

Article

The Development of a Secure Online System to Protect Social Networking Platforms from Security Attacks

Basil Alothman ^{1,*}, Omar Alibrahim ², Nourah Alenezi ¹, Abrar Alhashemi ¹, Maryam Alhashemi ¹, Dalal Almardasi ¹, Omar Khattab ¹, Chibli Joumaa ¹ and Murad Khan ¹

¹ Department of Computer Science and Engineering, Kuwait College of Science and Technology, Kuwait City 35001, Kuwait

² Information Science Department, Kuwait University, Kuwait City 12037, Kuwait

* Correspondence: b.alothman@kcst.edu.kw

Abstract: Due to the rapid advancement of social media, a huge amount of data is generated daily. Due to this great spread and expansion of the data at the social or professional level, the risks of securing the information become a challenging job. In this regard, we conducted an in-depth interview to gather specific information about how infected users may be provided with information about recovering their hacked social networking accounts. Further, we have introduced a complete solution to help social network users to improve the idea of using different applications from one appropriate platform. In order to build this secure platform for accessing the security applications such as bank accounts, etc., we set various security methods to access social network websites, such as sending an OTP to their respective mobile devices, email or by fingerprint. Further, we also added a camera to identify the wrong or fake registration process of an intruder. The camera captures an image of the intruder registering to a social network website using the legitimate user's information. In addition, the application also has a solution for forgetting the password or security questions that are sent to the user via email. Finally, the application saves the password, which can be recovered when the user forgets it.

Keywords: social networks; social media; cyber security; network security; authentication



Citation: Alothman, B.; Alibrahim, O.; Alenezi, N.; Alhashemi, A.; Alhashemi, M.; Almardasi, D.; Khattab, O.; Joumaa, C.; Khan, M. The Development of a Secure Online System to Protect Social Networking Platforms from Security Attacks. *Appl. Sci.* **2023**, *13*, 11731. <https://doi.org/10.3390/app132111731>

Academic Editors: Christos Bouras, Hazra Imran, Aman Singh, Basit Qureshi, Yasir Javed and Omar Cheikhrouhou

Received: 11 September 2023
Revised: 30 September 2023
Accepted: 23 October 2023
Published: 26 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Social media users have increased significantly in the past few years. In fact, in 2017, the number of social media users reached 2.5 billion people around the world. Within two years, this number jumped to 3.5 billion. This is equivalent to a 29% increase and 45% of the world's population. However, many people do not understand the significance of these numbers and their impact on the security and privacy of social media, especially when user education becomes pivotal to overcoming data theft, privacy, and fraud risks. For example, the problem of identity theft, i.e., intentional and unauthorized use of a person's identification information, has massively increased on social media. Nearly 10% of adults in the United States experienced encrypted identity theft in 2016, up from 7% in 2012, and consumer agencies have seen registered complaints about identity theft nearly quintuple since 2001 [1].

Given these problems, in this paper, we propose a security system that adopts an intrusion detection system (IDS) on computers and mobile devices to detect suspicious activities and unauthorized access when logging in to social media accounts. This system is a real-time monitor or a personal mobile security system that closely monitors your online accounts, constantly looking for various indicators of unauthorized access. For example, suppose a hacker attempts to hijack an account. In that case, the system notifies the owner with an alert message, allowing them to regain control of their accounts to minimize the likelihood of a successful intrusion. Previous research has emerged urging awareness

and showing the extent of risks. For example, Digital-PASS [2] is a simulation utilizing gasification to expose users to realistic privacy threats in a safe, controlled environment, teaching them to exercise security and privacy pragmatism in their own social media usage. The system relies on the use of role reversal.

The rest of the paper is organized as follows: Section 2 presents related works preceded by the problem statement in Section 3. The proposed design of the system is presented in Section 4. Implementation and testing are depicted in Section 4.2, followed by the results and discussions in Section 5. Finally, the conclusion is presented in Section 6.

2. Related Works

In this part, we will deal with all the papers and resources related to our paper that will help us know more data about a study that revolves around the threat of hackers and how to protect and secure devices. However, our focus will mainly revolve around social networking sites and how we can protect applications from breaching privacy. In this regard, we studied several articles and presented their studies in the following paragraphs.

A study focused on researching the increase in the use of smartphones has widely spread in South Africa and has become a part of users' lives [3]. The authors claimed that the percentage of smartphone users in 2018 reached 51%. However, many users do not know how to secure their devices. A small percentage among them are those who know about cyber security, and most of them are from the male category. However, females are more vulnerable to electronic attacks compared to the male category. Similarly, the research urges young people in schools to be taught how to protect themselves and integrate a curriculum on the internet and its dangers as the attacks on it increase yearly. Further, the authors explained in detail how the hackers target small companies with home computers and Internet of Things (IoT) devices [3].

The risks of security increase for institutions and individuals, and the greater focus is on individuals. Especially social media users, are mostly unaware of the importance of information security. In addition, it negatively affects the companies where users with limited cybersecurity knowledge mainly operate the workstations. Therefore, training workshops and hands-on practices related to information and cyber security are required to reduce the number of attacks on social media platform [4]. In similar research to [4], the authors of [5] show that the number of social media users may rise to 5 billion by 2020. Further, they explained that mobile phones are becoming integral to people's lives. Similarly, many users, specifically children, download applications and games without checking their level of security. This application increases the risk of data theft, and the ads running in the applications often lead to suspicious websites and malicious programs. The authors performed a survey by asking many affected users about information security, and many of them were unaware of it. Even after explaining the security concerns related to malicious programs and their dangers to the data, around 27% of the users still became victims of the same attacks [5].

Research led by authors from Israel Aerospace Industries shows how important cyber security risks are and how to prevent them. The authors suggested that it is recommended to focus first on users from the beginning of primary school, as they are vulnerable to these dangers in playing interactive video games. Further, it is essential to make technology serve us in preserving our privacy, and monitor any attacks on institutions or individuals. According to the authors, around 31% want to communicate with new people, but the user is unaware of the security risks of the means intruders have of stealing information or fraud. As people may unintentionally share information about themselves, they are unaware of the long-term severity and spear, phishing, and social engineering types of the cyber-attack [6].

Advanced technology such as the cloud, artificial intelligence, and many others have become revolutionary in the last decade. However, these technologies may pose a danger and be more harmful than their benefits. Therefore, the users of these technologies must be aware of the most important skills that protect them from risks and attacks. Similarly,

digital competency is increasing every day between technological giants. However, many of these technological giants consider the users to already be aware of information security. However, it is not true that every user knows the importance of information and cyber security. According to the study in this research, most virus attacks affect users aged 18 to 24 years old [7].

Due to the lack of knowledge regarding securing the electronic world, recently, a huge increase in the problems and crimes is noted. Therefore, the countries of the world must devise the most appropriate solutions before escalating crimes in the future. In recent research, the authors Ahmad et al. presented a questionnaire for the country of Bangladesh to analyze the problems stemming from the digital world, and it was discovered that 77% of people were exposed to crimes and became victims of Internet fraud, and 62% have been blackmailed [8]. In similar research presented in [9], a chart-based system is designed to counter cybercrimes. The proposed method illustrates the tricks used by fraudsters. Similarly, the system contains many advantages, such as a list of famous names for fraud that has been drawn up, and malware has been identified for people to avoid. Further, different mechanisms have been put in place that detect cyber security threats, and others that determine whether the sites on the internet are valid or not. Finally, this research aims to raise awareness among people to avoid being victims.

Social engineering is a technique to divert people's minds, deceive them, and manipulate their data. Similarly, phishing is one of the types of social engineering that targets a particular group to control their information, i.e., deceive people through communication by phone [10]. The research used a questionnaire to analyze people's awareness levels. It was found that people have experience and a high level to confront the attacks used by fraudsters and information thieves [11]. Similar research was conducted in [12], where the authors presented the severity of a cyber threat. The authors explained that cyber threats are one of the biggest problems countries and individuals have suffered recently. In addition, they affect many areas, making them more vulnerable to danger and differ in their methods. They may be theft or extortion, or bank breaches that affect the world as a whole and not only the individual, which compels us to protect networks from intrusions. Finally, the paper's author aims to create a game to analyze the level of interconnection between fraudsters and gamers.

The internet has become important worldwide from an economic, social, and commercial standpoint. However, several social media platforms have emerged, which can lead to significant losses through security breaches and the infiltration of personal information. Secret threats are unauthorized access to the network. There are many attacks, privacy and security problems in social media, and easy access to a person's information by attackers [13]. Similarly, we cannot underestimate the importance of social networking sites in social development. Still, an understanding is needed regarding privacy and creating protection for the user's data, because most people do not have sufficient information on the issue of privacy and threats to security and bank accounts through social media. Privacy can be protected by increasing confidence in social network developers, as stated in [14]. There are some factors affecting users' capability to identify and mitigate threats, which have been described as business environmental, societal, political, legislative or constitutional, organizational, economic, and personal. In addition, various challenges involving both traditional and digital tools have been evaluated to indicate the need to profile high-risk workers and to establish preparation systems for all levels of an organization to ensure the failure of hackers [15].

Employees' inability to comply with information systems security protocols is a severe threat to IT security administrators. Workers have been justifying the activity of IT security policy breaches through the neutralization concept, which offers them a logical explanation and provides a new perspective on how they can explain such actions [16]. Similarly, information security is becoming more important, as organizations are increasingly exposed to risk because the executives can evaluate the organization using a holistic approach and can ensure that new systems and procedures are implemented in a timely manner.

However, there is a gap in the relationship between the managers and the information security strategy. The gap may be closed by exploring how managers perceive the security of their organizations and the factors that influence their decisions about developing an information security strategy [17].

Many children and adolescents use social media networks and are not aware of the security risks present in these networks. For instance, identity theft, intrusion of personal information, or cyberbullying may lead to suicide and similar problems. The social networking platform Facebook has 1.23 billion active users. Facebook provides several solutions to protect their users' privacy, such as phishing protectors, etc. Similarly, the McAfee social protection platform has an advantage in protecting users from downloading other people's photos from social networking platforms [18]. In addition, Facebook is popular with billions of users, but with its spread, there is a lack of awareness of the dangers around it. For example, many users share their personal data without being aware that many misuse the internet and cause harm to people. Similarly, most users do not read Facebook's terms that give them a certain degree of control over their data. Finally, using a social networking platform, a user should be fully aware of all the risks associated with it [19]. Many Facebook users are adolescents between the ages of 16–19 years. However, most believe the application will not abuse their data. However, third-party malicious software and spyware exploit their information [20].

Most social media programs, including Twitter, are preparing to counter cyber-attacks through a particular organization. This organization determines security-related information [21]. In the research presented in [22], the authors aim to anticipate possible attacks on Twitter in the future due to the lack of required security solutions. These solutions work in a sophisticated way to avoid attacks in the future. Since the internet's advent and the world's development, social media programs have evolved significantly. For example, the Twitter social network accounts work on exchanging tweets, making electronic friendships, and others. Because of the ease of re-tweeting, it makes it easier for criminals to seize information. Research work to discover harmful information and thus alerts users about any malicious tweet, cyber security problems, or attacks targeting personal accounts is presented in [23]. According to this research, online network invasion has been an ongoing sinister act that brought inconvenience worldwide. Culprits involved are untraceable unless with the use of social network protocol tools. State measures put in place also regulate network violations. The existence of the node and the edges has regulated the theft of online private data. Similarly, the monopartite analysis captures vital hackers and their tools more than the bipartite analysis. Further, eliminating hackers will involve establishing active network customized measures, which will hasten malicious detection and network invulnerability [24].

Computer hacking entails changing systems content without the developer's permission to break through computer security and access documents. Generally, breaking into a computer requires two hundred and six key codes to pass the information using permutation and combination. Similarly, the password-hacking algorithm uses twenty-six alphabetic letters in a small or large case and ten digits followed by a unique character. To prevent hacking, an operator must present an ID and a PIN to use the account when accessing the system [25], resulting in increasing the security of a computer system. In this regard, malevolent cyphers are written and kept secretly in android applications within personal computers and phones. These cyphers help the users in enhancing the security of the smart phone devices.

Similarly, jurisdiction laws are enacted to protect personal data from being breached. The android is made up of four operations, which the Trojan horse compromises. It is written in Java programming language and made to run by customizing the software development kit. Also, avoiding installing content from unsecured sites, and downloading and updating newer antivirus applications is the best protection method. Applications that do not request 'allow' should not be installed before verifying their security [26]. In addition, Java house three-dimensional coding tools were launched for protrusion tests

among users. Specific post-clarification measures are set to manage diversity from network users and sites, enhancing the extent of network vulnerability amongst active users while setting and giving guidelines on network accessibility. Identifying users and their roles on different sites and their activities helps monitor their contribution to cyber security [27].

3. Problem Statement

One of the main problems of social networks is that their users are always exposed to various types of security threats such as phishing, malware, security breaches, and other internet risks. Also, social networks have facilitated access to all information and data from different forms and locations. Therein lies the risk that this network information can come with. They result in making us vulnerable to the risks, threats, and attacks in cyberspace. In recent decades, the security threats and attacks on various Gulf countries have increased exponentially. For example, during a cyber-attack in Saudi Arabia, a virus crippled tens of thousands of computers at Saudi Aramco, the kingdom's oil giant, by wiping their disks. There was also a cyber-attack on the Kuwaiti Ministry of Interior website about one year ago, where the hacker entered the site as a regular user, and then spread irrelevant information such as advertisements of various websites, displaying dance and singing videos, etc. In order to secure multiple government and non-government organization in the State of Kuwait, we present a solution for securing social media from fraud, extortion, kidnapping, and abuse of information. There are tricks by which third parties, like hackers, can obtain private information and use it for illegal purposes, which endangers the personal security of individuals. This paper aims to educate users because people are not fully aware of the importance of the information they disclose on social networks. Similarly, social network users often disclose more information than they should due to the need to communicate with others. Therefore, we need a security solution that protects them from hackers because the media applications for smartphones do not have the necessary measures to protect the user's private information.

4. Proposed Design

4.1. Overview of the Proposed System

Cyber-attacks have increased on the internet, and the number of hackers has increased recently. In this regard, we proposed a solution which protects the user from cyber-attacks. The proposed system uses a system to recognize a benign user from a hacker. The user's data is saved in the database, and only technical support can access it. A social network user can turn on its location. However, it entirely depends on the user's choice of protection. The proposed system uses a camera, which takes a picture of the user if the user entered a password incorrectly for the first time. Similarly, the integrated system sends an email to an actual user. Suppose the system is accessed by someone else. In that case, the existing user can perform necessary action to countermeasure the attack by disconnecting the internet, logging out from social networking websites, etc. The overview of the proposed system is shown in the following Figure 1.

The proposed system is used to serve users of social networking platforms and provide them with the necessary security using multiple ways. As shown in Figure 1, the user fills in their data, chooses the type of protection, and finally stores it in the secure database for future use. As soon as the user saves their data, the proposed system sends a message to the user's email and informs it to choose a username and password for future login. In addition, the user can protect their communication with social networking platforms by entering their address in the proposed system. Similarly, the unauthorized user with incorrect credentials will be denied using the social networking platform. Finally, the system components are shown in Table 1.

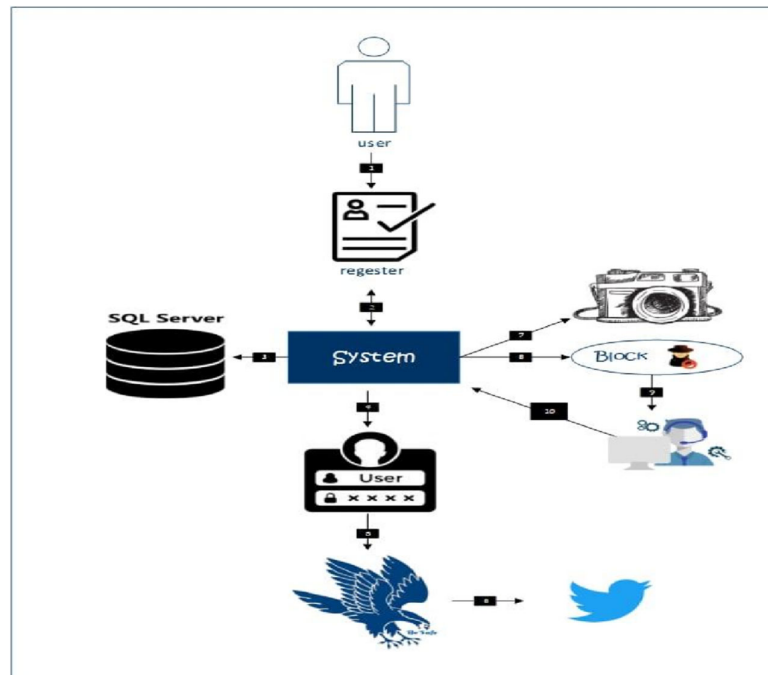


Figure 1. An overview of the proposed system.

Table 1. System components.

Component	Description
(1) User	The target users of this application are any user who uses social networking programs constantly and has an account. The proposed system provides services to all age groups, such as children, adolescents, youth, and the elderly.
(2) Log-in	There are two options to log in to the proposed system: (1) a user with existing account information can directly log in with the correct credentials, and (2) a new user will first register to use the services provided by the proposed system.
(3) Safety	The proposed system relies on protecting social media platforms from misuse. In this regard, the proposed approach provides many services, and the user must choose the program to be protected and the method that will be protected. However, in the case of misuse, the proposed system catches a picture of the hacker.
(4) Support	The proposed system sends various notifications to the support staff in case of misuse or wrong attempts at accessing the system.
(5) System	The system is considered a parent center as it prevents hackers from seizing personal accounts as much as possible.
(6) Database	The proposed system supports a database where the users' information is stored.

The working mechanism of the proposed system is illustrated in Figure 2.

1. Validate user compliance/authentication/validation: Once the user enters the correct username and password, the identifier generated from the username and password will match the identifier in the database. Otherwise, an incorrect message will be displayed to the user;
2. Choose the right social networks security: after successfully logging in to the system, the user is provided with a number of options to choose the correct social network to log in;
3. Alerting support or user: if the username or password does not match any identifier, a rejection message is displayed, and a warning message will be sent to the owner of the account;

4. Notify the user/support/admin: The system will send an alert to the user and technical support in the event of a breach. Technical support will contact the user to solve the problem.

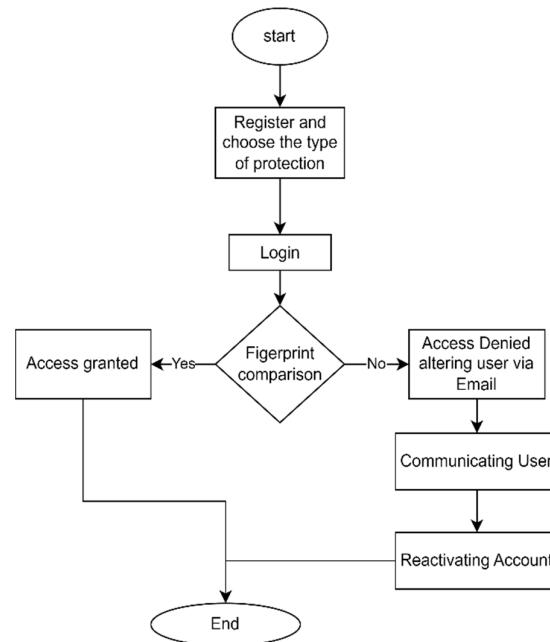


Figure 2. Flowchart diagram of the proposed system.

4.2. Implementation and Testing

In this section, we will explain in an in-depth and detailed way as to how to implement the proposed system. As shown in Figure 3, the user is provided with a number of options, such as an administration panel, links to social media pages, etc.

Figure 3. Registration page in the proposed system. “كلية الكويت للعلوم والتكنولوجيا” means “Kuwait College of Science and Technology” and “جامعة خاصة” means Private University.

The description of each of the tabs is explained in the following sections.

1. Main Information: a user puts his data, and the proposed system stores it in an integrated database;
 - a. First Name: given the name of the user;
 - b. Last Name: family name of the user;
 - c. Email: the email that the user sets to register on the sites;
 - d. Phone: user phone number;
 - e. Username: a unique name for each user;

- f. Password: A secret log-in detail that no one can see except the user. Password must have at least eight characters. In this way, we help user to create a strong password. Password must contain the following elements:
 - Uppercase letters (English, A through Z);
 - Lowercase letters (English, a through z);
 - Special characters (for example! \$, #, %);
 - Digits (0 through 9);
 - Do not use a space in a password;
 - The password must differ from the user's log-in name;
 - Confirm password: to confirm the user's password and prevent anyone who does not know the password from entering.
2. Social media selection: the user chooses the application he wants to protect, or a user can choose all six applications;
3. Authentication types: the way that the user wants to protect himself is chosen;
 - a. Email: A one-time passcode OTP code is sent via email;
 - Authentication button: a button used to confirm if the code is correct;
 - Resend button: a button to resend the code in case it did not arrive.
 - b. Question: A set of five questions will user answered at the time of registration. After the registration, the user will log in with two random questions;
 - c. Fingerprint: A previously registered fingerprint match is requested when the user is registered. When writing to a user, the system gives a unique identification ID to each user to register a fingerprint in the system.
4. Alert box: an explanation of authentication type;
5. Issues:
 - a. All the requirements must be met for registration;
 - b. The user is not allowed to register if the password is less than twelve digits, and the username is less than five characters.

A message will appear informing the user that he or she has registered successfully. Also, a message containing the username will be sent via email. After a user completes the registration process, the user can log in with the correct username and password. When he logs in, a list of applications that the user has selected will appear. For example, a user who selected four different applications is shown in Figure 4.

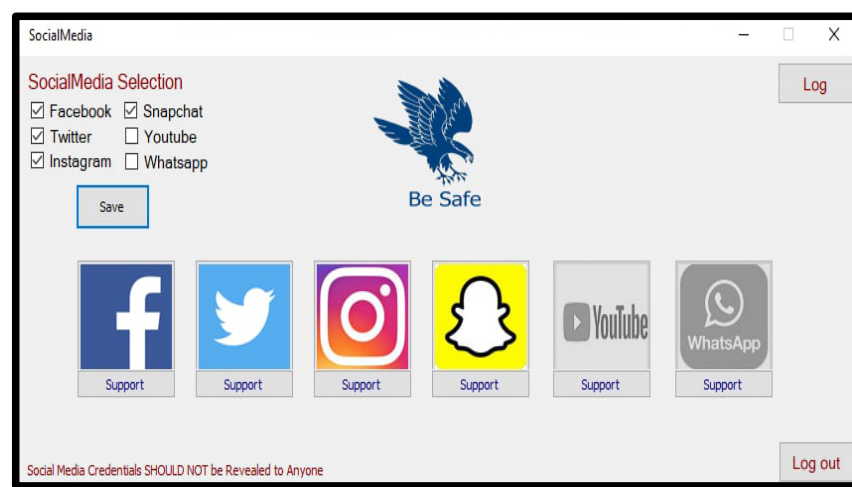


Figure 4. User page.

When a user clicks on the selected application, for example, Twitter, it moves to a page containing the username and password, as shown in Figure 5. The system also allows a user to remember the username and password for future use.

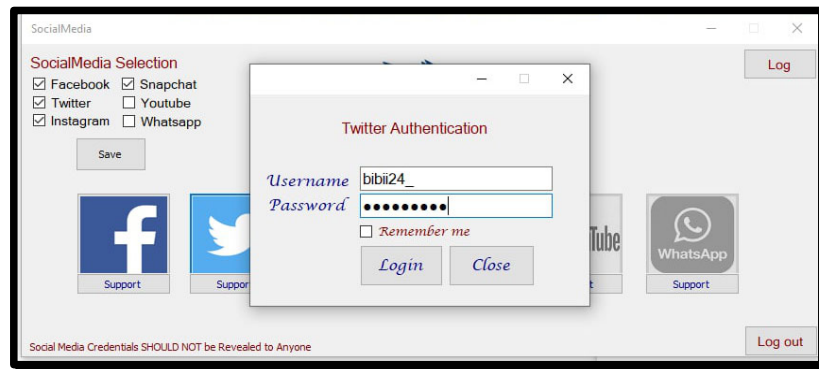


Figure 5. Twitter authentication.

As shown in Figures 6 and 7 support is provided to each user to retrieve their log-in credentials. This will help a user to retrieve the correct log-in information in case they forget it.

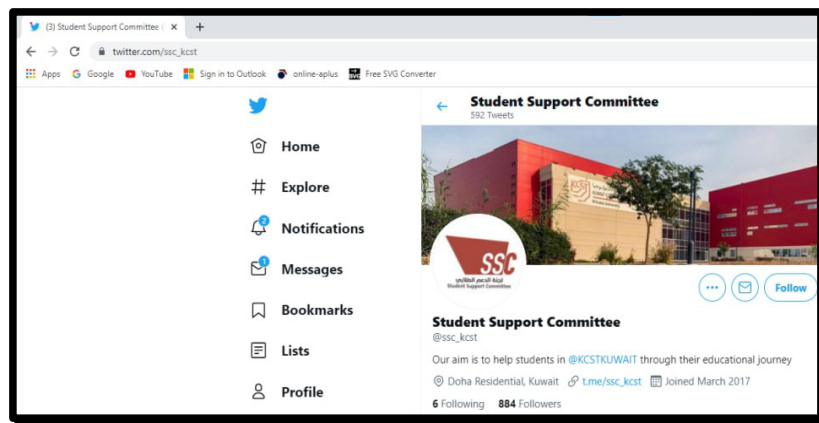


Figure 6. The Twitter page for the Support Committee.

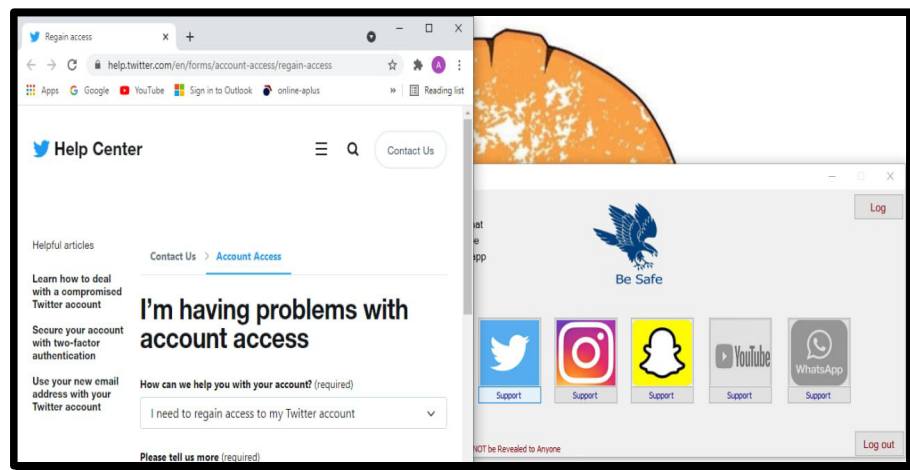


Figure 7. Twitter support.

When the user tries to log in with the wrong password, a message will be displayed. In addition, an email will be sent to the user that alerts the user that someone was trying to log in to their account. Further, the proposed scheme provides a unique option of storing the information related to each log-in attempt in a log file, as shown in Figure 8. This helps the user to identify any illegal attempt by the attacker.


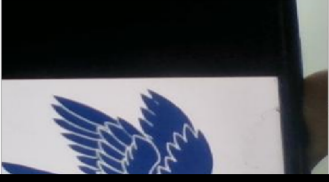
ID	UserName	Password	Image	LogDatetime
47	AAbrar_	asdfg		5/27/2021 12:3...
48	AAbrar_	ttttt		5/27/2021 12:4...

Figure 8. Activity log of the log-in attempts.

- ID: a unique number that the system sets for each user;
- User Name: the user name logged in with;
- Password: wrongly typed password;
- Image: the picture taken by the camera of the user who entered the wrong password;
- Log Date Time: the time that the user entered the wrong password.

Also, as shown in Figure 8, a log-out button is set to help the user to log out from the system safely. Finally, the fingerprint authentication is shown Figure 9 via the Arduino Uno.

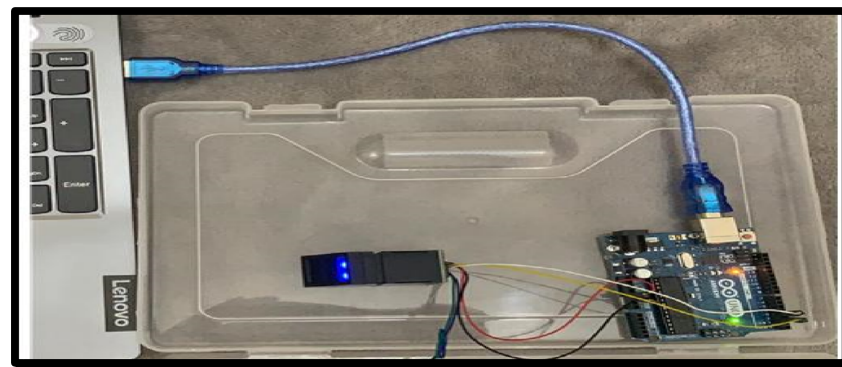


Figure 9. Fingerprint authentication via Arduino Uno.

5. Results and Discussion

In order to validate the proposed system, a survey was conducted with 21 participants of different ages and educational levels. In addition, in the survey, each user is asked a number of questions related to their experience while using the social networking platforms. For example, they are asked about the types of violations users were subjected to, where they were subjected, and whether or not they had sufficient experience.

Table 2 and Figure 10 show the distribution of the participant’s gender percentage as male and female, i.e., 42.90% are female, and 57.10% are male.

Table 2. Specifications on gender.

Responses	Standard Deviation	Female	Male	Gender
21	8.3666	12	9	All Data
		57.10%	42.90%	Percentage

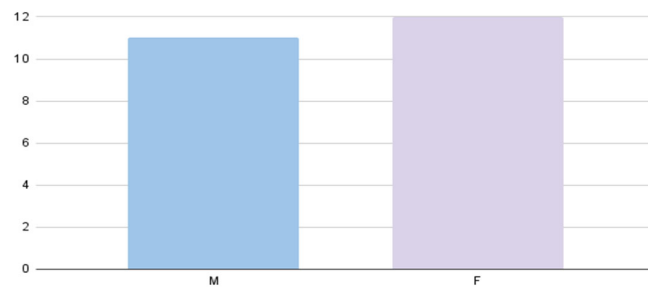


Figure 10. Count of gender.

Table 3 and Figure 11 show the age group participating in the questionnaire, where 76.20% of participants' ages range from 21 to 40. Similarly, Figure 12 shows the level of education among the participants, where the highest percentage are bachelor's degree holders.

Table 3. Specifications of age group.

Percentage	All Data	Age Group
0	0	14–20
76.20%	16	21–40
23.80%	5	over 40
	7.7781	Standard Deviation
	21	Responses

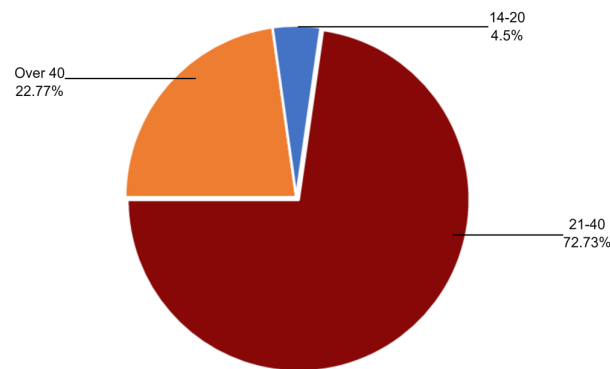


Figure 11. Count of age.

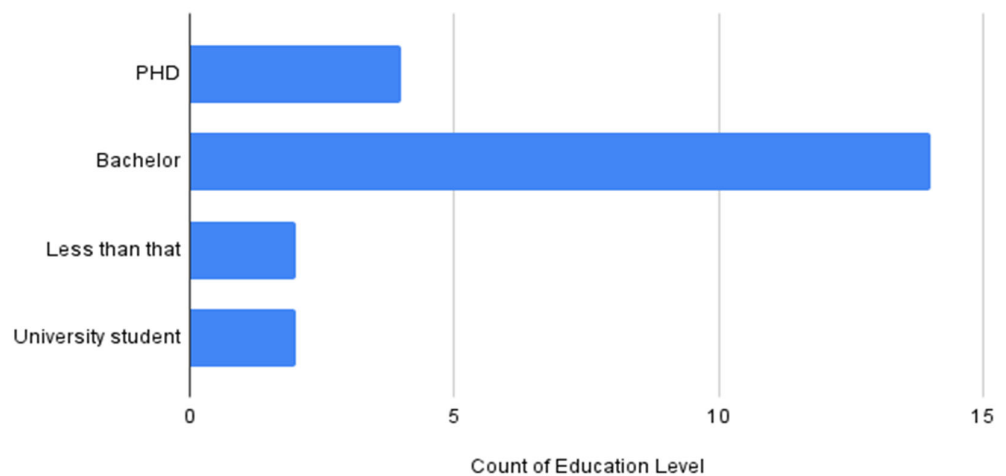


Figure 12. Count of educational level.

Table 4 and Figure 13 show that 61.9% of participants do not read and understand the security policies related to social media. Table 5 and Figure 14 show participants' responses about who encounter a problem of forgetting their password, which is 52.40%.

Table 4. Do you read and understand security policies related to social media?

Responses	Standard Deviation	Maybe	No	Yes	
21	6	1	13	7	All Data
		4.80%	61.90%	33.30%	Percentage

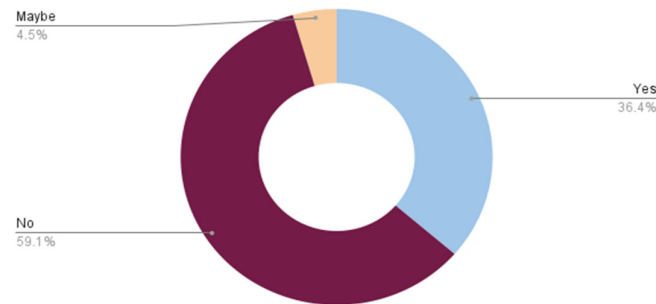


Figure 13. Security policies related to social media.

Table 5. Have you faced any issues like forgotten passwords?

Responses	Average	No	Yes	
21	10.5	10	11	All Data
		47.60%	52.40%	Percentage

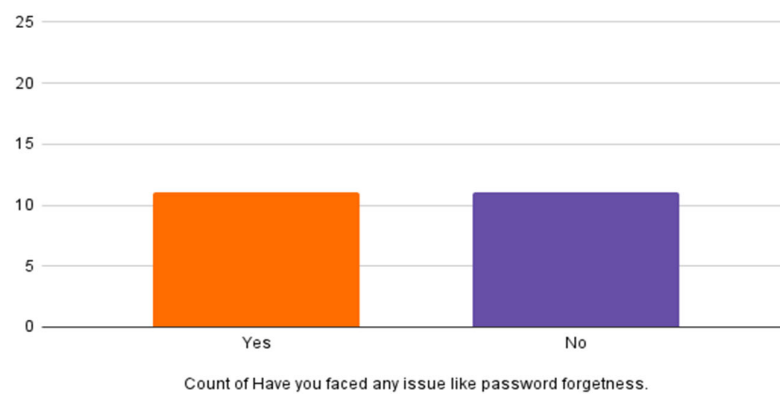


Figure 14. Forgotten passwords.

Table 6 and Figure 15 show how participants save their passwords: tablet, phone note, secret place, personal memory, or software. The majority of participants rely on phone notes and personal memory, 43.50% and 39.10%, respectively.

Table 6. How do you save your password?

Percentage	All Data	Conservation Place
4.30%	1	On my tablet
43.50%	8	Phone note
4.30%	1	Secret place
39.10%	9	In my mind
8.70%	2	Software to save it.

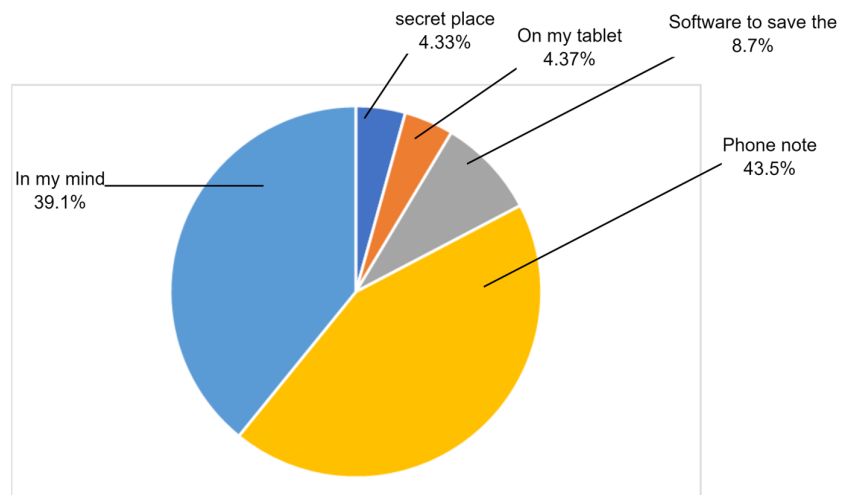


Figure 15. Saving passwords.

Table 7 and Figure 16 show how participants' accounts are hacked: 43.5% do not know how they are hacked and 34.8% are hacked with a link, and 13% via SMS. Table 8 and Figure 17 show whether participants use public networks such as those in cafes or airports, which is 47.8%.

Table 7. Specification on how participants' accounts were hacked.

Percentage	All Data	Account Hacked
43.50%	9	I do not know.
4.30%	1	From the card
34.80%	7	Link
13.00%	3	Form SMS
4.30%	1	From the password

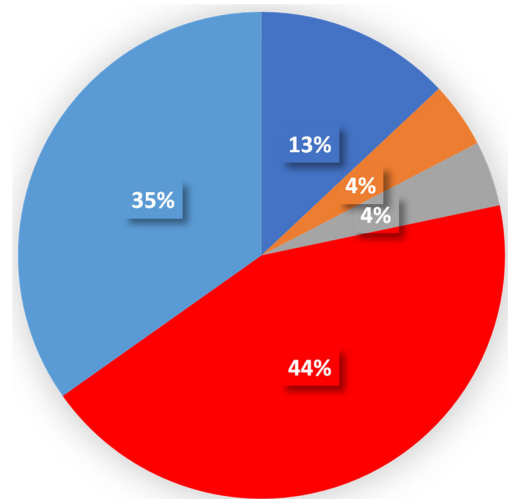


Figure 16. Hacked account.

Table 8. Specification on whether participants use public networks.

	Standard Deviation	No	Yes	
21	0.7071	11	10	All Data
		52.20%	47.80%	Percentage

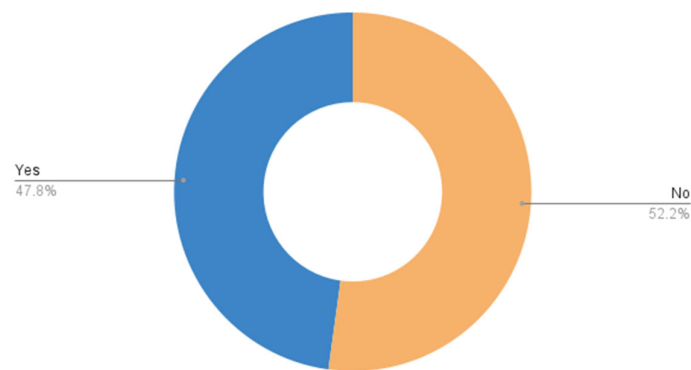


Figure 17. Public networks.

Table 9 and Figure 18 show whether participants deal with a program to achieve the level of protection through social media where the majority of them (78.30%) do not use it.

Table 9. Specifications on whether participants deal with a program to increase protection through social media.

Responses	Standard Deviation	No	Yes	All Data
21	7.7781	16	5	Percentage
		78.30%	21.70%	

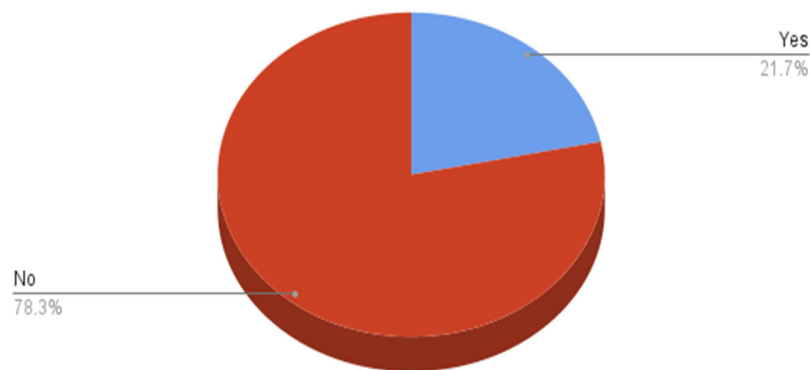


Figure 18. Level of protection.

Table 10 and Figure 19 show the last time participants changed their passwords.

Table 10. Specifications on when it was the last time participants changed their password.

Percentage	All Data	Specifications
30.40%	7	long time
43.50%	8	short period
26.10%	6	Recently
	21	Responses
	2.081665999	Standard Deviation

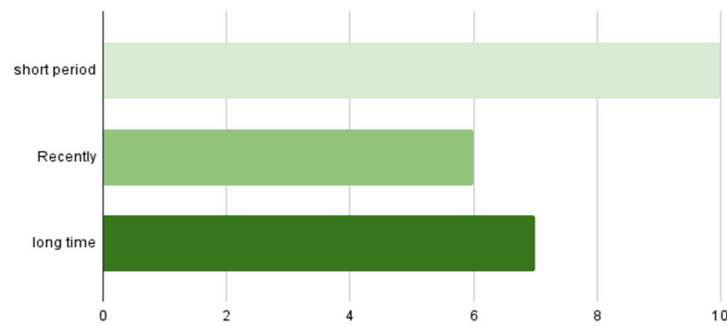


Figure 19. Changing passwords.

Table 11 and Figure 20 show how long per day participants use social media, where the majority of them spend 8–10 h.

Table 11. Specifications in how long per day social media is used.

Percentage	All Data	Social Media Time
29.20%	4	2–4 h
20.80%	5	5–7 h
33.35%	8	8–10 h
16.70%	4	more than 10 h
	5.25	Average
	21	Responses

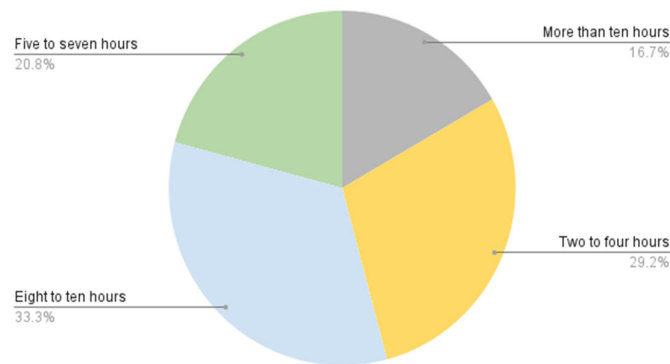


Figure 20. Social media usage per day.

Figure 21 shows the social media accounts that are hacked: Instagram comes first, followed by WhatsApp and email.

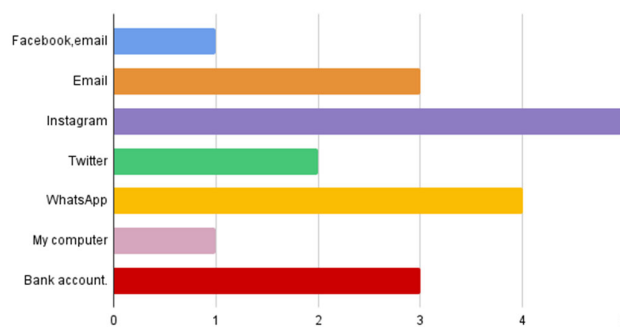


Figure 21. Hacked social networks.

Figure 22 shows that only 13% of the respondents report their cases to the Anti-Cyber Crime Department at the Ministry of the Interior in Kuwait.

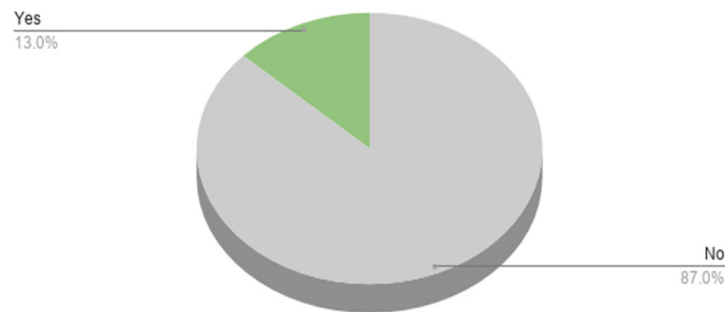


Figure 22. Reporting on hacks.

Figure 23 shows whether the participants use a complex password in terms of letters, numbers, and special characters. It is shown that the majority (50%) use the password of 8–16 character length.

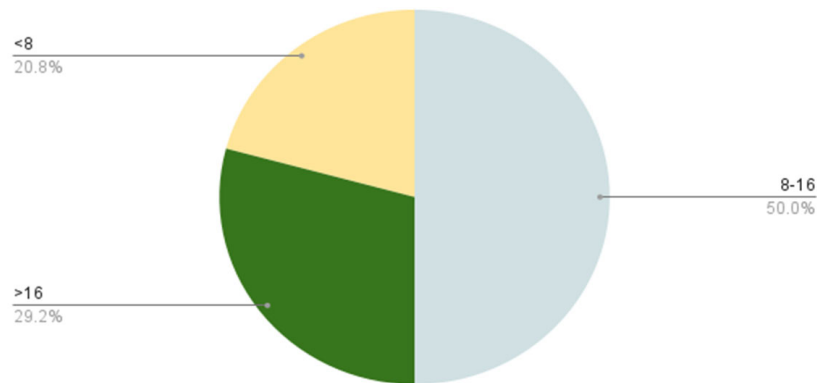


Figure 23. The complexity of passwords.

Figure 24 shows whether the participants are aware of recovering their accounts. The under curve area shown in green color depicted that the 43.5% do not know how to regain their accounts.

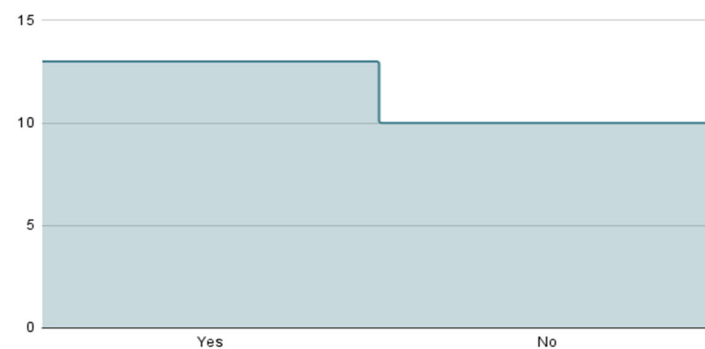


Figure 24. Recovering accounts.

Due to concerns about violations, 39.1% of participants cancelled their accounts to find a quick solution without searching for one that would protect them, as shown in Figure 25.

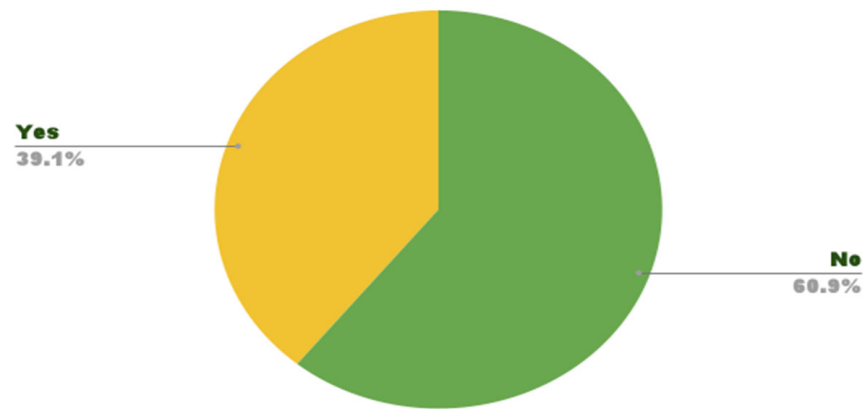


Figure 25. Account on social media.

After getting various types of information from the surveyed data, we offer the same participants use of the proposed system to protect their social media platforms. After a span of 6 months, we interviewed the same participants for the same questions. The results of the survey after implementing the system are shown in Figure 26. We can see that most of the participants are now satisfied, and they can use their social media platforms without any security concerns.

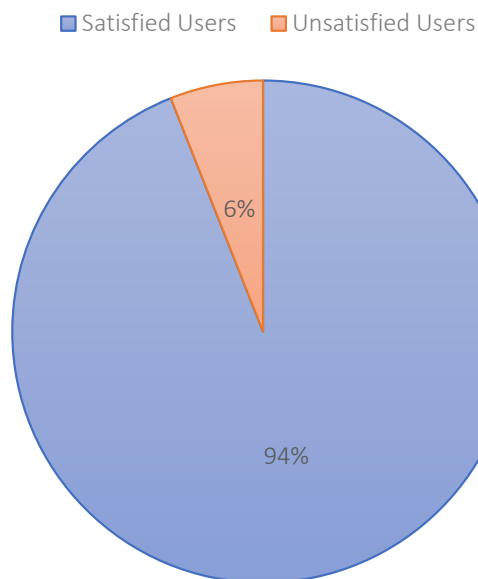


Figure 26. Satisfaction of the users while using the proposed system.

6. Conclusions

In this paper, we examined the risks of using social networking platforms. We also conducted research confirming that most users do not have sufficient knowledge of cyber security practices and how to cope with the issues associated with social networking websites. The current study's results demonstrated this knowledge's importance in keeping personally identifiable information secure. However, individual actions alone are insufficient. As cyber-criminals increasingly develop advanced and sophisticated attacks, social media platforms must be hardened against them. For this reason, in this paper, we have proposed a novel system that protects social media users to mitigate hacking risks. We have also proposed a system that reduces the problems of social media penetration when the user is authenticated. Specifically, we presented how to build the system from scratch and how the system is deployed to handle the issues related to social networking websites.

Author Contributions: B.A., O.A., C.J., O.K. and M.K. conducted the research into the academic landscape and drafted and supervised the research. N.A., A.A. and D.A. created the flowchart implementation design, and general survey while A.A., M.A., D.A. and N.A. performed the survey on different participants. N.A. and M.A. works on implementation and B.A., O.A., C.J., O.K. and M.K. prepare the initial draft of the paper and evaluated the survey results while the paper was written jointly by all the authors. All authors have read and agreed to the published version of the manuscript.

Funding: We deeply acknowledge Kuwait College of Science and Technology for supporting and providing a research environment to conduct this study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. David, B.; Marguerite, D.; Lynn, L. Risk and protective factors of identity theft victimization in the United States. *Prev. Med. Rep.* **2020**, *17*, 101058.
2. Kambiz, G.; Sean, S.; Jake, R.; Blake, P. A Novel Approach to Social Media Privacy Education Through Simulated Role Reversal. *Procedia Comput. Sci.* **2020**, *177*, 112–119.
3. Venter, I.; Blignaut, R.; Renaud, K.; Venter, M. Cyber security education is as essential as “the three R’s”. *Heliyon* **2019**, *5*, e02855. [[CrossRef](#)] [[PubMed](#)]
4. Aldawood, H.; Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In Proceedings of the IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia, 4–7 December 2018; pp. 62–68.
5. Susanne, B.; Menno, D.J.; Marianne, J.; Pieter, H.; Janina, R. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telemat. Inform.* **2019**, *41*, 55–69.
6. David, T. The Human Factor in the Social Media Security—Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manuf.* **2015**, *3*, 1096–1100.
7. Zoltán, N. Digital competence and the safety awareness base on the assessments results of the Middle East-European generations. *Procedia Manuf.* **2018**, *22*, 916–922.
8. Ahmed, N.; Kulsum, U.; Bin Azad, I.; Momtaz, A.S.Z.; Haque, M.E.; Rahman, M.S. Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective. In Proceedings of the IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 21–23 December 2017; pp. 788–791.
9. Abdullah, A.S.; Mohd, M. Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-Sector. In Proceedings of the 2019 International Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 25–26 September 2019; pp. 26–31.
10. Coventry, L. Keynote: Tackling the Awareness-Behaviour Divide in Security (Step 1): Understand the User by Lynne Coventry. In Proceedings of the 2014 Workshop on Socio-Technical Aspects in Security and Trust, Vienna, Austria, 18 July 2014.
11. Abdullah, M.S.; Zainal, A.; Maarof, M.A.; Nizam, M. Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News. In Proceedings of the Cyber Resilience Conference (CRC), Putrajaya, Malaysia, 13–15 November 2018; pp. 1–4.
12. Maqbool, Z.; Pammi, V.S.C.; Dutt, V. Cybersecurity: Effect of Information Availability in Security Games. In Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, 13–14 June 2016; pp. 1–5.
13. Thakur, K.; Kumar, H. Challenges in Protecting Personated Information in Cyber Space. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 167–171.
14. Nader, A.; Norita, N. User Oriented Privacy Model for Social Networks. *Procedia-Soc. Behav. Sci.* **2014**, *129*, 191–197.
15. Aldawood, H.; Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet* **2019**, *11*, 73. [[CrossRef](#)]
16. Mikko, S.; Anthony, V. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Q.* **2010**, *34*, 487–502.
17. McFadzean, E.; Ezingard, J.-N.; Birchall, D. Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Inf. Rev.* **2007**, *31*, 622–660. [[CrossRef](#)]
18. Fire, M.; Goldschmidt, R.; Elovici, Y. Online Social Networks: Threats and Solutions. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 2019–2036. [[CrossRef](#)]
19. Sohoraye, M.; Gooria, V.; Nundoo-Ghoorah, S.; Koonjal, P. Do You Know Big Brother is Watching You on Facebook? A Study of the Level of Awareness of Privacy and Security Issues among a Selected Sample of Facebook Users in Mauritius. In Proceedings of the International Conference on Computing, Communication and Security (ICCCS), Pointe aux Piments, Mauritius, 4–5 December 2015; pp. 1–7.

20. Ari, K.; Dita, P.; Harin, C.; Yustiyana, S. Information Privacy Concerns on Teens as Facebook Users in Indonesia. *Procedia Comput. Sci.* **2017**, *124*, 632–638.
21. Dionísio, N.; Alves, F.; Ferreira, P.M.; Bessani, A. Cyberthreat Detection from Twitter using Deep Neural Networks. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 14–19 July 2019; pp. 1–8.
22. Aldo, H.; Victor, S.; Gabriel, S.; Héctor, P.; Jesús, O.; Karina, T.; Mariko, N.; Victor, M. Security Attack Prediction Based on User Sentiment Analysis of Twitter Data. In Proceedings of the IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan, 14–17 March 2016; pp. 610–617.
23. Erkal, Y.; Sezgin, M.; Gunduz, S. A New Cyber Security Alert System for Twitter. In Proceedings of the IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, USA, 9–11 December 2015; pp. 766–770.
24. Samtani, S.; Chen, H. Using Social Network Analysis to Identify Key Hackers for Keylogging Tools in Hacker Forums. In Proceedings of the IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 319–321.
25. Mamatha, G.; Ashoka, B.M. Unofficial Hacking Algorithms. In Proceedings of the International Conference on Control, Automation, Communication and Energy Conservation, Perundurai, India, 4–6 June 2009; pp. 1–5.
26. Woo-Sung, C.; Dea-Woo, P. Malicious Code Hiding Android APP's Distribution and Hacking Attacks and Incident Analysis. In Proceedings of the 8th International Conference on Information Science and Digital Content Technology (ICIDT2012), Jeju, Republic of Korea, 26–28 June 2012; pp. 686–689.
27. Park, A.J.; Frank, R.; Mikhaylov, A.; Thomson, M. Hackers Hedging Bets: A CrossCommunity Analysis of Three Online Hacking Forums. In Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Barcelona, Spain, 28–31 August 2018; pp. 798–805.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.