CASE STUDY

University of Jeddah - College of Computer Science and Engineering
CCCY 112 - Computing Ethics Syllabus
Dr. Bahiya Aldissi
07/11/2021

TABLE: We cooperated and shared all the work, but the division was in the beginning:

Ghaidaa Al sultan **ID: 2116345**	Description of the application, First question, page layout and **Collaboration with the team** question 3 (point 2 :work history) question 5 (point 2:copyright)
Bushra Dajam **ID:2110054**	question 4 Individually, **Collaboration with the team** question 3 (point 1 and 4: health and fininacl data) , question 5 (point 3:patents)
Rawan Almalki **ID:2110668**	question 2 Individually **Collaboration with the team** question 3 (point 3 :web browsing behavior) question 5 (point 1: trade secrets) question 1 (point 4)

The All-in-One application is a Saudi application that serves different members of society and contains many areas such as health, finance and the web and provides services such as keeping medical records, bank transfers, and many more. The application can be obtained through the electronic stores on the device. All devices are supported.

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

1-In a proactive step to keep application data protected from external threats and data access attempts, setting a **next-generation firewall** is important as it is the first line of defense for the application, where all network data from outside must pass through the firewall and only passes data that has been verified as legitimate. The principle of the work of the firewall is to filter packets that pass through it, examine the address, ports, and protocols, and determine if they will be allowed to pass or not[18].

2- The proxy server will be used when requesting a site or service, as it acts as an intermediary and requests it on behalf of the application services user. The most important service it provides as it provides better protection is to hide the user's identity by changing the user's IP address and hiding it from the requested site, so the IP cannot be known. The proxy server also works to filter content that does not comply with the policies of the All-in-One application, this service helps protect data from malicious use [21].

3-The financial and health data of users and other sensitive data are periodically shared with the relevant authorities, so it must be protected during its transmission over the network from eavesdropping by the third party, so we will use **encryption**, anything can be intercepted during its transmission over the network, but encryption makes it impossible to see The data sent and accessed, the encryption is by using a key for encryption and converting the plain text into an encrypted text that can only be read with the presence of the encryption key, the algorithm WPA2 is the most secure and an AES-based encryption mode[18]. and We review the SSL/TLS [22], to ensure all data transmitted through the networks is secure. This ensures a dependable and secure communication system between network users by limiting excessive traffic in the application to improve network and online systems of data sharing speed, accuracy, and security [22].

4- The huge amount of sensitive and personal information in the All-in-One application makes it a great target for hackers, so attempts to infiltrate will not stop, and to stop these attempts we will use the **Intrusion Detection System Knowledge-based (IDS**), Much like antivirus software, it watches all packets passing through the network and compares them to a database of attack signatures or attributes of known dangerous threats. Where it monitors all protection devices and components. Detects and informs the system when an intrusion situation occurs and responds to them by blocking hackers or blocking the server.All of the alerts are based on the detection of known-malicious data, therefore they're all reliable.,With a high rate of accuracy and no false positives, an IDS can detect threats.[11]

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

Weak authentication is the source of many security breaches. Stronger authentication is becoming increasingly important, And what the application contains of sensitive and confidential data, it is necessary to provide strong authentication and to ensure that this .information is only accessed by its owners

The application consists of several layers that must be protected and prevent unauthorized .access, network layer, application layer, end user layer

we will talk about each layer in terms of how to implement authentication in it

1-network layer

The network is the gateway for hackers to attack the application, so making sure that the application is protected against intruders and unauthorized persons is important. After examining the application network, we found some problems and weak authentication strength and procedures will be implemented to solve this problem
users who want to enter a network will be authenticated
By proving their identity, username and password, with the presentation of the user's identity card, this procedure protects against unauthorized access and proof of the user's identity.

2- application layer

The password is weak, and it can be easily stolen or guessed. Whatever the strength of the password is, it does not mean anything if the hackers deceive the user and get it through phishing or social engineering, so the password is not enough to be an authentication factor and more than one authentication factor must be available,
Users use easy-to-remember password patterns and methods. Hackers are aware of common formulas people use to create passwords.
Multi-factor authentication is making sure that everyone trying to log in is the legitimate user, by requiring more than one proof of identity
Each authenticator should be of a different class, something, [23]
something they have, or something they care about, so it adds extra protection for users and reduces the impact of compromised credentials. The password may be compromised, but when the second factor of authentication is requested, they will not be able to log in or access important data., Requesting multi-factor authentication is more secure and provides a high level of protection and user identity verification, which is suitable for an all-in-one application.As I mentioned earlier, multi-factor authentication must consist of three different factors that are not related to each other or can be accessed through the network if they are compromised, so the user will be authenticated on several factors including:
First, knowledge: It is the user's proof of his knowledge of it, which is the password that is entered when trying to log into the application next to the user name
Second: Possession: It is something that the user only possesses, and since the application is on mobile phones, and each user has his own mobile device, after making sure the password is correct, the authentication will be done again by sending a one-time password via a text message to the user’s mobile, including the temporary code and an alert. Please do not share this code with another person to avoid being scammed .[23]
Third: vital signs
Including recognizing the identity of the user through the face print. This feature works to match the characteristics of the face of an individual and compare it with an approved face stored in a database or fingerprint, where most smart devices contain fingerprint scanners and the most common for ordinary consumers To improve the user experience, there is no specific authentication approach that is suitable for all users, so after authenticating the password and username, the user will be given a choice between two factors to authenticate it either by face-fingerprinting or by sending a temporary code as a text message

3- End user level

Violations may occur, putting user data at risk as a result of the loss or theft of the user's device, so setting a passcode for the user's device is important and hinders and prevents unauthorized accessIt blocks additional entries to the device.
Despite the security measures and precautions that are applied to protect the application from unauthorized access, the end user may be the cause of unauthorized access, so the process of educating the user is very important, one of the most famous methods used in deceiving the user is phishing by sending mail messages A fake email or text that asks the user to enter his data for the purpose of updating the data or any convincing reason, and the user falls into this trap,, the best way to counter is to tell the user that the application will not ask him for data via mail or text messages, also when logging in to the application and sending the password For once, it is accompanied by the phrase “Swiping the code exposes your account to fraud.”

Password is the front line to protect user accounts, and choosing a weak password may lead to an all-in-one application network hacking.

When creating a password for the first time, the user will be asked the password to be:

1 - The password must contain at least numbers, letters and a capital letter

2 The password is not the username

3 - The number of fields should not be less than 8

Also, a maximum of 3 login attempts will be placed, after which a text message will be sent to the user's mobile notifying an attempt to log in to his account.

There will be a period of inactivity in the event that the application is not used for a maximum period of 10 minutes, the user account will be logged out and the password will be required to be re-entered.[23]

3. Privacy of users is not compromised

All firms must protect their data from cyber-attacks. The cyberattack's unparalleled success has exposed serious flaws in both governments' and businesses' present approaches to cybersecurity.The nature of this ransomware is extremely disruptive to a business's financial daily operations, and cloud technology is one approach to protect against such attacks. Multiple data centers in various geographic areas are used by cloud service providers. This prevents service interruptions; for example, if one of the servers fails, others can take its place.As a minimal security measure, cloud companies also enable multi-factor authentication and suspect login detection. To limit the danger of data loss, they keep numerous copies of their data in separate locations.[7]

- **financial data**

  Because financial services firms and institutions lose money every year due to crimes including mortgage and insurance fraud, online banking fraud, and check and card fraud, it's important to choose an all-in-one financial data protection app.[8]

  The application protects financial data by using the authentication methods that were previously mentioned.[9]

  The Fair Credit Reporting Act one of the privacy laws that all-in-on application will use. also we will use a standard named Payment Card Industry Data Security Standard (PCI DSS).

  The major federal regulation governing the collecting and reporting of consumer credit data is the Fair Credit Reporting Act. Its rules control how credit information about consumers is collected, held, and shared with others, including customers.[1]

  PCI DSS is a standard for businesses that engage with major credit card networks branded cards.To combat credit card fraud, the standard was established to tighten safeguards surrounding cardholder data. This standard was chosen because it prevents data breaches, builds customer trust, avoids fines and penalties, and complies with global data security requirements.[10]

- **work history**

  All users of the application and customers have the right to express what they want freely and to protect their rights and work records. And after the talk was about (the right to communicate) and (the right to know and access to information), it became about the protection of human rights and the protection of his work history, especially the right to privacy (the sanctity of private life), users' data, personal information and communications must be protected in all ways.[7]

  The data of the users, their personal information and the work record are stored, collected and processed electronically, not only by the network administration and the specialized companies, but by everyone who has the ability and ability to do so, whether from hackers, service providers, the government or other countries and companies. These means enabled their users to violate the privacy Each other and publishing their work records without considerations, so these immoral behaviors have been limited and laws, ethics and penalties

have been established in the Kingdom of Saudi Arabia that govern these means and their users. Ethics and the extent of the privacy of the application, even if it is a media.[1]
Therefore, you must provide the following:
1-Install reliable anti-virus and anti-malware software.
2-Make sure to update your operating system and other software regularly, especially when security patches are released. Vulnerabilities in out-of-date software are often used by hackers as a way to break in - don't give them a chance.
3-Be careful what you click on. Hackers often perform "phishing" attacks by sending fake emails that claim to be from your bank or eBay but take you to a different site to steal your login credentials.
4-Protect your online privacy and security with two-factor authentication as much as possible.

- **web browsing behavior**

  When conducting research that uses Web logs to gather and analyze user behavior, privacy is a major consideration.Individual users' web surfing activity can be characterized by the sequence of viewed online pages and the time of visits as they engage with the World Wide Web during each browsing session.Servers have made great use of this hidden browsing sessionsm, The patterns in web browsing behavior reveal critical information about people, such as their locations and affiliationsAs a result, it is the service provider's, i.e. data holder's, responsibility to guarantee that disclosing this data does not jeopardize individual user privacy. and To protect user behavior data from browsing the web, which includes cookies, the user must be informed in the privacy policy what data is collected, how it is used and with whom its data is shared, while ensuring that this data is protected, the user's cookie data is periodically disposed of within a period of time A maximum of 21 days and its destruction in a secure manner that prevents leakage or loss, that data collection is limited to the minimum amount of data that can achieve the purposes of the application, ensuring the protection of user data from unauthorized access by encrypting it and storing it in secure servers and it is only viewed by the concerned persons [12] All privacy policies that are followed fall under the National Data Governance Policies.

- **health information**

  Using computer networks and health databases, individual health information and general medical data are becoming more freely available in electronic form.Both medical practitioners and patients benefit from the growth of electronic data within a modern health information infrastructure, will take place More autonomy for patients, better care, advancements in health research and public health monitoring, and current safety technologies are just a few examples.also eill follow the health Insurance Portability and Accountability Act. Patients have the right to be educated about their privacy, access to their medical records, and a method for correcting errors under the rule. It also necessitates patient consent to release personal information.Special provisions for health information disclosure for research, public health, law enforcement, and commercial marketing are included in the rule. Personal identifiable information in whatever form, whether sent electronically, on paper, or orally, is subject to the rule.The Ministry of Health is bound to keep any personal information about you private unless you freely choose to share it; this information is not used for any reason other than that for which it was gathered. The owner of personal data has the right to revoke his consent to distribute his information at any time.One of the main reasons for this regulation is that users are afraid of being ostracized if they seek therapy for mental health issues. It will not be kept a secret, and it will have an impact on future work assignments and advancement.[13]

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

The All-in-one app has to adhere to the CITC (Communications and Information Technology Commission) and Saudi NCA (National Cyber Security Authority) policies.

- We must guarantee that the Application follows the Corporate Security Policy, which outlines management commitment and key objectives for risk-based information security procedures. The policy will guard and protect the information from the app, the developers, the end-users, and partners. This is accomplished by improving information security, protecting the rights of all computer networks, and safeguarding the users' interests, morals, and shared values, and overall protection of the national economy. This is achieved by fair informational practice within and across the borders.
- We also have to ensure the All-in-one app adheres to Information Security Aspects in IT Management policy. This creates an overall approach to the information security of the application. The policy aligns itself to the CIA model (Confidentiality, Integrity, and Availability). The policy divides the data into categories that may include: top secret, confidential and public display data.
- We also have to ensure the Application also has to adopt Cybersecurity Governance. This provides an environment where we as the developers and the to the board of directors overseeing the application create an environment that promotes and ensure a secure environment. Cybersecurity awareness and training is conducted to all partners all requirements in accordance to Data Protection in the Kingdom of Saudi Arabia. We also have to ensure we are in Compliance with Legal Requirements as per the government and laws. We have to observe laws and regulations applicable our niche as highlighted by the government. i.e. Information Security Assessment, Information Security Auditing, and Compliance with Defined Policies.
- When developing the All-in-one app we have to ensure we comply to the Cybersecurity Resilience policy. This means that we develop the application under the framework that puts in place the future of the application at hand. This means the preparedness for, response to and recovery from cyber-attacks. This also means developing an application that is easy to recreate, improve and upgrade in the case of change in cyber-attacks landscape and the change in technology.

All-in-one also follows these policies Identity and Access Management, Email Protection and, reduce BYOD policy, Information System and Processing Facilities Protection and Cloud Infrastructure and Services License.

The application will provide a cybersecurity protection guarantee for logical access to informational and technical assets through this policy, preventing illegal access and limiting access to what is needed to complete activities linked to the application.[5]

Multiple user identities and associated access permissions are initiated, captured, recorded, and managed using identity and access management (IAM) technology. According to company policies and their specific functions, all users are authenticated, approved, and evaluated and prevent identity threats. The application addresses identity-related cybersecurity requirements such as confirming a user's identity using a user name and password, as well as the possibility of authentication using a variety of factors such as vital signs and a one-time password, as well as a periodic review of login identities and permissions. The reason for choosing it is that many organizations face difficulties in managing identity and access. Identity and access management is important asset in the economy, especially in decision-making to support investments. Identity and Access Management (IAM) is a key driver for businesses, as it facilitates digitization, security management, and regulatory compliance.

E-mail is one of the most common ways to communicate with consumers, and it's also the most convenient way to spread ransomware. Users who are unaware of the risks are more likely to click on links and attachments without hesitation, assuming that the emails are legitimate.The number of spam, email viruses, denial of service, and other attacks that infect an email server will be minimized when it is protected.Email protection by employing new

technology to filter undesired messages such as phishing emails and validating the identity of the sender to see if it is a trustworthy source or not. To make it as safe as possible, We used a strong password with multiple variants that is difficult to guess . Do not connect to any other networks that you are unfamiliar with.
BYOD: It's a company policy that permits employees to access private computing resources using their own devices.[5]Increased use of the BYOD policy has led to an increase in cyberattacks and at the same time, it helps the employee productivity and increase the income, thus in the All-in-One application we are trying to balance the use of their own devices.[1] According to a study, The policy of "bring your own device" could pose serious security risks and have negative implications depending on employee ethics and the lack of safeguards in the formulation of corporate policies.[4]
When employing the personal devices of application workers, the security of mobile device devices must be assured, as well as the secure handling and storage of sensitive and commercial information of the application.
Data and information kept on mobile devices and gadgets should be deleted. BYOD When devices are misplaced.Virus, program, and malware protection, as well as the installation of an application firewall, is required to ensure the security of systems and information processing devices, including user devices and application infrastructures. These are used to protect systems and information processing devices to ensure the continuity and operation of the application.[1]
To achieve certain goals, cloud computing service providers must obtain a cloud infrastructure and services license, which includes identifying cloud computing service providers operating cloud computing infrastructure in the application, increasing the trust of application users, and controlling and protecting data missions.[2] According to a study in 2019, personal data leaks have increased and now account for over 90% of all data leaks from cloud storage. These consequences can be avoided by enhancing cloud storage administrators' abilities. One-third of the accidents that occurred in the cloud in Russia was caused by the company's employees, so the sensitive powers should be given to highly qualified people. Each detected unlocked service resulted in the exposure of personal data history.[3] So in an all-in-one app, we will only grant access to licensed service providers to reduce the possibility of information and data leakage. Through which roles and responsibilities are defined and it is clear to all parties involved in implementing the controls.

5. Relevant intellectual property rights are not violated (4 marks)

Intellectual property is describes individual works of art owned or created by a single person or group. Intellectual property is safeguarded by Copyright ,Patent and Trade secret laws .

- **Trade secrets**

Trade secrets do not protect the document itself or the way in which the information is presented. On the contrary, it protects the information contained in this documents well as any information shared inside the development team in order to promote the application's goals. This is an important difference, because unlike other branches of intellectual property law, to successfully use the commercial secrecy law, it is not necessary to prove that the above-mentioned documents were copied or deleted from an entity and used in another entity. It is sufficient to prove that the person who knew the secretly disclosed information, whether in the above-mentioned documents, team meetings, emails or other means, disclosed the information to a third party for reasons other than giving the information to that third party .Or the secrets of commercial application may be stolen from cyberspace or advanced computer technologies by major external parties and are difficult to discover [14],Therefore, The use of confidentiality materials prescribed in the Saudi labor system, which obligate the

employee to keep the secrets of the facility in which he works, is the mechanism employed to secure these secrets., which obligate the employee to preserve the secrets of the facility in which he works, and the development of a number of items that protect and maintain the facility's rights well. Putting additional requirements on employees who have access to sensitive facility secrets, such as the requirement not to work for a competitor for a certain period after the end of his relationship with the facility. It is important not to disclose the trade secrets of the application with customers or others with whom you have a business relationship until you've signed a non-disclosure agreement, which is usually focused on preserving both parties' sensitive information, and holding the other party fully responsible in the event that he discloses those secrets. One of the benefits of such agreements is that they safeguard even those secrets that are not considered patentable. The lists of users that have been provided to him can be a trade secret that he may not disclose, And if he discloses it, he will be fully responsible for any damages that may occur .According to the Regulation on the Protection of Confidential Commercial Information, the Saudi Ministry of Justice [15].The creativity employed in developing the application will be protected, and all features, functions, algorithms will be protected from infringement and copyright issues.

- **Copyright**

  Copyright is a legal right created in accordance with the law of the Kingdom of Saudi Arabia that gives us the exclusive right to use and distribute our application from today until 70 years after our death .[1]Also, if our rights are infringed upon or violated, we must report it, such as stealing the logo of our application or others the contents of our application, such as the music for the background of our application, according to the law of the Kingdom of Saudi Arabia. [16] Where we can claim compensation for the violation of our rights and damages caused to us. in addition to copyright law, it provides for certain penalties in the event of infringement, including:

  1-Warning to the offender

  2-A fine not exceeding 250,000 Saudi riyals

  3-A judicial order not to print, produce, publish or distribute the offending work, in addition to withholding copies and related materials,

  4-Confiscation of copies of work and materials used in infringement of our rights

  5-Imprisonment of up to six months.[16]

- **patent**

  The All-in-One application has obtained a software patent from the Saudi Authority for Intellectual Property, which allows only the owners of the application the freedom to modify it and protect the features included in the instructions saved on the computer.

  Our application contains unique software and therefore patented software and has been officially documented.[1]

  It is illegal to create software for the program, use it without authorization, sell it illegally, or copy it, and there are serious penalties for doing so.

  Patent infringement is defined as the use of a patent for which permission has not been obtained, and the penalties can be up to three times the sum specified by the owner.[1]

  the most prominent and most important current companies that have obtained a patent in their programs and applications. The patent has been granted for the originality and distinction of these applications from others and has a special impact in the hearts of users for its ease of use and ease of access:

  1- Facebook

  2 - Airbnb [20]

  the advantages that motivate large companies, institutions, and people to obtain a patent are:

1- When all-in-one obtains a patent, it will give them the right to protection and non-exposure, which gives them the right to be distinguished and to remove spoilers.
2 All-in-one have the right to keep the idea and not share it or allow others to complete it or sell it to others.[19]

- **Trademark**

The All-in-One application logo has been registered as a trademark by the Saudi Ministry of Commerce, where the logo symbolizes the services of the application and is uniquely designed as the logo is important to distinguish the application by the community, so the All-in-One application is the sole owner of this logo and no one has the right Anyone using, copying or modifying the logo, and in the event that this happens, According to the executive norms of the Saudi Trademarks System, the All-in-One application has the right to launch a lawsuit and be fined and imprisoned.[25]

References

[1] George W. Reynolds, Ethics in Information Technology, Sixth Edition, Cengage Learning, (2018),
[2] *Communications & Information Technology Commission*, 2021. [Online]. Available: https://www.citc.gov.sa/.

[3] Maklachkova, V. V., Dokuchaev, V. A., & Statev, V. Y. (2020, October). Risks Identification in the Exploitation of a Geographically Distributed Cloud Infrastructure for Storing Personal Data. In *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)* (pp. 1-6). IEEE.
[4]Dhingra, M. (2016). Legal issues in secure implementation of bring your own device (BYOD). *Procedia Computer Science*, *78*, 179-184
[5]"Critical Systems Cybersecurity Controls", *National Cybersecurity Authority*, 2021. [Online]. Available: https://nca.gov.sa/. [Accessed: 05- Dec- 2021].

[6]S. Jobs and G. Beahm, *I, Steve*. Melbourne, Vic.: Hardie Grant, 2011.

[7] A. Campbell, "How small businesses can protect their financial data: Unprecedented success of WannaCry attack exposed major lapses in business, govt towards cybersecurity," *The Business Times,* 2017. Available: https://www.proquest.com/newspapers/how-small-businesses-can-protect-their-financial/docview/1911217276/se-2?accountid=142908.

[8] Adams, R. (2010). Prevent, protect, pursue–a paradigm for preventing fraud. *Computer Fraud & Security*, *2010*(7), 5-11

[9]C. Coombe-Whitlock, "Scam warning: Over half of financial firms hit by data breach - how to protect your money," *Express (Online),* 2020. Available: https://www.proquest.com/newspapers/scam-warning-over-half-financial-firms-hit-data/docview/2373908564/se-2?accountid=142908.
[10]L. Irwin, "4 powerful benefits of PCI DSS compliance - IT Governance Blog En", *IT Governance Blog En*, 2021. [Online]. Available: https://www.itgovernance.eu/blog/en/4-powerful-benefits-of-pci-dss-compliance. [Accessed: 06- Dec- 2021].

[11] S. More, M. Matthews, A. Joshi and T. Finin, "A Knowledge-Based Approach to Intrusion Detection Modeling," 2012 IEEE Symposium on Security and Privacy Workshops, 2012, pp. 75-81, doi: 10.1109/SPW.2012.26.

[12]Fawaz, K., 2021. DATA PROTECTION AND CYBERSECURITY LAWS IN SAUDI ARABIA. [online] CMS. Available at: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/saudi-arabia> [Accessed 5 March 2021].

[13] Malin, B. A., Emam, K. E., & O'Keefe, C. M. (2013). Biomedical data privacy: problems, perspectives, and recent advances.

[14] R. B. Wiley, "Protecting Trade Secrets Under Uniform Trade Secrets Act," *Int. J. Commerce Manage.,* vol. 8, *(1),* pp. 120-123, 1998. Available:

https://www.proquest.com/scholarly-journals/protecting-trade-secrets-under-uniform-act/docview/212811964/se-2?accountid=142908

[15] Paul B. Keller & Jihad Hakamy, What to Know about Trade secret in Saudi Arabia, Law 360 (Apr. 26, 2016), http://www.law360.com/articles/777433/what-to-know-about-trade-secret-law-in-saudi-arabia

[16]*Laws.boe.gov.sa*, 2021. [Online]. Available: https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/67d159e6-ee98-4efc-a2ee-a9a700f1708 [Accesse 07- Dec- 2021].

[17]T. Chang *et al*, "The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic, Semi-Automatic or Manual?" *The Institute of Electrical and Electronics Engineers, Inc.(IEEE) Conference Proceedings,* pp. 1-4, 2018. Available: https://www.proquest.com/conference-papers-proceedings/method-capturing-encrypted-password-packets-wpa/docview/2170728839/se-2?accountid=142908.

[18] Jingyao S., Chandel S., Yunnan Y., Jingji Z., Zhipeng Z. (2020) Securing a Network: How Effective Using Firewalls and VPNs Are?. In: Arai K., Bhatia R. (eds) Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70. Springer, Cham. https://doi.org/10.1007/978-3-030-12385-7_71

[19] Advantages and disadvantages of getting a patent | nibusinessinfo.co.uk", *Nibusinessinfo.co.uk*, 2021. [Online]. Available: https://www.nibusinessinfo.co.uk/content/advantages-and-disadvantages-getting-patent. [Accessed: 07- Dec- 2021].

[20] "Recent Software Patent Examples from Top Companies - The Rapacke Law Group", *The Rapacke Law Group*, 2021. [Online]. Available: https://arapackelaw.com/patents/softwaremobile-apps/recent-software-patent-examples/. [Accessed: 07- Dec- 2021].

[21]B. Jefferson, "What is a Proxy Server and Are They Good for Security?", *Lepide Blog: A Guide to IT Security, Compliance and IT Operations*, 2021. [Online]. Available: https://www.lepide.com/blog/what-is-a-proxy-server-and-are-they-good-for-security/. [Accessed: 17- Sep- 2020].

[22] D. S. Karjala, "Intellectual Property Rights in Japan and the Protection of Computer Software," in Intellectual Property Rights in Science, Technology, and Economic Performance, Routledge, 2019, pp. 277-289.

[23] J. Knafo and F. 8, “Top 10 password policies and best practices for system administrators,” *The Devolutions Blog*, 02-Feb-2018. [Online]. Available: https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators/.

[24] U. Vekua, “A guide to the types of Authentication Methods,” *Veriff*, 05-Jul-2021. [Online]. Available: https://www.veriff.com/blog/types-of-authentication-methods. [Accessed: 07-Dec-2021].

[25] R. Decree, "Trademarks, Law and Regulations | The Embassy of The Kingdom of Saudi Arabia", *Saudiembassy.net*, 2021. [Online]. Available: https://www.saudiembassy.net/trademarks-law-and-regulations. [Accessed: 07- Aug- 2002].