Research Article

Awareness of Security Threats in Social Media

Alaa Alsubhi[1], Mohammed A. AlZain[1], Mehedi Masud[1, *], NZ Jhanjhi[2], Jehad Al-Amri[1], Mohammed Baz[1]

[1]College of Computers and Information Technology, Taif University,
P.O. Box 11099, Al-Hawiya-Taif, 21944, Saudi Arabia
[2]School of Computer Science and Engineering, SCE, Taylor's University, 47500, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract

Social media are sites on the Internet that allow users to interact and communicate with each other and since it is easy to use and produce a fast way to communicate. According to these features, it becomes very popular to everyone either the young generation or the old generation. But we need to be concerned about security and privacy. Is our information safe? Will we be safe while we using these sites? This paper presents the reasons that make us unsafe in social media. We'll also show some of the ways that we should follow to protect ourselves. So, in short, we can say that this research aims to increase the awareness of the risks of social media threats. Also, suggest some solutions to reduce the damage that may happen.

Keywords: Security Threat, Social Media, Big Data, Security Attacks and Cyber Crime.

1. Introduction

In the current generations, social media is the best way to communicate with our friends or family. From our view, social media are websites or applications that allow users to be under one roof to (share, write, post photos or video and sometimes shared their locations too) for free and have one condition that is availability internet to access such as (Instagram, Twitter, Snapchat, YouTube ...etc). But it is the time now to think clearly, we don't pay for any things and all of it for free. Also, remember that there are millions of employees that they need to pay for them. Then, how do founders earn their money?

The answer is our personal information and everything we post; Yes, believe or not it is the biggest source of income for them and some advertisements that show on the website or application. Part of the mission for saving and protecting our data and information is the responsibility of the company and on the other hand, the responsibility falls on us. Therefore, in this research, we aim to raise the awareness of privacy, security, and the risk that may occur when we underestimate it. So, this research paper content seven sections. The second section of the paper will talk about the big data role in social media. While the Third section will be about a security threat, the relation between threat and attack, cybercrime that may happen to the users, types of threats, examples of threats, and cybercrime on social media. The Forth section will discuss the literature review, while the Fifth section will be analysing the ways to protect and prevent attacks and vulnerabilities that we can use to protect ourselves as possible as we can. And Finally, the last two sections will be about the results and the conclusion.

2. The big data role

First of all, to understand anything we need to at look his history, Though the Idea of big data itself is comparatively new, the root of the big data sets goes to the 60s and 70s. Around 2005, people began to realize how much data users generated through Social Media. The development of open source frameworks, such as (Hadoop) was really important to deal with the growth of huge data because Of course, it makes work with it easier and cheaper to store [2],[3],[4]. The expression of big data means that is a huge amount of data sets that could not deal with it by using the old classical applications or software that applied to data processing. And since it is a huge amount of information that requires a processing system which is automatically working, cost-effective, and have the ability to make a decision. The big data based on three things speed, size, and types of sources of data or we can classify it as 3vs where Volume is the size, Velocity is speed, and Variety is the data type [5]

3. Security threats

There is a lot of definitions of security threat such as: In RFC 4949, the Internet Engineering Task Force defines it as "A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm". Also, in SP800-160, NIST defines it as "An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss" [6]. There is more than one kind of security threat, it's classified into [5]:

- **Classic Threats:** It's depending on the user's information that has been shared on the internet. By clicking on malicious links,.. etc. The users become a victim of it. The main goal is to steal private information such as passwords, bank information...etc.

- **Modern Threats:** They need to get the confidence of the users, so they win by their personal information either straight or un-straight. And that is their main goal.
- **Other kinds of Threats**:
  - **Click jacking**: Where it is an old way but by applying it in social media and adding to some new techniques, it will give a great effect. It works similar to a malicious link and users can not be aware of it.
  - **Cross-Site Scripting (XSS):** Users be attacked at the moment of opening this site.
  - **Malicious Applications:** Untrusted applications get the attention of a lot of users and winning their trust. And access is allowed for the developers to the information that has been store in their application.

Look at Fig.1 That shows a summary of the three threats (Classic, Modern, and Others) and examples of each one of them.

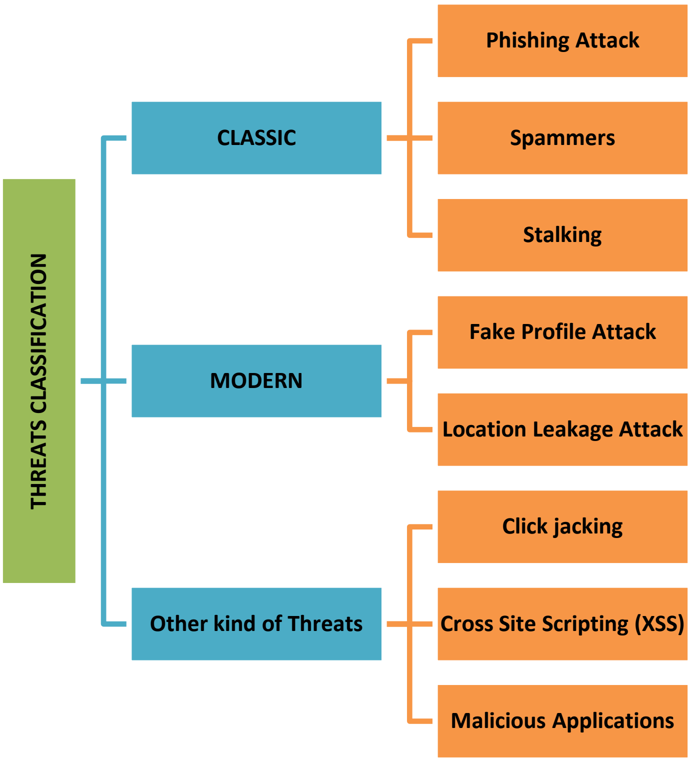

Fig.1. The classification of threats security.

3.1. Security threats and security attacks

We define the Threats before as " a potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could breach security and cause harm"[6],[7]. It is a possibility of danger or risk that may take advantage of a vulnerability. We understand from the two definitions that the relationship between threats and attack are the threats are led to the occurrence of the attack. It is impossible to discover and solve all the threats because they are renewable and may sometimes occur when the site is updated. We can compare threats as a hidden door that are not apparent to everyone, attacker by it turn need to look for it until he found at least one and then exploit so he can enter to the website or the system. Look at Fig.2 to understand the example where it is shown, the hacker looking for some threats on a system and even if the system uses a protection method It is still possible to get an attack.

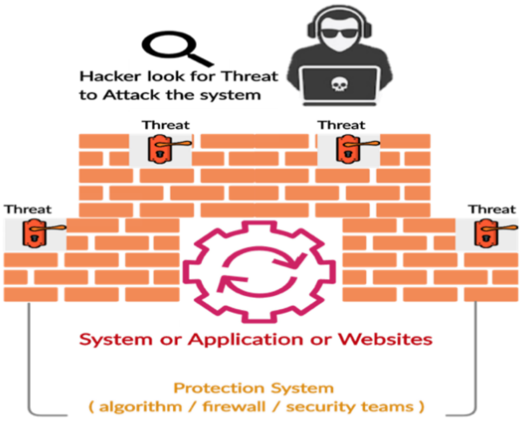

Fig.2. It is an example where hacker try to attack.

3.2. Types of threats

Confidentiality, Integrity, and Availability these three are the components of what is known as the CIA triad and with other security concepts, it is the basis of the STRIDE threat model. It is proposed by Microsoft in 1999 and it is the most popular classification. When you take the first letters from each concept (Spoofing identity, Tampering with data, Repudiation, Information Disclosure, Denial of service, Elevation of privilege) you will get the word STRIDE [6],[1]. Table 1 is a summary of the STRIDE and an explanation of each one of them. Also, it shows their related to the security property.

Table 1. Summary of the Threat, explanation and Related Security Property [1].

3.3. Examples of cyber security threats

As a hunter, cyber security threats become more dangerous if it is not ever seen[8],[9],[10]. You can use protection tools as many as you can[11], but you will remain in danger because simply hackers or the hunters are still succeeding to exploit any lacuna on the system. This may happen because either they found a lacuna that you’re not aware of it or they attack you by lacuna that you aware of it but you didn't fix it or solve it for any reason. In both cases, we still losing somethings. Security threats are constantly changing so it is hard keeping up with them[9],[12]. We will explain 6 of the cyber security threats [13]:

Number 1(Humanity Nature): Yes, whether they mean it or not. They are considered the main threats to cyber security. And we mean any person how can access the system. A lot of hackers use what is known as "social engineering": It is an attack that targets human behavior for a particular person, by manipulating him and gaining his trust. So, he can access his personal information or his secret numbers. Rather than target the device, it targets the human element. It is also called brain breakthrough.
Previous employees, this considered as serious issue on the big companies especially if the employee where work in a sensitive position. Because they may sell the company information or they may set some viruses, ransomware. To get retaliation from someone or make money.
Example: Capital One (It is an American bank specializing in credit cards, loans. etc. And it got a good reputation because it is a bank that depends on technology) where the data have been breach for a hundred million accounts. And it was a previous employee not on Capital One, but it was a previous employee on AWS (Amazon Web Services) where the bank uses their cloud host. According to that, they expect between 100 to 150 million dollars are the costs of the hack.

Number 2 (Different Kinds of Malware): Malware are the most insidious threat. It can be either adaptive or metamorphic (where it changes completely every iteration). According to the CIS Center for Internet Security in 2019, The most malware are:

- **Emotet**: It is a cybercrime process founded by Russia, it is found in 2014.
- **Kovter:** It is hidden without files that is target the Windows systems.
- **ZeuS:** It is a trojan horse that works on Microsoft Windows. And it is usually used to theft bank information.
- **WannaCry:** It is a ransomware attack that started in 2017 has managed to topple more than 230,000 devices.

- It encrypts all data on the computer, then it shows a message that you have to pay $ 300 for your data.
- **Gh0st RAT:** It is a trojan horse for Windows that GhostNet operators used to hack a lot of computer networks. So we can say it is a cyber espionage computer program. "Rat" refers to his ability to work remotely.

Number 3(Form-Jacking): We can understand it from his name, takeover forms on the websites by using Its loopholes. Often, they use JavaScript code on the final page of the forms for stealing the users' finances.
Examples: Ticketmaster attacks (it is an American company that sells and distributes tickets) and The British Airways attack that it lost more than $17 million.

Number 4 (Unsuitable Patch Management): The goal of it is to cover a puncture of any type. Where the systems always issued new patches to fix the weaknesses of the OS or programs. It gives a gap in your information technology security Infrastructure.
Example: Eternal Blue, it was developed by the National Security Agency where leak by a group of hackers in 2017. It uses a lacuna on Microsoft that led to global attacks.

Number 5 (Old Hardware or Software): we need to keep our devices and OS update to the latest version. because if you are using old software or old OS you will not be able to repel attacks.

Number 6 (MitM Attacks): Man-in-the-middle or Tapping, happens when the attacker sitting between two entities while transactions. Their objective is the same (getting your business data or the users' data).
Example: When a group from the Russian GRU attempted to hack OPCW at Hague. They use (Wi-Fi spoofing device) to get the results of some investigation. They fail on their attack.

3.4. Cyber Crime on Social Media

Cybercrime is different from the normal crime that happened Physically (Like stealing from a store), the action of stealing is known by all governments and countries as a crime and has penalties that differ from country to another. So, what about stealing information, does the penalties of it are the same? The Answer is NO, Because the crimes that are actually happening on the ground (Physically) have penalties are recorded and written in the constitution and Accredited in the courts. But crimes that occur on the Internet (cybercrime) a large percentage is not included in the same penalties. This has been one of the main reasons for the increase in attacks and violations on the Internet. Simply because “by Putting manners aside", **No law, No deterrence, No fear.**

We can say that Cybercrime is a criminal activity that happens by uses a computer or a networked device and most of them do it to earn money. Some of them use advanced techniques and they have good skills. And the others are novice hackers [14]. Some cybercrime occurs because of trust from users to the other one:

- **Cyberextortion:** Penetrate the other devices and take private pictures or secret messages from them that they do not want anyone to Seen it, then begins to blackmail and ask money in return for preserving or deleting it. Also, if the hacker has abnormal tendencies, he may begin to extortion the victim to meet him (This might happen to kids, teenagers, or women).

- **Theft, sale publishing of corporate data:** As what happened to Adult Friend Finder in 2016 where up to 400 million accounts have been breached and it said that the leak cover 20 years of sign-ins, including the deleted accounts [15]. Since users' private information was published, a lot of people have been harm as they didn't want their family or friends to know that they use it (Especially the married).

Stride	Explanation	Security property
Spoofing Identity	Someone uses else’s password and authenticate as if he the owner.	Authentication
Tampering with Data	Like: modification on data (delete, write, Etc)	Integrity
Repudiation	Users can refuse complete an action.	Non-repudiation
Information Disclosure	Reading or access to the data without permission.	Confidentiality
Denial of Service	The system shut down or not available to use	Availability
Elevation of Privilege	User get obtains a higher level of privilege than that for which he has been authorized.	Authentication

- **Ransomware attacks:** A malicious program that sets restrictions for accessing the computer system that hit by it, and requests a ransom paid to the program maker in order that the legal user can be accessing his files again. Some types of it encrypt the files on the system's hard drive and display a message asking the user to pay for their information. In the worst scenario, it may lead to someone's death. As what happened on September 11, when a German woman went to the University Hospital in Düsseldorf, in Germany, due to a disease threatening her life, which requires her to be treated as soon as possible. The medical staffs were surprised that all hospital data have been encrypted by ransomware, which requires one of three things: As for work to decrypt files that may take days and months, and this process may not succeed, it was excluded. Or the network is completely isolated and backup copies are restored, but this also, may take days for things to return to normal, which made the hospital exclude this solution. The last solution remains, but it is the fastest and costly, which is to negotiate with the attackers and pay the ransom in order to decrypt the files, and this is what the authorities resorted to. The patient was transferred to another hospital but she died on the way [16].

4. Literature review

PAPER 1: Soumya.T.R and S. Revathy [5] In their survey they discussed about similar threats to networks and the proposed solutions to protect the networks from such threats. They classified the data as Structured, Semi-Structured, and Unstructured (That is what the big data deals with it). They have mentioned that Big data based on (size, speed, and type sources of data), then they talked about threats in a social network which is also called cyber threats. They classified threats and the solutions as shown below in Table [2].

Table 2. Classification Threats and Solutions [2].

Category	Name of the threats	The suggested solutions
1. **Classic**	**Phishing attack**	1- Be careful from spams 2- Use only trusted websites and application 3- Use firewall and spam filters
	Spamming	1- Use of captcha and bot unfriendly question 2- Block unwelcome account 3- Stop the auto-follow
	Stalking	1- Profile privacy and stop showing location 2- Avoid from the stranger users and report about them
2. **Modern**	**Fake profile attack**	1- Social account audit and analyze the red flag words
	Location leakage attack	1- Disable geo tagging and no public sharing 2- Put your profile on privacy mode
	Account compromise attack	1- Using tools to detect the spam and phishing 2- Identify spam emails
3. **Other kinds**	**Click jacking**	**The solutions are the same of phishing attack**
	Cross site scripting	1- Be aware from pop ups risk 2- Use firewall and spam filters
	Malicious applications	**The solutions are the same of cross site scripting**

PAPER 2: Kanika S. et al. [17] In their paper they focused on the perspective of users of social media about privacy. A lot of people used social media either for personal use or for professional use. According to the privacy and trust model look in Fig.3, Trust is the main factor people based on it posting their information. In their literature review, they mentioned a bunch of privacy concerns such as (personal information identity steal, phishing scams, single access sign-on, etc.). It was one of the reasons to quit social media. And they talk about different attacks on social media (like active and passive attacks). Also, they mentioned the positive side of social media (for example social media providing a mechanism to connect the world and we can't forget E-commerce that makes our lives easier). In the past years, social networking means a lot to the young generation because of the feeling that they are doing a marvelous job. More followers to their accounts, it is means the world to them. But of course, they do not understand the threat, by doing all of this they are losing their privacy and confidentiality. After that, they defined privacy according to the relation between privacy and social networking, (the data of the user is not secure). There are many types of risks users may fall victim to it such as:

- **Identity Robbery**: steal personal information such as (name, date of birth, age..etc.)
- **Sexual Crimes:** Young kids who use those websites get attacked exposed by some kind of sexual hunters and they try to locate the victim's location.
- **Spam Advertising:** commercial advertisements are widely used by companies. Besides that, they may use our information to improve target their communication.

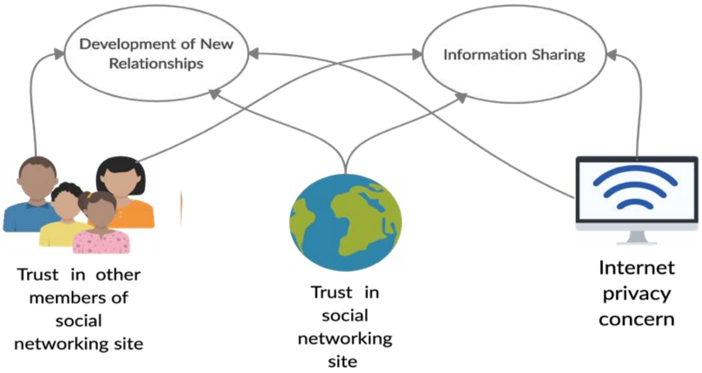
Development of New Relationships
Information Sharing
Trust in other members of social networking site
Trust in social networking site
Internet privacy concern

Fig.3. The privacy and trust model [8].

PAPER 3: S. Kumar and V. Somani [18] In their research paper, They are focused on the threats of social networks and developed measures to protect user identification on the internet. They split up social network structure to users where they are linked by one particular sort of interdependency. firstly, Social networking destinations as (Facebook, WhatsApp, Instagram, Twitter, etc). Secondly Social media locales as (YouTube, Flickr, Digg, and so more). according to social structure, followers dragging a huge number of users who speak to potential victims, to start Phishes and scammers they are sending risky messages to victims. Also, they division the Cyber threats that the users may face into:

- **Privacy Related Threats:** It is related to the user's personal information (Id, birth dates, phone numbers) where should not appear on the user page so hackers can't use it in social designing strategies.
- **Traditional Networks Threats:** Since social networks include a lot of user information and store it. It becomes a target for spammers, phishing, and malevolent assaults.

Usually, security issues are two: one is individuals security the other is personal computer security to protect the information and the data that they stored it in their systems. And they found that the most threats happened because of:

- Users are not worried about the importance of personal information.
- Users aware of the threats but they pick the wrong protection setting.
- Shortage in instruments or correct authentication system to deal with or manage security.

As they mentioned before the factors that reason threats, they set the following procedures for circumventing threats related with the social site:

- Building knowledge about the risk of information divulgence.
- The governments need to offer instructive classes about security issues.
- Empowering control and authentication that must be exceptionally solid.
- Using the antivirus tools and they should keep the default setting
- Providing unique security tools that Allow clients to evacuate their records and control privacy.
- Modifying the existing enactment

And for safety, they supply some essential suggestions such as: chosen an exceptionally strong password, changing it frequently, read privacy policies, no trust over the internet, provide less personal information to any website, and do not give it to anyone.

PAPER 4: Twinkle A., Monika S., and Sunil K.[19]. In their paper, they proposed and proved the effectiveness of the Random Forest algorithm. Random Forest Algorithm uses in the classification process tree (more than one) where each tree brings out one classifier Which is it by turn vote to decide who gets the most vote then it used for describing the datasets. For their model they use NLTK Library and the Wordnet as sub-library where words such as on, of, and, etc. was the most important for the calculation of specific phrase. The implementations were based on some factors as Age, Gender, Hashtags Etc. Also, the implementations were divided in their paper into three major modules first of all the data have been collected from social media (Facebook and Twitter) by using their APIs, then they cleaned the data by removed unnecessary data finally classification module according to the training data set. they performed their experiments in Waikato Environment for Knowledge Analysis (WEKA). According to their results where above 81% efficiency and the precision factors got 0.80. They recommended using the Random forest algorithm.

PAPER 5: Mamoona H. and others [20]. The main goal of their paper is to identify and analyze common cyber security vulnerabilities. Where they covered 78 studies from 2007 (where most cybercrimes were reported in 2007 and later) - 2018 to achieve a systematic mapping study. Also, in their mapping study, they found that the most cyber security Vulnerabilities repeated on:

- **Denial-of-service (Dos):** It was ranked first by (37%)
- **Malware**: Where took (21%).
- **Phishing:** (9%)

And they figured out the main victims either namely organizations (95%) or individuals (11%)
they organized the applications that were key targets of cybercrimes into: -

- **Infrastructure:** Such as Social media, Mobile applications, Application servers, and so on.
- **Applications:** Like Banking, E-commerce, etc.
- **Organizations/agencies:** DARPA (Defense Advanced Research Projects Agency), Aircraft attitude sensors.

And they mentioned some popular techniques used to protect or to mitigate attacks are the intrusion detection system and firewalls where the most use followed by traffic analysis, finally was anti phishing and signature-based techniques. In the end, they concluded that organizations where target more than individuals. Notwithstanding, individuals were the goal of phishing attacks as a result that there is a serious need to increase cyber awareness. And there are no standard measure techniques that may use by everyone (organizations or individuals).

5. Protecting from attack and vulnerabilities

Now we know, no matter how hard we try to detect or solve threats, there may be some threats that we don't know about it or maybe impossible to solve it. So, from our opinion, the first protection key is Reducing the personal information that we publish on social media. Also, there are some of the guidelines that we need to walk on it:

- Access control is an important part of security. Weak access control leads to Intruders' unauthorized access. It is important for companies to legalize the Access, Monitor the employee activities within the company, and keep a record of its operations.
- Using a strong password and change it frequently, a mix of uppercase and lower case letters, numbers, and symbols. Also, always reset all default passwords.
- Keep your Operating system (OS), application, anti-virus software, computer /phone, and programs always Updated. When a new version is released usually it fixes some security vulnerabilities of the previous version.
- Install Network Protection such as (firewall, Avast, Kaspersky, and so on).
- Ensure that people or employees understand the importance of data protection. Because the negligence and recklessness of one of them may lead to the wasting of all the exerted efforts.

6. Results

Since the attacks target either individuals or companies, we Note that data protection is everyone’s responsibility, so we have distributed it according to their roles:

- **The role of the individual:** Staying away from suspicious sites and set up the firewall and anti-virus programs. Also, they must try to reduce the dissemination of his information on social media.
- **The role of the family:** It is should for the families who notice that their children are attached to social media, remind them of important protection strategy, and to educate them about them. such as (no posting for personal information, don't share location with other users, no real friendship on social media, no connect with strangers, and finally Ask for help from your parents when you got in a trouble)
- **The role of the school:** Giving educational classes about protection over the internet to increase awareness for the students and to ensure that they understand the importance of security protection for our information. Also, schools might set up a consulting office so the students can inquire or consult about any problem that they face.
- **The role of governments:** Governments need to stop tolerating companies about information security and take strict measures Where it should be enacted laws and set up the minimum level of protection that companies, websites, or applications must abide by. If the default is done by them, they will be fined.
- **The role of companies and owners of social media sites:** Appointing their own security team and permanent monitoring. Set security and protection as one of the basic and important things when creating a site or company, not secondary. Because it affects credibility and reliability for the users.
- **The role of developers and programmers:** They should develop their own algorithms that help in raising the protection on the websites, such as (Random Forest Algorithm).

7. Conclusion

At the end of this research paper, we have concluded that it is impossible for programmers and manufacturers to discover and solve all security threats in their websites, applications, and systems. Because of many reasons we mentioned it before as threats are renewable, or not solvable in some cases...etc. We also discussed some solutions that may reduce the harm and help us protect ourselves, such as random forest algorithm that the manufacturers may use it in their websites also the traditional tools for security protection such as firewall, spam filters, and Install network protection as Kaspersky, Avast and so on. Also, we clarified everyone's role is to protect our information. We will repeat this one more time, the first protection line is to reduce or refrain from the dissemination of our personal information on social media and do not trust others.

References:

1. Group, T.T.W., The treacherous 12: cloud computing top threats in 2016. Cloud Security Alliance.
2. What is big data? [cited 2020 6 November]; Available from: <https://www.oracle.com/big-data/what-is-big-data.html>
3. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
4. Samra, H.E., et al., A Conceptual Model for Cloud-Based E-Training in Nursing Education, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 295-310.
5. Revathy, S.T.R.a.S., Survey on Threats in Online Social Media, in International Conference on Communication and Signal Processing 2018, IEEE: India.
6. Hell, M. What is a security threat? 2019 [cited 2020 6 November]; Available from: <https://debricked.com/blog/2019/05/29/what-is-a-security-threat/>.
7. Al-Hamami, A.H. and G.M.W. Al-Saadoon, Security Concepts, Developments, and Future Trends, in Handbook of Research on Threat Detection and Countermeasures in Network Security, IGI Global. p. 1-16.
8. Altwairqi, A.F., et al., Four Most Famous Cyber Attacks for Financial Gains. International Journal of Engineering and Advanced Technology, 2019. **9**(2).
9. Alshambri, H., et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 2020. **8**(1).
10. Masud, M. and Hossain, M. S., Secure data-exchange protocol in a cloud-based collaborative health care environment. Multimedia Tools and Applications, vol. 77, no. 9, pp. 11121-11135, 2018.
11. Faragallah, O.S., et al., Efficiently Encrypting Color Images with Few Details based on RC6 and Different Operation Modes for Cybersecurity Applications. IEEE Access, 2020. **8**(1).
12. AlZain, M.A., et al., Managing Multi-Cloud Data Dependability Faults, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 207-221.
13. Crane, C. The Top 9 Cyber Security Threats That Will Ruin Your Day. 2019 [cited 2020 14,november]; Available from: https://www.thesslstore.com/blog/the-top-9-cyber-security-threats-that-will-ruin-your-day/.
14. B. Hamid, N. Jhanjhi, M. Humayun, A. Khan and A. Alsayat, "Cyber Security Issues and Challenges for Smart Cities: A survey," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-7, doi: 10.1109/MACS48846.2019.9024768.
15. Up to 400 million accounts in Adult Friend Finder breach, in BBC. 2016.
16. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1.
17. Kanika Sharma , S.G., Preeti Gupta and Prince Arora, Use's perception on social media privacy concern, in 2018 4th International Conference on Computing Sciences. 2018, IEEE.
18. Somani, S.K.a.V., Social Media Security Risks, Cyber Threats And Risks Prevention and Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 2018. **4**(4): p. 125-129.
19. Twinkle Arora , M.S.a.S.K.K., Detection of Cyber Crime on Social Media using Random Forest Algorithm, in 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC). 2019, IEEE: India.
20. Mamoona Humayun, M.N., NZ Jhanjhi and sajjad Mahmood, Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 2020.