جامعة المجمعة
Majmaah University

JEAS

JOURNAL OF ENGINEERING AND APPLIED SCIENCES

A Refereed Academic Journal Published by the
Publishing and Translation Center at Majmaah University

Vol. 10 Issue (1) (May. 2023) ISSN: 1658 - 6638

مركز النشر والترجمة جامعة المجمعة
Publishing & Translation Center

Publishing and Translation Center - Majmaah University

IN THE NAME OF ALLAH,
THE MOST GRACIOUS,
THE MOST MERCIFUL

Kingdom of Saudi Arabia
Ministry of Education
Majmaah University

جامعة المجمعة
Majmaah University

JEAS

JOURNAL OF ENGINEERING AND APPLIED SCIENCES

A Refereed Academic Journal Published by the
Publishing and Translation Center at Majmaah University

Vol. 10, Issue (1) (May - 2023) ISSN: 1658 - 6638

Publishing & Translation Center - MU

About the Journal

Journal of Engineering and Applied Sciences (JEAS)

Vision

Pioneer journal in the publication of advanced research in engineering and applied sciences.

Mission

A peer-review process which is transparent and rigorous

Objectives

a) Support research that addresses current problems facing humanity.
b) Provide an avenue for exchange of research interests and facilitate the communication among researchers.

Scope

JEAS accepts articles in the field of engineering and applied sciences. Engineering areas covered by JEAS include:

Engineering areas	Applied Sciences areas	Computer Sciences areas
Architectural Engineering	Applied Mathematics	Computer Sciences
Chemical Engineering	Applied Physics	Information Technology
Civil Engineering	Biological Science	Information Sciences
Computer Engineering	Biomathematics	Computer Engineering
Electrical Engineering	Biotechnology	
Environmental Engineering	Computer Sciences	
Industrial Engineering	Earth Science	
Mechanical Engineering	Environmental Science	

Correspondence and Subscription

Majmaah University, Post Box 66, Al-Majmaah 11952, KSA

email: jeas@mu.edu.sa

Journal of Engineering and Applied Sciences

Journal of Engineering and Applied Sciences

Editorial

Scientific publishing has brought many challenges to authors. With increasing number of scientific journals, varying scopes, reviewing requirements, and cost of publishing to authors, finding the right journal to publish an article is a decision many authors must bitterly confront and resolve. The publication of scientific findings is an integral part of the life of researchers. The process of publishing has evolved to become an efficient system of decimating knowledge and collaboration among scientists. Science journals have institutionalized procedures to manage large volume of article submissions per year. In many cases, journals began to define narrower scopes for a dual purpose: managing submissions and delivering outstanding research.

Based on recent studies, the scientific publishing world consists of more than 25 thousand active journals in various disciplines and fields. Science Direct hosts 3,348 journals (as of February 2014). The Directory of Open Access Journals lists in its search engine more than 9,800 open access online journals.

According to recent estimates, the number of scientific journals grows by 3% per year worldwide. With this large number of journals, journals may find it harder to stay afloat.

In its inauguration, the board of editors is honored to introduce to the scientific community the Journal of Engineering and Applied Sciences - JEAS, another scientific journal from Majmaah University. The board has pledged a commitment to JEAS authors and readers to bring the most dynamic and vibrant journal management with better satisfaction.

Dr. Mohamed Alshehri

Contents

Measurement of Benefits, Reasons, and Barriers to Students' Adoption of Electronic Applications .

Mohammed Yahya Alghamdi [1], Mohammed Zakariah [2], Ali Aloway [3], Abdullah Alshehri[4], Fahad Al-Wesabi [5], Ahmed S. Khalaf [6], Younis A. Younis [7]

1. Department of Compute Science, Faculty of Science and Arts of Baljurshi, Albaha University, KSA, myahya@bu.edu.sa
2. Department of Computer Science, Faculty of Computer Science, King Saud University, KSA, mzakariah@ksu.edu.sa
3. Department of Information Technology, Faculty of Computer Science and IT, Albaha University, KSA, aalowayr@bu.edu.sa
4. Department of Information Technology, Faculty of Computer Science and IT, Albaha University, KSA, aashehri@bu.edu.sa
5. Department of Information Technology, Faculty of Computer Science and IT, King Khalid University, KSA, falwesabi@kku.edu.sa
6. Department of Compute Science, Faculty of Science and Arts of Baljurshi, Albaha University, KSA, akhalaf@bu.edu.sa
7. Department of Compute Science, Faculty of Information Technology, University of Benghazi, Libya, younis.younis@uob.edu.ly

Abstract

Over the past decade, electronic applications, particularly social networking applications (SNAs), have been gaining considerable popularity, including among educated young people. The advantages of SNAs are apparent in many sectors, with education being no exception. SNAs are also playing the main role in enhancing the quality of education. The aim of this paper is to explore SNAs use (e.g., Twitter, Facebook, and YouTube) in higher education students enrolled at Albaha University, Saudi Arabia, focusing on their associated advantages, barriers, and reasons for adoption, as well as differences between the participants with respect to the study variables. The research methodology was a survey approach and the sample size reached 243 students, including 123 males and 120 females. The survey was distributed to students electronically. The results indicate that most students benefit from SNAs, and these resources motivate them to engage with SNAs to enhance their education. Barriers were also identified that must be addressed for effective education. No difference was found between male and female students in terms of benefiting from SNAs, as well as the reasons and barriers, thereby indicating the availability of SNAs for both genders and the flexibility of their use at any time and place, as well as awareness in both genders about their use. A noticeable difference was identified in the extent of the benefits derived from SNAs between participants older and younger than 20 years, and differences were also found in the reasons underpinning these benefits. This reflects a disparity in the use and mastery of SNAs between the two age groups. Students aged 20-25 years also encountered greater barriers to SNAs use compared to students aged younger than 20 years, which may be attributed to the lower familiarity of older students with SNAs.

Keywords: Web 2.0 applications, electronic applications, technology-enhanced learning, e-learning, computer-based education.

Introduction

In the current era, every person who wants to connect with others can do so due to the availability of social networking applications (SNAs). As such, individuals can connect and interact worldwide, breaking the barriers imposed by borders. Over the past decade, SNAs use has dramatically increased, because of which it has gained more momentum [1]. Smartphones are a great source of connection as almost every person owns one and connecting with others using this device is the easiest way to connect to SNAs. Almost every individual has an account with an SNAs, and these online applications play a major role for every individual. SNAs have a significant influence on many fields, including education, and in the case of the education sector, benefits have been identified in the form of increased collaboration between students and higher student participation[2]. Also, when students use SNAs, it is easier for them to review and track team project progress, e-learning resources are abundantly available, and video conferencing is frictionless. In addition, SNAs provide connectivity, and in the context of education, it is the students who lead student collaboration [3]. This connectivity of students allows them to create new friends and classmates for possible collaboration to develop projects and work collectively on specific tasks. SNAs are playing a key role in enhancing the quality of education, and the benefits of SNAs are not limited to students as even faculty members benefit from these platforms [4]. Faculty members can encourage students to participate in educational tasks with the help of SNAs. With the significant increase in SNAs usage by lectures and students in higher education institutions worldwide because of the COVID-19 pandemic, this research is critical to see how SNAs can be integrated and implemented in sharing educational materials, interacting between lecturers and their students, and determining the usefulness of SNAs for students. The contribution of this research study is to examine the use of SNAs (such as Twitter, Facebook, and YouTube) by higher education students enrolled at Albaha University in Saudi Arabia. It does this by concentrating on the benefits, challenges, and reasons for adoption of these SNAs as well as any differences in participant characteristics regarding the study variables. We develop the following research questions:

- Question 1: How do the participants benefit from SNAs?
- Question 2: What are the participants' reasons for using SNAs?
- Question 3: What barriers do the participants face in using SNAs?
- Question 4: What is the relationship between the participants' reasons for using SNAs and the extent of their associated benefits?
- Question 5: What is the relationship between the participants' barriers to the use of SNAs and the extent of their associated benefits?

The research study also seeks to test the following hypotheses:

- Significant statistical differences exist

between the mean scores of the sample in terms of benefits, reasons, and barriers with respect to the variable of gender.

- Significant statistical differences exist between the mean scores of the sample in terms of benefits, reasons, and barriers with respect to variable of age.

To achieve the research aims, we prepared a survey to get information from students at Albaha University. The questionnaire contains two demographic variables: gender and age; also, it has 20 items distributed on three main dimensions: benefits, reasons for using SNAs, and barriers.

As shown in Figure 1, the research revolves around the three components of benefits, barriers, and motivation.

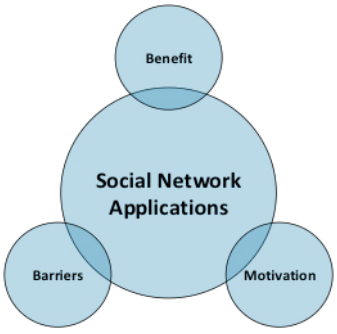

Fig. 1. Major Study Details with Social Networking Applications.

Literature Review

An author with more than 5 years of teaching experience at public universities has concluded that the traditional medium of teaching – that is, the face-to-face medium – is more beneficial. However, the major issue with this medium is that it is dependent on time, space, and the place of teaching, which needs to be taken care of by everybody, including teachers, students, and educational institutions.

Based on the above issue, a literature review on SNAs shows that the use of SNAs in education sectors have grown exponentially [5]; also, SNAs offer a more interactive and collaborative method of communication between learners and help them to obtain knowledge [1,5]. SNAs can supplement the traditional teaching and learning methodologies that are currently used by institutions of higher education. In a similar work, Erhel et al. [6], conducted a long-term study to evaluate the impact of using twitter on students' outcomes; the study concluded that twitter is a more interactive and engaging platform for learning compared to the traditional mode of teaching (e.g., lectures). Of the many SNAs that have been deployed online, Al-Qaysi et al. [7], suggested that some are more efficient than others for higher education, including Facebook, Twitter, and LinkedIn. Along with SNAs, media-sharing platforms such as YouTube, Flickr, Tumblr, wikis, and blogs can also play a major role in higher education.

Further to the above discussion, Jones [8], suggested that recent SNA technologies are no longer intended solely for entertainment and leisure; these technologies are becoming a major asset for interactions and learning. Another recent study focused on undergraduate students' tweeting activities in several universities of Singapore [9]. It was found that among many other benefits, the students were able to converse with their peers and interact with the instructor more freely and share knowledge efficiently. In

addition to the abovementioned benefits of SNAs in education, Menkhoff et al. [9] and Wheeler [10], stated other benefits. Even if the application is on computer or mobile, they identified three major benefits for the universities. The first benefit is that SNAs allow students to engage in blended learning, which promotes better learning; for example, Twitter helps students in learning face-to-face and sometimes in communicating with faculty members when they are at home. The second benefit of SNAs is that they allow students to be involved in collaborative studies and learning. Finally, the use of SNAs helps students by giving them a platform to post their questions, problems, and issues on blogs and Twitter to address difficulties in their subjects.

Concerning the daily usage of SNAs such as Facebook, Twitter, and LinkedIn, it is estimated that millions of people, mostly young people, are engaging with them worldwide. According to one study [11], involving a sample of approximately 3,000 students in the USA, 90% used Facebook and 37% used Twitter. A similar study was conducted by Smith and Anderson [12], which found that approximately 71% of university students were Facebook users. Further research on Facebook [12,13,14], revealed that it is the most frequently used SNA for both personal and educational purposes.

The ways in which people acquire knowledge has changed dramatically over the past decade, especially with the emergence of SNAs. The influence of SNAs has been felt both in the formal and informal education system. Formal education refers to the educational structure from nursery to the university level, which also includes specialized training and vocational learning for all age groups, and informal learning means acquiring knowledge by interacting and sharing information in a social environment [15]. Numerous studies have been conducted to estimate the use of SNAs. In this context, a study was conducted by the Islamic University of Bahawalpur in Pakistan where approximately 600 students were involved, nearly 90% of whom stated they used SNAs for educational purposes; noteworthily, most of the students were Facebook users [16]. In another study conducted at the University of Science, Malaysia, approximately 300 students showed great interest in Facebook and considered it an important tool for them to learn English language skills [17].

All the above-mentioned studies were concerned with the students' perspective, but teachers also show substantial interest in SNAs as a tool for facilitating teaching and learning. In this context, Waycott et al. [18], conducted a research study in Australia with 20 lecturers from various departments, including management, humanities, information technology, and health sciences. The students were asked to create and share their content on SNAs. The findings showed that using these platforms for their work and allowing the students to have transparency created new perspectives in learning.

Based on the above discussion and literature, it is becoming evident that there

are many positive aspects associated with the application of SNAs in education. Thus, upgrading the current paradigm of traditional learning to include social network-based learning to promote better educational outcomes is proposed. The areas that may have a greater influence on SNAs are social learning, communication, academic culture, and many others in the future. SNAs can support and create a more efficient educational environment and further enhance performance in the field of education for both the student seeking knowledge and the teacher delivering information [19].

Comparatively few studies [20,21], have analyzed the positive influence on student performance through the use of SNAs. According to Troussas et al. [22], SNAs influence the educational process in general and enhance student performance and collaboration between students and teachers. Additionally, Yusof et al. [23], highlights the benefits of SNAs, the e-learning environment, and the reasons for implementing SNAs. Educational processes based on group study are also influenced by SNAs. Similar results were reported in an Australian study of SNA use in education, wherein the students appeared to be excited and adequately inspired by the social learning settings they encountered [24].

Research Methodology

The research team prepared a questionnaire that included 2 demographic variables: gender and age. It also included 20 items distributed on 3 main dimensions: benefits (9 items), reasons for using SNAs (6 items), and barriers (5 items). The tool's apparent validity was also verified by presenting it to a group of professors who specialize in the fields of education technology, e-learning, and computing. Based on their opinions, some paragraphs were amended. The internal consistency and reliability of the questionnaire were also verified by administering it to a sample of male and female students (n = 43). Internal consistency was determined by calculating the Pearson correlation coefficient between the total score of each dimension and the total score of the scale, as well as the degree of each statement and the degree of the college for the dimension to which the statement belonged. This ranged between 0.793 and 0.886, and all of them were large, acceptable coefficients. Statistically significant results were established using the significance level of 0.01. The reliability coefficient was determined by calculating the coefficient of stability, Cronbach's alpha, for the paragraphs of each aspect of the survey, and for the paragraphs of the questionnaire. The results indicated that the values for all stability coefficients were high, ranging from 0.849 to 0.916. This shows that the previous results regarding the validity of the scale can be applied reassuringly in this study, as well as the reliability of its results. The target population comprised of all students at the Faculties of Sciences and Arts of Baljurashi, Computer Science, and Information Technology, amounting to 650 students, and the appropriate sample size was calculated according to Robert Mason's equa-

tion. The sample size reached 243 students, including 123 males and 120 females, as shown in Table 1. The survey was distributed to students electronically via emails and WhatsApp groups. The recruitment strategies used did not contribute to any bias in the obtained data. Given that it was important to protect the students' identities and encourage honest, non-attributional answers, the survey was anonymous, and students were not asked to provide any personal details about themselves.

Table 1. Frequency and Percentage of the Sample Distributed According to the Study Variables.

Variable	Category	Frequency	Percentage
Gender	Male	123	50.6
	Female	120	49.4
Age	Less than 20 years	212	87.2
	20-25 years	31	12.8

Before taking part in the research study, students were required to sign a consent form. Before beginning the research procedures, the Scientific Research Deanship at Albaha University granted ethical permission for the study. The aim of the research was to measure students' advantages, reasons, and barriers to using SNAs at the university. The research methodology was a survey approach that investigated students' reasons for using SNAs at Albaha University. The research instrument was an online multiple-choice questionnaire consisting of several themes. One of the themes focused on the benefits students derived from the use of SNAs (Theme questions are included in Table 3). Another theme focused on the reasons why students to use SNAs (Theme questions are included in Table 4). The final theme focused on the barriers students face regarding the use of SNAs (Theme questions are included in Table 5).

After creating the questionnaire with Google Forms, it was distributed electronically via emails and WhatsApp groups to the participants. Regarding the analysis of the students' responses, questionnaire data were analyzed using multiple statistical tests in SPSS. Further details about how the results were analyzed and presented is presented in the next section.

Data Analysis and Research Results

Determine the Degree of Response and Relative Weights

The degree of response was determined based on the weighted average value and considering the cut-off scores of the study tool scale. This was achieved by adopting the following criterion to estimate the degree of response, as the length of the 5-point Likert scale used in this tool was determined (from 1 to 5) and the range was calculated (5-1 = 4), which was divided by the number of the 5 periods of the scale to obtain the length of the period (i.e., 4/5 = 0.8).

Table 2. To Determine the Degree of Response, Relative Weights, and Arithmetic Means.

M	Relative Response	Period	Arithmetic Average	Degree of Response
1	20-35.9 %	(1) to less than (1.8)	1-1.79	Strongly disagree
2	36-51.9%	(1.8) to less than (2.6)	1.8- 2.59	Disagree

M	Relative Response	Period	Arithmetic Average	Degree of Response
3	52-67.9%	(2.6) to less than (3.4)	2.6-3.39	Neutral
4	68-83.9%	(3.4) to less than (4.2)	3.4– 4.19	Agree
5	84-100%	(4.2) to (5)	4.2-5	Strongly agree

This was then added to the lowest value in the scale (namely, 1) to determine the upper limit for the first period. The same process was applied for the remaining periods, as calculated repetitions of the members of the study population on the questionnaire for each statement under each of the alternatives to the answer by giving a ranking scale for each of the response alternatives as follows: strongly agree (5), agree (4), neutral (3), disagree (2), strongly disagree (1) (see Table 2).

Results for the First Question: How Do the Participants Benefit from SNAs?

The frequencies, percentages, arithmetic means, and standard deviation were calculated for each of the statements associated with the first dimension (i.e., benefit). The arithmetic averages were arranged in descending order to determine the higher expressions. The results are shown in Table 3. Table 3 shows that the total expressions for this dimension had a score of "strongly agree", with an arithmetic mean of 4.25 and a small standard deviation of 0.61. This indicates that there was agreement among the sample members about the total of this dimension. Most of the expressions for this dimension were rated "strongly agree", with 5 statements, and 4 expressions for this dimension were rated "agree".

Statement 2, which reads “I think the traditional learning style should be improved by using SNAs in the educational process”, ranked first with a score of “strongly agree”. It had the largest arithmetic mean (4.59) and a small standard deviation (0.60). Statement 5 had the lowest score, the text for which was, “I get more help from my SNAs members in my studies than in my lecture hall”. This statement had the degree of “I agree” and was associated with the lowest arithmetic mean (3.82) and a standard deviation of 1.10.

Table 3. Mean and Standard Deviations for the Expressions of the First Dimension: Benefits of SNAs Arranged in Descending Order According to the Mean

M	Phrases of the first dimension: benefits		Practice degree					The Mean	Standard division	Degree
			strongly disagree	disagree	Neutrals	agree	strongly agree			
1	I think the traditional learning style should be improved by using SNAs in the educational process.	F	0	0	14	71	158	4.59	0.60	strongly agree
		%	0	0	5.8	29.2	65			
2	I use SNAs to communicate with professors to inquire about assignments and other educational aspects.	F	14	0	14	43	172	4.48	1.03	strongly agree
		%	5.8	0	5.8	17.7	70.8			
3	When I started using and learning from SNAs, my performance and level of study improved.	F	0	14	15	86	128	4.35	0.84	strongly agree
		%	0	5.8	6.2	35.4	52.7			
4	I use SNAs to search and learn from the lessons available, such as using YouTube or Telegram.	F	0	14	15	114	100	4.23	0.81	strongly agree
		%	0	5.8	6.2	46.9	41.2			
5	I think social networking apps have a positive impact on self-development.	F	0	0	14	115	114	4.41	0.60	strongly agree
		%	0	0	5.8	47.3	46.9			
6	Using SNAs, I am developing more technology and communication skills than the traditional method.	F	0	0	29	86	128	4.41	0.69	agree
		%	0	0	11.9	35.4	52.7			
7	The use of social network applications allows me to participate more in scientific discussions with online groups.	F	0	29	29	85	100	4.05	1.01	agree
		%	0	11.9	11.9	35	41.2			
8	I see that learning from SNAs is more attractive to me than traditional learning.	F	14	28	15	86	100	3.95	1.21	agree
		%	5.8	11.5	6.2	35.4	41.2			
9	I get more help from my SNAs members in my studies than in my lecture hall.	F	0	43	43	72	85	3.82	1.10	agree
		%	0	17.7	17.7	29.6	35			
The total of first dimension: benefits								4.25	0.61	strongly agree

Results for the Second Question: What are the Participants' Reasons for Using SNAs?

The frequencies, percentages, arithmetic means, and standard deviation were calculated for each of the statements associated with the second dimension (i.e., reasons for using SNAs). The arithmetic averages were arranged in descending order to determine the higher expressions, and the results are shown in Table 4.

Table 4 shows that the total expressions for this dimension had a score of "strongly agree", with an arithmetic mean of 4.38 and a small standard deviation of 0.50. This indicates that there was agreement in the sample group regarding the total of this dimension. Most of the expressions for this dimension were rated "strongly agree" (with 5 statements), and only one statement was rated "agree". Statement 6, which reads "I use SNAs to learn about news and events", ranked first with a score of "strongly agree", the largest arithmetic mean (4.58), and an average standard deviation (0.79). In last place was Statement 3, the text for which was, "I use SNAs because they are free".

This statement had a degree of "agree" and was associated with the lowest arithmetic mean (4.16) and a standard deviation of 1.00. The researchers attributed this to the fact that one of the main reasons for using SNAs is that students liked to learn about events, news, and information to know what was going on around them, and they were also attracted by the ease of information sharing.

Table 4. Means and Standard Deviations for the Expressions of the Second Dimension: Reasons for Using SNAs are Arranged in Descending Order According to the Mean.

M	Phrases of the second dimension: Reasons Use		Practice degree					The Mean	Standard division	Degree
			strongly disagree	disagree	Neutrals	agree	strongly agree			
1	I use SNAs to know news and events.	F	0	0	15	56	172	4.58	0.79	strongly agree
		%	0	0	6.2	23	70.8			
2	I use SNAs because sharing information is so easy.	F	0	14	0	86	143	4.47	0.77	strongly agree
		%	0	5.8	0	35.4	58.8			
3	I use SNAs because they contain lots of entertainment, fun, and games.	F	0	0	14	116	113	4.41	0.6	strongly agree
		%	0	0	5.8	47.7	46.5			
4	I use SNAs because of their flexibility as they enable me to learn anytime and anywhere.	F	0	0	15	128	100	4.35	0.59	strongly agree
		%	0	0	6.2	52.7	41.2			
5	I use SNAs to stay in touch with my friends.	F	0	14	29	71	129	4.30	0.89	strongly agree
		%	0	5.8	11.9	29.2	53.1			
6	I use SNAs because they are free.	F	15	0	15	113	100	4.16	1.0	agree
		%	6.2	0	6.2	46.5	41.2			
The Total of the second dimension: Reasons Use								4.38	0.5	strongly agree

Results for the Third Question: What Barriers Do the Participants Face in Using SNAs?

The frequencies, percentages, arithmetic averages, and standard deviation were calculated for each of the statements associated with the third dimension (i.e., barriers to use). The arithmetic averages were arranged in descending order to determine the higher expressions, and the results are shown in Table 5.

Table 5 shows that the total expressions of this dimension had a score of "agree", with an arithmetic mean of 3.44 and a large standard deviation of 1.07. This reflects the fact that there was a difference between the sample group members with respect to the total of this dimension. Most of the expressions for this dimension were rated "agree" (4 statements) and only a single statement was rated "neutral". Statement 4, which reads "There are many SNAs, but I find it difficult to know which one is most appropriate for education", ranked first with a score of "I agree".

Table 5. Means and Standard Deviations of the Third Dimension Expressions: Barriers to Use are Arranged in Descending Order According to the Mean.

M	Phrases of the third dimension: Barriers to use		Practice degree					The Mean	Standard division	Degree
			strongly disagree	disagree	Neutrals	agree	strongly agree			
1	There are many SNAs, but I find it difficult to know which one is most appropriate for education.	F	0	0	86	84	73	3.59	1.25	agree
		%	0	0	35.4	34.6	30			
2	The search process in SNAs takes a lot of effort.	F	0	58	57	70	58	3.53	1.10	agree
		%	0	23.9	23.5	28.8	23.9			
3	Using SNAs wastes a lot of time.	F	14	43	58	56	72	3.53	1.24	agree
		%	5.8	17.7	23.9	23	29.6			
4	I think SNAs cause me to get distracted from studying.	F	14	58	28	85	58	3.47	1.25	agree
		%	5.8	23.9	11.5	35	23.9			
5	Frequent use of SNAs negatively affects the student's level.	F	57	43	14	86	43	3.06	1.48	Neutral
		%	23.5	17.7	5.8	35.4	17.7			
The Total of the third dimension: Barriers to use								3.44	1.07	agree

It had the largest arithmetic mean 3.59 and a large standard deviation 1.25. In last place was Statement 5, which reads "Frequent use of SNAs negatively affects a student's level". This had a degree of "neutral" and corresponded to the lowest arithmetic mean (3.06) and the largest standard deviation (1.48) among all expressions of a capacity. It is worth noting that the standard deviations were high for all paragraphs of this dimension, thereby reflecting existence of disparities in the participants' opinion relating to barriers to the use of SNAs.

Results for the Fourth Question: What is the Relationship Between the Participants' Reasons for Using SNAs and the Extent of their Associated Benefits?

To answer this question, the Pearson correlation coefficient was calculated between the total dimension of the usage reason and the total dimension of the benefit of SNAs. The value of the correlation coefficient was 0.765 ** with a significance level of 0.000. This means that there was a positive correlation between the reasons for using SNAs and the benefit of the SNAs to the participants. This can be attributed to all the students' reasons for using social networking applications, which led to an increase in the usefulness of applying them in the educational process (e.g., in this scientific research). We found that one of the reasons among students for using SNAs was to search for information and facts and, furthermore, to share them easily and conveniently. Thus, the benefits become very high.

Results for the Fifth Question: What is the Relationship Between the Participants' Barriers to the Use of SNAs and the Extent of their Associated Benefits?

The Pearson correlation coefficient was calculated between the total dimension of the barriers to SNA use and the total dimension of benefiting from SNAs. The value of the correlation coefficient was -0.654 - ** with a significance level of 0.000, meaning that a negative correlation existed between the two variables. This can be attributed to the fact that when students encounter fewer barriers toward the use of SNAs, their level of interest in the educational process increases (and vice versa). In this research study, we found that the extent to which students benefit from SNAs in the educational process is high compared to the barriers to their use.

Verification of Hypothesis

In the research undertaken by Azizi et al.[25], the researchers examined the connection between SNA addiction and academic attainment in a sample group of students from Iran. The results demonstrated a negative and statistically significant relationship between these two variables. To verify the validity of the research hypotheses linked to calculating the differences between the responses of the sample group according to the demographic factors of the study, it was necessary to test the moderation of the normal distribution among the participants to ensure the equilibrium distribution between the study sample categories. The Kolmogorov-Smirnov test was used to determine whether the data obtained from the sample followed the normal distribution, in order to determine the appropriate tests for each case, as parameter tests are used when the distribution is normal, and the significance level of the test is greater than 0.05, while non-parametric tests are used when the distribution is abnormal and the significance level of the test is less than 0.05. Table 6 shows the results. The importance of 0 for sig value of this Table is to measure the level of significance of the normal distribution of the sample, according to its variables, and through the 0-value shown in this table for sig value, it indicated that there was no normal distribution for the sample.

Table 6. Results of One-Sample Kolmogorov-Smirnov Test to Examine Normality of Study Sample.

Variable	Statistics value	Sig. value
Gender	5.363	0.000
Age	3.531	0.000

Based on the results shown in Table 6, two independent samples were used: namely, the Mann-Whitney U test with two variables (in this case, gender and age).

Verification of the First Hypothesis

The first hypothesis for this research was the following: statistically significant variations exist between the mean scores of the sample in terms of benefits, reasons, and barriers with respect to the variable of gender.

Table 7 shows the importance for sig(2-tailed) value with the level of significance for all the tool's dimensions was greater than 0.05. Hence, for the variable of gender, no differences that are statistically significant were identified at the level of

Table 7. Results of the Mann-Whitney U Test for Independent Two Samples to Reveal the Differences Between the Sample Mean Responses that are Attributed to the Gender Variable.

Dimensions	Gender	N	Mean Rank	Sum of Ranks	Mann-Whitney U	Sig. (2-tailed)
Benefits	Male	123	121.26	14914.5	7288.5	.866
	Female	120	122.76	14731.5		
Reasons	Male	123	122.59	15078.0	7308.0	.893
	Female	120	121.40	14568.0		
Barriers	Male	123	123.73	15218.5	7167.5	.693
	Female	120	120.23	14427.5		

significance (*oc*= 0.05) between the average responses of the sample members in all dimensions of the study tool.

Verification of the Second Hypothesis

The second hypothesis for this research was the following: statistically significant variations exist between the mean scores of the sample in terms of benefits, reasons, and barriers with respect to variable of age. Table 8 demonstrates that the degree of

Table 8. Results of the Mann-Whitney U Test for Independent Two Samples to Reveal the Differences Between the Sample Mean Responses that are Attributed to the Age Variable.

Dimensions	Age	N	Mean Rank	Sum of Ranks	Mann-Whitney U	Sig. (2-tailed)
Benefits	<20	212	130.40	27645	1505.0	.000
	20-25	31	64.55	2001		
Reasons	<20	212	137.14	29073	77.0	.000
	20-25	31	18.48	573		
Barriers	<20	212	109.77	23271	693.0	.000
	20-25	31	205.65	6375		

significance for all the tool's dimensions was less than 0.05. This demonstrates the existence of statistically significant variations between the sample members' average responses in the dimensions of benefits and reasons according to age at the level of significance (*OC*= 0.05).

In particular, the differences are in favor of the age group aged less than 20 years. The findings also demonstrate the existence of statistically significant variations in the sample members' average responses in the barriers dimension according to the age variable, favoring the 20–25 age group.

Discussion of Results

The research findings confirm that SNAs have utility for students at Albaha University in terms of advancing learning in the context of higher education. These results are in line with other findings that have been published in the literature that indicate the value of SNAs for students in various educational processes. For example, a research project undertaken with a sample group of 160 students enrolled in social studies and philosophy courses at the Uni-

versity of Delhi found, through interviews, that 71.25% of the participants used Facebook to facilitate discussion and research collaboration [26]. A comparable study was conducted at Boston University's pharmacology department, which found that 60 % of the students used Twitter to promote their professional knowledge and improve their educational outline [27].

It is reasonable to account for these results by referencing the fact that students who took part in this study viewed SNAs as having valuable educational applications and, accordingly, were motivated to use them to achieve educational goals (e.g., communicating with faculty members). SNAs serve as a valuable complement to traditional pedagogical tools and approaches. The findings of this study agree with those of numerous other studies, including [4, 28, 29], which have emphasized the educational value of SNAs in terms of facilitating teacher-student communication and improving academic attainment.

This study's results also indicate that the motivation of students at Albaha University to use SNAs stems in part from their value in enabling geographically and temporally unrestricted learning. As revealed in the literature review, information sharing is a crucial issue that drives many students to SNAs adoption, which stems from the fact that many online platforms, including Facebook and WhatsApp, offer features for file sharing and the dissemination of curricular materials.

This can be accounted for by referencing the fact that one of the fundamental reasons for students' use of SNAs relates to the ability they afford to keep updated about current events. This study's results are consistent with those reported elsewhere, including in Deng et al. [30], Valdez et al. [31], and Phua et al. [32], which found that the convenience of information sharing, the flexibility of SNAs, and the utility of SNAs in serving as an up-to-date source of news constituted the major reasons why students used SNAs for educational purposes.

This study's results highlight several barriers associated with the use of SNAs from the standpoint of students. For example, members of the sample group reported that the use of SNAs often resulted in wasted time. This is consistent with the results reported in [33], which suggested that a key barrier to students' adoption of SNAs is the negative impact that their overuse can have on focus, concentration, and academic attainment.

This result was accounted for by referencing the fact that the substantial number of SNAs, paired with the availability of diverse features on the existing and widely used SNAs, increased students' difficulties in identifying the optimal application for educational support. The responses given by the students also indicate that SNAs do not have a negative impact on their academic attainment, and that students have an adequate level of awareness about the use of SNAs and, in particular, how to exploit SNAs to achieve educational goals. As such, this study's results are consistent with those of several prior studies. For ex-

ample, Deng et al. [30] indicated that SNAs, when used in an effective way, positively influence students' academic attainment. It is important to recognize, however, that the improper use of SNAs may negatively influence students [33, 34].

This was attributed by the researchers to the students' reasons for using SNAs, which resulted in an increase in the utility of employing them in an educational context (e.g., to facilitate scientific research). We identified that one student's reason for using SNAs was to search for relevant data and share it with others conveniently. Hence, the benefits of SNAs are high for use cases such as these. In the previously referenced study of Hassan et al. [35], the researchers looked at how user advantages and continuing use of SNAs might be improved through motivating feedback. The findings showed that gamification has a positive relationship with the capacity for affective counsel, quantified self has a positive relationship with the usage of informational guidance and affective feedback, and social networking has a good relationship with social feedback.

The researchers accounted for this by referencing the fact that when there are limited barriers to students' use of SNAs, the degree to which they are interested in the educational process increases (and vice versa). In the present research, we found that the benefits associated with students' use of SNAs for educational purposes substantially outweigh the barriers to their use. In Azizi et al.'s research [25], the correlation between SNAs addiction and academic attainment was investigated in Iranian students. According to the results, SNAs addition and academic attainment were negatively correlated, and the relationship was statistically significant.

The researchers accounted for this by referencing the fact that the study revealed that no differences existed between male and female students regarding the benefits derived from SNAs, as well as the reasons and barriers. This reflects both the availability and accessibility of SNAs for members of both genders, and it also shows that both males and females have similar levels of awareness with respect to SNAs. Li et al.'s research [36], assessed whether an SNA-based game effectively improved problem-solving skills and mental health understanding in young people. The researchers also examined gender differences in learning outcomes and learning reason, and the results demonstrated that no differences were apparent.

The researchers accounted for this by referencing the fact that a noticeable difference existed in terms of the degree to which students benefitted from SNAs and the reasons underpinning the benefit in the age group consisting of students younger than 20 years. This reflects the greater usage rates and skill levels of younger SNA users compared to older SNA users. The study also found that students aged between 20 and 25 years encountered more substantial barriers in comparison to their younger counterparts, which could stem from their lower level of familiarity.

Pfeil et al. [37], investigated age differences

in MySpace usage to illuminate disparities in social capital between adolescents (individuals aged 13-19 years) and elderly people (individuals aged 60 years and above). It was found that the younger participants used varied forms of media available on MySpace, including music and video, with greater frequency compared to their older counterparts. The researchers also found that adolescents made more substantial use of self-references and negative emotions in their profile descriptions compared to the older participants.

Research Recommendations and Future Work

The research findings highlight several recommendations that can be given to students, faculty members, and universities. First, using SNAs, both students and faculty members can receive diverse benefits. For example, students can engage in e-learning in a more efficient way when they leverage SNAs, and they can also use these platforms to communicate with others, solve problems without needing to attend a physical location, and share information. In the case of faculty members, they can motivate students to engage in educational activities using SNAs. Teachers can benefit from frictionless communication with students, which also represents a benefit for students, and for students with limited interpersonal capabilities and social anxiety, SNA-mediated communication can ensure equal access to educational resources such as teacher time. An important recommendation is for higher education institutions to minimize the difficulties associated with accessing SNAs on campus by providing free Wi-Fi both for students and faculty members. At the same time, delivering training sessions to raise awareness about effective ways to exploit SNAs for educational purposes is something that higher education institutions should implement if resources are available. The findings of this study have substantial implications for educators. They will enable educators to understand how students at Albaha University are using SNAs for educational purposes, and they also highlight the optimal SNAs to use with students to improve their preferences and, in turn, enhance their academic attainment.

Regarding this study's limitations, the barriers that were identified as relevant for students offer opportunities for further research to address these barriers and minimize their impact on student performance. Undertaking one-on-one interviews with students would also be a worthwhile future research direction that could yield qualitative data to complement this study's quantitative data, potentially illuminating issues such as the difficulties faced by students. Additionally, the fact that this study's sample group was recruited from only two faculties at Albaha University highlights the importance of conducting comparable studies in other Saudi Arabian universities to enable the generalizability of these results. Focusing on other majors (e.g., medical students) may also represent a fruitful avenue for further research.

For future work, a machine learning tech-

nique will be applied to predict students' usage of SNAs for education, communication, or entertainment. Generally, machine learning consists of two types of paradigms: supervised and unsupervised. We will focus on a supervised technique wherein the students' data will be obtained after questionnaire responses have been used as an input for processing. Supervised learning takes these inputs as parameters and relates them to features, which lead to category classes. The goal of this learning will be to classify the responses received from the students into the following classes: SNA use for education, SNA use for communication purposes, or SNA use for entertainment. The classification will be facilitated based on the features, and these features will be taken as input parameters for analysis. To predict the students' interests, all the students' responses should be learned based on the areas of interest. Once the learning phase has been completed, weights will be assigned to these features based on the question of which category can be classified. The students' response data will be divided into a training set and test set at a proportion of 70% to 30%. After training the classifier, testing will be undertaken using tenfold cross-validation. Finally, a random student's record will used for prediction and performance evaluation. Based on the strength of the learning, it may be possible to make a correct and accurate prediction. The authors intend to perform these steps as we gather more data because, in this scenario, the data received will be abundant.

Conclusion

The phenomenal growth of digital technology, notably social networking applications (SNAs) applications, has had a tremendous impact on the field of education recently. Students may participate in discussions, interact with information, and access a variety of learning tools. This research recruited a sample of students from Albaha University to discern whether students benefitted from SNAs, to identify the reasons that motivated them to use SNAs, and to identify barriers associated with their use of SNAs for educational purposes. A noticeable difference was identified between the two age groups in the extent of benefits from SNAs and the reasons underpinning these benefits.

Acknowledgment

This research was funded by the deanship of Scientific Research, Albaha University, KSA (Grant No: 1440/19). Also, this research study is a part of a funded project entitled" The Effectiveness of Using Social Networks Applications in University Education: An Applied Study on Albaha University". Thus, the support and assistance of the university is very much appreciated.

References

[1] S. Galvin, and C. Greenhow. "Educational networking: A novel discipline for improved K-12 learning based on social networks." In Educational networking, pp. 3-41. Springer, Cham, 2020.

[2] J.A.N. Ansari, and N.A. Khan,

2020. Exploring the role of social media in collaborative learning the new domain of learning. Smart Learning Environments, 7(1), pp.1-16.

[3] B. Sarwar, S. Zulfiqar, S. Aziz, and K. Ejaz Chandia, 'Usage of Social Media Tools for Collaborative Learning: The Effect on Learning Success With the Moderating Role of Cyberbullying', J. Educ. Comput. Res., 2019.

[4] A. Y. S. Eldin, 'Faculty Members' Behavior towards Technology Acceptance and its Impact on a Value-Added Configuration', Int. J. Acad. Res. Bus. Soc. Sci., vol. 10, no. 3, 2020.

[5] J.S. Barrot, "Scientific Mapping of Social Media in Education: A Decade of Exponential Growth". Journal of Educational Computing Research, 59(4), 2020.

[6] S. Erhel, N. Michinov, A. Noël, and C. Gonthier. "Tweet to teach: Using a twitter-based instructional method to improve student motivation and academic outcomes in higher education." The Internet and Higher Education 55 (2022): 100876.

[7] N. Al-Qaysi, N. Mohamad-Nordin, & M. Al-Emran, "A Systematic Review of Social Media Acceptance From the Perspective of Educational and Information Systems Theories and Models". Journal of Educational Computing Research, 57(8), 2085–2109, 2020.

[8] A. Jones, "How Twitter saved my literature class: A case study with discussion," Cutting-Edge Technol. High. Educ., 2011.

[9] T. Menkhoff, Y. W. Chay, M. L. Bengtsson, C. J. Woodard, and B. Gan, "Incorporating microblogging ('tweeting') in higher education: Lessons learnt in a knowledge management course," Computers in Human Behavior, vol.51, pp.1295-1302, 2015.

[10] S. Wheeler, "Open content, open learning 2.0: Using wikis and blogs in higher education," Changing Cultures in Higher Education: Moving Ahead to Future Learning, 2010.

[11] S. Kuppuswamy and P. B. S. Narayan, "The Impact of Social Networking Websites on the Education of Youth," International Journal of Virtual Communities and Social Networking, vol.2, no.1, pp. 67-79, 2010.

[12] A. Smith and M. Anderson, "Social Media Use 2018: Demographics and Statistics | Pew Research Center," 2018.

[13] P. A. Tess, "The role of social media in higher education classes (real and virtual)-A literature review," Comput. Human Behav., 2013.

[14] E. Hargittai, "Whose space? differences among users and non-users of social network sites," Journal of Computer-Mediated Communication, vol.13, no.1, pp 276–297, 2007.

[15] R. Harahap, S. Sutikno, and S. A. Matondang, "Digital Technology for Non-Formal Learning during the Covid 19 Pandemic," AL-ISHLAH J. Pendidik., vol. 14, no. 3, pp. 3375–3382, 2022.

[16] I. Hussain, "A Study to Evaluate the Social Media Trends among University

Students," A Study to Evaluate the Social Media Trends among University Students, vol. 64, pp. 639-645, 2012.

[17] M. K. Kabilan, N. Ahmad, and M. J. Z. Abidin, "Facebook: An online environment for learning of English in institutions of higher education?," The Internet and Higher Education, vol.13, no.4, pp.179-187, 2010.

[18] J. Waycott, J. Sheard, C. Thompson, and R. Clerehan, "Making students' work visible on the social web: A blessing or a curse?," Computers & Education. vol.68, pp. 86-95, 2013.

[19] N.R. Moşteanu, "Teaching and Learning Techniques for the Online Environment. How to Maintain Students' Attention and Achieve Learning Outcomes in a Virtual Environment Using New Technology. International Journal of Innovative Research and Scientific Studies, 4(4), 278–290, 2021.

[20] R. B. Lee, R. Baring, M. S. Maria, and S. Reysen, "Attitude towards technology, social media usage and grade-point average as predictors of global citizenship identification in Filipino University Students," International journal of Psysiology, vol.52, no.1, pp. 213-219, 2017.

[21] R. Harahap, S. Sutikno, and S. A. Matondang, "Digital Technology for Non-Formal Learning during the Covid 19 Pandemic," AL-ISHLAH J. Pendidik., vol. 14, no. 3, pp. 3375–3382, 2022.

[22] C., Troussas, A. Krouska, & C. Sgouropoulou," Impact of social networking for advancing learners' knowledge in E-learning environments". Educ Inf Technol 26, 4285–4305,2021.

[23] F. H. Yusof, M. binti, S.Z. Bakar, A. binti, D.W. Amat, D. binti, Othman, Z. binti, Sumery, binti, H. Sarijari, binti, & A. Qomariyah, "ESL Teaching: Preferences on The Use of E-Learning Apps in Maximising Effective Teaching and Learning Experiences for Open and Distance Learning (ODL)". International Journal of Academic Research in Business and Social Sciences, 11(6), 1123–1139, 2021.

[24] S. Waters, W. B. Russell, and M. Hensley, "Cyber Bullying, Social Media, and Character Education: Why It Matters for Middle School Social Studies," The Clear. House A J. Educ. Strategies. Special Issue, pp. 195-204, 2020.

[25] S. M. Azizi, A. Soroush, and A. Khatony, 'The relationship between social networking addiction and academic performance in Iranian students of medical sciences: a cross-sectional study', BMC Psychol., vol. 7, no. 1, pp. 1–8, 2019.

[26] M. Madhusudhan, "Use of social networking sites by research scholars of the University of Delhi: A study," The International Information & Library Review, vol.44, no.2, pp. 100-113, 2012.

[27] L. Dvorkin Camiel, J. D. Goldman-Levine, M. D. Kostka-Rokosz, and W. W. McCloskey, "Twitter as a medium for pharmacy students' personal learning network development," Currents in Pharmacy Teaching and Learning, vol.6, no.4, pp 463-470, 2014.

[28] M. R. Dragseth, 'Building student engagement through social media', J. Polit. Sci. Educ., vol. 16, no. 2, pp. 243–256, 2020.

[29] N. Rathika, S. Thanuskodi, and others, 'Social Networking Sites acts as a Platform for Sharing Knowledge and Creative Ideas: A Study of University Students in Tamil Nadu, India', 2020.

[30] S. Deng, J. Tong, Y. Lin, H. Li, and Y. Liu, "Motivating scholars' responses in academic social networking sites: An empirical study on ResearchGate Q&A behavior," Information Processing & Management, vol.56, no.6, pp. 1-13, 2019.

[31] G. F. D. Valdez et al., "The utilization of social networking sites, their perceived benefits and their potential for improving the study habits of nursing students in five countries," BMC Nursing, vol.19, no.52, pp. 2-14, 2020.

[32] J. Phua, S. V. Jin, and J. (Jay) Kim, "Uses and gratifications of social networking sites for bridging and bonding social capital: A comparison of Facebook, Twitter, Instagram, and Snapchat," Computers in Human Behavior, vol.72, pp. 115-122, 2017.

[33] Q. L. H. T. T. Nguyen, P. T. Nguyen, V. D. B. Huynh, and L. T. Nguyen, "Application Chang's extent analysis method for ranking barriers in the e-learning model based on multi-stakeholder decision making," Universal Journal of Educational Research, Vol.8 no.5, pp. 1759 - 1766, 2020.

[34] N. A. Adzharuddin, "The Influence of Social Network Sites (SNS) upon Academic Performance of," International Journal of Humanities and Social Science, vol. 4, No. 10(1), 2014.

[35] L. Hassan, A. Dias, and J. Hamari, 'How motivational feedback increases user's benefits and continued use: A study on gamification, quantified-self and social networking', Int. J. Inf. Manage., vol. 46, pp. 151–162, 2019.

[36] T. M. H. Li, M. Chau, P. W. C. Wong, E. S. Y. Lai, and P. S. F. Yip, 'Evaluation of a web-based social network electronic game in enhancing mental health literacy for young people', J. Med. Internet Res., vol. 15, no. 5, p. e80, 2013.

[37] U. Pfeil, R. Arjan, and P. Zaphiris, 'Age differences in online social networking – A study of user profiles and the social capital divide among teenagers and older users in MySpace', Comput. Human Behav., vol. 25, no. 3, pp. 643–654, 2009.

A Comparative Analysis for Arabic Sentiment Analysis Models In E-Marketing Using Deep Learning Techniques.

Sara Almutairi [1], Fahad Alotaibi [2]

1. faculty of computer and information technology, King Abdulaziz University, Saudi Arabia, Riyadh, 11564, smateralmutairi@stu.kau.edu.sa

2. faculty of computer and information technology, King Abdulaziz University,Saudi Arabia, Riyadh, 11564, fmmalotaibi@kau.edu.sa

Abstract

The Internet has a huge amount of information when it comes to analysis, much of which is valuable and significant. Arabic Sentiment Analysis (SA) is a method responsible for analyzing people's thoughts, feelings, and responses to a variety of products and services on social networking and commercial sites. Several researchers utilize sentiment analysis to determine the opinions of customers in various areas, including e-marketing, business, and other fields. Deep learning (DL) is a useful technology for developing sentiment analysis models to improve e-marketing operations. There are a few studies targeting Arabic sentiment analysis (ASA) in e-marketing using deep learning algorithms. Due to a number of difficulties in the Arabic language, such as the language's morphological features, the diversity of dialects, and the absence of suitable corpora, sentiment analysis on Arabic material is restricted. In this paper, we will compare several Arabic sentiment analysis models. Also, we discuss the deep learning algorithms that are employed in Arabic sentiment analysis. The domain of the collected papers is Arabic sentiment analysis in e-marketing using deep learning. Our first contribution is to introduce and present deep learning models that are used in ASA. Secondly, investigate and study Arabic datasets utilized for Arabic sentence analysis. We create and develop a new Arabic dataset for Saudi Arabian communication companies, namely Sara-Dataset, to increase the quality and quantity of their services. Third, each collected study is assessed in terms of its methodology, contributions, deep learning techniques, performance, Arabic datasets in emarketing, and potential improvements in developing Arabic sentiment analysis models. Fourth, we analyzed several papers' performance in terms of accuracy, F-measure, recall, pre-procession, and area under the curve (AUC). Also, our comparative analysis includes feature selection (e.g., domain-specific selection) methods that are used in Arabic sentiment analysis. Fifth, we also discuss how to improve Arabic sentiment analysis using preprocessing techniques (e.g., word embedding). Finally, we provide a design model for analyzing Arabic sentiment about communications services provided by Saudi Arabian enterprises.

Keywords: Deep Learning; Comparative; Arabic Sentiment Analysis; E−marketing; Accuracy; Dataset; Feature Selection; Pre−processing CNN; LSTM.

Introduction

Sentiment analysis is an artificial intelligence technique that employs techniques to analyze whether an opinion is positive or negative. It's a powerful tool in the election process and social media to classify people's opinions towards things (e.g., products) [1–3]. Sentiment analysis is recognized as a significant technology for effectively studying customers' opinions. Pre-

paring data, recognizing and identifying respondents, and evaluating findings are the primary components of sentiment analysis[4–10]. There are several studies targeting sentiment analysis in e-Marketing using deep learning algorithms. In this paper, we will conduct and analyze several studies addressing sentiment analysis in e-marketing using deep learning algorithms. First, we discuss and analyze Arabic sentiment analysis studies in e-marketing. Then, we will conduct a comparative analysis of Arabic sentiment analysis models using deep learning. The collected study is evaluated in terms of its methodology, contribution, deep learning techniques, performance, Arabic datasets, Emarketing, and potential improvements in developing Arabic sentiment analysis models. After that, we evaluated the performance of several papers in terms of accuracy, F-measure, recall, pre-procession, and area under the curve (AUC). In this paper, we will introduce a design model for Arabic sentiment analysis. We create a dataset for communications services provided by Saudi Arabian enterprises.

The rest of the paper is structured as follows: In Section 2, we present Arabic sentiment analysis and deep learning techniques, including artificial intelligence, machine learning, Arabic sentiment analysis, and Arabic datasets. Section 3 discusses ASA studies that employ deep learning, and Arabic sentiment analysis in e-marketing. In Section 4, we address comparative analysis for ASA models. Section 5 introduces a proposed design model for analyzing Arabic sentiment about communications services provided by Saudi Arabian enterprises. In Section 6, we conclude the paper and list future works.

Deep learning and sentiment analysis

In this Section, we will address the artificial intelligent, machine learning, deep learning models (CNN and LSTM), sentiment analysis, Arabic sentiment analysis, and our created Arabic dataset.

Artificial intelligence and machine learning

Artificial intelligence (AI) is the simulation of human intelligence processes by computer systems. There are many applications of AI, including speech recognition, natural language processing, expert systems, handwriting recognition, and robotics [11].

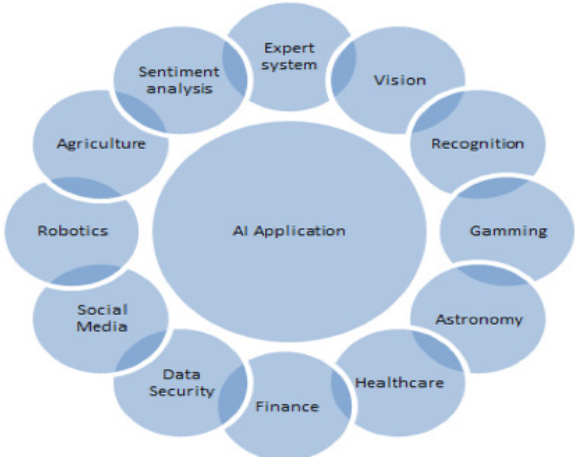

Fig. 1. AI applications

As shown in Fig. 1, AI has different applications such as sentiment analysis, robotics, and gaming. In this paper, we will focus on sentiment analysis. Machine learning and deep learning are parts of AI.

Machine learning: The challenge of text categorization with syntactic or linguistic

characteristics It is part of artificial intelligence that is used to classify objects and things Machine learning is classified as supervised, unsupervised, or hybrid [12]:

Supervised learning: supervised learning is a sort of machine learning technique that makes predictions using a data set called the training data set. These data sets include both input and response values. It makes use of a high number of variables in supervised learning methods. Several techniques exist depending on their work on classification, such as classification trees, fuzzy logic, Naïve bayes network, genetic algorithms, neural networks, and support vector machine.

Unsupervised learning: This is a unique form of machine learning that is utilized in most situations to draw varied conclusions from data groups made up of input data with no labeled responses. When labeled training papers are unavailable, this method is utilized. Dividing the graph or data into groups—each group is called a cluster—makes it easier to analyze. Each cluster consists of elements that are similar. Clustering techniques can detect groups without prior knowledge or previous groups (the original data is unclassified, so it is considered unsupervised learning), and there are several cluster approaches used such as k-means, k-medoids, EM clustering, and outlier detection algorithms.

Deep learning algorithms

Deep learning is machine learning that enables computers to learn to perform classification methods directly from images, text, or voice. We will explain the convolutional neural network and long short-term memory architecture.

Convolutional Neural Network (CNN)

The Convolutional Neural Network is one of the most well-known and often utilized deep learning networks. CNN is a type of deep learning architecture or multilayer neural network. CNN is a neural network with several hidden layers, each of which has a number of two-dimensional planes filled with many neurons. Where the feature extraction module integrated into the CNN architecture is concerned, each neuron operates independently [13]. Fig. 2 depicts a CNN architecture.

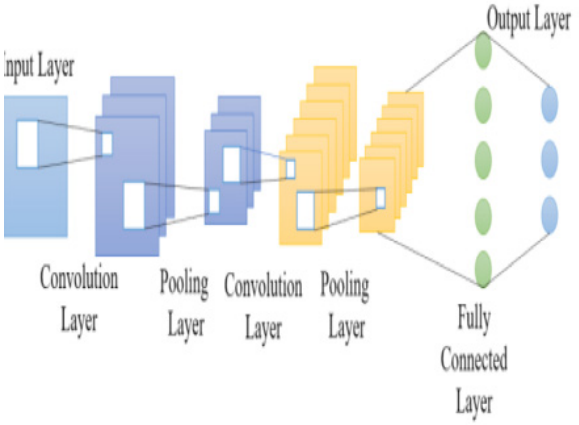

Fig. 2. CNN architecture [13]

CNN architecture includes:

- Input layer: The input layer can accept the input raw data set directly, where, the pixel values of one image are considered the input layer of CNN.
- Convolutional layer: It is composed of several convolutional filters. The output feature map is created by convolving the input picture, which is ex-

pressed as N-dimensional metrics.

- Pooling layer: It is also known as the down-sampling layer. Its primary purpose is to complete the second feature data extraction before moving on to the convolution layer.
- Fully connected layer: All the features maps are connected as inputs in this fully connected layer. The nodes of the neurons in the later layer are connected to the nodes of the neurons in the previous layer in general, but the nodes of the neurons in each layer are unconnected.
- Output layer: The number of neurons required for classification is usually proportional to the number of types to be identified.

Long Short-Term Memory

The LSTM architecture is regarded as a recurrent neural network (RNN) that was developed to overcome the limitations of the conventional RNN in terms of developing long-term dependencies. The parts of the LSTM unit are the gate, memory cell, output, and input gate, as shown in Fig. 3. The extra gates are in charge of regulating the flow of data into and out of the cell, while the memory cell is responsible for retaining values over time. Specifically, Fig 3 reports two architectures of LSTM. First, in Fig 3.a, an LSTM with a memory cell and two gates is shown. Figure 3.b, on the other hand, depicts an LSTM with a memory cell and a forget gate. Besides, one input layer, one output layer, and one self-connected hidden layer make up an LSTM cell. It is possible that the concealed unit contains basic units that can be fed into successive LSTM cells [14].

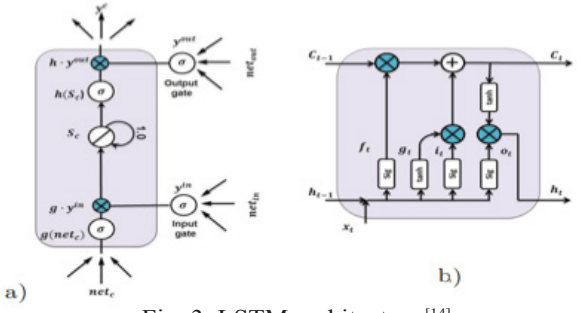

Fig. 3. LSTM architecture [14]

Arabic Sentiment Analysis (ASA)

SA is the automated extraction of expressed concepts from a given text. Using traditional techniques for managing and analyzing huge amounts of data is considered a critical challenge. The researchers developed an effective approach for studying and managing people's opinions on social media called sentiment analysis

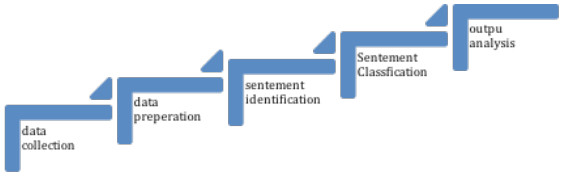

Fig 4. Sentiment analysis model.

As depicted in Fig. 4, sentiment analysis consists of data collection, data preparation, identification, classification, and output analysis. The collecting data stage involves collecting data from social media about the domain problem. Then the data is cleaned to be suitable for the classifier. Then the classifier will categorize the data as positive or negative.

Effective data science methodologies are used to classify a person's feelings and sentiments on social media. Data science is an interdisciplinary field that makes use of scientific methods, procedures, and algorithms to extract attitudes from tweets

on Twitter. The classification of emotions has a key role in many application domains, including marketing, and business sectors can develop appropriately with the help of human emotions. Numerous methods, including deep learning, neuro-fuzzy, and optimization algorithms, are used to extract and classify sentiment [15].

Twitter provides a very important platform for speech and ideas. The users can discuss a wide range of occasions, products, and e-marketing strategies. There are several studies focusing on customer opinions toward products and the public's thoughts and attitudes toward a certain quality or a specific product [10, 16, 17, 18]. Nhan et al.[8] suggest that modern computational linguists have not paid enough attention to the Arabic language. They used sentiment analysis on social networks, which is a critical strategic technique for learning about customer interests. The main challenges, on the other hand, are efficiency, accuracy, and time consumption.

ASA datasets

They mention several limited datasets collected from Twitter, webpages, and blogs. OCA, LABR, and NA are examples of Arabic datasets. Also. In this subsection, we will explain most famous datasets and our created dataset called Sara-dataset

- OCA (Opinion Corpus for Arabic): this Arabic Corpus includes 500 film reviews, 250 good and a lot of bad, gathered from various Arabic online pages and blogs. It's only available in a limited size and for a certain film domain.
- LABR (a large scale Arabic book reviews dataset): is Arabic dataset contains over 63,000 book reviews have been written and graded on a scale of one to five stars. It applies only to a certain domain.
- NA: is an Arabic dataset which is used for Arabic sentiment analysis and contains a huge multi-domain dataset (33K annotated reviews for movies, hotels, restaurants, and products).
- Arabic Health Services Dataset (AHSD): This dataset contains over 2,000 posts, but the number of negative and positive records is not equal. This information relates to medical services in the context of health care.
- Arabic Twitter Dataset (ArTwitter): its politics datasets collected from Twitter social media. This dataset has thousands of records with balanced data.
- The Arabic Sentiment Tweets dataset (ASTD) was compiled. Twitter consists of fifty-four thousand Arabic tweets. It is an unbalanced dataset. It has 2479 tweets, distributed into positive and negative posts.
- *Our dataset, "Sara-Dataset".* We develop a new Arabic dataset for three Saudi Arabian communication firms to improve the quality and quantity of their services by collecting customer feedback. We selected three firms, which are Zain, Mobily, and Saudi Telecom (STC). We are targeting Twitter. We applied several preprocessing techniques, such as removing re-tweets, removing diacritics, removing punctu-

ations, removing repeating characters, normalization, removing URLs, creating word tokens and removing them, and removing Arabic stop words. Our dataset consists of 32336 tweets. After preparation, it becomes 20,000 tweets. Fig. 5 shows that Zain company take around 14000 tweets.

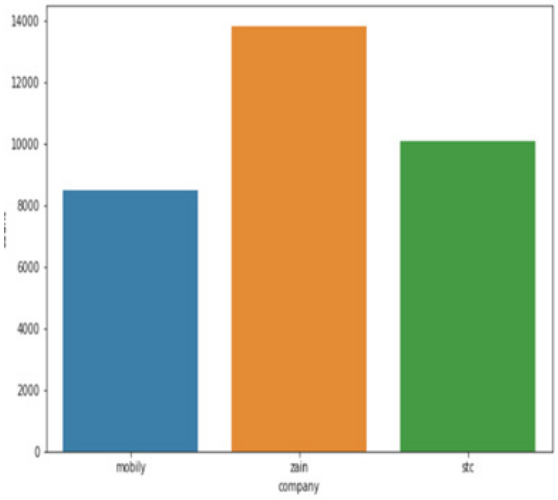

Fig 5. The distribution of tweets amongst companies.

The features of our dataset are (id, text, created_at, author_id, language, city, is_retweet, company, followers_count, tweet_count, listed_count, name, and Label). Table 1 displays a tweet sample from our dataset.

Table 1. Displays a tweet sample features

id	1.55365E+18
text	"السلام عليكم انترنت زين حاليا ضعيف جدا وبفر وثقيل ويعلق وبه عطل الان زين فايبر والبنق جدا سيء"
language	Arabic
city	Riyadh
company	Zain

ASA studies using Deep learning

There are several studies targeting ASA models using deep learning, such as:

Deep learning in ASA

Nassif et al. [1] introduce a full survey about using deep learning techniques in Arabic sentiment analysis. They selected papers from journals, conferences, and workshops in the field of Arabic sentiment analysis using deep learning techniques. The fields of collected datasets are marketing, social media, news, healthcare, education, business, politics, sport, and economics. The sources of the collected datasets are Wikipedia and blogs, news pages, online comments, Facebook, product reviews, and Twitter. Twitter is the most popular source, with 55 papers using it to generate datasets. Convolutional Neural Network (CNN), Long Shot Term Memory (LSTM), Deep Belief Network (DBN), Gated Recurrent Unit (GRU), Recursive Auto Encoder (RAE), Artificial Neural Network (ANN), Hierarchical Bidirectional LSTM (HBiLSTM), Bidirectional LSTM (BiLSTM), Bidirectional GRU (BiGRU), and Deep Neural Network (DNN) are used to perform sentiment analysis in Arabic.

Al-Ayyoub et al. [2] introduce numerous studies focusing on sentiment analysis in Arabic. There are few studies in Arabic SA, as depicted in Table 2.

Table 2. Arabic sentiment analysis published during 2010-2018

Year	# number of papers
2010-2012	Around 28 papers
2013-2016	Around 175 papers
2017-2018	Around 125 papers

Abbasi et al. [4] merge Arabic and English sentiment analysis. They are targeting binary SA problems in Web Forum (WF) postings related to English and Arabic. Each post is classified as supporting or not supporting labeling on a given issue. They use extraction and selection feature methods. They used a root extraction algorithm. They offered pre-processing features (e.g., word n-grams) in English text. They used heuristic data for ranking features, which has better performance than a genetic algorithm (GA). They used the Support Vector Machines (SVM) classifier to test the performance of their technique on a couple of small datasets, each including thousands of postings written in a mixture of languages. The experimental results using an entropy-weighted genetic algorithm with SVM achieve accuracy of over 91% on the 83 benchmark datasets in English and Arabic forums.

Guellil et al. [3] do a survey about sentiment analysis, which is used to classify and identify the sentence as a positive sentence or not. The collected study uses three approaches: a lexicon-based approach, a corpus-based approach, and a hybrid approach. Two of the most serious issues confronting the ASA are the diversity of dialects and the scarcity of Arabic resources. This study focuses on the most recent work, with the period of collected papers being between 2015 and 2019.

Medhaffar et al. [5] used three supervised machine-learning methods: support vector machine (SVM), Naive Bayes (NB), and MultiLayer-Perceptron (MLP) algorithms. They used the Python language, extracting their features using the Doc2Vec tool to classify the text as positive or negative. They evaluate the performance of the three models (SVM, NB, and MLP) in classifying the text as positive or negative in terms of accuracy, precision, and recall. The MLP achieves more than 78% accuracy, which is better than the other two algorithms. They achieved an error rate of 0.23, 0.22, and 0.42 using SVM, MLP, and binary NB, respectively. SVM has a precision of 76%, while BNB has a precision of 60%, and MLP has a precision of 78%. Alayba et al. [7] used a combination of CNN and LSTM to improve the accuracy of sentiment classification of short messages taken from Twitter as positive or negative. They used many data sets, such as Main-AHS, SubAHS, Ar_Twitter, and ASDT. Then, by applying the deep learning combination algorithms, which are CNN and LSTM, they achieve accuracy as shown in Table 3.

Table 3. ASA models using Arabic dataset

Dataset Description	Algorithms	Accuracy
Arabic Health Services Dataset	CNN+L-STM	94.24%
Arabic Health Services Dataset	CNN+L-STM	95.68%
Arabic Twitter Dataset (ArTwitter)	CNN+L-STM	88.10%
Arabic Sentiment Tweets Dataset (ASTD)	CNN+L-STM	77.62%

Alayba et al. [7] introduce an Arabic-language dataset containing opinions on healthcare services that was gathered via Twitter. The dataset consists of 2026 tweets. where they show how to acquire data from Twitter as well as how to filter, preprocess,

and annotate Arabic text to create an Arabic sentiment analysis dataset. They show how to acquire data from Twitter as well as how to filter, preprocess, and annotate Arabic text to create an Arabic sentiment analysis dataset. They used modern, standard Arabic dialects. They used machine learning and deep learning algorithms. They used multinomial NB, Bernoulli NB, LR, linear support vector, stochastic gradient descent, and nu-support vector as machine learning algorithms. Also, they used CNN and DNN as deep learning algorithms. Table 4 shows that multinomial NB, SVM, LSV, stochastic gradient descent, and DNN achieve over 90% accuracy in the classification of health services as positive or negative, as depicted in Table 4.

Table 4. Machine and deep learning algorithm in healthcare ASA.

Algorithm	Type	Accuracy
Multinomial NB	Machine learning	90.14%
Bernoulli NB	Machine learning	89.16%
LR	Machine learning	86.94%
Support Vector machine	Machine learning	90.88%
LSV	Machine learning	91.37%
Stochastic Gradient Descent	Machine learning	91.87%
Nu-Support Vector	Machine learning	87.82%
CNN	Deep learning	85%

According to Maha et al. [9], improving Arabic sentiment accuracy is considered an open problem. They used deep learning to improve Arabic sentiment analysis. Additionally, they explain the difficulties that face Arabic language accuracy. They used convolutional neural networks and long short-term memory models to predict the sentiment of Arabic tweets, but they did not achieve high accuracy. To classify the sentiment of Arabic tweets, they used ensemble models that combined CNN and long-short-term memory models. The CNN has an accuracy of 64.30 and an F1 of 64.09. LSTM has a dropout rate of 0.2, an accuracy of 64.75%, and an F1-score of 62.08%. The accuracy of the ensemble model is 65.05%, and the F1-score is 64.46%. They obtained the dataset from Twitter and prepared it using the following methods: Dates, numbers, and URLs are removed. Emojis are separated by a space to be treated as words, and diacritics and elongation are removed.

Altaher et al. [19], make shifting from traditional techniques to deep learning algorithms. They used stop-word and stemming as pre-processing methods and they used feature and information gain as feature weighting. Then, applying a deep learning algorithm to effectively and accurately classifies Arabic tweets either as positive or negative tweets. We collected a dataset consisting of 500 Arabic tweets, and the tweets mainly discuss general topics about education. the feed-forward architecture as deep learning. The accuracy when using deep learning is 90%. Using SVM, DT, neural network they accuracy are 85%, 67%, and 80%, respectively.

Khalil et al. [20], introduce semantic classification for multi-label Arabic emotion analysis (e.g., annoyed, happy and angry). They presented an optimized Bidirectional LSTM network. Where they used four optimizer techniques, which are Adam,

Adamax, Nadam, and RMSpro. They used word embedding models for pre-processing. They used Task E-c: Detecting Emotions (multi-label classification) dataset. Where this task contains 2278 tweets for training, 585 tweets for development, and 1518 tweets for test data.

Manshu et al. [21], they used the Amazon dataset for books, electronics, kitchen domain. They apply CNN deep learning algorithm to measure the sentiment analysis via products. They achieve accuracy 81.98%. They use a new method of feature selection method where they combine between domain feature specification and domain independent features.

ASA in E-marketing

Several studies are targeting marketing and business analysis [15] [22-25]. In [15] Stock market investment is a significant aspect of every country's economy. Market research is an important part of making an investment in that filed. The SA is applied into market data, where these data are collected and per-processed before training and testing. This will assist investors in predicting where their money should be placed in the stock market, as well as in preserving the market's economic equilibrium.

The goal of Rosool et al. [10] is to determine what the public thinks about the top two worldwide apparel companies and compare the positive and negative sentiments of everyday consumers toward each one. It was found that positive reviews of Adidas are higher than those of Nike. While the neutral values record the satisfaction level among the online Twitter users for both brands, which is more than 60% of total reviews as depicted in Table 5,

Table 5. People opinions about Nike and Adidas products

Nike			Adidas		
Positive	Negative	Neutral	Positive	Negative	Neutral
24.5%	11.9%	63.6%	27.2%	11.7%	61.1%

Elzayady et al. [26], using traditional machine learning and deep learning algorithm in sentiment analysis. They used machine learning algorithm in sentiment analysis, which are KNN and DT. They used two Arabic datasets, which are HTL (hotel review) and LBAR (book review). The experimental results showed that there is no correlation between classifier and N-gram for feature representation. The best result in accuracy is 76.6% using the KNN algorithm with the HTL dataset. Using the NB algorithm with the LABR dataset and bigram features achieves an accuracy of 81.1%. On the other hand, using deep learning Using the HTL dataset, the accuracy is 85.38%; using the LABA dataset, the accuracy is 86.88%.

Al-Bayati et al. [27] mention that deep learning models have been provided to address and solve the Arabic sentiment analysis problem. They develop a sentiment analysis model using the LSTM deep learning algorithm. This model may be used to forecast Arab reactions to current political events, making this a crucial sector in decision-making. In commercial and marketing, where, Arabic enterprises and others

sell their products to Arab consumers, they would gain from such a project since it would allow them to automatically collect feedback on their products and services to improve them.

They used Large-Scale Arabic Book Reviews (LABR), then selected a deep neural network, which is the LSTM. Converting texts to sequence numbers using word embedding method. Finally, the outputs of the LSTM layer are given to the SoftMax layer, which normalizes them and classifies the emotion of the input text as positive or negative. The experimental results show that the best accuracy and F-score are achieved when the hyperparameter LSTM out is set to 50 and the batch size is 256, where the accuracy is 82% and the F-score is 81.6%.

Yadav et al. [28], mention that social media is a strong tool for individuals to communicate their feelings in the form of thoughts and viewpoints. Marketing should research and analyze people's emotions and reactions to products.

Al-Bayati et al. [27], introduce a comprehensive overview of the most widely used deep learning models in sentiment analysis. They present a sentiment classification taxonomy and explore the consequences of common deep learning architectures, which are convolutional neural networks, recursive neural network, recurrent neural network (LSTM and gated recurrent units), and deep belief networks. They also highlight the most Arabic datasets used by deep learning to develop Arabic sentiment analysis models, which are the Stanford large movie review (IMDB), Yelp dataset, Stanford sentiment treebank (SSTb), Amazon review dataset, CMUMOSI, MOUD, Getty Images, Twitter Dataset, and Twitter Image Dataset. They mention the applications where sentiment analysis is performed, which are crime prediction, politics, business review analysis, business review, and financial market prediction. Also, they introduce the drawbacks of using deep learning for Arabic sentiment analysis. Whereas the main disadvantage is ensuring that the ASA provides the expected results. DL algorithms need a large amount of labeled data for training. In addition, some deep learning algorithms need to restart their parameters from the starting point, which incurs overhead in terms of time.

Comparative analysis for ASA models

In this section, we introduce a comparative analysis for Arabic sentiment analysis using a deep learning algorithm. We will analyze other researchers' reflections on our research. Then we are going to keep listing all the technologies used in developing ASA models.

Researches reflection on our research

In our research, we will focus on sentiment analysis to analyze people’s opinions about e-marketing products. Previous techniques suffered from low performance and accuracy when dealing with large datasets. Additionally, researchers do not compute the time complexity when the dataset becomes large. These problems will be solved in our proposed model, in addition to improving the company’s sales through the analysis of

online product reviews. Tables 6.a and 6.b show machine learning and deep learning algorithms, accuracy, and enhancements that can be made in developing ASA models. Also, Table 6b shows research reflections on our work.

Table 6.a Deep learning algorithms and its reflection for our research

Paper Number	Year	Dataset source	Algorithms
[29]	2016	From Twitter. consisting of 1103 tweets (576 as positive and 527 labeled as negative	Lexical+ SVM.
[26]	2016	HTL and LABR which belongs to book rating	CNN+LSTM
[19]	2017	Arabic tweets are collected that consisting of 500 tweets related for education area	DT and SVM as traditional machine learning and the feed forward architecture as deep learning
[9]	2018	Arabic Sentiment Tweets Dataset (ASTD).	CNN is coupled with LSTM
[30]	2019	Twitter Arabic Hotels reviews	(LSTM) and Bidirectional LSTM
[20]	2021	SemEval 2018) contains 4372 tweets, which are organized into three categories: training, development, and testing	Bidirectional LSTM

Table 6.b Deep learning algorithms and its reflection for our research

Paper Number	Accuracy	Reflection	Enhancements
[29]	84.01%	we will usedeep learning with large dataset	Hybrid algorithm enhance the accuracy of semantic analysis The data set is small
[26]	Using HTl dataset, the accuracy is 85.38%. Using LABA dataset, the accuracy is 86.88%	Several papers using combination of CNN and LSTM	The accuracy is increased when using deep learning algorithm. And we must increase the datasets
[19]	Using deep learning accuracy 90%. using SVM 85'%	Deep learning algorithm outperform machine learning algorithm	Deep learning with weighting characteristic need time consuming
[9]	65.05% using ensemble learning	Ensemble learning can enhance the accuracy of ASA	accuracy has to be improved
[30]	82.6%	When dealing with huge dataset, the RNN has the overfitting problem	Solving overfitting problem
[20]	75.5% accuracy for validation and 49.8% for testing	SemEval is considered as large scale	accuracy has to be improved

Studies analysis

We can conclude that the researchers develop Arabic sentiment analysis using several types of Arabic datasets, and machine-learning, deep learning algorithms. combination between deep learning algorithms.

- Arabic datasets: Most studies are collecting datasets from Twitter web pages, newspapers, and blogs to form Arabic corpora, then making pre-processing to

enhance the optimization. Also, some researchers develop a sentiment analysis model using datasets such as HTL for hotel reviews and LABR for book ratings. Main-AHS, Sub-AHS, Ar-Twitter ASDT (Arabic Sentiment Tweets Dataset), and Human-Annotated Arabic Dataset (HAAD) are also available in ASA. Stanford large movie review (IMDB), Yelp dataset, Stanford sentiment treebank (SSTb), Amazon review dataset, CMU-MOSI, MOUD, Getty images, Twitter dataset, and Twitter image dataset.

- Machine learning: Traditional machine learning includes supervised algorithms, unsupervised algorithms, and hybrid algorithms (supervised and unsupervised).
- Deep learning. Researchers use deep learning with different architectures.
- Combinations between deep learning algorithms such as CNN and LSTM increase the accuracy of ASA.
- Ensemble learning merges several learners to enhance the detection rate and performance accuracy. We will use ensemble-learning techniques such as bagging (randomly selected training data) or boosting (focusing on enhancing incorrect classification instances).
- Also, researchers are using several preprocessing techniques, such as
- Word Embedding
- Normalization, stop-word removal, negation terms and stemming
- Tokenization and segmentation of tweets.
- Spelling Correction.

There are several Arabic sentiment analysis levels such as:

- Sentence level
- Document level
- Phrases level
- Multidimensional level
- Multimodal level

Proposed Model

Our proposed model's key contribution is the development of Arabic sentiment analysis to gauge consumer perception of Saudi Arabian communication companies in order to increase the quality and quantity of their services through gathering client feedback. After we created our Arabic dataset, Sara-Dataset, our proposed work is to develop Arabic sentiment analysis for Saudi Arabia's opinions toward Saudi communication enterprises. As mentioned in the dataset section, the size of the datasets is small. Our model will use a large dataset, as mentioned in Section 2. Our model will select the best preprocessing, feature selection, and deep learning methods. We will enhance model accuracy using ensemble learning. As depicted in Fig. 6, our design model consists of the following steps:

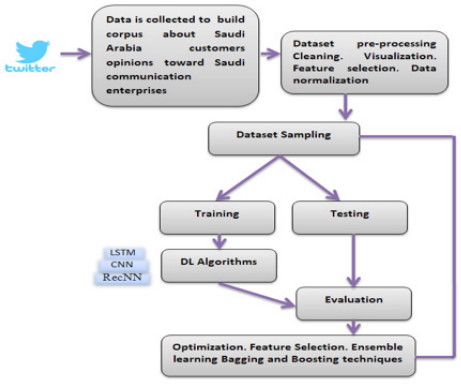

Fig. 6. Our proposed ASA model

1. Collecting dataset. We collected Sara-database from Twitter to build a corpus about Saudi Arabia's customers' opinions toward Saudi communication enterprises.
2. Pre-processing. This step is responsible for cleaning data, normalization, and identifying features. In this step we used several techniques such word embedding, filtering technique, normalization, stop-word removal, negation terms and stemming, tokenization and segmentation of tweets and spelling correction
3. Sampling. To generate a random sample for training and testing, the dataset is divided into K-fold cross validation.
4. Evaluation. Our model will be evaluated in terms of accuracy, precision, recall, f-measure, and area under the curve. Also, improving the quality and quantity of a company's services through customer feedback
5. Optimization. We will enhance our model in terms of feature selection methods and using bagging and boosting ensemble learning techniques. There are several issues related to our proposed ASA models. First, the main limitations of our model are the scarcity of Arabic resources and the fact that we do not cover all Arabic dialects. Second, we will combine several deep learning algorithms to enhance accuracy. Third, we will use bagging and boosting ensemble-learning techniques. Also, we will try using SMOTEDNN (Synthetic Minority Oversampling Technique with Deep Neural Network) to address air pollution classification [31]. SMOTEDNN was created to classify air pollution, and its accuracy is 99.90%. Finally, we'll try to apply transformer deep learning, which has a higher accuracy rate than deep learning [32].

Conclusion and Future Works

Several studies pertain to English sentiment analysis. Due to the difficult structure of Arabic language, Arabic sentiment analysis has several limitations and restrictions. This paper conducts a comparative analysis of Arabic sentiment analysis using deep learning. The domain of the collected papers is Arabic sentiment analysis in e-marketing using deep learning. The comparative metrics are: contribution of papers, deep learning techniques, performance, Arabic datasets, and potential improvements in developing Arabic sentiment analysis models. There is a shortage of Arabic sentiment datasets compared to English. One of the primary results of this analysis is that there is still a huge need for substantial research to acquire a better knowledge of Arabic dialects. There is no Arabic sentiment analysis model that can accurately handle all Arabic dialects. This has created a large gap in our understanding of ASA that researchers will try to fill in future research. Due to its complicated structure, numerous dialects, and scarcity of resources, the Arabic language has a number of constraints. Although the accuracy of Arabic sentiment analysis has increased using a deep learning model, there is still potential for improving accuracy.

A large Arabic dataset that we created belonged to a Saudi Arabia n communication corporation. Consequently, the aim of our future work is to develop a sentiment analysis model by incorporating deep learning techniques into our dataset. To improve the accuracy of our proposed Arabic sentiment analysis model, we must select the best preprocessing, feature selection, and deep learning methods for our dataset.

Conflict of Interest

The authors declare no conflict of interest

Acknowledgements

I thank all who in one way or another contributed in the completion of this thesis. First, I give thanks to God for protection and ability to do work. My special and heartily thanks to my supervisor, Professor Fahad Alotaibi who encouraged and directed me. His challenges brought this work towards a completion. It is with his supervision that this work came into existence. For any faults I take full responsibility. I also thank my family who encouraged me and prayed for me throughout the time of my paper.

References

[1] Nassif, Ali Bou, Ashraf Elnagar, Ismail Shahin, and Safaa Henno “Deep learning for Arabic subjective sentiment analysis: Challenges and research opportunities.” Journal of Applied Soft Computing 98 (2020): 106836.

[2] Al−Ayyoub, M., Khamaiseh, A. A., Jararweh, Y., & Al−Kabi, M. N. (2018). “A comprehensive survey of arabic sentiment analysis.” Journal of Information processing management, 56 (2019): 320-342.

[3] Guellil, Imane, Faical Azouaou, and Marcelo Mendoza. "Arabic sentiment analysis: studies, resources, and tools." Social Network Analysis and Mining 9.1 (2019): 1-17.

[4] Abbasi, Ahmed, Hsinchun Chen, and Arab Salem. "Sentiment analysis in multiple languages: Feature selection for opinion classification in web forums." ACM transactions on information systems (TOIS) 26.3 (2008): 1-34.

[5] Mdhaffar, S., Bougares, F., Esteve, Y., & Hadrich-Belguith, L. (2017, April). Sentiment analysis of tunisian dialects: Linguistic ressources and experiments. In Third Arabic Natural Language Processing Workshop (WANLP) (pp. 55-61).

[6] Alayba, Abdulaziz M., Vasile Palade, Matthew England, and Rahat Iqbal. "A combined CNN and LSTM model for arabic sentiment analysis." In International cross-domain conference for machine learning and knowledge extraction, pp. 179-191. Springer, Cham, 2018.

[7] Alayba, Abdulaziz M., Vasile Palade, Matthew England, and Rahat Iqbal. "Arabic language sentiment analysis on health services." In 2017 1st international workshop on arabic script analysis and recognition (asar), pp. 114-118. IEEE, 2017.

[8] Abdullah, Malak, and Mirsad Hadzikadic. "Sentiment analysis on arabic tweets: Challenges to dissecting the language." International Conference on So-

cial Computing and Social Media. Springer, Cham, 2017.

[9] Heikal, Maha, Marwan Torki, and Nagwa El-Makky. "Sentiment analysis of Arabic tweets using deep learning." Procedia Computer Science 142 (2018): 114-122..

[10] Rasool, Abdur, et al. "Twitter sentiment analysis: a case study for apparel brands." Journal of Physics: Conference Series. Vol. 1176. No. 2. IOP Publishing, 2019.

[11] Zhang, Yudong, Saeed Balochian, Praveen Agarwal, Vishal Bhatnagar, and Orwa Jaber Housheya. "Artificial intelligence and its applications." Mathematical problems in Engineering 2014 (2014).

[12] Ang, Jun Chin, Andri Mirzal, Habibollah Haron, and Haza Nuzly Abdull Hamed. "Supervised, unsupervised, and semi-supervised feature selection: a review on gene selection." IEEE/ACM transactions on computational biology and bioinformatics 13, no. 5 (2015): 971-989.

[13] A. Khan, Sohail, A., Zahoora, A. Qureshi," A survey of the recent architectures of deep convolutional neural networks" Artificial Intelligence Review, 53(8), 2020, pp. 5455–5516. doi:10.1007/s10462-020-09825-6.

[14] F. Kratzert, D. Klotz, C. Brenner, K. Schulz, M. Herrnegger,"Rainfall–runoff modelling using long short-term memory (LSTM) networks. Hydrology and Earth System Sciences", 22(11), pp. 6005-6022, 2019.

[15] Bhardwaj, Aditya, Yogendra Narayan, and Maitreyee Dutta. "Sentiment analysis for Indian stock market prediction using Sensex and nifty." Procedia computer science 70 (2015): 85-91.

[16] Berthon, Pierre R., et al. "Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy." Business horizons 55.3 (2012): 261-271.

[17] Chen, Liang-Chu, Chia-Meng Lee, and Mu-Yen Chen. "Exploration of social media for sentiment analysis using deep learning." Soft Computing 24.11 (2020): 8187-8197.

[18] Revathy, G., Saleh A. Alghamdi, Sultan M. Alahmari, Saud R. Yonbawi, Anil Kumar, and Mohd Anul Haq. "Sentiment analysis using machine learning: Progress in the machine intelligence for data science." Sustainable Energy Technologies and Assessments 53 (2022): 102557.

[19] Altaher, Altyeb. "Hybrid approach for sentiment analysis of Arabic tweets based on deep learning model and features weighting." Int. J. Adv. Appl. Sci 4.8 (2017): 43-49.

[20] Khalil, Enas A. Hakim, Enas MF El Houby, and Hoda Korashy Mohamed. "Deep learning for emotion analysis in Arabic tweets." Journal of Big Data 8.1 (2021): 1-15.

[21] Manshu, Tu, and Wang Bing. "Adding prior knowledge in hierarchical attention neural network for cross domain sentiment classification." IEEE Access 7

(2019): 32578-32588.

[22] Napitu, F., Bijaksana, M. A., Trisetyarso, A., & Heryadi, Y. (2017, November). Twitter opinion mining predicts broadband internet's customer churn rate. In 2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) (pp. 141-146). IEEE.

[23] Xu, Feifei, and Vlado Keelj. "Collective sentiment mining of microblogs in 24-hour stock price movement prediction." 2014 IEEE 16th conference on business informatics. Vol. 2. IEEE, 2014.

[24] Zvarevashe, Kudakwashe, and Oludayo O. Olugbara. "A framework for sentiment analysis with opinion mining of hotel reviews." 2018 Conference on information communications technology and society (ICTAS). IEEE, pp1-4, 2018.

[25] Singla, Zeenia, Sukhchandan Randhawa, and Sushma Jain. "Statistical and sentiment analysis of consumer product reviews." 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017. Pp1-6.

[26] Elzayady, Hossam, Khaled M. Badran, and Gouda I. Salama. "Arabic Opinion Mining Using Combined CNN-LSTM Models." International Journal of Intelligent Systems & Applications 12.4 (2020).

[27] Al-Bayati, Abdulhakeem Qusay, Ahmed S. Al-Araji, and Saman Hameed Ameen. "Arabic sentiment analysis (ASA) using deep learning approach." Journal of Engineering 26.6 (2020): 85-93.

[28] Yadav, Ashima, and Dinesh Kumar Vishwakarma. "Sentiment analysis using deep learning architectures: a review." Artificial Intelligence Review 53.6 (2020): 4335-4385.

[29] Aldayel, Haifa K., and Aqil M. Azmi. "Arabic tweets sentiment analysis–a hybrid scheme." Journal of Information Science 42.6 (2016): 782-797.

[30] Al-Smadi, Mohammad, Bashar Talafha, Mahmoud Al-Ayyoub, and Yaser Jararweh. "Using long short-term memory deep neural networks for aspect-based sentiment analysis of Arabic reviews." International Journal of Machine Learning and Cybernetics 10, no. 8 (2019): 2163-2175.

[31] Haq, Mohd Anul. "Smotednn: A novel model for air pollution forecasting and aqi classification." Computers, Materials and Continua 71 (2022): 1.

[32] [32] Adoma, Acheampong Francisca, Nunoo-Mensah Henry, and Wenyu Chen. "Comparative analyses of bert, roberta, distilbert, and xlnet for text-based emotion recognition." In 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 117-121. IEEE, 2020.

A Framework for Cybersecurity Awareness in Saudi Arabia.

Mead Rashed Albediwi [1], Kishwar Sadaf [2]

1. Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia, 411203859@s.mu.edu.sa

2. Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia, k.sadaf@mu.edu.sa

Abstract

The rapid advancement in technology has improved people's lives, but it has also increased the risks that come with using the Internet, including cybercrimes. Lately, Saudi Arabia, a booming economy, has become one of the prime targets of cyberattacks. The massive amount of cyberattacks targeting Saudi Arabia can be attributed to the lack of cybersecurity awareness among Saudi people. The objective of this study is to propose methods on the national level to increase the awareness of cybersecurity among Saudi people. We conducted a cybersecurity assessment survey to assess the cybersecurity awareness among Saudi people. The survey result indicated negligent behavior and lack of awareness. To address this issue, we proposed a cybersecurity awareness framework which targets all strata of Saudi Arabia demography. The proposed framework not only emphasized training programs in schools, universities and organizations but also addresses the awareness issue in people from informal backgrounds. The framework also includes the importance of incident response and its role in reducing incidents.

Keywords: Cybersecurity; Cybersecurity Awareness; Cybersecurity Framework.

Introduction

Cyberattacks are on the rise, and Saudi Arabia ranks second in terms of attacks, as the Kingdom issued an order to establish a specialized body in the field of cyber security to protect infrastructure from potential attacks. Internet users are on the increase which leads to an increase in cyberattacks and has caused financial losses. And if we compare between year 2019 and 2020, the statistics show an increase of 71% cyberattacks (Fig. 1) [1]. It shows the top ten sectors targeted in the first quarter of 2020. Therefore, there is a need for awareness programs because of their importance in raising the culture of smart users. Cybersecurity awareness has several definitions, including: "security awareness is the continuing learning and recognition of the importance of information security issues and the level required to achieve good security awareness and knowledge of individuals' security duties". Another definition of security awareness is "the knowledge and commitment of users to their security mission". These definitions of awareness do not include important elements like graduality and the process of progression which are important in any training. Authors in [2] defined awareness as the security knowledge that was gradually acquired during continuous and attractive training.

The Kingdom of Saudi Arabia is a target for many cyberattacks, due to the digital transformation and the use of technology

in most areas. According to many reports, Saudi Arabia is the most vulnerable Gulf country to malicious cyberattacks which calls for the need for a strong structure for cybersecurity. Among the attacks that targeted the Kingdom, the attack on Saudi Aramco was well known. Saudi Aramco was exposed to multiple cyberattack attempts, including the Shamoon virus, which paralyzed computers by scanning the disks. Many attacks were targeted towards Saudi ministries and institutions [3].

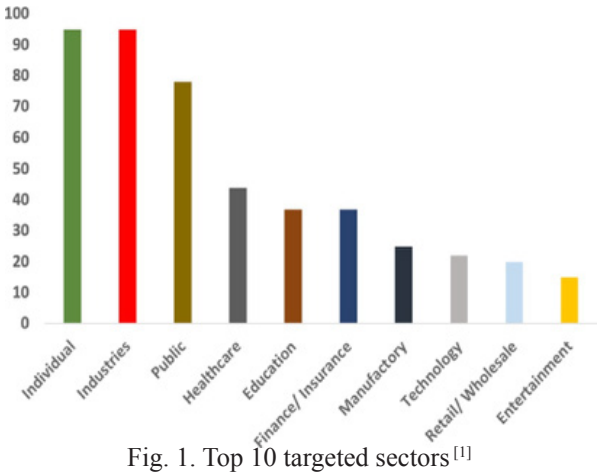

Fig. 1. Top 10 targeted sectors [1]

Irrespective of the high level of cybersecurity, naïve users can cause massive damage to their data as well as to the system. Therefore, awareness about the risks associated with internet technologies must be made prevalent among people to reduce the avenues of attacks. There are many studies [4], [5],[6], and [7] etc. on cybersecurity and how to activate awareness programs to raise awareness of cyber security in more than one way, but there is still a gap between Internet users and cybersecurity. The main reason is the user's lack of awareness, which leads to the attacker exploiting his weaknesses, as well as due to employee negligence in following the policies described in the organization, which leads to the continuation of cyberattacks, and this does not mean that the losses are limited to the physical aspect only, but include the loss of personal data. Cybersecurity is a growing concern in Saudi Arabia, as the country continues to develop its digital infrastructure and relies increasingly on technology. However, the country still faces a number of cyber threats, including cybercrime, hacking, and cyber espionage. Cybersecurity awareness is extremely important in today's digital world, as the number of cyber threats continues to increase. Fig. 2 shows our approach to develop a comprehensive cybersecurity awareness program for Saudi Arabia.

Fig 2. Workflow of our proposed approach of increasing cybersecurity awareness in Saudi Arabia

To assess the level of current cybersecurity awareness, we conducted a survey on Saudi people of all age groups who interact with the internet through smartphones, PCs, or any IoT devices. The survey result shows that people do not pay needed attention to the security concerns. The survey findings also confirm the survey done in [1]. In this paper, we propose a comprehensive framework to raise the level of awareness

of cybersecurity targeting Saudi society in all its age groups. Our framework addresses awareness among common strata of people like students, employees, kids, older people etc. The framework includes elements of educational training, awareness program for general public and incident response and reporting process. Incident response is an important aspect of a comprehensive cybersecurity awareness program that helps minimize the damage caused by a security breach or cyberattack, respond rapidly to security incidents, and maintain public trust. As far as we know, our framework is the only work that focuses on engaging all strata of Saudi population in awareness program as well as encouraging an environment of reporting cyber incidents. Our framework explains how training people in formal sectors like school, universities, organizations etc. can be trained in cybersecurity irrespective of their specialties. The most important aspect of our framework is reaching out to people from informal sectors through planning, policy making and tools. Also, our framework makes cybercrime reporting interactive so that no incident goes unnoticed by the government and can be delt swiftly.

This paper is organized as follows. Section 2 present some related work in the field of cybersecurity awareness and cybersecurity awareness programs in different countries and discuss the current cybersecurity strategy of Saudi Arabia. In Section 3, we present an assessment of the survey that we conducted. Subsequently, an analysis is drawn subsection 3.1. In Section 4, our proposed framework is presented and explained. In Section 5, other cybersecurity awareness frameworks are compared with our proposed framework. Lastly, a conclusion is drawn in Section 6.

Related Work

Due to the shifting of all major processes from conventional methods to the smartphone or IoT platforms, security has become the biggest challenge for the governments. The cyber criminals take advantage of unaware, naive users by stealing their money or information. Nowadays governments have also become susceptible to cyberattacks resulting in massive data loss, national security breach, financial loss and many more compromised systems. Generally, a cyberattack starts by targeting a person who is not aware about the security concerns. One such small incident snowballs into a big catastrophic event resulting in huge loss. The research fraternity has been coming up with proposals, tool and techniques to address this issue. In [8], authors researched the efforts of South Africa in the field of awareness and education in cybersecurity, and it became clear that it does not have awareness and education initiatives in cybersecurity. So, they proposed a framework for cybersecurity awareness in South Africa and create a cybersecurity culture in South Africa among Internet users. Authors reviewed previous studies in cybersecurity to identify gaps in awareness research [9]. They found that there is still a lack of cybersecurity awareness, and they suggested improvements, to improve the current practices and target the youth

section. In [10], author measured the level of situational awareness in the Internet users and then created a multi- level framework based on analyzing conditions. And based on these conditions, faster and more efficient actions are taken. Gcaza et.al in [11] studied the culture of cybersecurity. They emphasized that to reach a culture of cybersecurity, awareness and education must be raised. Alsmadi et.al in [12] discussed the extent of states 'commitment to cybersecurity through the Global Cybersecurity Index. There is a gap in teaching methods, so they suggested changing teaching methods. Authors in [13] highlighted the importance of cybersecurity and how organizations seek to defend their assets. They proposed cybersecurity models based on the sensitivity of the assets. In [4], authors addressed awareness of cybersecurity, and directed the effort at children and their use of smart devices. The built-in hardware restrictions successfully protect users. Alzubaidi [1] measured the current level of awareness in Saudi society and made recommendations to enhance awareness. Author also pointed out low incident reporting by people.

Cybersecurity Strategies in Developed Countries and Saudi Arabia

Authors in [8] reviewed the cybersecurity strategies in the United States of America (US), United Kingdom (UK), Canada and Australia. These countries have cybersecurity strategy in place for many years. All of these strategies have at least one national education and awareness initiative because it plays an important role in improving economic and social well- being. For the sake of brevity, we will not dwell into the details of these countries' strategies. Their strategies are summarized in Table 1.

Table 1. Cybersecurity strategies applied in the aforementioned countries

Country	US	UK	Canada	Australia
Year	2009	2011	2011	2009
The initiative	National Initiative for Cybersecurity Education (NICE)	Get Safe Online	Get Safe Online	Broadband Management, Communications and the Digital Economy (DBDCE) and the Australian Competition Commission (ACCC)
The campaign	stop think connect	Get Safe Online	Get Cyber Safe	*Stay Smart Online*
Host organization	DHS Department of Homeland Security	Get Safe Online	public safety canada	*Stay Smart Online*
The target audience	For all segments of society: children, college students, parents, teachers, professionals, Americans, the government, and companies.	Individuals and companies	General Canadian Audience	Home users, children, teenagers, schools and small businesses.

Topics they covered	Cyberbullying, identity theft and phishing, child protection online, and e-learning integration. Banking services, cybersecurity. Internet fraud and deception.	Fraud, games, dating, banking, money transfer, privacy, cloud computing, data encryption, data loss, protection of company sites	Email security, file sharing, mobile security, fraud.	Mobile parental controls, passwords, file sharing, spam, online shopping

Each country has its own cybersecurity target depending on native factors like level of education, infrastructure to support cybersecurity awareness, demography etc. Developed nations have different security needs as compared to developing nations. The countries have tailored made cybersecurity awareness policy which caters to their need.

Cybersecurity in Saudi Arabia: The Internet became available to everyone in the Kingdom in 1999. Saudi Arabia's Security Vision 2030 emphasizes Saudi Arabia's need to advance safely and flexibly by providing a security basis to ensure the Kingdom's development into a knowledge-based economy. SA implemented the national cybersecurity into the presidency of the republic to become the focal point of cybersecurity in the Kingdom in 2017. The Ministry of Communications and Information Technology (MCIT) was the first national security strategy in 2011. In 2016, the Kingdom of Saudi Arabia faced a wave of cyber-attacks. The Director of the Saudi Cyber Security Center (NCSC) also stated that the Kingdom responded to nearly 1,000 attacks targeting infrastructure and seeking to steal data, and cause services interruption. These incidents fall under the responsibility of the Saudi Computer Emergency Response Team (CERT-SA), which was established in 2006 and is a trusted reference for information. CERT provides consulting services on how to deal with accidents. It collects information about a specific event, performs post-incident analysis and prepares reports if requested, conducting the analysis and developing prevention of cyber accidents. The cost of cyber accidents can also be determined. CERT-SA is not a responsible central authority and is often seen as an interactive organization providing information on current threats and supporting incident response. There have been efforts to create a support platform for CNI (Critical National Infrastructure) and government security and services such as: Incident Response Planning Malware Analysis, Supervision and Consultation. This platform has not yet been introduced.

The Kingdom is one of the 18 members to sign the Arab Convention to Combat Cybercrime, but it has not yet been ratified. The Kingdom of Saudi Arabia is keen to pay attention to information technology, communications and cyber and make it one of the main pillars. It is the largest market for information and communication technology in the East and invested nearly $ 14 billion in the technology and

communications sector as well as cybersecurity in 2016. The Kingdom of Saudi Arabia has prioritized cybersecurity as the highest level. It has realized the increasing urgency to take over the defense against cyber-attacks due to the increase in attacks in recent years [14]. In Saudi Arabia there is National Cybersecurity Authority (NCA) which is responsible for handling cybersecurity in Saudi Arabia. They have a vision to seek to achieve cybersecurity that combines confidence, security and growth, which is comprehensive and in line with the vision of the Kingdom and strengthen the protection of technical systems and infrastructure as well as enhance the confidence of investors and individuals in cyberspace and supports economic growth. The authority has been keen on designing a cybersecurity reference framework based on best practices and challenges. It is a model that contains multiple aspects of cybersecurity. The framework includes six themes and eighteen elements for cybersecurity in order to develop the national strategy for cybersecurity. The six axes contained in the framework:

- Unify: in the sense of the integration of all components of cybersecurity.
- Manages: How to manage infrastructure and risks.
- Assure: which is to ensure that cybersecurity is protected.
- Defend: developing cyber defense mechanisms against risks.
- Partner: About building partnerships and sharing information.
- Build: is concerned with building a strong and secure base (NCA, 2021).

The Saudi Arabian Monetary Agency (SAMA) has developed a cybersecurity framework to enable member organizations to effectively identify and address cybersecurity risks. To be able to protect information assets and online services, member organizations must adopt the framework [15]. Although the Kingdom has several cybersecurity frameworks which encompass all the major security aspects, the aspect concerning awareness among people has little focus. As stated earlier, cyber users who are not aware of risks associated with technologies, applications etc. and their careless actions around these applications can have dire consequences. Our survey (discussed in next section) shows that people are not security conscious when it comes to cyberspace. Therefore, awareness of the security risks among people whether adults or kids is necessary for a secure cyberspace. Our framework is dedicated to increase the awareness through multiple channels and addresses all the age-group.

Cybersecurity Awareness Assessment

To assess the current awareness of cyber risks among Saudi people, we conducted a survey targeting technology savvy people. Using Google forms, a questionnaire was created. The questionnaire contains 30 questions. A question was also raised to the participants about who is responsible in their opinion for raising awareness in cybersecurity. And finally, reporting accidents and the extent to which individuals perceive its importance. 530 Saudi citizens

completed the questionnaire. The survey was published using social media.

Upon completion of the questionnaire, we analyzed the results to assess the level of awareness of the end user in the Kingdom and verify reliability using the SPSS program. 7% of the participants were less than 18 years old, 13% were older than 45 years, and the largest percentage was 79% for ages between 18 and 45 years. Gender ratio was 60% of males and 40% of females. Participants were asked general questions about the type of operating system used and the extent of security in their devices according to their belief, as well as with regard to protection programs, their activation, the use of virus programs and the activation of updates in the devices etc. and about users' behavior to measure their awareness of cyber threats when they use cyberspace. Regarding the e-mail address and whether the sender and recipient address is verified, the answers were as follows: 53% answered yes, 30% answered sometimes, 16% said no. Regarding sharing the email address, 73% said no, and 26% said yes. For the question "are you logging out of the email account when you finished it", the answers were: 27% answered yes, and around 70% answered they don't. Regarding passwords, the questions were "Do you prefer simple or complex passwords?" 52% answered simple and 47% complex, "in terms of changing passwords continuously, 13% answered yes, 30% answered occasionally, and 56% answered no, about using different passwords for accounts, the answers were 55% yes and 44% no.

Regarding browsing websites, downloading applications, and using public networks, the questions were as follows: Checking addresses and links before clicking on them, 44.3% answered yes and 55.7% answered no. With regard to sharing personal information with anyone, the answers were as follows: 41% answered with those we know, and 57% said no. Due to the importance of this question and its connection to some extent with social engineering, it was necessary to ask a question about the meaning of social engineering. 17% said they knew about social engineering and 83% said they did not know. With regard to communicating with people you do not know, 13% answered yes, 45% said no, and 42% sometimes. On downloading applications, is the application developer checked? Answers were 32% yes and 67% no. About the permissions allowed for the app before it is loaded, 38% responded by reading the permissions before downloading the app, and 61% answered no. This question is every important. When users install malicious applications without verifying the permissions needed by those applications, they unknowingly give full control of their device to the application developer. The developer or publisher can exploit this condition. About the use of Wi-Fi networks in public places 17% answered yes, 37% answered occasionally, and 45% said no. For the question about reporting any security incidents or cybercrimes, 55% answered yes and 41% said they did not know the authorities responsible for handling such incidents. And the

importance of knowing the opinions of the participants about who is responsible for raising awareness in the Saudi society (Government, media, individuals, education) the answers varied as follows: 62% answered the government, 66% of the media, 32% of individuals and 57% education. Answers were taken using a Likert scale (yes, no, I don't know, sometimes).

Assessment Result Analysis

In this study, the different participants' practices and knowledge in cybersecurity were evaluated through a survey. To measure the reliability and consistency of the survey, we employed Cronbach's Alpha assessment method (Table 2). Table 3 shows the demographic information of the participants of the study.

Table 2. Reliability Statistics

Cronbach's Alpha	No. of Items
.708	27

Table 3. Demographic information of research respondents

	Variables	Numbers	Percentage
Sex	Male Female	317 213	59.8% 40.2%
Age (year)	Under 18 18-45 Over 45	39 422 69	7.4% 79.6% 13%
Technology usage time	1-4 hours 4-8 hours More 8 hours	101 286 143	19.1% 54% 27%

With regard to the user's behavior when using technology and the extent of his keenness in securing his data, there are a number of questions given using the Likert scale (yes, no, sometimes) and the results (Table 4) are as follows:

Table 2. Reliability Statistics

Question	Yes	No
In public places, do you use Wi-Fi networks?	94	239
Do you verify the sender and address before opening emails?	285	86
When you finish your e-mail, do you log out of your e-mail?	144	282
Do you regularly back up programs?	137	214
Are you constantly changing your passwords?	71	300
Do you respond and communicate with people you do not know?	70	243

There are many risks in accessing the Internet and therefore, potential threats must be prevented. For this, 10 questions were asked about monitor user behavior, and users' answers were yes or no, as shown in the table below (Table 5).

Table 5. Questions for monitoring user behavior

Question	Yes	No
When downloading an application from the stores on mobile devices, do you check with the application publisher?	174	356
Do you know about malware such as virus and worm?	230	300
Do you know what are the allowed permissions of the application before downloading it in your devices?	204	326
Do you check the URLs and links of the internet pages before clicking on them?	235	295
Do you know what social engineering means?	90	440
Do you know what does the word hacker mean?	500	30
Do you use different passwords for your accounts?	293	237
Do you know the importance of backup?	350	180
Do you know what is a phishing attack?	117	413
Do you share your email address with everyone?	139	391

Authors [1] conducted a survey to measure the level of awareness, and the questions about cybercrime and reporting them. The results are that 21.7% were victims of cybercrime and 29.2% reported the crime, while 70% did not report and the reasons are shown in the following figure (Fig. 2) adapted from [1].

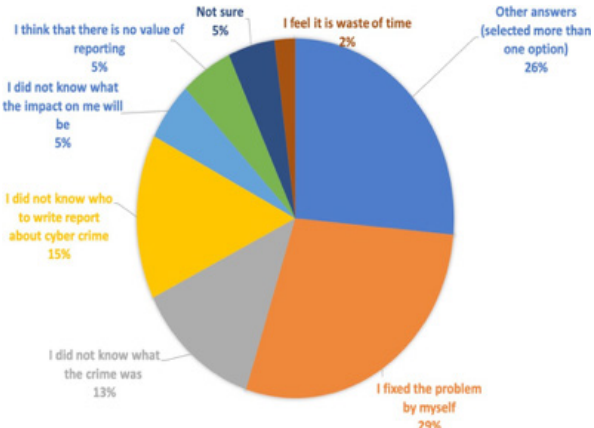

Fig. 2. Reporting incidents

Regarding cybercrime and the way individuals deal with it, a question was asked to the participants "in case you were exposed to a cyber-attack, do you report it?". The answers are shown in Table 6. The participants were also asked about their opinion on the responsibility to raise awareness of cybersecurity in Saudi Arabia. More than 60 % considered the government and media responsible for creating awareness.

Table 6. Incident Response

In the future, if you are exposed to a cyber-attack, will you report it?		
	Frequency	percent
Yes	295	55.7
No	15	2.8
I do not know the responsible party	220	41.5

In this survey, the following is evident:

- About passwords and their importance in terms of security, the largest percentage prefer simple passwords, and about changing passwords, 56% replied that they did not change passwords.
- About the importance of backing up and doing it, 66% knew about the importance of backup and only 25% were the ones doing the backup.
- Regarding the sharing of personal information and its connection with social engineering, the percentage was 41.7% who responded by sharing information with those they know about their knowledge of social engineering, and 83% said they did not know it.
- Despite the threats that occur when connecting to public networks, 17.7% answered that they use public networks. 37.2% answered sometimes.
- With regard to cyber incidents and the process of reporting them, 41.5% replied that they did not know the responsible authorities.

From our survey result, it is evident that there is a need for a rigorous cybersecurity awareness program that increases the level of sense of cybersecurity among people. It is also important to have awareness programs for unqualified people and nontechnical person, such as housewives and elderlies. These findings validate our awareness framework. All the components of our framework address these issues.

Proposed Framework

The cybersecurity framework aims to enrich information technology security and contains a set of policies and procedures to enhance cybersecurity strategies

[16]. The Fig. 3 adapted from [16] shows the five main basic processes that define the cybersecurity framework.

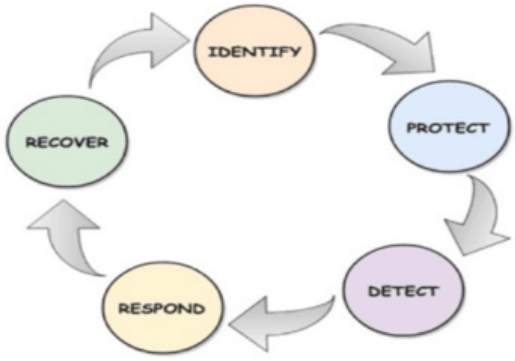

Fig. 3. Cybersecurity Framework Strategies

The framework for cybersecurity proposed here (Fig. 4) focuses on enhancing the cyber awareness of the Saudi society. The framework depends on following key factors, namely:

- The objective must be clear.
- Availability of tools and resources.
- Developing an action plan to implement the policies.

The framework is based on the needs and requirements of individuals to reach a good level of awareness of cybersecurity, and it targets all groups of society to eliminate avenues through which attackers can take advantage. The framework includes a number of strategies and policies which are important for a clear and efficient awareness program. The following figure presents our proposed framework for cybersecurity awareness and its components. An aware and able society makes a strong shield of defense against attackers. Cybersecurity awareness among mass can be effective against cyberattacks if all the sections of society become conscious while interacting with internet technologies thus closing avenues through which attacks can happen.

Our framework considers all those sections of society who use internet technologies through smartphones, computers, tablets or IoTs etc. Our framework proposes cybersecurity training in schools, universities, colleges and organizations as well-trained persons can educate others. The main awareness program targets those sections of Saudi society who do not possess the required technological knowledge. Our framework proposes different tools and methods to increase awareness among these people. Beside awareness and training, the framework also offers incident response which addresses the issues related to attack incidents like how there are responded to and make it easier for people to report incidents so that these incidents would not become major crisis.

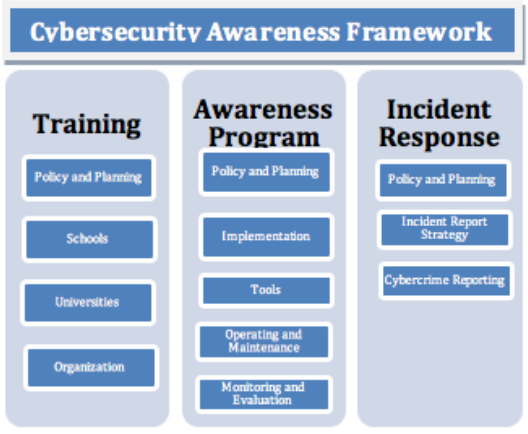

Fig. 4. Cyber Security framework

Training

Students and employees whether government or non-government make the majority of tech savvy population of Saudi Arabia. As many universities in Saudi

Arabia are providing cybersecurity related programs, schools and various organizations are yet to include a rigorous approach towards increasing cybersecurity awareness. To have an effective training across these institutes policies must be defined to layout the ways in which the training will be carried out.

- After implementing the cybersecurity policy, ensuring regular monitoring and evaluation of the executed process.
- Continuing and expanding awareness programs and campaigns to reach specific target groups.
- Ensuring that there is a link between awareness efforts and the national cybersecurity strategy.

Training in schools

This program targets students in schools. Since cyberattacks target all segments of society, including school students, the attacks lead to losses in various fields. So, it is necessary for learners in the school to realize their responsibility to protect themselves and their information while using the Internet. It is necessary to equip them to be able to take responsibility for their security through awareness and education programs. Authors explained that awareness programs for school students are of great importance because most students do not understand the concept of cybersecurity, so it is important to develop awareness programs in education as a curriculum [17]. A strategy must be developed to improve cybersecurity in the school environment. Some important points to consider for defining the training policy:

- Having a plan that clarifies the basics of cybersecurity within the school and improving the educational efforts of learners in schools.
- For the government to undertake a unified policy for schools and ensure its implementation.
- Providing schools with how to deal with cybersecurity incidents.
- Providing training packages for learners with regard to cybersecurity and making them aware of the importance that the topics are appropriate for the age of the learners.
- Providing the necessary resources for training and education in the field of cybersecurity through cooperation with the academic community.
- Emphasizing importance of parental involvement through assistance in cybersecurity awareness efforts and the exchange of instructions with teachers.
- Including cybersecurity in school curricula.
- Ensuring that educational investments are effective and that they fulfill the needs of the cybersecurity environment.
- Implementing strategies are mandatory for students and teachers [17].

Training in universities

The training in universities is of paramount importance as graduates with advanced cybersecurity skills will form an effective defense against the cyberattacks. Various universities across Saudi Arabia are offering courses related to cybersecurity. However, requirement for state-of-

the-art cybersecurity courses in universities and colleges have become inevitable. There must be a plan that clarifies what will be the cybersecurity within the university and improving the educational efforts of learners at the university.

Followings are some points to consider while developing cybersecurity program for universities and colleges:

- The government should undertake a unified technology policy for universities and ensure its implementation.
- After implementing the cybersecurity policy, ensure regular monitoring and evaluation of the executed process.
- Providing universities with how to deal with cybersecurity incidents.
- Recruitment of cybersecurity professional and providing training packages for learners with regard to cybersecurity.
- Provide the necessary resources for training and education in the field of cybersecurity through cooperation with the IT industry.
- Following up on cybersecurity developments nationwide through social media, the media, posters, brochures and workshops.
- Including cybersecurity in the curricula.
- Ensure that educational investments are effective and that they fulfill the needs of the cybersecurity environment.
- Implementing strategies are mandatory for students and teachers.

All of the above recommendations are the responsibility of the government in the first place, especially the Ministry of Education, as it is responsible for the school and university system, and schools and universities are responsible for implementing the policies, measures and procedures. This means cooperation between government, schools and universities by working together to optimize and raise cyber awareness. In addition to the importance of providing tools that help in implementing the procedures and measures, with the importance of monitoring what is being implemented and continuous evaluation to ensure the effectiveness of the procedures and that they lead to the desired goal. If these recommendations are taken into account, the state of cybersecurity awareness in schools and universities will improve greatly [17].

Training in organizations

This cybersecurity training targets employees at their workplace whether government or non-government. Cyberattacks also target workers in different sectors. It is necessary for employees to realize their responsibility to protect themselves and their information while using the Internet as their ignorance can pose threats to the organization's data and eventually leading to massive cyberattacks resulting in financial loss, credit loss etc. Therefore, it is necessary to equip them to be able to take responsibility for their security through awareness and education programs. Therefore, there must be a strategy to improve cybersecurity awareness in the work environment. Followings are some key points to consider:

- Having a plan that clarifies what will be cybersecurity within the company or organization and improving awareness efforts for employees.
- Providing the organization with how to deal with cybersecurity incidents.
- Providing training packages for employees with regard to cybersecurity and making them trained.
- Provide the necessary resources for training and education in the field of cybersecurity through cooperation with the academic community.
- Ensure that there is a link between awareness efforts and the national cybersecurity strategy.
- Implementing strategies are mandatory for employees.

Responsibility of all the aforementioned recommendations falls on companies and managers to impose policies on employees and they must comply with them and apply measures and procedures. This means collaboration between managers and employees working together to improve and raise the level of cyber awareness. In addition to the importance of providing tools that help in implementing the procedures and measures, with the importance of monitoring what is being implemented and continuous evaluation to ensure the effectiveness of the procedures and that they lead to the desired goal [17].

Awareness Program Policy

The awareness programs are directed at people who are not technology professionals and do not have any background on cyber safety such as housewives, the elderly, general businessmen etc. There are various methods which can help in increasing and educating non-technical people about the dangerous of using the internet via smartphones, computers, tabs etc. The existence and diversity of technologies can contribute in achieving the desired goals, which can raise the level of cyber awareness in Saudi society of all age groups. The power and widespread use of social media, television etc. can play a major role in increasing the cybersecurity awareness. The security awareness program can be defined as a program whose main objective is to train users on the threats they may face during their use of cyberspace and how to deal with situations that may endanger sensitive data [18].

In this section, we discuss awareness programs components and how to use them. Basic components of a security awareness program can be summarized as:

1. Planning
2. Implementation
3. Operating and Maintenance
4. Monitoring and evaluation

Planning: Planning is very important before undertaking any awareness program operations. With only proper and effective planning, awareness program can achieve maximum outreach and awareness among people. During planning, requirement analysis is done. Tools, personnel, organizations, strategies etc. are decided which will be utilized in awareness programs.

Implementation: After planning, implementation of operations described in planning is carried out. The implementation

must include all the steps in their entirety. An awareness program can become successful only if all each and every component are properly deployed.

Operation and Maintenance: This phase ensures that the program is effective and efficient in increasing the awareness and is sustainable.

Monitoring and evaluation: Periodic monitoring and evaluation of the awareness program assess the effectiveness of the program and check if all the components are working properly as intended and has not lost its efficiency.

Below are some tools which can be used in the awareness programs:

1. Social media: social media is considered one of the successful methods due to its ubiquity and frequent use in almost all circles of society. It can help in cyber awareness and has an effective role in creating public opinion, as well as regarding awareness of cybersecurity through a group of thinkers and influencers and their presentation of issues of interest to cybersecurity that help in forming the awareness of users.
2. Campaigns: Campaigns can be used to create and implement cybersecurity awareness programs at the district level. Responsible individuals are given the task of supervising the campaigns and evaluating them periodically to ensure their effectiveness. The campaigns deal with different topics, according to the category they are directed to.
3. Educational games: A number of studies have proven the effectiveness of educational games in raising the level of cyber awareness and are directed towards those under 18 years old.
4. Victims' stories: A neglected entity but can prove instrumental in raising awareness. People can become conscious while using cyber applications if they get testimonials from cyber victims and learn how even simple action can cause severe damage. Social media, television, websites can be used to relay these stories to people and let them know that ordinary people can also become a victim of cyberattacks.
5. Blogging, special publications, television programs, advertisements, hoardings can also be utilized to increase awareness among those sections of society which are not alert about the dangers of internet if not used properly.

Incident Response

The massive increase in cybercrime demonstrates the need for strategies to address these attacks. In [19], authors discussed the UK's approach to countering these attacks, with an explanation of the importance of participation by all. The United Kingdom has established a Government Response Center (the new National Cyber Security Center (NCSC)), which is a bridge between the government and users and is the source of advice and guidance on cybersecurity. The importance of developing basic criminal laws against cyber-crimes would enhance users' confidence in cyberspace. The Anti-Cyber Crime Law in the Kingdom of Saudi Arabia was established in 2007 (ACCL). It defines crimes

and their penalties, and covers the basic areas for combating cybercrimes, such as data interference, privacy infringement, maintaining public order and morals, as well as punishing attempts to commit cybercrimes even if they do not succeed. However, this law does not provide adequate protection against identity theft and does not adequately protect data privacy. The definition of bullying in this law does not contain provisions against aiding or abetting the commission of a cybercrime. Saudi Arabia has also established a national CERT (Computer Incident Response Team) (CERT-SA, 2018). It is a group of information security experts responsible for protecting against security incidents, discovering them, dealing with them and responding to them, as well as providing instructions on how to deal with incidents [20]. Despite having CERT in Saudi Arabia, our survey reveals that cyberattack victims seldom report to the authorities. There are several reasons behind this hesitancy on the part of victims. One, the people are not aware that there is a government authority to which they can report the attacks, second, there is a lack of interactive portals/ applications through which they can report the crime and third, they don't care as they don't understand the consequences of a simple cyberattack. To overcome this issue, an incident response strategy is needed focusing on the importance of easy and interactive cyber incident reporting and, speedy response.

To have a successful incident response strategy, policy and proper planning are necessary. Without them, security incidents cannot be resolved in time. Planning: The effectiveness and efficiency of incident response depend on coherent and lucid planning. Planning defines the role and responsibility of the stakeholders; procedures and processes to undertake in events of incidents, continuity plans etc. When cyber-attacks occur, it is best to have ready procedures, tools etc. to investigate the attacks, limit their spreading and stop them from turning into disaster or crisis.

Policy: A policy is the law or order of guidelines for reaching specific goals. This is done by clarifying the steps and being implemented as a protocol. Incident response policy may explain:

- The way the incident response program works.
- The expectations from the program.
- Whom to contact, how to report an incident.
- Management members.
- Various governmental and non-governmental constraints.
- Incident response procedures and processes.

Incident response strategy

Well-prepared strategies are essential in the event of a cyberattack. The most important strategy is protecting the state's infrastructure. When a cyber incident is reported and is accepted and contained and treated before more damage occurs can be attributed as an effective incident response strategy.

There are a number of steps involved in incident response strategy:

- The attack. When it occurs, it may be a simple virus in the form of a code that infects a computer or a complex multi-stage malware by cyber criminals/ agents. The organization detects the attack using security sensors or control devices.
- Investigation of the attack. After the attack is discovered, the process of investigating the attack begins and gathering evidence to ensure that the sensor has reported an active cyber-attack, then the incident response process begins.
- Containment. After investigating the incident and the response of the agency, it moves to contain the attack, first removing the attacker, then fixing the vulnerability that allowed the attacker to enter.
- Reform. The defenders repair the damage, return the agency to normal operation, and officially close the incident.
- After the accident. After handling the incident, attacks from the same attacker are followed up using the same tools and techniques to detect it and respond quickly, which increases security.

Cybercrime reporting

There are ways through which people can report cybercrime but these are not specific, well known and interactive. In the event of a cyber-crime or cyberattack some questions must be addressed, like:

- Are there competent authorities that the victim can turn to report the crime?
- If there is a competent authority, will it be known to everyone?
- The procedures used for reporting the crime are simple or complex?
- It is important when a cyber-crime occurs that there are official bodies that the victim can resort to report the crime and try to reach the person responsible, either through the helpline number or a website.

There are sites that provide these procedures, for example in the Kingdom of Saudi Arabia, there is a site of the National Cybersecurity Authority (NCA). CERT is a part of NCA. The victim can report the cyber incidents through emails, or logging into their Absher (a governmental portal for residents and citizens) account. The victim is required to fill out certain fields for reporting with attack details data knowing that this data will be dealt with complete confidentiality. But such kind of sites are not known to all members of society. Therefore, it is necessary for the awareness and training program to include the definition of such sites and their importance in trying to reduce cybercrimes as well as to address them and to help address security vulnerabilities. We recommend the use of hotline numbers, applications through which victims can report the issue quickly without delay. Dedicated smartphone application having simple and interactive interface should be developed to address the reporting issue. A 27 X 7 Hotline numbers should be publicized to reach every section of society. NCA should provide separate reporting mechanisms for individual users as well as organization. NCA also provides a platform where organizations can report vulnerabilities in applications. NCA then

publish these vulnerabilities. After fixing them, updates are also published by NCA.

Comparison

In this section, we present a comparison (Table 7) of our proposed framework with other awareness frameworks. Based on the target audience, we compared our framework with other available frameworks. We found many articles [5], [7], [21] etc. assessing the level of cybersecurity in either educational institutions or private/public organizations. We assessed the cybersecurity awareness among people from formal and non-formal sectors. Our framework provides an all-inclusive approach of creating awareness among the masses to circumvent any cyberthreat vector. The frameworks [22], [23], [24], [25], and [26] are directed towards either academia or organizations. Moreover, these frameworks do not particularly focus on incident reporting and response process and people from non-organized sectors.

Table 7. Framework Assessment

Framework	Educational Institution	Organizations	General Public	Incident Reporting
`Proposed Framework	✓	✓	✓	✓
[22]	X	✓	X	X
[23]	✓	X	X	X
[24]	✓	X	X	X
[25]	X	✓	X	X
[26]	X	✓	X	X

Conclusion

The cyberspace is not limited to only tech savvy people but general people of all sorts. So, the need for cybersecurity emerged. It is important to spread awareness and educate users about the risks of cyberspace and how to protect themselves and their data while using internet-based applications as well as when cyber-attacks occur and the ability to deal with them. In this paper, we conducted a survey aimed at all age groups in Saudi society that examines the users' behavior about their use of technology as well as their background knowledge in terms of information security. The result showed a lack of awareness in cybersecurity. And, since the Kingdom is considered a target for cyberattacks, and there were a number of attacks that targeted important and vital areas therefore, awareness is important for people, especially non-tech. Based on our survey and available research, we proposed a cybersecurity framework to increase the level of awareness among Saudi people. The framework delivers components which aim at training in schools, universities and organizations, with clarification of policies at each point along with the training programs, their components and the tools used, to suit all groups and interests. Our framework also targets the section of people who are neither school/college/university students nor employees in any organization. So, reaching this section and creating awareness about cybersecurity is very crucial in having a robust defense against the cyber-

attacks. Apart from these creating awareness, our framework considers the element of incident response and its related policy and planning and, illumination of its importance in responding to attacks and the ability to deal with the incident.

Acknowledgements

The authors would like to extend thanks to College of Computer and Information Sciences, Majmaah University for providing support for this study.

References

[1] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," 2021.

[2] M. M. Al-Daeef, N. Basir and M. M. Saudi, "Security awareness training: A review," 2017.

[3] L. Ajmi, N. Alqahtani, A. U. Rahman and M. Mahmud, "A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia," 2019.

[4] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, "A review of using gaming technology for cyber-security awareness," 2016.

[5] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, Cybersecurity Awareness Level: The Case of Saudi Arabia University Students. International Journal of Advanced Computer Science and Applications, p. 3., 2021.

[6] H. De Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," 2017.

[7] R. Sabillon, J. Serra-Ruiz and V. Cavaller, "An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada," 2019.

[8] N. Kortjan, "A cyber security awareness and education framework for South Africa," 2013.

[9] N. H. Abd Rahim, S. Hamid, M. L. M. Kiah, S. Shamshirband and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," 2015.

[10] H. Tianfield, "Cyber security situational awareness," pp. 782—78.

[11] N. Gcaza and R. von Solms, "Cybersecurity Culture: An ill-defined problem," pp. 98--109, 2017.

[12] I. Alsmadi and M. Zarour, "Cybersecurity programs in Saudi Arabia: issues and recommendations," 2018.

[13] F.F Alotaibi, "Evaluation and Enhancement of Public Cyber Security Awareness," 2019.

[14] M. Hathaway, F. Spidalieri and F. Alsowailm, "Kingdom of Saudi Arabia cyber readiness at a glance," 2017.

[15] A. Al-Sheikh, "Cyber Security Framework Saudi Arabian Monetary Authority," 2017.

[16] "Cybersecurity Framework" https://thehackernews.com/2019/07/best-cybersecurity-frameworks.html, 2019.

[17] E. Kritzinger, M. Bada and J. R. Nurse, "A study into the cybersecurity

awareness initiatives for school learners in South Africa and the UK," 2017.

[18] B. Gardner and V. Thomas, "Building an information security awareness program: Defending against social engineering and technical threats," 2014.

[19] J. Saunders, "Tackling cybercrime--the UK response," pp. 4--15, 2017.

[20] T. S. Alshammari and H. P. Singh, "Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index," Archives of Business Research, vol. 6, 2018.

[21] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," Big Data Cogn. Comput., vol. 5, no. 2, May 2021, doi: 10.3390/BDCC5020023

[22] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," PeerJ Comput. Sci., vol. 7, p. e703, Sep. 2021, doi: 10.7717/PEERJ-CS.703.

[23] H. K. Alkahtani, "Raising the Information Security Awareness Level in Saudi Arabian Organizations Through an Effective Culturally Aware Information Security Framework - Search." , Doctoral Thesis, Department of Computer Science, Loughborough University, 2018.

[24] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," Inf. 2021, Vol. 12, Page 417, vol. 12, no. 10, p. 417, Oct. 2021, doi: 10.3390/INFO12100417.

[25] M. Hijji and G. Alam, "Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees," Sensors (Basel)., vol. 22, no. 22, Nov. 2022, doi: 10.3390/S22228663.

[26] F. A. Almarshad, A. I. A. Alzahrani, and G. Wills, "A Framework to ensure Information Security Awareness in the Middle East," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 22, no. 1, 2022, doi: 10.22937/IJCSNS.2022.22.1.76.

Testing Serverless Applications with AWS Lambda: An Automatic Move to Serverless Architectures

Shamiksha Mishra [1], Abdullah Alenizi [2], Subrata Dutta [3]

1. Department of Computer Science & Engineering, NIT Jamshedpur, India, 2019ugcs033@nitjsr.ac.in

2. Department of IT, College of Computer & Information Science, Majmaah University, Saudi Arabia-11952

3. Department of Computer Science & Engineering, NIT Jamshedpur, India

Abstract

In serverless computing, servers' computing resources are distributed dynamically by the cloud service provider. Consumers are charged based on the usage of resources, not on prepurchase computing capability. Programming models, abstractions, and platforms for cloud services and technologies need to evolve. This paper aims to provide large scalability and low configuration costs for cloud applications. This paper explores testing strategies for a system that allows users to request rides on unicorns from the Wild Rydes fleet. The proposed application to build, deploy and tested, for serverless services developed for the Amazon Web Services cloud platform. The results have been obtained for the parameters Duration, Error count & success rate, Call, Throttle, Total concurrent execution and compare with the existing work. The results have a less duration, with very high success rate with zero error. This paper will help users to help in state of art transportation service so that people can travel faster and easier.

Keywords: Serverless computing;Lambda; DynamoDB.

Introduction

Companies like Apache Open Whisk, Azure Function, Google Cloud Functions, and Open Lambda were among the first to offer serverless computing, a cloud-based service in which application logic is divided into functions and run in response to events [1]. These events are frequently triggered inside between cloud platform services as well as outside. This makes it possible for developers to swiftly and simply create distributed apps across several cloud providers. Applications described by their events are triggered by actions and events in serverless computing. Because events are handled in response to event streams, this language is similar to active database systems. These ideas are fully embraced by serverless function platforms by dispersing their event-processing logic across their clouds.

In addition to event-driven infrastructure, container management, and software development techniques are now being discussed. With serverless computing for multi-level elasticity and graphics processing unit (GPU) virtualization, scalable event-driven computing is possible. [2]. IoT applications benefit from serverless computing, which overlaps with edge and Fog computing infrastructures. Serverless

computing allows large applications to be decomposed into smaller functions. This allows individual scaling of application components but creates a new problem of managing a large number of functions [3]. The field of serverless computing is extremely active. The point at which the use of serverless or virtual machines becomes more cost-effective has been calculated in several studies. Serverless computing is becoming increasingly important. It translates naturally into a microservices architecture and is on a growth and adoption trajectory [4,5]. It is seen as the next wave of cloud computing services. More and more mobile and Internet-of-Things (IoT) apps are powered by serverless computing, which is rapidly spreading across different cloud providers. Serverless cloud computing, which simplifies the management of intricate internal infrastructures and simply concentrates on data analytics solutions, is the solution to these issues. The most popular program is known as Amazon Web Services (AWS). Users from all over the world can access a wide range of infrastructure and cloud solutions through the app [6].

Data analytics has its own set of challenges, including those related to the infrastructure needed to carry out the analytics activities, the expense of doing so, as well as infrastructure, storage, and security. The Internet of Things (IoT), 5G Internet, smart cities, and other upcoming technologies all rely on cloud computing services to handle and store more data. The vulnerabilities and security concerns of the cloud paradigm will therefore increase as a result of the heterogeneity of new firms adopting the aforementioned technologies [7,8]. The biggest obstacle to effective data analysis is the infrastructure needed to handle the massive amounts of data. Its infrastructure consists of powerful processing units that deliver great performance in terms of execution time, sizable storage systems, data saved across multiple locations, and effective embedded software systems.

It is expected that as the cloud becomes more widespread, the associated problems can be solved and serverless computing will dominate the future of cloud computing. It is important that the system be extensible, so that different data sources and providers can be easily incorporated (e.g., metering systems), and that it be scalable so that the system can be used from smaller installations (e.g., a building) to very large installations (likely entire neighborhoods), with deployment costs proportional to installation size.

Motivation

The motivation behind this work is to develop a testable serverless application using AWS Lambda. Using the AWS Lambda computing service, users can run code without having to set up or maintain servers. Codes run on a highly available computing infrastructure using Lambda, and Lambda manages all aspects of computing resource management, such as capacity provisioning, server and OS maintenance, and auto-scaling. The Lambda platform enables the operation of virtually any type of back-end service and applica-

tion. The proposed system combines AWS Amplify, Amazon Cognito, API Gateway, AWS Lambda, and Amazon DynamoDB. The AWS Amplify service makes it easy to build full-stack applications on AWS using tools and features tailored for front-end web and mobile. Amazon Cognito can authenticate, authorize, and manage web and mobile application, users. APIs can be created, published, maintained, monitored, and secured using Amazon API Gateway. APIs can be provided for custom client applications as well as APIs for third-party app developers. A key benefit of DynamoDB is encryption at rest, so sensitive data is protected without making encryption at rest cumbersome or complex. On-demand backups are possible with DynamoDB. To analyze a large amount of data using serverless architecture patterns that reduce the operational complexity of running and managing applications, this research attempts to research serverless cloud computing platforms (AWS).

Our main contributions to this research work are as follows:

- Addressing the serious issues of first-generation serverless computing that bring its potential for automatic scaling into conflict with the two main streams in computing - data-centric and distributed computing - as well as with open source and specialized hardware.
- To build, deploy and testing the proposed applications without configuring or managing the servers.
- To allow users to request rides on unicorns from the Wild Rydes fleet.
- To provided errorless and cost-effective application

The rest of the article is organized as follows. Section two contains the current state of the art developed by various researchers. Section three describes the research methodology and proposed framework. Section 4 discusses the experimental analysis and results. In section 5, summarization the conclusion of the paper is done.

Related Work

The idea of serverless computing in the IT industry holds significant potential for extending its capabilities to a broader range of industries. Therefore, the implementation of serverless computing is not limited to infrastructure improvements [9,10]. The future of cloud computing will be driven as much by business factors as by technological advances. Cloud customers are choosing serverless computing because it allows them to focus on industry- or domain-specific issues rather than server management or distributed systems issues. Due to the robustness of this consumer promise, serverless computing has a very good chance of being mainstream in the future [11].

It is used for many different things, such as serverless messaging, training neural networks [12], processing videos [13], and large data [14, 15, 16]. Without a doubt, both the general public and experts can benefit from their efforts. This is due to the critical relevance of comprehending how these technologies operate. Big Data analytics are incredibly important in today's online

environment, particularly when it comes to the analysis of data from multi-tenant systems that are connected over the Internet and produce a lot of multi-structured data. In [15], the authors focus on Amazon Web Service while discussing multi-tenant data analytics of the serverless cloud architecture (AWS). There are two different application kinds involved. How well Big Data functions under the constraints of time, traffic, and data size. One generates static data while the other generates live dynamic data.

A tried-and-true Spark execution engine called Flint [16] uses Amazon Lambda to offer a pure pay-as-you-go pricing model. Without the necessity for a real Spark cluster, a developer can utilize PySpark as usual with Flint.In addition to the primary Spark data processing engine, Apache Spark [17] is a robust all-in-one analytics engine for machine learning and large-scale distributed computing that includes libraries for SQL, machine learning, graph computation, and stream processing. Applications involving analytics, machine learning, and artificial intelligence can benefit from Spark. Amazon Virtual Private Cloud (Amazon VPC [18] permits the construction of a logically isolated section of the AWS cloud when some AWS services are launched on an extremely virtual network. Users have complete control over how subnets and networks are set up.

To reduce overall data volume and adhere to privacy laws, the increasing adoption of new Internet-of-Things (IoT) devices necessitates more efficient bandwidth consumption, lower latency, and data pre-processing closer to the source. Even though open-source programs and commercial serverless cloud providers already exist [19].The authors discussed how cloud computing and its platforms are evolving, with serverless computing emerging as the next stage. In [20], the authors systematically reviewed several research papers on serverless computing and described various techniques to reduce execution time, cost, or both. The design, implementation, and deployment of serverless applications face additional obstacles, and the serverless computing platforms available today are far from ideal. To the best of our knowledge, these difficulties have not been thoroughly explored. This paper is the first to thoroughly explore how to capture the difficulties developers face when building serverless applications to fill this knowledge gap.

Amazon's AWS Lambda was the first broadly used FaaS platform, even though serverless architecture has been around for more than ten years [21]. However, Google and Microsoft also provide their own FaaS services, known as Google Cloud Functions (GCF) [22] and Azure Functions [23], respectively. Researchers still create serverless programs using Amazon Lambda today. Similar features and advantages are provided by Google Cloud Functions, Azure Functions, and Amazon Lambda. Writing serverless apps can be done in a wide variety of languages. The support for programming languages varies among AWS Lambda, Azure Functions,

and Google Cloud Functions. All services can run serverless Java and Python functions natively. Yet, there are distinctions in addition to that. Go and Ruby can only be used with AWS Lambda and Google Cloud Functions, whereas JavaScript and TypeScript are only available with Azure Functions.

It's imperative that do more than just communicate theories and notions. Instead, it is now necessary to weigh the advantages and disadvantages of serverless computing, take into account how far the industry has come, and decide what still has to be done and improved.

It is possible to extend serverless computing's capabilities beyond the IT industry to a wide range of other industries. In this way, serverless computing goes beyond improving infrastructure. The future of cloud computing is driven equally by business factors and technological advances. Rather than focusing on server management or distributed systems, cloud customers choose serverless computing because of its flexibility. Serverless computing has a very good chance of becoming mainstream in the future because of its robust consumer promise.

The main research gap addressed in this proposed work is highlighted below:

- First-generation serverless computing, with its autoscaling potential at odds with prevailing trends in modern computing, including data-centric and distributed computing, as well as open source and custom hardware, must be addressed.
- To Builds and deploys application without configuring or managing the underlying servers.
- Serverless breaks down applications into smaller and smaller pieces, known as decomposition. This will lead to better observability across applications.
- As the cloud adoption rate grows, we predict the issues related to it can be resolved and serverless computing will grow to dominate the future of cloud computing.
- Containers enable serverless applications to run within fewer attack points than traditional architectures and to have only one set of credentials to access them.
- It is essential that the system be extensible, so that differing data sources and providers can be incorporated easily (such as measurement systems), and that it be scalable, allowing the system to be used from smaller installation (e.g., one building) to very large installations (probably entire neighborhoods), with deployment costs proportional to installation size.

Research Method

The objectives mentioned in the previous section would be fulfilled by using the following research process which is shown in Fig. 1 below.

Research Process

- Research gap and critical analysis
- Problem formulation
- Framework for serverless computing
- Build a serverless application

- Validate the result

Serverless architecture

Services can be developed and run without having to be in control of the underlying infrastructure thanks to a technique for creating software called serverless architecture. By writing code and deploying it in this way, a cloud service provider will create servers to operate any scale of applications, databases, and storage systems. Function as a Service (FaaS) is one of the most well-liked serverless concepts. Each function responds to a trigger, such as an HTTP request or an incoming email, by carrying out a certain action. Users provide their functions and triggers in a cloud provider account during standard testing methods. Depending on the circumstance, the cloud provider either creates a new server or executes the function on a server that is already running when a function is called. Fig. 2 shows the architecture of serverless computing.

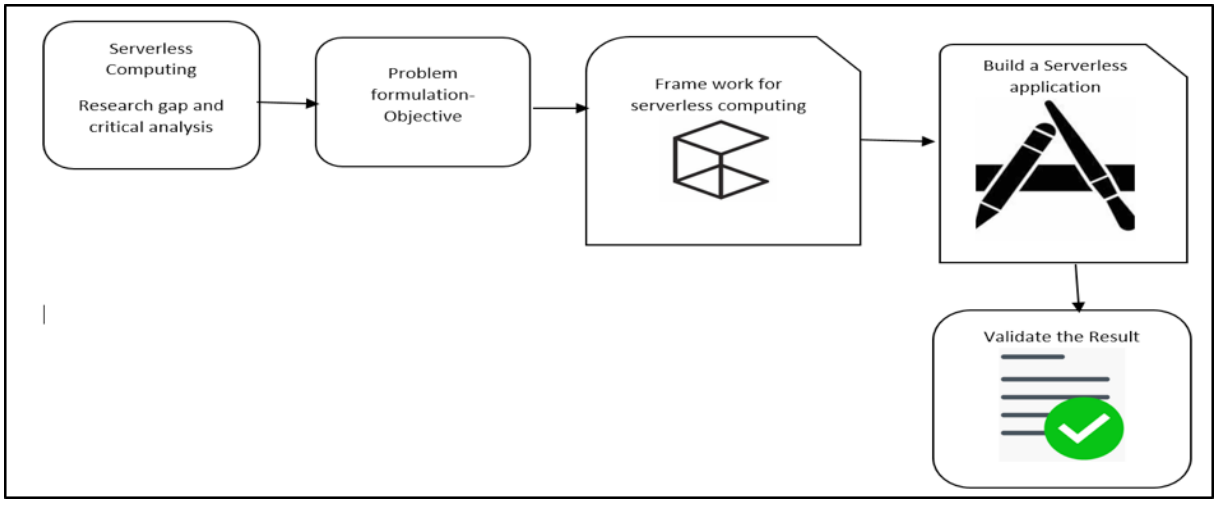

Fig. 1. Research Process

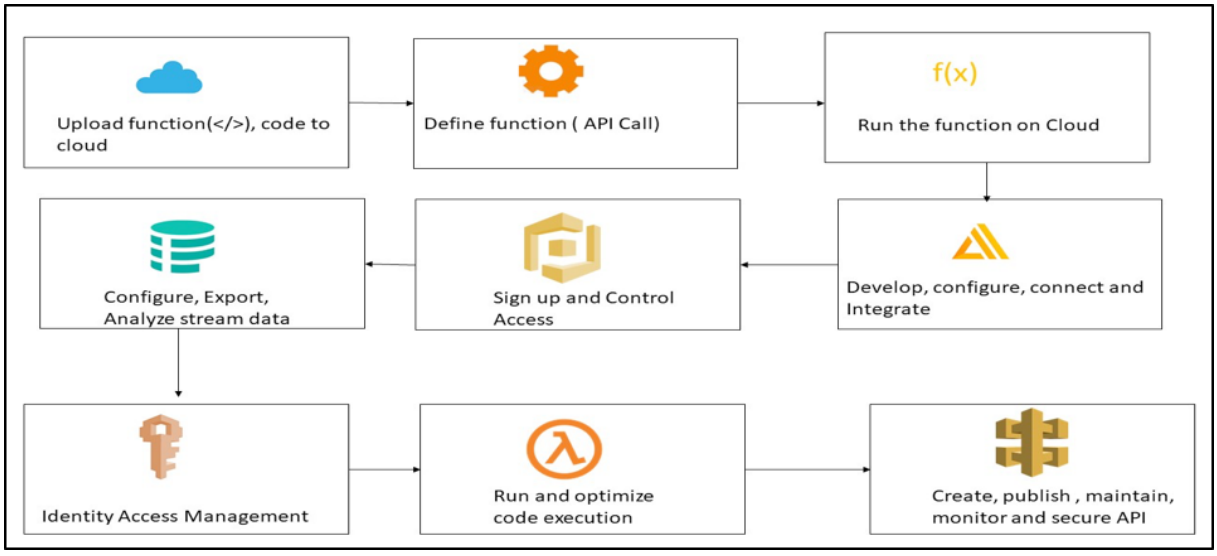

Fig.2. Architecture of Serverless Computing

Experimental Setup Analysis

Users were able to submit requests for rides on unicorns from the Wild Rydes fleet via a custom app. Users can specify where they want to be picked up through an HTML-based interface, and a RESTful web service submits the request and sends a nearby unicorn to the backend. Users have the option to register and sign in through the application, in addition to being able to do so before requesting a ride. The application uses AWS Lambda, Amazon API Gateway, Amazon DynamoDB, AWS Cognito, and AWS Amplify Console as its architecture[21]. HTML, CSS, JavaScript, and picture files are hosted in the amplifier Console and then loaded into the user's browser. Lambda and API Gateway are used to send and receive data from a public API via JavaScript. By allowing user management and authentication, Cognito secures the backend API. The Lambda function of the API can use DynamoDB's persistence layer as the last service to store data.

Fig. 3 shows the proposed serverless computing architecture based on AWS Lambda, Amazon API Gateway, Amazon DynamoDB, AWS Cognito, and AWS Amplify Console. Amplify Console hosts static web resources such as HTML, CSS, JavaScript, and picture files and loads them into users' browsers. Using Lambda and API Gateway, JavaScript is used in the browser to communicate with a public API.

By allowing user management and authentication, Cognito secures the backend API. The Lambda function of the API can use DynamoDB's persistence layer as the last service to store data. Wild Rydes fleet application links to a RESTful Web service on the back end, providing users with an HTML-based user interface that lets them specify the location where they want to be picked up to submit the request and send a nearby unicorn. Users can log in and register with the service before requesting a ride.

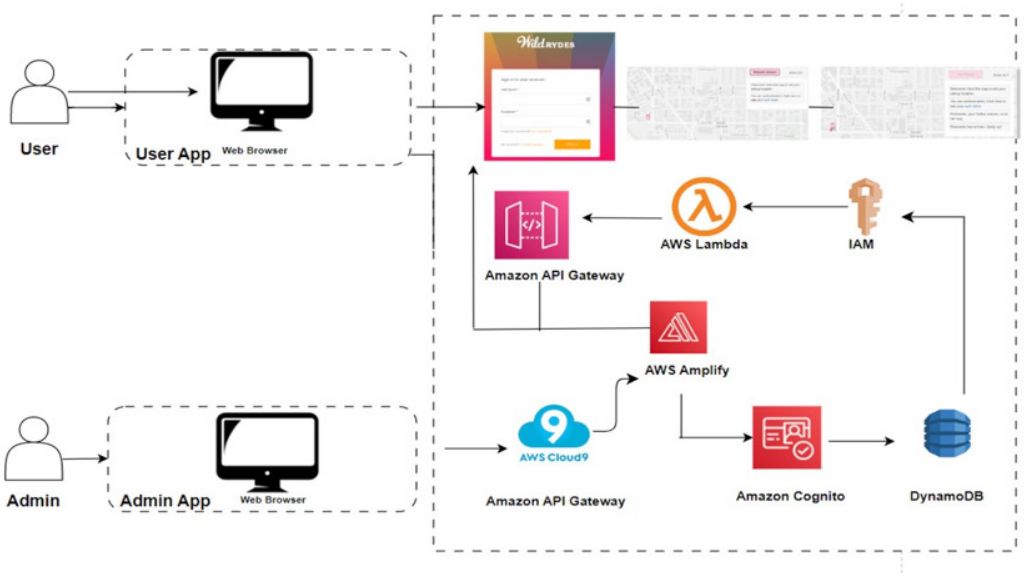

Fig.3. Serverless Computing Architecture: Wild Ryde's fleet using several AWS services

4.1 Analytics of Real-Time Data Streams

The cloud platform offered by Amazon Web Services serves as the foundation for the implementation's infrastructure (AWS). AWS services give customers and tenants the ability to swiftly build the infrastructure they need to suit their business demands. AWS manages and maintains these services. It blends;

A. a. Analyzing real-time data streams
B. b. Data analytics for dynamic web applications STEPS

1. 1. Install and configure the AWS command line interface
2. 2. Setting up the AWS Cloud9 IDE
3. 3. Static Web Hosting

- Creating the Git repository
- Deploying the site using the AWS Amplify Console

4. User management

- Creating an Amazon Cognito user pool and integrating an app with our user pool
- Update the site configuration
- Validate the deployment
- Create a new user for our user pool

5. Create a serverless backend

- Create a Lambda function to process requests
- Create an Amazon DynamoDB table
- Create an IAM role for the function
- Validate the implementation.

6. RESTful API

- Create a new Rest API,
- Deploy the API
- Update the site configuration,
- Validating the implementation.

Install and Configure the AWS Command Line Interface

Using pip, first install the AWS shell, which enables us to access the AWS command line interface. Amazon will request an AWS access key ID, and download an access key file by logging into an AWS account, going to security credentials, access keys, and clicking "Create new access key."

AWS Cloud9 IDE Setup

The AWS Cloud9 integrated development environment (IDE) allows us to develop, run, and debug code directly from our browsers. Code editors, debuggers, and terminals are included. There is no need to install or configure any files on laptop, as Cloud9 is already equipped with the most important tools for common programming languages. It is possible to access AWS resources from the Cloud9 environment using the same user account as used to log in to the AWS Management Console

Static Web Hosting

Amazon Amplify hosts static web resources such as HTML, CSS, JavaScript, and image files for static web hosting. These resources are loaded into the user's browser. We will then deploy the website we just committed to Git through the Amazon Amplify console. Setting up a location for our static web application's code is handled by the Amplify console, which also provides several features to ease the lifecycle of this application and promote best practices.

User Management

To secure the backend API, Cognito pro-

vides user management and authentication features. To manage our users' accounts, we will set up an Amazon Cognito user pool in the next step. Next step is to set up websites where users can sign up as new users, validate their email addresses, and log in to the website. Visitors to a website are asked to create an account. Only need the email address and password to register. In this app, Amazon Cognito can be set up to demand extra qualities. After registration, Amazon Cognito sends users a confirmation email with a verification code. After receiving the verification code, users must enter their email addresses and password on our website. Through the Amazon Cognito console, we can also verify user accounts with fake email addresses.

Login is possible after users confirm their account (either by email verification or by manual confirmation through the console). To log in, users must enter their username (or email address) and password. JSON Web Tokens (JWTs) are returned by Amazon Cognito after communicating with the JavaScript function, authenticating with SRP, and retrieving JSON Web Tokens (JWTs). Using JWTs, in the next step we will authenticate against the RESTful API that we created with Amazon API Gateway using information about the user's identity. There are two ways for users to sign in to Amazon Cognito. Another choice is to use Cognito User Pools for the login and sign-in features in our application, or Cognito Identity Pools for user authentication through SAML identity solutions, identity systems, or social identity providers like Facebook, Twitter, or Amazon. A user pool powers the given registration and sign-in pages.

Build a Serverless Backend

By using the lambda functions of the API, Amazon DynamoDB provides a persistence layer for storing data. In this step, we will create a backend process for our web application using AWS Lambda and Amazon DynamoDB. In the first step, we deployed a browser application that allows users to request unicorns to be shipped to the desired location. A cloud-based service is invoked by JavaScript running in the browser to fulfil these requests. Fig. 3 shows the serverless architecture using Amazon Lambda and DynamoDB. A Lambda function has been implemented that is called every time a unicorn is requested. When the front-end application requests a unicorn, the function selects one from the fleet, records the request in DynamoDB, and then provides details about the unicorn dispatched. The next step is to implement this connection. In this step, we will only isolate and test our function.

RESTful API

With Lambda and API Gateway, JavaScript is executed in the browser to communicate with a public backend API. With Amazon API Gateway, the Lambda function generated in the preceding step is made available as a RESTful API. Using our Amazon Cognito user pool from the previous step, it is secured. AJAX calls the exposed APIs by adding JavaScript client-side to our static-hosted website. The

static website launched in the first stage already has a page prepared to connect with it using the API that was implemented in this step. The map-based interface located at /ride.html can be used to make a unicorn ride request. Users can choose their pick-up location on a map and request a ride after logging in via the /signin.html page by clicking the "Request Unicorn" button in the top right corner of the website. A stream was created in Kinesis into which information was written and from which information was read to allow users to select W. Built on a serverless architecture, Wild Rydes backend services are easy to use and cost-effective to maintain, allowing us to reliably meet the needs of our ever-growing user base. Unicorns have the advantage of being fast, secure, and reliable. Their numbers have increased dramatically recently, making mass transportation more accessible. Wild Rydes are produced by pairing idle unicorns with idle ryders within a short travel distance. A key factor is the shortest time to destination and proximity to the destination. Our serverless architecture streamlines and lowers the cost of scaling our backend services, enabling Wild Rydes to more consistently satisfy the demands of its steadily growing user base. Fig 4 and Fig. 5 shows, after choosing a location on a map and clicking on request unicorn, the lambda function was assigned a unicorn and display all those details on the application and also saved them on AWS Dynamodb.

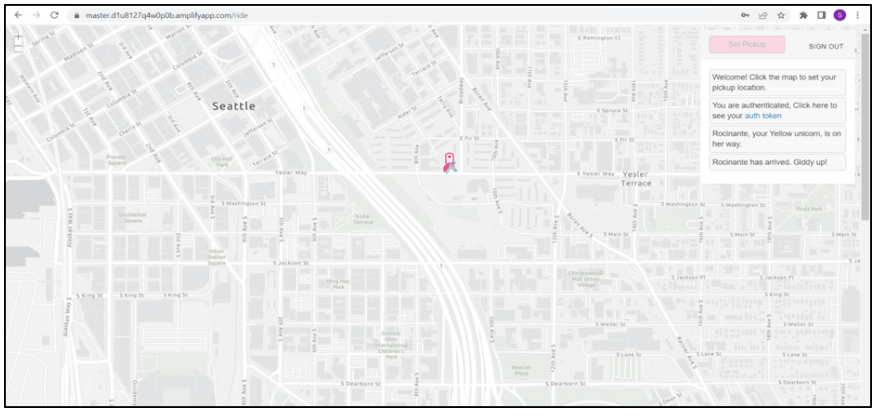

Fig.4. Request unicorn: location 1

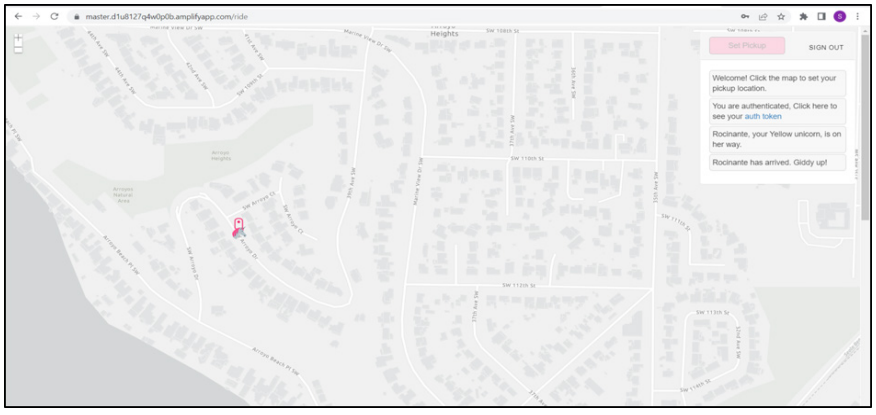

Fig.5. Request unicorn: location 2

Results & Discussion

In Kinesis, a stream was created into which information was written and from which information was read to allow users to follow Wild Ryde's unicorns on a live map. For data analysis, two different types of programs were run to provide a foundation. Some of the experimental results include time delay, data processing performance on the Amazon platform, data aggregation using an aggregate matrix function, and performance analysis for both types of datasets. Amazon CloudWatch receives runtime metrics for Lambda's functions. The metrics displayed provide an overall view of all function runtimes. To view metrics for the unqualified resource, select Filter by. To view metrics for a specific function version or alias, select Aliases or Versions, select the alias or version, and then select Monitor. Logs generated by Lambda functions are automatically stored in Amazon CloudWatch Logs. Logging statements can be used to validate code. Click the Monitor section to view logs for a specific function version or alias.

Performance Metrics

- Duration
- Error count & success rate
- Call
- Throttle
- Total concurrent execution

A performance metric provides information about the performance of a single function call. For example, the Duration metric indicates how many milliseconds a function spends processing an event. The Average and Max metrics provide information about how much time is required for a function call. The Average and Max metrics give an idea of how fast function processes events. The latency for the real-time stream of the producer of the analytics application data stream is between 12.40 and 13.00 milliseconds (Fig.6). The obtained results are better than the work reported in [15]. The continuous peaks in the real-time data stream, where data production is proportional to time, are recorded.

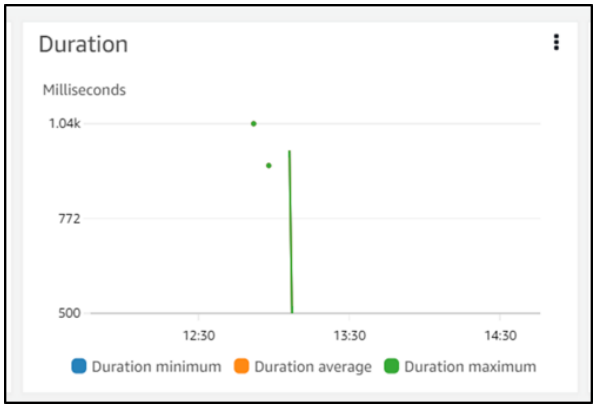

Fig.6. Function spends milliseconds processing an event (Duration metric)

The call metric of the Lambda function indicates the result of its execution. When Lambda returns an error from a function, it sends a 1 to the Errors metric. Consider summing the Errors metric with a period of 1 minute to determine the number of function errors per minute, as shown in Fig.7, success rate is 100%.

Invocations (Calls) that result in a function error - the number of times that function is called. Lambda runtime exceptions and exceptions are thrown by code including function errors. When timeouts or configuration errors occur, the runtime returns errors. By dividing errors by calls, cal-

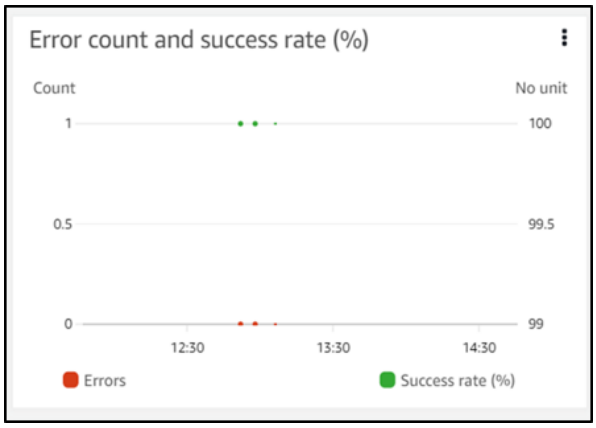

Fig.7. Error count and success rate

culation of error rate can be done. Error metrics include a timestamp that indicates when the function was called, not when the error occurred.

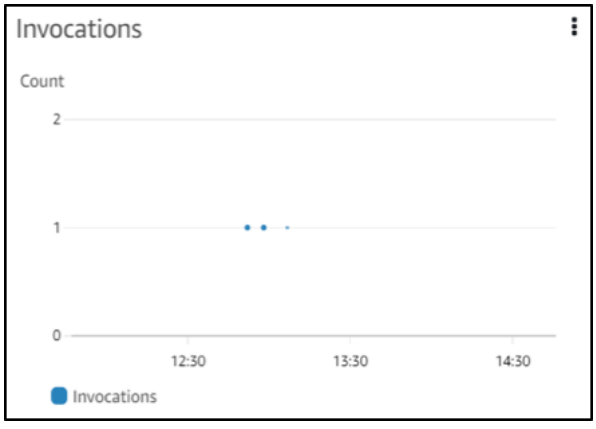

Fig.8. Invocations that result in an error

The total number of calls to function code, including both successful and unsuccessful calls. A call record is not created in response to a throttled call request or a call error. The value of Invocations represents the total number of calls that have been resolved.

A throttled call request or a call error does not result in the creation of a call record. The total number of calls that have been resolved is represented by the value of Invocations. Fig.9 shows there is no counting of throttled requests or other invocation errors. The concurrency metric reports

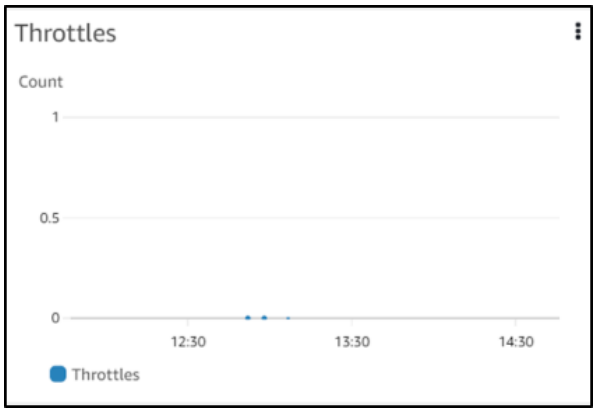

Fig.9. Invocation request

the number of instances processing events across functions, versions, aliases, or regions in a Lambda account. These metrics can be viewed along with the Max statistic to see where they are concerning concurrency limits. The number of function instances processing events at once is shown in Fig. 10. If the reserved concurrency limit for the function or the concurrent execution limitation for the Region is surpassed, more invocation requests will be throttled. The AWS Kinesis application was used to perform real-time data analysis. SQL queries are required for the analysis program to provide the appropriate analysis results.

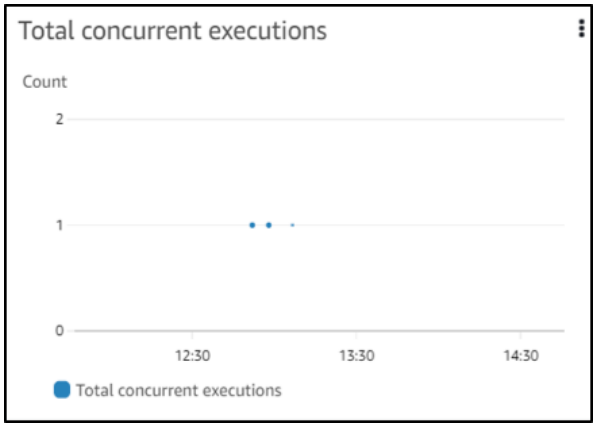

Fig.10. Total Concurrent execution

The Kinesis analytics application generated the aggregated data sets after performing an analysis of the raw input data. In

Kinesis, a feed was made to follow the unicorns of Wild Ryde on the real-time map. Before analysis, the input stream was used to collect the source data, which was made up of duplicate records and unaggregated records. We filtered the aggregated datasets for analysis after using data analytics to assess the data from these datasets. In Fig.11, two datasets with aggregated columns like minMagicPoints and maxMagicPoints are displayed in place of magic points.

Data continuously evolves, grows, and be-

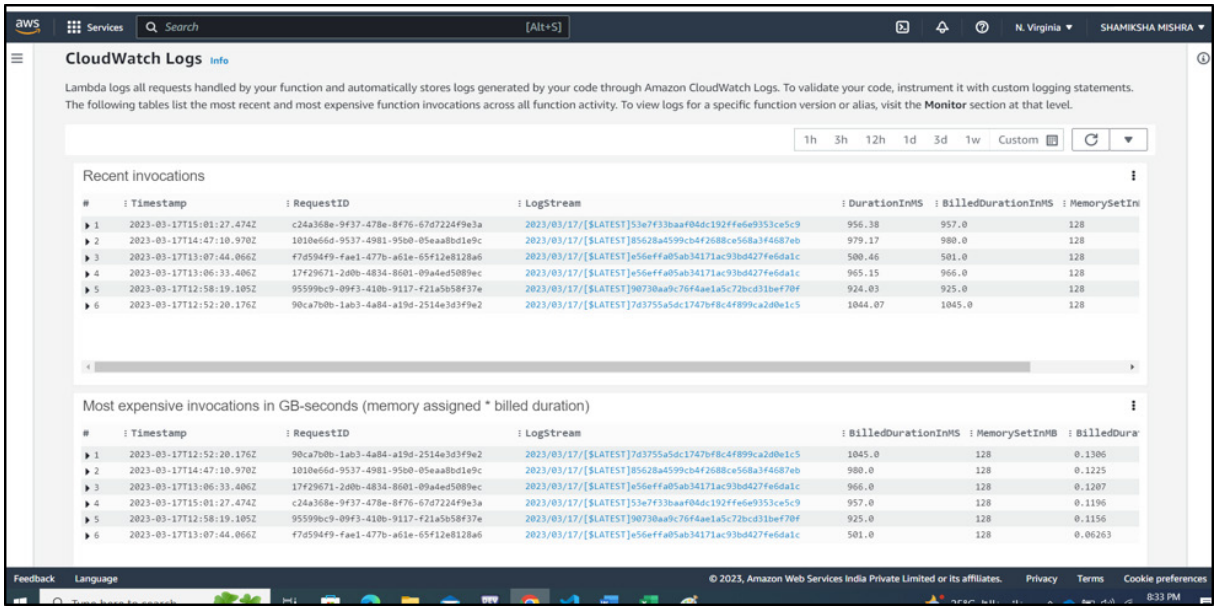

Fig.11. Aggregated data after data analytics

comes more complex with every activity in our ever-evolving, vast, and frustratingly complex technological world. In the modern economy, data is one of the most valuable commodities, but without organization, segmentation, and interpretation, it is practically worthless.

Conclusion and Future work

In this study, we build, deploy and tested the methods and techniques for Amazon Lambda serverless applications. After that, we performed data analysis on these multitenant systems using real-time data streams and dynamic website click data. A system performance metric can be used to determine the performance of a single function call. In a real-time data stream, there are constant peaks where data creation increases over time. During execution, the Lambda function's call metric displays the results. Lambda runtime and code both throw exceptions when a function fails. If a timeout or configuration issue occurs, the runtime will return an error. An error or throttled call request does not result in the creation of a call record. Calls are represented by the value of Invocations, which represents the total number of calls that have been resolved. To get the right analysis results, SQL queries are needed. Real-time tracking of Wild Ryde unicorns was created using Kinesis. Prior to analysis, the input stream was used to gather the source data, which included duplicate and unaggregated records. Data analytics

was used to analyze these datasets, and the aggregated datasets were filtered after analysis. Instead of magic points, two datasets are created with aggregated columns (miniMagicPoints and maximumMagicPoints). Because the platform is self-managed, users can concentrate on using the data rather than managing the platform's environment.In response to customer demands, cloud sites can expand or contract. A lack of storage space would have slowed down the internal system when executing tests with a large amount of data.

Future Work

A major focus of future research will be addressing various security problems related to cloud security and examining the latest developments. A better development environment, more efficient application assembly lines, and improved monitoring tools are available. A promising perspective, serverless integrates well with legacy systems and architectures, can come together with other technologies like Edge, and is integrated with legacy systems. There are many organizations that would benefit from serverless computing. By reducing the number of things your teams need to think about, you still allow them to develop whatever custom application functionality you require. Through the combination of the best architecture and an application, organizations can build the most innovative infrastructure for a high-performance operation.

References

[1] Li, Y., Lin, Y., Wang, Y., Ye, K., & Xu, C. Z. (2022). Serverless computing: state-of-the-art, challenges, and opportunities. IEEE Transactions on Services Computing.

[2] Naranjo, D. M., Risco, S., de Alfonso, C., Pérez, A., Blanquer, I., & Moltó, G. (2020). Accelerated serverless computing based on GPU virtualization. Journal of Parallel and Distributed Computing, 139, 32-42.

[3] Kjorveziroski, V., Filiposka, S., & Trajkovik, V. (2021). Iot serverless computing at the edge: A systematic mapping review. Computers, 10(10), 130.

[4] Sadek, J., Craig, D., & Trenell, M. (2022). Design and Implementation of Medical Searching System Based on Microservices and Serverless Architectures. Procedia Computer Science, 196, 615-622.

[5] Kjorveziroski, V., Bernad Canto, C., Juan Roig, P., Gilly, K., Mishev, A., Trajkovik, V., & Filiposka, S. (2021). IoT serverless computing at the edge: Open issues and research direction. Transactions on Networks and Communications.

[6] AL-Jumaili, A. H. A., Muniyandi, R. C., Hasan, M. K., Paw, J. K. S., & Singh, M. J. (2023). Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations. Sensors, 23(6), 2952.

[7] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(1), 223-246.

[8] Tabrizchi, H., & Kuchaki Rafsanja-

ni, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[9] Golec, M., Ozturac, R., Pooranian, Z., Gill, S. S., & Buyya, R. (2021). IFaaS-Bus: A security-and privacy-based lightweight framework for serverless computing using IoT and machine learning. IEEE Transactions on Industrial Informatics, 18(5), 3522-3529.

[10] Casale, G., Artac, M., Van Den Heuvel, W. J., van Hoorn, A., Jakovits, P., Leymann, F., ... & Zhu, L. (2020). Radon: rational decomposition and orchestration for serverless computing. SICS Software-Intensive Cyber-Physical Systems, 35, 77-87.

[11] Chleier-Smith, J., Sreekanti, V., Khandelwal, A., Carreira, J., Yadwadkar, N. J., Popa, R. A., ... & Patterson, D. A. (2021). What serverless computing is and should become: The next phase of cloud computing. Communications of the ACM, 64(5), 76-84.

[12] Andi, H. K. (2021). Analysis of serverless computing techniques in cloud software framework. Journal of IoT in Social, Mobile, Analytics, and Cloud, 3(3), 221-234.

[13] Shafiei, H., Khonsari, A., & Mousavi, P. (2022). Serverless computing: a survey of opportunities, challenges, and applications. ACM Computing Surveys, 54(11s), 1-32.

[14] Muller, L., Chrysoulas, C., Pitropakis, N., & Barclay, P. J. (2020). A traffic analysis on serverless computing based on the example of a file upload stream on aws lambda. Big Data and Cognitive Computing, 4(4), 38.

[15] Ali, M. H., Hosain, M. S., & Hossain, M. A. (2021). Big Data analysis using BigQuery on cloud computing platform. Australian JofEng Inno Tech, 3(1), 1-9.

[16] Kim, Y., & Lin, J. (2018, July). Serverless data analytics with flint. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 451-455). IEEE.

[17] https://spark.apache.org/

[18] Sharma, V., Nigam, V., & Sharma, A. K. (2020). Cognitive analysis of deploying web applications on microsoft windows azure and amazon web services in global scenario. Materials Today: Proceedings.

[19] Computers | Free Full-Text | IoT Serverless Computing at the Edge: A Systematic Mapping Review (mdpi.com)

[20] An empirical study on challenges of application development in serverless computing https://ieeexplore.ieee.org/abstract/document/9305905/

[21] Serverless Computing - AWS Lambda - Amazon Web Services (https://aws.amazon.com/lambda)

[22] Cloud Functions | Google Cloud (https://cloud.google.com)

[23] Azure Functions – Serverless Functions in Computing | Microsoft Azure (https://acloudguru.com/azure/functions)

Smart Analysis and Detection System for New Host-Based Cryptojacking Malware Dataset

Hadeel Almurshid

Computer Science Department, Prince Sultan University, Riyadh 11586, Saudi Arabia,
221421254@psu.edu.sa

Abstract

Cryptocurrency is a quickly growing technology in the finance industry, with the first cryptocurrency, Bitcoin, being created in 2009. Each cryptocurrency has its own unique hash value, and cryptocurrency mining involves participating in a guessing competition to release a unique hash into circulation, with the winner receiving a modest bonus in the form of bitcoin. However, as more bitcoins are discovered, it becomes increasingly difficult to obtain more, resulting in a need for extra computer resources and power. Consequently, the increasing popularity of cryptocurrency has led to a rise in cryptojacking malware, which secretly uses victims' computing resources to mine cryptocurrency. This malware can be either web-based or host-based, with similar execution and goals but differing in implementation and injection. Cryptojacking has affected numerous devices worldwide, but few studies have been carried out to detect it, especially the host-based type. Furthermore, the current studies on cryptojacking have limited datasets, which are often outdated or small, and the prediction models developed from these datasets may not be accurate. To address this gap, we conducted a thorough analysis of cryptojacking's behavior, lifecycle, impact, implementations, and possible detection methods. Additionally, we created an up-to-date dataset consisting of 114,985 samples, with 57,948 categorized as benign and 57,037 as cryptojacking. The dataset was used to build a smart cryptojacking detection system, with 5 different convolutional neural network models trained and evaluated against a subset of the dataset. The best performing model achieved an accuracy of 98.4%, an F1-Score of 98.3%, a precision of 98.4%, and a recall of 98.4%. Our proposed method, which involves running Windows executables in an isolated environment and closely monitoring their CPU usage, provides a thorough understanding of cryptojacking malware behavior and enables detection of the malware. The comprehensive dataset collected facilitates efficient detection model development. Additionally, evaluating the dataset with 5 different CNN algorithms and assessing their performance using established evaluation metrics ensures the effectiveness of our proposed method and dataset.

Keywords: Cryptocurrency; Cryptomining; Blockchain; Cryptojacking Malware; Host-based; Machine Learning; Deep Learning; Convolutional Neural Network (CNN); Dataset.

Introduction

Cryptocurrency has emerged as one of the fastest-evolving technologies in finance. Money has taken various forms throughout history, such as goods, cowrie shells, metal, banknotes, and more. However, the true revolution of money came in 2009 when an anonymous person or group named Satoshi Nakamoto introduced Bitcoin, the first-ever cryptocurrency [1]. Bitcoin's primary aim is to eliminate the need for intermediaries to control transactions. Instead, it relies on a computer algorithm called the blockchain [2] [3] [4], which operates based on

trust in the algorithm rather than any individual or institution.

Each cryptocurrency has a unique hash, and cryptocurrency mining involves solving a complex mathematical problem to guess the hash and release it into circulation. The winner of the mining competition receives a small amount of cryptocurrency as an incentive, encouraging users to support the peer-to-peer network [1]. However, as more bitcoins are discovered, obtaining more becomes increasingly challenging, requiring more computer resources and electricity.

As mining becomes more difficult and resource-intensive, attackers have developed an illegal mining technique called cryptojacking, which allows them to receive the mining reward without using their resources. Cryptojacking malware is a new type of malware that can be classified into web-based and host-based cryptojacking [5]. In web-based cryptojacking, the attacker takes advantage of client-side web scripting technologies, such as JavaScript and WebAssembly, to inject the cryptomining code into a legitimate website to force visitors' devices to mine cryptocurrency for them. In host-based cryptojacking, the attacker first needs to download the cryptominer into the victim's device and then run the miner to force the device to mine cryptocurrency for them without the victim's knowledge.

Research Problem and Motivation

In recent times, cryptojacking has become a widespread issue affecting numerous devices worldwide [5]. This is due to the high resource requirements of mining, which can cause the victim's device to overheat and experience performance issues. Despite this, there has been a limited amount of research on detecting cryptojacking. Most of the research conducted on cryptojacking detection has focused on web-based cryptojacking malware [6] [7] [8] [9] [10] [11], with little research conducted on host-based cryptojacking malware in 2022 and 2023 so far. Additionally, some studies have used outdated or insufficient datasets to build prediction models, further highlighting the need for more comprehensive research.

In this study, we aim to provide a thorough analysis of cryptojacking malware, with a specific focus on host-based cryptojacking malware. Our study includes examining its behavior, lifecycle, implementations, and impact, as well as proposing potential detection solutions. We also introduce an up-to-date dataset of host-based cryptojacking malware that can be utilized to train and test machine learning and deep learning models, evaluate intrusion detection systems, and develop new mitigation strategies. Additionally, we can analyze this dataset to provide insights into the tactics and techniques used by attackers, helping to better defend against this growing threat. Overall, our dataset represents a valuable contribution to the cybersecurity field, and we hope it will inspire further research and innovation in the fight against this emerging malware.

Contributions and Paper Structure

As a result of the identified shortcomings

and gaps in research, particularly with regard to detecting host-based cryptojacking malware, we have primarily made the following contributions:

- Conducting a comprehensive study of the behavior and implementation of cryptojacking malware, as well as its impact.
- Analyzing and comparing various current methods for identifying cryptojacking malware.
- Introducing a large and up-to-date dataset of host-based cryptojacking malware.
- Evaluating the effectiveness of our dataset by testing and examining a range of deep learning algorithms.

Therefore, our contributions are significant in advancing cybersecurity by intensely studying and analyzing cryptojacking malware, providing a new dataset of host-based cryptojacking malware, conducting a thorough dataset analysis, and evaluating the performance of different CNN models for detecting and classifying this type of malware. The remainder of this work is structured as follows. Section 2 provides a brief overview and background of cryptocurrency, cryptomining, and cryptojacking malware categories. Section 3 summarizes and discusses the state-of-the-art cryptojacking malware detection techniques and highlights their limitations. Section 4 describes the research methodology of building the new dataset of host-based cryptojacking malware in detail. It also explains the malware cryptojacking analysis, sources of the samples, the data collection process, the dataset's composition, and the dataset's evaluation using different CNN models. Finally, section 5 summarizes the paper's conclusions and discusses the implications of the findings. Also, it highlights the study's limitations and suggests future research directions.

Background

This section provides background about cryptocurrency, cryptomining, and cryptojacking malware. To fulfill our first research objective, we conducted a comprehensive analysis of both types of cryptojacking malware, examining how they operate, are created and distributed, and the consequences they have on infected systems.

Cryptocurrency

Many people may ask: Why do people use cryptocurrency? What makes it valuable and trusted? What is cryptojacking and how is it used to make money? These questions could be answered by first understanding the history of money and how it has evolved up until today. By learning about the origins and development of money, we can gain a better understanding of the potential benefits and risks of using cryptocurrency, as well as the impact of cryptojacking on the cryptocurrency ecosystem.

Money has always been an essential need for humankind, dating back to the earliest records of history. In the past, people relied on direct bartering to exchange goods and services [12]. However, this system had several drawbacks. For instance, goods were not always divisible, making it challenging

to make exchanges. For example, a person wanting to buy a water bottle with a fully-grown cow would be out of luck. Additionally, determining the value of different goods could be challenging. For example, a farmer wanting to buy a diamond ring might have to offer several cars to match its price. To overcome these issues, our ancestors developed a more generic form of money.

Initially, cowrie shells were used as a form of currency [13], and they were used extensively and for an extended period, compared to other forms of primitive money. For many people, cowrie shells were considered ideal since they were durable, easy to count and clean, and difficult to counterfeit. However, as trade increased, the use of cowrie shells became more prevalent, leading to an oversupply and consequent depreciation. Other less common forms of primitive money included whale teeth and Rai stones.

Subsequently, human society transitioned from primitive money to coin money. Initially, coins were made from various metals, including copper, bronze, iron, aluminum, gold, and silver. Metals thus formed the basis of the transition from primitive money to coined money [14]. Initially, metal chunks were used as money, based on their weight. Subsequently, they were stamped to create coins, marking the first step in the shift from weighted to counted money.

As civilization evolved, new machines were invented for minting and printing, leading to the emergence of paper money [15]. These two forms of currency have endured over time and continue to be widely used today. Nowadays, when most people hear the term 'money,' they typically think of banknotes and coins.

Initially, banknotes and coins were backed by valuable objects, particularly gold. However, due to the perceived constraints of this system, bankers eliminated the gold standard in 1971, as declared by former U.S. president Richard Nixon [16]. This decision marked the introduction of what is now known as fiat currency. Unlike previous forms of money, fiat currency derives its value solely from the trust placed in the governing authorities [2], without any direct backing by precious metals or other tangible assets.

Money has continued to evolve with the advent of digitalization. Nowadays, a significant amount of money exists in digital form, with bank account balances being represented by digital numbers that are monitored and controlled by banks. Instead of relying solely on cash, many individuals now use credit cards for their purchases. The combination of the shift towards digital transactions and the concept of fiat currency has laid the groundwork for the development of cryptocurrency, which represents a true evolution in the realm of money.

In 2009, an individual or group operating under the pseudonym Satoshi Nakamoto introduced the world to Bitcoin, the first cryptocurrency. Bitcoin operates on the premise that it does not require trust in any particular entity or institution, but rather in the integrity of a computer algorithm

known as the blockchain [2]. It is decentralized and not managed by any government or central bank; instead, it is overseen by a vast network of computers around the globe. The more people trust and use Bitcoin or other cryptocurrencies, the more valuable they become. This is demonstrated by Bitcoin's price, which surged from $500 in 2015 to over $20,000 in 2022 [17].

Cryptomining

The process of obtaining a Bitcoin can be accomplished by either purchasing or mining it. Bitcoin is essentially a unique hash. Mining Bitcoins entails attempting to solve a complex mathematical problem to predict a hash of a Bitcoin that has not yet been released into circulation. This procedure is analogous to gold mining [1], where miners must expand their territory and use more resources to acquire more gold. In cryptocurrency mining, also known as cryptomining, the more Bitcoins that are discovered, the more challenging it becomes to obtain more of them. This complexity is reflected in the need for additional computer resources and electricity [1]. The mining function is a critical component of cryptocurrency because there is no authority to add new coins to circulation, and this is the only method for doing so.

Cryptojacking Malware

Cryptojacking is the illegal mining of cryptocurrency. As the mining process becomes very expensive, attackers invented a new type of malware that is called cryptojacking malware to force the victim's device to mine cryptocurrency for them. The malware can be found in two types, web-based and host-based.

Web-based Cryptojacking Malware

The interactive technologies of web browsers, including JavaScript and WebAssembly (Wasm), have frequently been exploited for malicious purposes [5]. In the context of cryptojacking, a harmful mining code is injected into a website to force visitors' devices to mine cryptocurrency. The trend of this attack began in 2017, when a service provider named Coinhive introduced a mining script that could be directly inserted into a web page to mine a particular cryptocurrency, Monero [10]. The company's objective was to provide website owners with a way to generate revenue as a substitute for using advertisements. However, hackers misused the service by illegally injecting the script into legitimate websites to mine cryptocurrency. Figure 1 depicts the lifecycle of web-based cryptojacking malware.

The illustrated lifecycle begins with the attacker signing up with a service provider, who then provides a unique API key to the attacker. This API key is used in a script that the attacker injects into a public website. Whenever a user visits the infected website, the malicious code runs in the background and mines cryptocurrency. Since the code includes the attacker's API key, the attacker will receive the revenue generated by the mining operation.

Host-based Cryptojacking Malware

In contrast, host-based cryptojacking malware requires direct installation onto the

victim's machine for cryptocurrency mining such as xmrig, T-Rex, ccminer, etc. [5]. The attacker may disguise the malicious mining code as seemingly harmless software, which can be downloaded by the user. Infected software is often located on online data-sharing platforms like Torrents and public clouds [18].

With attackers increasingly targeting more powerful machines, animators and video gamers have become primary targets [19]. Crackonosh, a miner malware, was found in multiple popular games, as per a report released by Avast [20]. The attacker uses a tool called InnoSetup [21] to inject miner software into a legitimate video game installer, allowing them to combine the miner installation with legitimate software. In essence, the miner and legitimate software are installed and operated simultaneously during installation. Figure 2 illustrates the lifecycle of the host-based cryptojacking malware.

The lifecycle of the host-based cryptojacking malware begins with the attacker using a tool like InnoSetup to merge legitimate software, such as a game, with a miner. A specific type of malware known as Crackanosh is an example of this. The attacker then uploads the infected file to a publicly available sharing platform. Once the victim downloads and installs the infected files, they become infected with the cryptojacking malware, and the attacker can generate revenue through their API key, which is included in the miner executable.

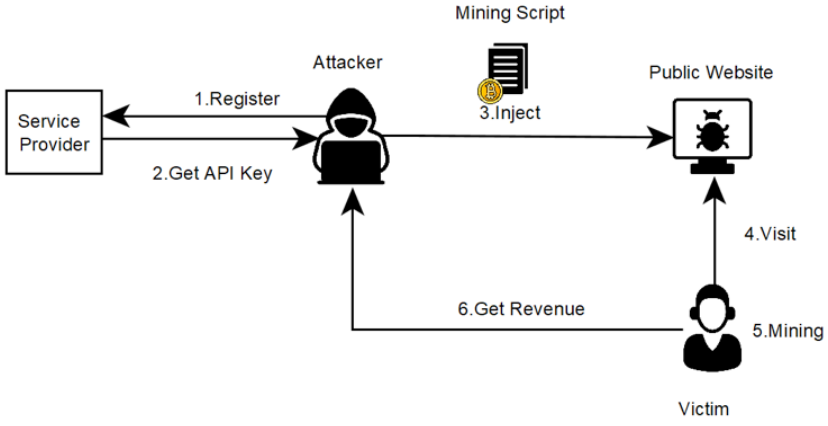

Fig. 1. Web-based cryptojacking malware lifecycle

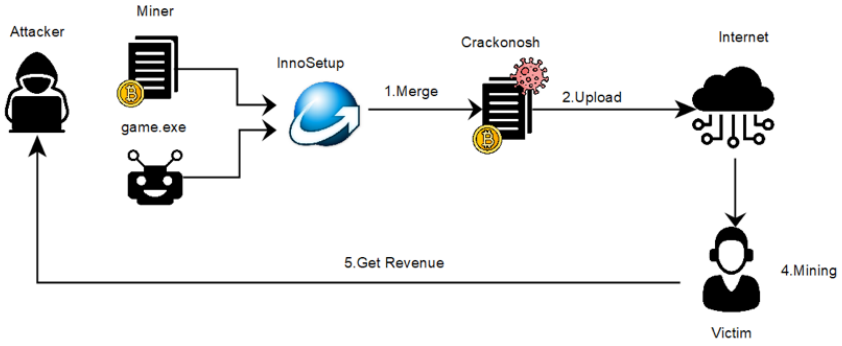

Fig. 2. Host-based cryptojacking malware lifecycle

Literature Review

As we mentioned earlier, Cryptojacking refers to the unauthorized mining of cryptocurrency using malware known as Cryptojacking Malware. It has significantly impacted both individuals and organizations, leading to increased costs, slow or non-functional devices, and higher electricity bills due to the computing power required. However, it is important to highlight that the effect of cryptojacking on the cryptocurrency and blockchain industry has not been thoroughly studied, providing a chance to explore new research directions [5].

In this section, to accomplish our second research objective, we aim to enhance the understanding of current research directions by analyzing and comparing various methods used to identify cryptojacking malware. This malware is classified into two categories: Web-based Cryptojacking Malware and Host-based Cryptojacking Malware [5]. Below is a recent review study of both types.

Web-based Cryptojacking Malware

In [6], Faraz Naseem et al. presented MINOS, a lightweight detector for web-based cryptojacking malware that aims to detect mining activities on websites utilizing the WASM programming language. The detector utilizes deep learning and implements a convolutional neural network (CNN) model that has been trained on a dataset of 300 samples, half of which are malicious. MINOS achieved an accuracy of 98.97% while consuming only 4% and 6.5% of CPU and RAM, respectively. It should be noted that MINOS is only compatible with the Google Chrome web browser.

In [7], Franco Tommasi et al. put forward MinerAlert, a new technique that detects web-based cryptomining in real-time using a web browser extension. The approach uses a Support Vector Machine (SVM) model that classifies web pages based on the analysis of hardware resources performance like CPU and web page behavior. The researchers gathered data from 604 websites, including 130 malicious ones. By running the model on a combination of several features, they achieved a maximum accuracy of 99.59%.

In [8], Aldo Hernandez-Suarez et al. presented a new approach in which they used a deep dense neural network (DDNN) to classify websites based on their network traffic and hardware performance. The dataset consisted of 8000 benign sites and 8156 cryptojacking websites, and 18 different features were used as input to the model (such as total processor idle time, disk reading/sec, disk writing/sec, number of subprocesses, etc.). Their deep learning model achieved a precision of 99.41%, a recall of 99.10%, and an F1 score of 99.25%.

In [9], HYUNJI HONG et al. introduced CIRCUIT, a novel approach for detecting cryptojacking websites by monitoring the memory heap. This technique involves generating heap graphs that depict the behavior of the JavaScript code and extracting reference flows to identify the call flow of JavaScript objects and detect

cryptojacking behavior. To aid in detection, CIRCUIT stores signatures for cryptojacking websites. The authors noted that CIRCUIT is particularly effective at detecting obfuscated cryptojacking scripts. Their approach successfully detected 1813 cryptojacking websites among the top 306K websites, which includes the Alexa top 100K, Majestic top 200K, and Alexa category top websites. However, CIRCUIT has limitations, such as difficulties in handling abnormally obfuscated mining scripts resulting in long reference flows, which in turn requires significant editing when comparing signatures. It may also face issues when dealing with very short reference flows.

In [10], Min-Hao Wu et al. have presented a solution based on artificial neural network (ANN) named MinerGuard. The system aims to identify the existence of web-based cryptojacking malware by relying heavily on monitoring the CPU usage of the webpage. The authors used a dataset of 850 websites, with 350 classified as miners, and obtained an accuracy rate of 99%, including the detection of zero-day attacks. However, it should be noted that MinerGuard is only compatible with the development version of Google Chrome and relies on the chrome.processes API

In [11], Khan Abbasi et al. have proposed a hybrid approach to detect and prevent web-based cryptojacking malware. The approach aims to detect malware in both WASM and non-WASM scripts and comprises three phases: 1) comparing suspicious URLs to a blacklist, 2) analyzing malware based on static signatures, and 3) conducting dynamic analysis of malware. The authors evaluated their proposed solution on a dataset of 1000 samples, 30 of which were malicious, gathered from Alexa and PublicWWW. The approach achieved an accuracy of 99.6%.

Host-based Cryptojacking Malware

In [22], Hamid Darabian et al. conducted a study on the effectiveness of machine learning algorithms in detecting cryptojacking malware. The study utilized a dataset of 1500 Windows Portable Executables that were registered in VirusTotal in 2018. Both static and dynamic analyses were performed on the malware samples. For static analysis, the authors employed Long Short-Term Memory (LSTM), Attention-based LSTM, and CNN algorithms. These ML models were implemented into the opcodes of the cryptojacking malware samples, and a 95% accuracy rate was achieved. In dynamic analysis, the malware samples were executed in a sandbox environment, and system call sequences were captured, resulting in a success rate of 99%.

In [23], Dmitry Tanana proposed a detection technique that relies on the analysis of CPU and RAM consumption to detect the presence of cryptojacking, regardless of whether it is web-based or host-based. The technique employs a decision tree algorithm that compares the CPU and RAM consumption of an application to a predefined threshold. The author tested the technique on a dataset comprising 20 web-based cryptojacking and 5 host-based

cryptojacking malware samples and validated it on 40 browser-based and 10 host-based cryptojacking malware samples, all of which were collected from VirusShare in 2019. The technique achieved an 82% success rate.

In [24], Ganapathy Mani et al. introduced a novel framework named DeCrypto Pro, which is designed to select the appropriate machine learning algorithm, such as Random Forest, k-Nearest Neighbor, or LSTM, based on the computing resources of the system being investigated. DeCrypto Pro utilizes performance counters, such as CPU usage, to classify an application as benign or malicious. The authors collected and monitored a dataset of performance counters by running benign software, including 7-Zip, SecureZip, PeaZip, WinRAR, WinZip, and Freemake, as well as malicious software such as XMRig, XMRStak, Coinhive, Computta, and GUIminer. The proposed framework achieved an F1-score of 89.99%, 97.62%, and 95.5% for k-Nearest neighbor, Random Forest, and LSTM classifiers, respectively.

In [25], Gilberto Gomes et al. presented the CryingJackpot intrusion detection system (IDS), an unsupervised approach to detecting cryptojacking. The proposed solution utilizes system events and network flow data of an application as features for clustering, using K-means, Agglomerative, DBSCAN, and ensemble machine learning algorithms. The system was evaluated on a public dataset (CSECIC-IDS2018) and achieved an F1-Score of 82%. Additionally, the authors evaluated the system on a separate dataset they created and obtained an F1-Score of 97%. CryingJackpot is capable of detecting both types of cryptojacking malware.

In November 2021, a systematic study of 128 research papers was conducted by Ege Tekiner et al. [5] Two datasets were collected for the purpose of analyzing cryptojacking malware. The first dataset was obtained from VirusTotal using academic access and contained 20,200 cryptojacking samples. The second dataset was obtained from PublicWWW and contained 6,269 URLs. Among the key findings, only 7 out of the 128 research papers examined host-based cryptojacking malware, and Monero was identified as the most targeted cryptocurrency.

According to the 2022 mid-year update cyber threat report from SONICWALL[26], although cryptocurrency prices had decreased, the volume of cryptojacking malware had still increased. However, our research shows that there has been very little focus on web-based cryptojacking malware in 2022 and almost no contributions toward host-based malware. This is likely due to limited access to host-based malware samples, such as those from VirusTotal and VirusShare, in comparison to publicly available website samples.

Attackers are increasingly targeting devices with more processing power for faster profit, making host-based cryptojacking malware the new trend [5]. The European Union Agency for Cybersecurity (ENISA) cryptojacking report [27] states that host-based cryptojacking botnets can generate

$750K in a month, while web-based botnets can only generate $30K.

The main objective of our study is to enhance the field of cryptojacking detection by generating an extensive and up-to-date dataset of over 100,000 samples and building multiple detection models to demonstrate its efficiency. The effectiveness of these models will be assessed using standard metrics such as accuracy, recall, precision, and F1 score to determine the best model. Table 1 summarizes the previous research in this area.

Table 1. Summary of Previous Studies

Work	Year	Dataset	ML-Based	Classifier	Type	Performance
Minos [6]	2021	Benign: 150 Malicious: 150	Yes	CNN	Web-based	Accuracy=98.97%
MinerAlert [7]	2022	Benign: 474 Malicious: 130	Yes	SVM	Web-based	Accuracy=99.59%
[8]	2022	Benign: 8000 Malicious: 8156	Yes	DDNN	Web-based	Precision=99.41% Recall=99.10% F1-score=99.25%
CIRCUIT [9]	2022	306K most popular websites	No		Web-based	1813 cryptojacking websites detected
MinerGuard [10]	2022	Benign: 500 Malicious: 350	Yes	ANN	Web-based	Accuracy=99%
[11]	2023	Benign: 970 Malicious: 30	No	-	Web-based	Accuracy=99.6%
[22]	2020	Malicious: 1500	Yes	LSTM, Attention-based LSTM, CNN	Host-based	Static: Accuracy=95% Dynamic: Accuracy=99%
[23]	2020	Malicious: Web-based: 60 Host-based: 15	Yes	DT	Both	Success rate=82%
DeCrypto Pro [24]	2020	Benign: 6 Malicious: 5	Yes	RF, KNN, LSTM	Host-based	F1-score: KNN=89.99% RF=97.62% LSTM=95.5%
CryingJackpot [25]	2020	Dataset1: CSECIC-IDS2018 Dataset2: Malicious: Web-based: 5 Host-based: 5	Yes	K-means, Agglomerative, DBSCAN, ensemble ML	Both	Dataset1: F1-score=82% Dataset2: F1-score=97%
Ours (Proposed)	2023	Benign: 20,000 Malicious: 20,000	Yes	5 CNN models Best performed: Color-based Scratch model [28]	Host-based	Accuracy=98.4% F1-score=98.3% Precision=98.4% Recall=98.4%

Research Methodology

We initiated this study by analyzing and explaining the characteristics of cryptojacking malware, including its behavior when impacting a system. Subsequently, we presented an up-to-date dataset of host-

based cryptojacking malware comprising 114,985 sample files. We proved the effectiveness of this dataset by training and evaluating 5 distinct CNN models using a subset of 40K balanced samples consisting of 20,000 benign and 20,000 cryptojacking samples.

Cryptojacking Malware Analysis

As noted before, cryptojacking malware does not cause direct harm like other kinds of malware (e.g., ransomware). At first glance, it may not seem as harmful; however, it causes severe consequences the longer it resides in the infected system. It greedily drains the infected system's resources, resulting in system deficiencies and high electricity consumption.

To enrich our first objective and gain a better understanding of the behavior of the malware, we executed multiple Windows executables in an isolated environment and closely monitored their CPU usage. The graphical representation in Figure 3 illustrates the typical CPU usage of the machine (7%), while Figure 4 depicts the CPU consumption when the cryptojacking malware was running (100%).

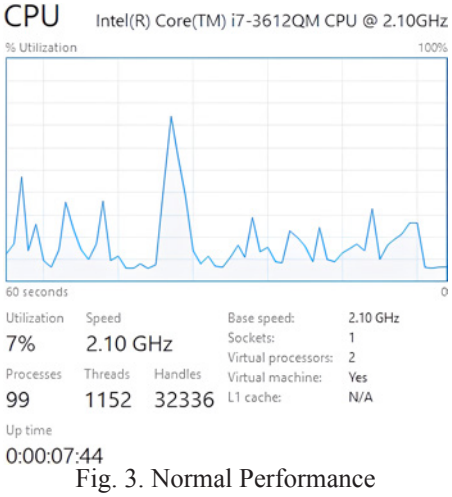

Fig. 3. Normal Performance

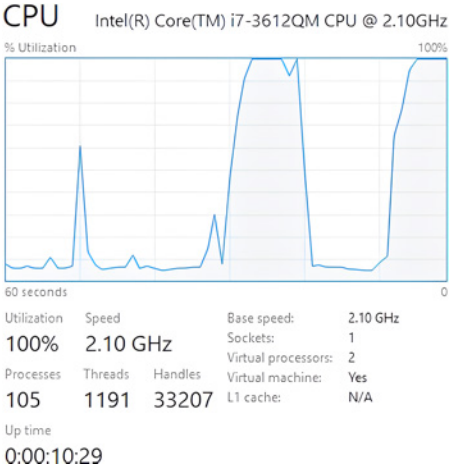

Fig. 4. Performance with Cryptojacking Malware Running

It is not surprising that the CPU usage increases significantly when running cryptojacking malware, as its primary function is to compute unique hashes for cryptocurrency mining using cryptography libraries and APIs. As a result, the performance of the system is affected due to the resource-intensive nature of these activities.

Dataset Collection

In this work, we aim to address the current gap in the literature regarding host-based cryptojacking malware detection [5]. To achieve our third research objective, we gathered a comprehensive dataset of 114,985 samples to facilitate the development of efficient detection models. The dataset was generated recently and collected in January 2023 using a premium VirusTotal [29] account. It includes executable files in a variety of formats, such as exe, pe, elf, apk, among others.

We used VirusTotal to search for both benign and cryptojacking samples and stored their hashes in two separate text files. The initial output was 57,037 hash values for executable files of cryptojacking malware

samples and 57,948 hash values for executable files of benign software samples. To further process the data, we divided each text file into several chunks of 5000 hash values. We then utilized VirusTotal to download the actual executable files for each chunk file. After this, we carefully cleaned the dataset by removing any files that were irrelevant or damaged. The resulting dataset contains a total of 114,985 samples, which is our final output.

Cryptojacking CNN-based Detection Analysis: A Case Study

Our final objective of evaluating the effectiveness of our dataset was achieved through testing it with 5 different CNN algorithms: Scratch [28], VGG16, ResNet50, VGG19, and DenseNet121.

To conduct our testing, we employed a balanced dataset of 40,000 samples. The executable files were converted to color images, and subsequently to grayscale images. We trained each algorithm twice - once with color images and once with grayscale images. We assessed the performance of each trained model using the evaluation metrics described in [30] [31]:

$$\text{Accuracy} = \frac{TN + TP}{FP + TP + FN + TN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

$$\text{F1 Score} = \frac{2 * Precision * Recall}{Precision + Recall} = \frac{2 * TP}{2 * TP + FP + FN} \quad (4)$$

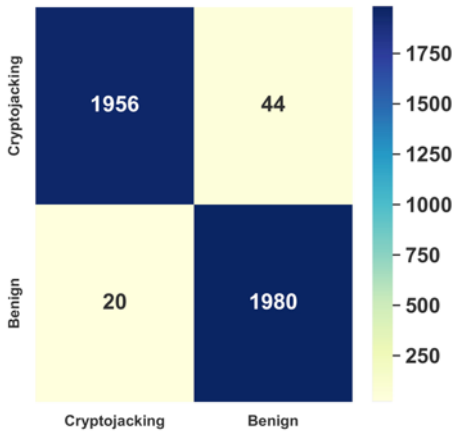

Fig. 5. Scratch Model Confusion Matrix

where TP is true positive score, FP is false positive score, TN is true negative score, and FN is false negative score [32] [33].

After conducting a comprehensive analysis and evaluation of all CNN models, the Scratch model [28] demonstrated the best performance in detecting cryptojacking malware when color images were used. It resulted in an accuracy of 98.4%, an F1-score of 98.3%, a precision of 98.4%, and a recall of 98.4%. Figure 5 shows the confusion matrix, and Figure 6 shows the loss and accuracy curve of the Scratch model's performance.

On the other hand, ResNet50 showed the best performance in detecting cryptojacking malware when grayscale images were used. It achieved an accuracy of 97.8%, an F1-score of 97.8%, a precision of 97.8%, and a recall of 97.8%. Figure 7 displays the confusion matrix, and Figure 8 displays the loss and accuracy curve of the ResNet50 model's performance.

All the tested models exhibited promising performance in terms of all the examined assessment detection parameters. The evaluation results for each model using

both color and grayscale images are presented in Table 2.

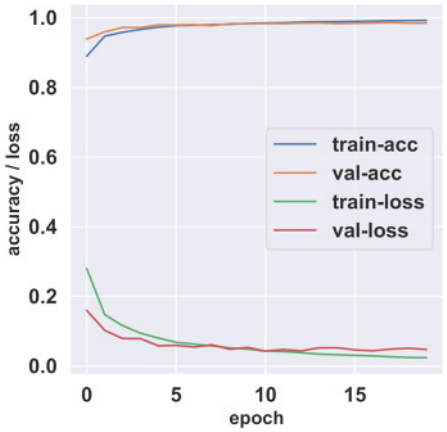

Fig.6. Scratch Model Loss and Accuracy Curve

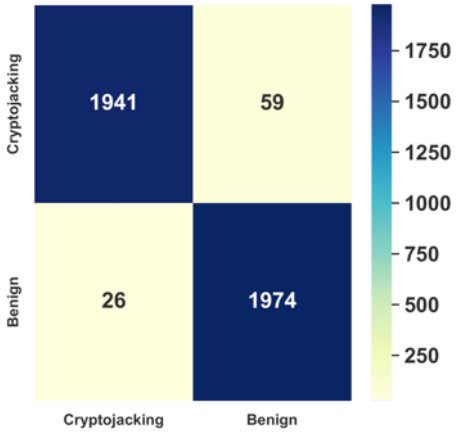

Fig. 7. ResNet50 Model Confusion Matrix

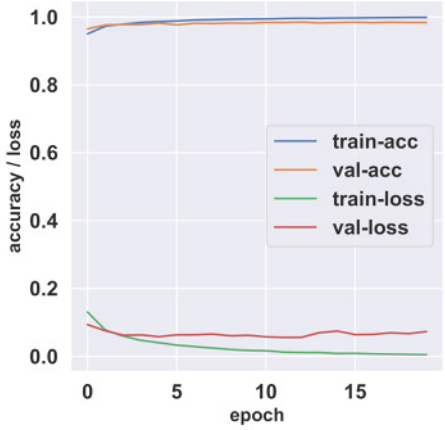

Fig. 8. ResNet50 Model Loss and Accuracy Curve

Table 2. Results of Evaluation Analysis

Model	Format	Accuracy (%)	F1 Score (%)	Precision (%)	Recall (%)
Scratch	color	98.4	98.3	98.4	98.4
	gray	97.7	97.7	97.8	97.8
VGG16	color	98.1	98.1	98.1	98.1
	gray	97.7	97.7	97.8	97.8
ResNet50	color	98.1	98.1	98.1	98.1
	gray	97.8	97.8	97.8	97.8
VGG19	color	97.8	97.8	97.8	97.8
	gray	97.2	97.2	97.2	97.2
DenseNet21	color	97.2	97.1	97.3	97.2
	gray	96.7	96.7	96.8	96.7

Conclusion and Future Work

To sum up, the use of cryptojacking malware poses a substantial danger to both individuals and organizations. This malicious software can covertly seize a victim's computer resources to mine cryp-

tocurrency without their awareness or consent. Despite being a relatively recent phenomenon, cryptojacking malware has already inflicted significant harm on numerous victims.

Our study is very important as it provides valuable insights into how cryptojacking malware works, is injected, implemented, and executed. This will serve further research into understating cryptojacking malware to help in creating better detection and prevention strategies. Additionally, we surveyed the current studies in the cryptojacking malware, thus helping in introducing current gaps and limitations to encourage more efficient solutions. Furthermore, we introduced a large up-to-date dataset of 114,985 samples for host-based cryptojacking malware. We demonstrated the efficacy of our dataset by training 5 convolutional neural network models against a subset of it, using both color and grayscale images. The Scratch model using color images performed the best, with an accuracy of 98.4%, an F1-Score of 98.3%, a precision of 98.4%, and a recall of 98.4% This research emphasizes the need for ongoing investigation into cryptojacking malware and the implementation of robust cybersecurity measures to safeguard against this growing threat. As a result, it is crucial for both individuals and organizations to remain vigilant and take appropriate measures to protect their systems and data against cryptojacking attacks.

While our study has yielded valuable insights into the features and actions of cryptojacking malware, it is important to acknowledge its limitations. These include:

- The dataset has been obtained from a single source, and the cryptojacking samples included in the dataset were restricted to those identified by antivirus software in VirusTotal.
- Our models were trained on a portion of the dataset, rather than the complete dataset.
- Restricting model training to only 5 models
- The malware was not statically analyzed
- Furthermore, there are numerous opportunities for further research that can broaden and enhance the findings of this study. The following are potential areas for future investigation:
- Increase the number of ML and DL models trained on the complete dataset
- Collect host-based cryptojacking malware datasets from multiple sources
- Conduct research to comprehensively analyze the impact of cryptojacking malware on the cryptocurrency industry
- Explore and analyze the different targets of cryptojacking malware.
- Examine and analyze the existing techniques used by organizations to detect and prevent cryptojacking malware
- Examine and analyze the existing techniques used by organizations to hinder the impact of the cryptojacking malware

References

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system, october 2008,” Metzdowd mailing list, 2008.

[2] E. Prasad, The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance, 1st ed. Belknap Press: An Imprint of Harvard University Press, 9 2021.

[3] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "Petroblock: A blockchain-based payment mechanism for fueling smart vehicles," Applied Sciences, vol. 11, no. 7, p. 3055, 2021.

[4] A. Allouch, O. Cheikhrouhou, A.Koubˆaa, K. Toumi, M. Khalgui, and T. Nguyen Gia, "Utm-chain: blockchain-based secure unmanned traffic management for internet of drones," Sensors, vol. 21, no. 9, p. 3049, 2021.

[5] E. Tekiner, A. Acar, A. S. Uluagac, E. Kirda, and A. A. Selcuk, "Sok: Cryptojacking malware," in 2021 IEEE European Symposium on Security and Privacy (EuroSP). IEEE, 2021, pp. 120–139.

[6] F.Naseem, A. Aris, L. Babun, E. Tekiner, and A. S. Uluagac, "Minos*: Alightweight real-time cryptojacking detection system." Network and Distributed Systems Security (NDSS) Symposium 2021, 2 2021.

[7] F. Tommasi, C. Catalano, U. Corvaglia, and I. Taurino, "Mineralert: an hybrid approach for web mining detection," Journal of Computer Virology and Hacking Techniques, vol. 18, p. 333–346, 2022.

[8] A. Hernandez-Suarez, G. Sanchez-Perez, L. K. Toscano-Medina, J. Olivares-Mercado, J. Portillo-Portilo, J. G.Avalos, and L. J. G.Villalba, "Detecting cryptojacking web threats: An approach with autoencoders and deep dense neural networks," Applied Sciences (Switzerland), vol. 12, no. 7, 2022.

[9] H. Hong, S. Woo, S. Park, J. Lee, and H. Lee, "Circuit: A javascript memory heap-based approach for precisely detecting cryptojacking websites," IEEE Access, vol. 10, pp. 95 356–95 368, 2022.

[10] M.-H. Wu, Y.-J. Lai, Y.-L. Hwang, T.-C. Chang, and F.-H. Hsu, "Minerguard: A solution to detect browser-based cryptocurrency mining through machinelearning," Applied Sciences, vol. 12, no. 19, 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/19/9838

[11] M. H. Khan Abbasi, S. Ullah, T. Ahmad, and A. Buriro, "A real-time hybrid approach to combat in-browser cryptojacking malware," Applied Sciences, vol. 13, no. 4, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/4/2039

[12] G. Davies, A History of Money: From Ancient Times to the Present Day, 3rd ed. University of Wales Press, 11 2002.

[13] P. Patel, A. Dalvi, and I. Siddavatam, "Exploiting honeypot for cryptojacking: The other side of the story of honeypot deployment," in 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA. IEEE, 2022, pp. 1–5.

[14] L. P. Krishnan, I.Vakilinia, S. Reddivari, and S. Ahuja, "Scams and solutions in cryptocurrencies— a survey analyzing

existing machine learning models," Information, vol. 14, no. 3, p. 171, 2023.

[15] Z. Mineau, D. Hoffman, J. Lor, and N. Choudhury, "Cryptocurrency: Is it the future of payments?" in Cybersecurity for Smart Cities. Springer, 2023, pp. 169–183.

[16] T. I. TEAM, "Fiat vs. representative money: What's the difference?" https://www.investopedia.com/ask/answers/041615/what-difference-betweenfiat- money-and-representative-money.asp, 10 2022.

[17] "Coinmarketcap - bitcoin," https://coinmarketcap.com/currencies/bitcoin/, 10 2022.

[18] M. Abdelrahim, B. Omonayajo, A. S. Mubarak, and F. Al-Turjman, "Crypto currency cloud mining," in 2022 International Conference on Artificial Intelligence in Everything (AIE). IEEE, 2022, pp. 488–492.

[19] A. Mozo, A´ . Gonza´lez-Prieto, A. Pastor, S. Go´mez-Canaval, and E. Talavera, "Synthetic flow-based cryptomining attack generation through generative adversarial networks," Scientific Reports, vol. 12, no. 1, p. 2091, 2022.

[20] "avastreport," https://decoded.avast.io/danielbenes/crack-onosh-a-new-malwaredistributed- in-cracked-software/, 3 2023.

[21] "Innosetup," https://jrsoftware.org/isinfo.php, 3 2023.

[22] H. Darabian, S. Homayounoot, A. Dehghantanha, S. Hashemi, H. Karimipour, R. M. Parizi, and K. K. R. Choo, Journal of Grid Computing.

[23] D. Tanana, "Behavior-based detection of cryptojacking malware," in 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). IEEE, 2020, pp. 0543–0545.

[24] G. Mani, V. Pasumarti, B. Bhargava, F. T. Vora, J. Macdonald, J. King, and J. Kobes, "Decrypto pro: Deep learning based cryptomining malware detection using performance counters." IEEE, 2020, pp. 109–118.

[25] G. Gomes, L. Dias, and M. Correia, "Cryingjackpot: Network flows and performance counters against cryptojacking," in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). IEEE, 2020, pp. 1–10.

[26] "Min-year update 2022 sonicwall cyber threat report," pp. 31–33, 6 2022.

[27] "Cryptojacking enisa threat landscape report," 2020.

[28] I. Almomani, M. Ahmed, andW. El-Shafai, "Android malware analysis in a nutshell," Plos one, vol. 17, no. 7, p. e0270647, 2022.

[29] "Virustotal," https://www.virustotal.com/gui/home/upload, 2 2023.

[30] A. Ammar, A. Koubaa, and B. Benjdira, "Deep-learning-based automated palm tree counting and geolocation in large farms from aerial geotagged images," Agronomy, vol. 11, no. 8, p. 1458, 2021.

[31] A. Noor, Y. Zhao, A. Koubˆaa, L.

Wu, R. Khan, and F. Y. Abdalla, "Automated sheep facial expression classification using deep transfer learning," Computers and Electronics in Agriculture, vol. 175, p. 105528, 2020.

[32] I. Almomani, A. Alkhayer, and W. El-Shafai, "An automated vision-based deep learning model for efficient detection of android malware attacks," IEEE Access, vol. 10, pp. 2700–2720, 2022.

[33] W. El-Shafai, I. Almomani, and A. AlKhayer, "Visualized malware multiclassification framework using fine-tuned cnn-based transfer learning models," Applied Sciences, vol. 11, no. 14, p. 6446, 2021.

Journal of Engineering and Applied Sciences (JEAS)

شركة مطابع جامعة المجمعة
Majmaah University Press Co.
0540010909