property right of copyright:

The copyright system in the Kingdom of Saudi Arabia was issued pursuant to Royal Decree No. M/41 dated 2/2/1424 corresponding to August 30, 2003.
Authors who express themselves through writing, sound, drawing, photography, motion pictures, and computer software are allowed copyright..Copyright is protected throughout his life and for fifty years after his death.

What are the types of software licenses?

Penalties for copyright infringement depend on the type of software licenses you have.
There are two types of software licenses,
1 Free and Open Source Code Licenses
2 closed source code licenses

How to copyright software

Software copyrights are used primarily by software developers and owners, usually the creator of the work, a publisher, or another company to which the copyright has been transferred.It can be difficult to verify that copying actually occurred in the absence of line-by-line copying of the codeInclude redundant code or software components into the real code to try to make copy detection easier. Even if the so-called copy does not include the same redundant software components as the original, it can be a strong indicator that copying has occurred.

Software copyright infringement

When running a program on a computer, it's nearly difficult to avoid copying some code because the program is normally copied automatically inside the computer's memory to allow it to execute. Copyright is infringed not only by obtaining a direct duplicate of the original work, but also by altering versions of the original, which is unique to software.

3-Intellectual property right for trade secrets:

Trade secrets are intellectual property rights (IP) information that we can sell or license to get money. Trade secrets are not registered with the government or regulatory agencies when the protection criteria are met, and therefore the right to a trade secret is automatic.

It is not a commercial secret unless three conditions are met:

1- The information should have commercial value because it is confidential.
2- The information must be confidential, meaning that it is known only to a certain group of people.
3- Take security measures to maintain the confidentiality of information.
Why are trade secrets important in an all-in-one application?
Intellectual property protects trade secrets in our all-in-one app from wrongful infringement, as trade secrets are kept without any formalities but with internal procedures. Trade secrets are only protected from retention as long as they are not disclosed, published, or illegally obtained, however, the above conditions must be met for the information to be considered a trade secret.
Protection of trade secrets from infringement:
When writing the contract with the employee, he agrees to terms that prevent him from using or disclosing trade secrets outside the scope of work.

4-Patent Intellectual Property Rights:

A patent is an intellectual property right to invent something useful. The invention can be a product, a new way of doing something, or a new solution to a particular problem. When applying for a patent for an invention, the inventor must disclose technical information to the authorities responsible for the way the invention works. Intellectual property rights provide the inventor with the freedom to make a decision, whether to allow or not allow others to use the invention for a commercial purpose, such as producing, selling, or importing it. The patent is only valid for 20 years, after the expiry of this period, the invention becomes public property and anyone can use it smoothly.

Three conditions for obtaining a patent title:

1- The invention must be new so that the invention does not form part of the latest technology. It is the modern meaning in the current science and made available to the general public all over the world. Therefore, the owner of the invention must make sure that his invention is new before he applies for a patent.
2- That the invention is innovative, so that if the invention is presented to a person skilled in the field of work of this invention, and he easily arrives at the idea of making this invention, then the invention is not considered inventive.
3- That the invention has industrial and practical applicability, as this invention can be repeated more than once.

Why is a patent important in an all-in-one application?

The intellectual property rights of the patent help us to ensure the protection of the idea of the work of our application, when it meets the required criteria of originality and usefulness, the patent will preserve the idea for 20 years, and also will monopolize the idea of the work of the application, by not enabling individuals or companies to create a similar idea within the scope of Business, this monopoly experts call the gold standard for intellectual property protection.

Patent Protection from Infringement:

The idea of the application can be protected by submitting a patent application to the Patent Office with a payment of 4000 Saudi riyals, and after about a year we start the procedures and we pay the publishing and granting fees of 5000 Saudi riyals, to obtain protection for the patent of an idea in our application among all applications.

Ways to encourage people to produce more quality applications through:

Educating people about the importance of intellectual property and how it facilitates many aspects of life.

- Thanks and appreciation to all the creators always for their achievements.

The effect of preserving intellectual property:

Being a catalyst for increasing technical development.

Intellectual property rights protect operating systems and designs.

Maintaining small and medium enterprises.

Contribute to the increase of economic development, and also of cultural development, and social development.

Intellectual property greatly improves the quality of life by:

The progress and renaissance of mankind through innovations in all areas of intellectual property.

Promote the ambition and innovation of the creators.

Conclusions

And here are the last drops of an enjoyable journey, and the last drops of a journey that elevated thought and reason, and the research was talking about a case study of applying all-in-one according to principles and conditions that we have studied in ethics, and we have made a lot of time and effort to conclude it well. Conclusion and we hope that the information That we have presented in this study is useful. We have succeeded in this study by the grace of God Almighty, and may God’s peace, mercy, and blessings be upon you.

References :

ABDULLAH, M.; ALSANEE, E.; ALSEHEYMI, N. Energy Efficient Cluster-Based Intrusion Detection System for Wireless Sensor Networks. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 9, 2014, 10-15

B. Abdullah, I. Abd-algafar, G.I. Salama, A. Abd-alhafez
Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System Proceedings of 13th International Conference on Aerospace Sciences and Aviati Technology (ASAT-13), Military Technical College, Cairo, Egypt (2009), pp. 1-5

Lemley, M. A. Convergence in the law of software copyright. High Tech. LJ (1995), 10, 1

G. Lowe. Casper: A Compiler for the Analysis of Security Protocols. In Proceedings of 10th IEEE Computer Security Foundations Workshop, pages 18–30, 1997.

S. Chatterjee, "Security and privacy issues in E Commerce: A proposed guidelines to mitigate the risk," in Advance Computing Conference (IACC), 2015 IEEE International, 2015, pp. 393-396.

IDENTITY, O., 2021. What is Multi-Factor Authentication (MFA), and how does it ￼work?. [online] OneLogin. Available at: <https://www.onelogin.com/learn/what-is-mfa> ￼[Accessed 7 December 2021].
Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, ￼Y., 2021. Multi-Factor Authentication: A Survey. [online] MDPI. Available at: ￼<https://www.mdpi.com/2410-387X/2/1/1> [Accessed 30 November 2017].

Griffin, P., 2021. Biometric Knowledge Extraction for Multi-factor Authentication and ￼Key Exchange. [online] ScienceDirect. Available at: ￼<https://www.sciencedirect.com/science/article/pii/S1877050915029804> [Accessed 8 ￼October 2015].

￼Invision. 2021. What is a Network Security Policy (NSP) | Invision. [online] Available at: ￼<https://invisionkc.com/network-security-policy/> [Accessed 2 December 2016].
￼algosec. 2021. What is a Network Security Policy | Crafting IT & Cyber Security Policies ￼| AlgoSec. [online] Available at: <https://www.algosec.com/resources/security-policy/> ￼[Accessed 7 December 2021]

algosec. 2021. What is a Network Security Policy | Crafting IT & Cyber Security Policies

￼| AlgoSec. [online] Available at: <https://www.algosec.com/resources/security-policy/> ￼[Accessed 7 December 2021].
￼Itgovernance.co.uk. 2021. What is cyber resilience | IT Governance UK. [online] ￼Available at: <https://www.itgovernance.co.uk/cyber-resilience> [Accessed 7 December 2021￼]

￼Microfocus.com. 2021. What is Cyber Resilience? | Micro Focus. [online] Available at: ￼<https://www.microfocus.com/en-us/what-is/cyber-resilience> [Accessed 7 December 2021￼]

￼CITC. 2021. Privacy Policy - CITC. [online] Available at: <https://www.citc.org/privacy-￼policy/> [Accessed 7 November 2021].

C. (n.d.). Communications and Information Technology Commission. Citc.Gov. https://www.citc.gov.sa/en/RulesandSystems/privacy/Pages/default.aspx

Controls and guidlines. (n.d.). National Cybersecurity Authority. Retrieved November 8, 2021, from https://nca.gov.sa/en/pages/legislation.html

Controls and guidlines. (n.d.). National Cybersecurity Authority. Retrieved November 8, ￼2021, from https://nca.gov.sa/en/pages/legislation.html The Island Now. 2021. Reasons ￼￼Why Patent is Important for Any Business - Blog - The Island Now. [online] Available at:
￼<https://theislandnow.com/blog-112/reasons-why-patent-is-important-for-any-business/> ￼[Accessed 8 December 2020].

How did we work:

Ruba Alsulami	**Introduction 1 ,3 ,5**
Aryam Mahjoub	**Conclusions 2 ,4 ,5**