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. 9 Issue (2) (November. 2022) 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. 9, Issue (2) (November - 2022) 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

Editorial..... ***vii***

ORIGINAL ARTICLES

Effects of Vibration Intervention on Grip Strength and Endurance Time of Young College Students.
Abdulelah M. Ali *1*

Parents' Awareness of Cybersecurity.
Abdulrahman Abdullah Alghamdi *10*

A Novel Classifier for Cyber Attack Detection System in Industrial Internet of Things.
Fathe Jeribi *30*

Effects of Vibration Intervention on Grip Strength and Endurance Time of Young College Students.

Abdulelah M. Ali

Department of Industrial Engineering, College of Engineering, Jazan Univirsity, Jazan 45142, Saudi Arabia abdulelahali@jazanu.edu.sa

Abstract

BACKGROUND: Maximal voluntary contraction (MVC) is widely regarded as signal of maximum grip strength and active muscle contraction in the forearm.

AIM: The aim of the study is to investigate the muscular performance and effects of anthropometric measurement on grip strength (GS) and endurance time (ET) of young college students before and after vibration therapy (VT) in supination forearm posture.

METHODS: A observational study design (4 days x 2 levels (before vibration exposure (BVE) and after exposure to vibration at frequency of 45 Hz, amplitude of 3g and duration of vibration exposure of 60 seconds) x 24 subjects) was used in this study. Changes due to intervention were assessed by measuring GS and ET at 50% MVC (before and after vibration training).

RESULTS: MANCOVA results showed vibration training frequency and training days significantly affect the GS ($p<0.001$) and ET ($p<0.05$) with maximum increase on day 4 after VT. Compared with day 1 before vibration exposure (BVE) and day 4 after 45 Hz vibration training, MVC grip strength increased by 53.1% and endurance time increased by 37.07%. The Pearson correlation test showed that frequency of VT and days of exposure were not significantly associated with ET and GS.

CONCLUSIONS: Results showed a significant increase in GS and ET relative to VT frequency and training days. In addition, body weight and PL were the most important factors affecting ET, and palm circumference and forearm circumference were the most important factors affecting grip strength.

Keywords: Supination posture, maximal voluntary contraction, grip strength, grip endurance time, and anthropometric measurements.

Introduction

Mechanical oscillations, called "vibrations", were revealed in ancient Greco-Roman as a therapeutic method (Cited in: [1]). In the 16th century, the Japanese used vibrations treatment to release inflexible and occasional muscle contractions. Physician John Kellogg fabricated a vibrating device in 1880s, such as a chair and portable devices, to treat patients with constipation, headaches, lower and back pain. However, John Kellogg did not perform experimental trials to certify his hypothesis. The first use of the vibratory intervention was

carried out in 1881 by Granville (Cited in: [1] to treat pain, then used as a therapeutic technique to increase the volatility of alpha and gamma motor neurons, thus allowing the patients to produce improved voluntary control [2].

Vibration intervention is considered as a potential neuromuscular training approach and has recently been accepted by health departments, fitness and rehabilitation centers as an addition or alternative to routine training [3]. This is due to the fact that vibration training improves muscular performance and strength [4], increases flexibility [5], and other fitness assistances [6]. Previous studies reported that training programs with vibration intervention [7, 8] improved muscle performance compared to training programs without vibration intervention. Earlier, ergonomics experts usually debated the adversative effects of VT [9]; however, recently, vibrating massagers or vibrating plates have been used for training and to enhance muscular performance [10, 11].

Grip strength (GS) assesses the ability of the hand to exert strength at maximum capability, and it also measures the degree of active muscular contraction of the hand and forearm muscles [12]. Significant differences in GS were reported between the vibration-treated and non-vibration-treated populations. In addition, a significant increase in the handgrip strength was reported after application of vibration treatment in healthy women [13]. Many researchers had performed VT using fixed frequencies: 25 Hz [14, 15], 35Hz [10, 15], 40 Hz [15] and 45 Hz [11, 14] and reported significant improvements in muscular performance. However, no consensus was found in defining the optimum VT frequency, which was confused by the use of different methods in different studies.

Grip strength is affected by a variety of factors, including hand posture, gender, shoulder and forearm posture, full-body posture, and anthropometry [16]. In the literature, various previous results have provided more accurate estimates of forearm and/or hand size than common anthropometric measurements and better interpretation of grip strength. Anthropometric measurements: height and weight [17]; and forearm and/or hand anthropometric variables: forearm circumference [17], palm length and palm width or circumference [17, 18] have been shown to be significant independent predictors of grip strength factor. Therefore, posture significantly affects grip endurance and grip strength [19, 20]. Fiebert et al. [21] pointed out that the supination posture is the most important grasping pose in endurance tasks [20]. However, Alam et al. [22] showed that the highest grip strength in men was in the forearm pronated position. Therefore, the purpose of this study was twofold: first, to investigate the effect of vibration intervention on muscle performance in terms of grip strength and grip time; second, to investigate the effect of anthropometric variability in young college students in the forearm supination position with GS and ET. However, no studies have examined the effects of frequency, amplitude, duration of exposure,

and days of training on NPs delivering VT using vibrating plates. Therefore, the novelty of this study is the method of vibration processing using an in-house designed vibration plate. Specifically, this study measured the GS and grip ET at 50% maximal voluntary contraction (MVC) before and after vibration therapy.

The null hypothesis for present study was: "days of exposure and training days had a no significant effect on MVC grip strength and grip endurance time."

Methodology of the Study

Design of Experiment

An observational study with 4 days x 2 levels (before vibration exposure (BVE) and after exposure to vibration exposure at a frequency of 45 Hz, amplitude of 3g and duration of vibration exposure of 60 seconds) x 24 subjects) were used in the current study. The frequency of exposure to vibration and the number of training days were independent factors. The number of training days (4 days) was chosen based on a pilot study in which the most enhancements in dependent variables were witnessed on day 4. Changes due to VT intervention were assessed by assessing MVC GS, grip ET at 50% MVC (before vibration exposure (BVE) and after vibration exposure).

Participants

In this study, 24 sedentary lifestyle (SL) participants who did not report any neuromuscular problems were voluntarily selected. Informed written consent was obtained and the study protocol was explained. The protocol of the experiment was approved by the Ethics Committee of department. The participants' anthropometric measurements were based on previous research [10, 11] (Table 1).

Table 1.
The anthropometric measurements of the participants

Item	Mean ± SD
Age (years)	21.1±3.2
Height (cm)	165.4±8.3
Weight(kg)	60.4±5.4
Palm Length (PL) (cm)	10.5±0.4
Palm Circumference (PC)(cm)	22.6±1.9
Forearm Length (FL) (cm)	24.7±0.6
Forearm Circumference (FC)(cm)	26.2±1.2

Experimental Rig

A spring-loaded vibration plate is invented in-house [11] to maintenance the forearm in a supination forearm posture. A vibrating device was installed in the midpoint below the vibrating plate. It is enclosed in a metal casing and its frequency is ranged from 15-65Hz. Eccentric masses are also designed and manufactured to deliver the chosen frequency and amplitude combination.

Protocol and procedure for the experiment

To perform vibration training, participants were instructed to sit in a chair which can be adjusted with a supine forearm position for MVC recordings and placed the forearm on the vibrating plate during training. Chair height was adjusted in such a manner that right forearm of the participant is in 0° of shoulder abduction, ensuring angle of elbow as the 90°-120°. Follow the steps below to give vibration training along with measurement (for detail about the experimental setup, recording of grip strength,

endurance, vibration levels and instrumentation refers to [10, 11]):

1. Ask participants to grip the dynamometer in a supine position (twice with a 120 seconds of rest prior to measure MVC) with a fixed span of grip prior to vibration exposure (BVE).
2. After a 5-minute rest, measure the ET at 50% MVC (with reference as the extreme of two trials).
3. The detaching of the grip dynamometer.
4. Apply four rounds of VT at 45 Hz for 60 seconds with a 30 second rest after each round.
5. A rest of 15 minutes.
6. Ask participants to repeat the trial according to point No. 1 and 2.
7. The detaching of the grip dynamometer.
8. Ask participants to repeat the trial for 4 days according to point No. 1 to 7 and on 5th day repeat the point No. 1 and 2.

Results

The data of GS and ET are summarized in Table 2. Multivariate analysis of covariance (MANCOVA) was performed using SPSS 25.0 to examine various factors and their interactions with covariates on dependent variable (Table 3). Pearson correlation test were also accomplished to assess the association between dependent variable and the covariates (Table 4).

The effect of vibration training frequency significantly affects both the GS ($p < 0.001$) and grip ET ($p=0.021$). Moreover, training days were also significantly affecting both GS and ET ($p<0.001$), (Table 3). In addition, Figures 1 and 2 showed significant increase in GS and ET with respect to training days with maximum increased on day 4 after VT. Compared with day 1 before vibration exposure (BVE) and day 4 after 45 Hz vibration training, MVC grip strength increased by 53.1% and endurance time increased by 37.07%. Further, the GS and ET after post training on day 5 was also increased as compared with day 4 before vibration exposure (Table 2, Figure 1 and 2).

In addition, age ($p=0.002$), PC ($p=0.018$), height, FL and FC ($p<0.001$) significantly affecting ET only. However, weight ($p=0.006$) also significantly affecting GS. The interaction of frequency of VT and training days were not significantly affecting GS and ET. Pearson correlation exhibited no substantial association of vibration training frequency and days of training with endurance time and grip strength (Table 4). PC ($r=0.236$, $p=0.008$), and FC ($r=0.303$, $p<0.001$) have found significantly positive correlation with GS. In addition, age ($r=0.220$, $p=0.013$), weight ($r=0.603$, $p<0.001$), height ($r=0.306$, $p<0.001$), PL ($r=0.597$, $p<0.001$), PC ($r=0.426$, $p<0.001$) and FL ($r=0.361$, $p<0.001$) had a significant positive correlation with grip ET.

Table 2. Summary of mean GS and ET with respect to training days and frequency of vibration training

Training Days	MVC Grip Strength (Kgf)		Endurance Time (Seconds)	
	BVE	45 Hz	BVE	45 Hz
Day 1	49.14	57.02	59.84	64.51
Day 2	56.15	62.71	67.24	71.27
Day 3	65.07	69.86	71.09	74.55
Day 4	70.66	75.23	77.81	82.02
Day 5	71.23		78.79	

Table 3. Summary of results of MANCOVA

Variables	Tests of Between-Subjects Effects						
	Source		Type III Sum of Squares	df	Mean Square	F	Sig. p-value
Co-variates	Age	MVC	7.124	1	7.124	0.22	0.636
		Endurance Time	844.36	1	844.36	9.94	0.002
	weight	MVC	248.61	1	248.61	7.86	0.006
		Endurance Time	127.90	1	127.90	1.50	0.222
	height	MVC	118.51	1	118.51	3.74	0.055
		Endurance Time	1199.5	1	1199.5	14.1	<0.001
	PL	MVC	17.329	1	17.329	0.54	0.461
		Endurance Time	149.05	1	149.05	1.75	0.188
	PC	MVC	91.649	1	91.649	2.89	0.092
		Endurance Time	490.69	1	490.69	5.77	0.018
	FL	MVC	4.536	1	4.536	0.14	0.706
		Endurance Time	1372.4	1	1372.4	16.1	<0.001
	FC	MVC	23.995	1	23.995	0.75	0.386
		Endurance Time	2094.8	1	2094.8	24.6	<0.001
Independent Variables	Frequency	MVC	990.79	1	990.79	31.3	<0.001
		Endurance Time	469.27	1	469.27	5.52	0.021
	Days of Exposure	MVC	7785.0	4	1946.2	61.5	<0.001
		Endurance Time	5741.8	4	1435.4	16.9	<0.001
	Frequency* Days of Exposure	MVC	51.469	3	17.156	0.54	0.654
		Endurance Time	5.310	3	1.770	0.02	0.996

In addition, age (p=0.002), PC (p=0.018), height, FL and FC (p<0.001) significantly affecting ET only. However, weight (p=0.006) also significantly affecting GS. The interaction of frequency of VT and training days were not significantly affecting GS and ET. Pearson correlation exhibited no substantial association of vibration training frequency and days of training with endurance time and grip strength (Table 4). PC (r=0.236, p=0.008), and FC (r=0.303, p<0.001) have found significant-

ly positive correlation with GS. In addition, age (r=0.220, p=0.013), weight (r=0.603, p<0.001), height (r=0.306, p<0.001), PL (r=0.597, p<0.001), PC (r=0.426, p<0.001) and FL (r=0.361, p<0.001) had a significant positive correlation with grip ET.

Table 4. Summary of the results of Pearson Correlation

		Age	weight	height	PL
MVC	Pearson Correlation	-0.173	-0.003	0.173	-0.104
	Sig.(2tailed)	0.052	0.970	0.052	0.247
Endurance Time	Pearson Correlation	0.220*	0.603**	0.306**	0.597**
	Sig.(2tailed)	0.013	0.000	0.000	0.000
		PC	FL	FC	
MVC	Pearson Correlation	0.236**	0.127	0.303**	
	Sig.(2tailed)	0.008	0.158	0.001	
Endurance Time	Pearson Correlation	0.426**	0.361**	0.119	
	Sig.(2tailed)	0.000	0.000	0.184	

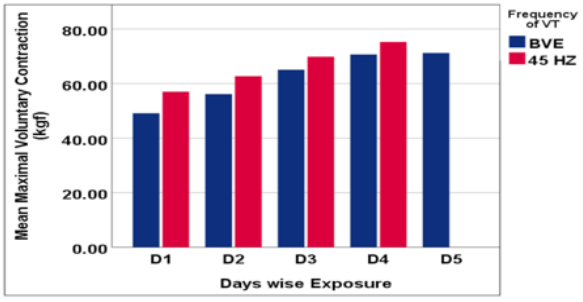

Fig. 1. Mean maximal voluntary contraction value with day's wise vibration exposure

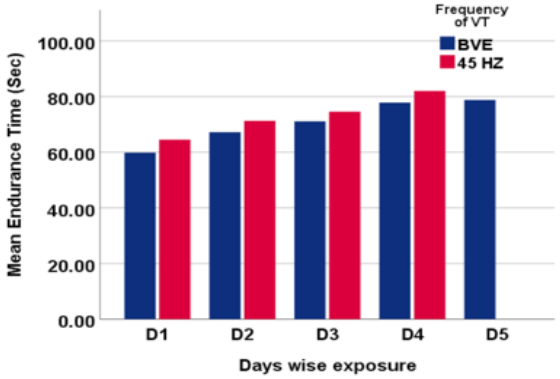

Fig. 2. Mean endurance time value with day's wise vibration exposure

Discussion

The interaction of the human with the applied vibration training depends to a large extent on the characteristics of the participants. In current study, vibration training frequency and training days had significant effects on both GS (p<0.001) and ET (p<0.05). In contrary, Alam et al. [10] found that VT frequency significantly affecting ET (p<0.001), but not the GS (p=0.161). However, the number of contact days significantly effect on both GS and ET (p<0.001).

In line with existing study, significant difference in grip strength between with and without vibration groups were stated [13]. Alam et al. [23] revealed significant differences in contact days, vibration training frequency, PL, and FL on GS and ET. Wu et al. [20], investigated GS in 482 participants in Taiwan, stated significant differences in GS by gender, age, and PL. In addition, they found, PL, second only to gender and age, were the most important variable influencing GS.

In addition, present study also shows that PL (r=0.236, p=0.008), and FC (r=0.303,

p<0.001) significantly having positive correlation with GS. Moreover, age (r=0.220, p=0.013), weight (r=0.603, p<0.001), height (r=0.306, p<0.001), PL (r=0.597, p<0.001), PC (r=0.426, p<0.001) and FL (r=0.361, p<0.001) had a significant positive correlation with grip ET. In another study by Alam et al. [24], they found that height (p = 0.012), age (p = 0.044), and FL (p = 0.039) significantly affects in supine posture. However, PC significantly affecting GS only in pronation (p = 0.036). The forearm pronated position produced 7.4% more GS than in the supination position. Moreover, grip ET was enhanced in the supination posture related to neutral and pronated forearm positions. Similarly, the current study showed a 53.1% increase in grip strength and a 37.07% increase in endurance time compared to day 1 before vibration exposure (BVE) and day 4 after 45 Hz vibration training.

Fiebert et al. [21] establish that PL was closely related to GS. PL offers superior thenar musculature, which may account for the robust correlation. Nicolay and Walker [19] established that anthropometric changes were autonomous of grip ET compared to GS. Additionally, they reported that forearm and hand dimensions were superior forecasters of GS than the height and weight. Contrary to the current findings, Heidi and Jonathan [25] reported a considerable difference between age and GS (p<0.001), but no substantial association between age and ET (r=-0.13, p=0.38). Likewise, Petrofsky and Lind [26] stated a significant enhancement in GS (p < 0.01), but endurance time in men was not significantly associated with aging (r=0.11, p>0.05). Differences in these outcomes may be due to differences in experimental methods, GS measurement devices, or methods used to measure anthropometric changes.

Conclusions

The present results showed significant effect of VT frequency and training days on both GS and ET. Therefore, the proposed combination of frequency, amplitude and exposure durations may be used as a guideline by the therapist to improve the muscular performance of young and elderly.

Conflict of Interest

None to declare.

References

[1] Clark, T., Woodley, R., De Halas, D., 1962. Gas-Graphite [1] V. Issurin, "Vibrations and their applications in sport," J. Sports Med. Phys. Fittness, vol. 45, pp. 324-335, 2005.

[2] R. Johnston, B. Bishop and G. Coffey, "Mechanical vibration of skeletal muscles," Physical Therapy, vol. 50, no. 4, pp. 499-505, 1970.

[3] M. M. Alam, A. A. Khan and M. Farooq, "Effect of Whole-Body Vibration on Neuromuscular Performance: A Literature Review," Work, vol. 59, no. 4, pp. 571-583, 2018.

[4] J. Nam-Gyu, K. Seung-Rok, K. Myoung-Hwan, and Y. Ju-Yul, "Effectiveness of whole-body vibration training to improve muscle strength and physical per-

formance in older adults: Prospective, single-blinded, randomized controlled trial," Healthcare (Switzerland), vol. 9, no. 6, pp. 652, 2021.

[5] A. Kinser, M. Ramsey, H. O'Bryant, C. Ayres and W. Sands, "Vibration and stretching effects on flexibility and explosive strength in young gymnasts," Med. Sci. Sports Exerc., vol. 40, no. 1, pp. 133–140, 2008.

[6] A. Kosa, D. Candow and J. Putland, "Potential beneficial effects of whole-body vibration for muscle recovery after exercise," Journal of Strength & Conditioning Research, vol. 26, no. 10, pp. 2907–2911, 2012.

[7] C. Delecluse, M. Roelants and S. Verschueren, "Strength increase after whole-body vibration compared with resistance training," Med. Sci. Sports Exerc., vol. 35, no. 6, pp. 1033–1041, 2003.

[8] M. Cardinale and C. Bosco, "The use of vibration as an exercise intervention," Exercise and Sports Sciences Reviews, vol. 31, pp. 3-7, 2003.

[9] Europian committee for standardization, "Mechanical vibration-Guide to the health effects of vibration on the human body," Brussels, 1996.

[10] M. M. Alam, A. A. Khan and M. Farooq, "Effect of vibratory massage therapy on grip strength, endurance time and muscle performance," Work, vol. 68, no. 3, pp. 619-632, 2021.

[11] M. M. Alam, A. A. Khan and M. Farooq, "Effects of different vibration therapy protocols on neuromuscular performance," Muscle, Ligaments and Tendons Journal, vol. 11, no. 1, pp. 161-177, 2021.

[12] L. Richards, "Posture effects on grip strength," Arch. Phys. Med. Rehabil., vol. 78, pp. 1154-1156, 1997.

[13] M. M. Luciana, C. Ana Carolina, F. Sueli, and F. Angélica, "Whole-Body Vibration Exercise in Different Postures on Handgrip Strength in Healthy Women: A Cross-Over Study," Frontiers in Physiology, vol. 11, no. 1, pp. 469499, 2021.

[14] A.L. Cristino de Souza, V.A. Mendonça, A.C. Coelho de Oliveira, and S. Ferreira da Fonseca, "Whole body vibration in the static modified push-up position in untrained healthy women stimulates neuromuscular system potentiating increased handgrip myogenic response," Journal of Bodywork and Movement Therapies, vol. 24, no. 4, pp. 233-238, 2020.

[15] T. Hazell, J. Jakobi and K. Kenno, "The effects of whole-body vibration on upper- and Lower-body EMG during static and dynamic contractions," Applied Physiology Nutrition and Metabolism, vol. 32, no. 6, pp. 1156-1163., 2007.

[16] K. S. Lee and J. Hwang, "Investigation of grip strength by various body postures and gender in Korean adults," Work, vol. 62, no. 1, pp. 117-123, 2019.

[17] M. Mohammadian, A. Choobineh, A. A. Haghdoost and N. N. Hashemi, "Investigation of grip and pinch strengths in Iranian adults and their correlated anthro-

pometric and demographic factors," Work, vol. 53, no. 2, pp. 429-437, 2016.

[18] Y. K. Kong and D. M. Kim, "The relationship between hand anthropometrics, total grip strength and individual finger force for various handle shapes," International Journal of Occupational Safety and Ergonomics , vol. 21, no. 2, pp. 187-192, 2015.

[19] C. W. Nicolay and A. L. Walker, "Grip strength and endurance: Influences of anthropometric variation, hand dominance, and gender," International Journal of Industrial Ergonomics, vol. 35, no. 7, pp. 605-618, 2005.

[20] S.-W. Wu, S.-F. Wu, H.-W. Liang, Z.-T. Wu and S. Huang, "Measuring factors affecting grip strength in a Taiwan Chinese population and a comparison with consolidated norms," Applied Ergonomics, vol. 40, pp. 811–815, 2009.

[21] I. M. Fiebert, K. E. Roach, J. W. Fromdahl, J. D. Moyer and F. F. Pfeif, "Relationship between hand size, grip strength and dynamometer position in women," J. Back Musculoskelet. Rehab. vol. 10, no. 3, pp. 137-142, 1998.

[22] M. M. Alam, I. Ahmad, A. Samad, A. A. Khan and M. A. Ali, "Grip strength and endurance: Influences of anthropometric characteristics, posture, and gender," MLTJ, vol. 12, no. 2, pp. 1-16, 2022.

[23] M. M. Alam, A. A. Khan, M. Farooq and S. Bhardwaj, "Effect of One Week Intervention of Vibratory Massage Therapy on Forearm Grip Strength and Endurance," in In 14th International Conference on Humanizing Work and Work Environment, NIT Jalandhar, 2016.

[24] M. M. Alam, I. Ahmad, Y. Kumar, A. Samad, Y. Upadhyay and A. A. Khan, "Investigation of the relationship between anthropometric measurements and forearm postures with grip strength in young adults," Journal of Musculoskeletal Research, vol. 24, no. 4, pp. 2250004, 2022.

[25] C. Heidi and A. Jonathan, "Tongue Strength and Endurance in Different Aged Individuals," Journal of Gerontology: Medical sciences, vol. 51, no. 5, pp. 247-250, 1996.

[26] S. Petrofsky and A. R. Lind, "Isometric Strength, Endurance, and the Blood Pressure and Heart Rate Responses during Isometric Exercise in Healthy Men and Women, with Special Reference to Age and Body Fat Content," Arch. , vol. 360, pp. 49-61, 1975.

Parents' Awareness of Cybersecurity

Abdulrahman Abdullah Alghamdi
Shaqra University, Shaqra, Saudi Arabia, Alghamdia@su.edu.sa

Abstract

The main objective of this study is to investigate parents' awareness of cybersecurity in Saudi Arabia. The era we live in imposes on all stakeholders to be aware of information systems regardless of their gender, age, or education level. Moreover, a lack of cybersecurity awareness can have a drastic impact on parents and their children, especially in terms of hacking, phishing, and blackmailing. Therefore, our study aims to investigate the extent to which parents are aware of cybersecurity. A sample of 558 parents, including 346 males and 212 females, was targeted through an online questionnaire. Descriptive statistics revealed that parents are, to a large extent, aware of the existence of cyber threats, and are willing to protect their family members against the latter. However, this knowledge needs to be put into practice by parents and governmental authorities by taking concrete measures.

Keywords:
Cybersecurity, Awareness; cyber threats; Saudi Arabia.

Introduction

The Kingdom of Saudi Arabia's Vision 2030 targets a comprehensive development of the country, its security, its economy, and the welfare of its citizens. One of its goals is the transformation towards the digital world, as well as the development of the digital infrastructure to keep pace with the rapid global progress in digital services, computer processing capabilities, and artificial intelligence data. In order to control this development, the National Cybersecurity Authority developed basic controls for cybersecurity. They consist of sub-components and basic functions, taking into account the main axes on which cybersecurity is based, namely: strategy, with data handling and massive storage capabilities in a way that prepares people, procedure, and technology [1][2].

Literature Review

Cybersecurity awareness among parents in Saudi Arabia has been investigated in several studies. Most research works showed that parents are concerned about their children' privacy [3]. Although social media have started taking some measures to protect kids by tailoring content to their needs, children can still access the Web using their parents' email address, and are still exposed to what their parents are. Therefore, children are exposed to security and privacy risks [4]. They can have their password revealed, which makes them vulnerable to phishing attacks. For these reasons, children need to know more about technology and about cybersecurity awareness [4]. This can help them to avoid cybersecurity breaches. Studies also showed that the majority of children are nowadays exposed to smartphones, Internet connected devices,

and social media [5]. Parents lack knowledge about how to protect their children [6]. They need to have protective and reactive approaches; yet the majority of parents do not have access to cybersafe online resources [6]. Furthermore, some children play games that are not suitable for their age [5]. Tensions and concerns exist between parents and children around cybersecurity, more specifically about boundaries and rules [7]. Moreover, some children, especially teenagers, might have reasonable privacy awareness [8]. Children spend a lot of time online, which can cause Internet addiction [8]. Their learning performance can consequently be negatively affected by wrong usage of the Internet [9]. Indeed, studying requires a lot of mental effort and time, but this time is usually wasted on social media and the Internet, instead. Parental control applications are sometimes encouraged to be used by parents to monitor their children [10]. Some studies claimed that the Internet has no effect, and that it is neither harmful nor beneficial [11]. Therefore, different studies have focused on diverse dimensions of Internet use among children, along with common concerns, the most prominent of which being cybersecurity.

A study by Al Shamsi found that children are exposed to different cyber threats, and stated that the awareness is efficient in influencing the behavior of children when using the internet. Children need to learn how to protect themselves [34]. Gogus et al. [35] found that only 75% of students aware of cybersecurity settings in social media. 17% of students who are active in social media do not care about whether their personal information is exposed publicly and seen by strangers. Dyer [28] recommended parents to be a role model for their children in internet usage, and to show them how to be cautious online, and teach them how to protect their privacy.

With the spread and daily usage of smartphones and rapid communication technologies across different societies, information published on the Internet has become the most dominant one for children. It has therefore become necessary to make them aware of cybersecurity while they learn basic skills, for instance through exercises integrated into their curricula to provide students with knowledge and awareness at school [12]. Furthermore, excessive use of the Internet may expose children and students to many risks. This means that there is a danger for individuals' personal information, highlighting the importance of cybersecurity awareness and its role in protecting personal information [13]. Since family members have become highly dependent on the Internet, such as for entertainment, shopping, learning, banking, and communication, parents must be aware of the risks of using the Internet. Such risks include infecting data and information stored on the computer with destructive viruses, penetrating user files, exploiting a computer to abuse others, or even stealing credit cards. It is not possible to completely get rid of these risks, but it is possible to take preventive steps to protect students from them [14]. Boundaries between seriousness and fun are not clear on the Internet, which

can cause issues related to cybersecurity breaches. The existence of cybersecurity awareness for parents, its meaning, how it works, and what the risks are, enable parents to protect themselves and their family from these risks [13]. Parents play a great, important, and effective role in protecting children from the risks they may face while using modern technologies [7], [15].

Research Problem

The Internet has become one of the biggest influences on young people, as they depend on it for various life affairs. They indeed use it for entertainment, meaning that they spend a lot of time on Web pages, which may affect their beliefs, way of life, and understanding of the world around them [8]. As the Internet has many positive sides in their lives, it also has many negative ones, especially when used without family supervision, and without understanding the risks it can yield on their convictions and values [9]. [16] stated that there has been an increase in the concerns about the potentially negative effects of the Internet on young people, because its negative usage, and this means that it can be dangerous for them. This confirms the importance of cybersecurity and its role in protecting them and their information. This cannot be done without the parents' participation to protect their family members [17]. Parents' awareness of the internet threats depends on the extent of their cybersecurity awareness and its importance, and on their strategies to protect their family from these risks [15]. This knowledge is developed from practice, mostly from training and education. Hence, the aim of this research is to reveal parents' awareness of cybersecurity, as well as to identify strategies used to help protect their family from the internet threats.

Research Questions

This research aims to answer the following main question: What is the level of parents' awareness of cybersecurity, and what are their methods to protect their family members from cyber threats. The following questions were derived from it:

1. From their own point of view, what is the level of parents' cybersecurity awareness and safely surfing on the Internet?
2. How do parents handle authentication and passwords?
3. What is the parents' level of family privacy protection?
4. What is parents' level in computer cybersecurity practices?
5. What are parents' greatest online fears?
6. What is parents' level in protecting family members from cyber threats?
7. What are the cybersecurity initiatives taken by the government to combat cyber threats?

Research Aims

This study aims to:

- Determine the level of parents' awareness of cybersecurity from their point of view.
- Determine the level to which parents use methods and strategies to protect family members from cyber threats from their point of view.
- Determine the level of parents' knowl-

edge and practices with regard to cybersecurity.

Research Importance

- The current study aims to generate data and answer questions with the following important objectives:
- Drawing parents' attention to the importance of cybersecurity awareness due to the influential role they play in families' life.
- Providing parents with innovative methods and strategies used by other parents in the community to protect their family from the internet threats.
- Drawing attention of education officials to implement effective methods and strategies, to protect students from the threats of the Internet, and to train teachers to use them.
- Providing the Arab Library with an important theoretical framework on the creative methods used by parents to protect their family from the internet threats.

Research limits:

Research limits are stated in the following headings:

- Objective limits: Determining the degree of cybersecurity awareness among parents by protecting private portable devices and storage media, dealing safely with Internet browsing services, and examining the creative methods they use to protect family members from Internet dangers.
- Spatial boundaries: Saudi Arabia society.
- Temporal limits: The second semester of the 2022 academic year.
- Human limits: Parents in relation to their children.

Research terms:

Cybersecurity: It is the activity that protects digital information and human resources associated with communications, that mitigates damages and losses that occur in the event of hacking, risks, or threats, and attempts to repair what was spoiled by these attacks.

Methods of protecting children from the threats of the Internet: It is procedurally defined by the different methods, strategies, and techniques used by parents. In our research, it is measured by the degree obtained by parents on the scale of methods of protecting family members from the threats of Internet attacks and breaches.

Theoretical Framework

Cybersecurity

The Kingdom of Saudi Arabia became aware of the importance of cybersecurity. It accomplished a remarkable achievement by obtaining the second rank globally, and the first one in the Arab world according to the Global Cybersecurity Index issued by the International Telecommunication Union of the United Nations [18].

Cybersecurity has elements that must be in place to ensure the protection of information, including [19][20]:

1. Confidentiality and security: Ensuring that information is not disclosed nor viewed by unauthorized persons.
2. Integrity and confidentiality of the content: Ensuring that the content of the

information is correct and has not been modified, destroyed, altered, nor tampered with at any stage of processing or exchange, neither in internal dealing, information stage, nor through illegal interference.

3. Continuity of information or service availability: Ensuring that the information system continues to operate, as well as the ability to interact with information and to provide service to information sites, and that the user is not be prevented from using or entering the system.
4. Non-denial of the behavior related to the information which performed it: Ensuring that the person connected to the information or its location denies that they have done a certain act, so that it is possible to prove this behavior and that a person did not do it at a certain time, and that the recipient of a particular message is unable to deny receiving this message.

Areas of cybersecurity use

Cybersecurity is used in many areas, the most important of which are:

1. Protecting all types of digital devices, technical equipment, as well as storage media from the risk of attacks, electronic intrusions, and partial or total destruction.
2. Taking measures to educate individuals about the dangers of attacks, cybercrime, and fraud methods.

The Internet and its cyberthreats

The Internet and social media have positive sides, as well as negative sides. They are useful when they are used to increase knowledge and information. However, when they are used as an alternative to interaction, they can lead to social withdrawal, which further leads to real psychological and sometimes physical problems [21]. Introversion is a feeling that is often associated with staying at home all day and being busy with the Internet instead of going out practicing some activities. Even people who go out keep getting busy with their mobile phones, laptops, or tablets during many events.

Problems have increased greatly with the emergence of the Internet in our homes, and they strongly affect individuals, families, and the society as a whole, especially adolescents and youth, as websites are open and uncensored [22]. Nowadays, even parents are observed to be addicted to the Internet by spending a lot of time online at the expense of family time. These habits make them exposed to various threats.

Among these problems are the following:

1. Electronic extortion:

It is the use of modern technical means to obtain material or moral gains through coercion from a person, several people, or an institution, and it is done by threatening to expose a person's secrets, photos, videos, or other sensitive information. This crime has been affected by contemporary practical and technological progress; thus, criminal methods have appeared with techniques that were not known before. Modern technologies have been used to commit crimes at various stages of planning, preparation, execution, deception,

and camouflaging to evade justice. Consequently, modern devices, tools, and techniques have been used to commit crimes that were characterized by violence, and scientific progress is accompanied by new and unknown crimes such as illegal entry into computer networks and information systems, spreading viruses, destroying programs, forging documents, attacking networks and banks, electronic terrorism, spreading rumors, lies, and unwanted behaviors that are incompatible with society. There are motives for blackmail, including psychological, ideological, and racial motives [23].

2. Insider cyber threats:
These are threats that come from within the information system. They can be intentional and unintended human errors, which mostly affect the progress of information, such as errors in programming systems and databases, writing off files by mistake, in system management during installation, in software that may lead to unexpected results, weaknesses, and loopholes. These errors enable the aggressor to penetrate through if they are not secured, or if the individual does not follow the methods of protecting the system such as passwords, locks, and crossing barriers, or if the spatial location of the system is equipped with means of prevention and protection [24].

3. Excessive use of the Internet:
Quitting the Internet has become a problem that many people face, but the unrealistic and excessive use of it is a problem that individuals and institutions must face. Studies have shown the serious damages of Internet addiction for individuals and groups [25][26].

4. Weak academic achievement:
Academic achievement declines when spending too much time on the Internet, neglecting studies, and not doing homework, especially if the student is not supervised by their family and school [27].

5. Electronic crimes:
Such crimes include sexual crimes, hacking crimes, privacy violation, theft of files, data, and personal photos, robbery of bank account numbers and money theft, as well as hacking of all kinds. With the spread of many programs that allow hacking of personal accounts and data, there have been many incidents of privacy violations and theft of data, personal photos, and emails, which some may exploit in the extortion of users, whether physically or otherwise.

Methods of protecting children from the internet threats

Various are the other strategies that parents can guide family members to use to protect themselves from the internet threats include:
Users can be encouraged to use a strong password that is difficult for hackers to crack. Recently, authentication methods have evolved to use biometrics, including eye, finger, and face scans, voice recognition, and hand engineering. All of this means securing and limiting access to the system through identification and transfer systems [29].
Moreover, users can receive training on digital citizenship, which is one of the most

important ways to develop cybersecurity and is considered a set of rules, controls, standards, norms, and principles used for optimal use of digital technology. All people who use the Internet, regardless of their age, education level, or the nature of their work, need to learn how to deal with technologies to preserve their security from penetration and to contribute to maintaining the security of the homeland [33]. It is possible to train students and qualify them to use information systems to maintain the security and confidentiality of information, and this will protect them from blackmail if their accounts are hacked and their files or personal photos are seized [30].

In addition to strong passwords and digital citizenship training, users can make backup copies of data and files for information systems or system status such as private passwords, e-mails, and data [31]. This is because they may forget such passwords or the data can be damaged or lost altogether. Users need to be made aware of preventing viruses that attack a system, by installing a virus-checking program on their devices, regularly updating it to ensure its ability to confront modern and advanced viruses, preparing backup copies of the software for retrieval if the original copy is damaged, and by educating students not to download any untrusted program in their accounts, nor to open anonymous links [32]. Looking at previous studies, it is clear that they were concerned by the availability of cybersecurity awareness and methods to protect children from internet threats. This study is complementary to the cross-sectional studies. The next section will be devoted to choosing the study method and procedures, building the study tools, and interpreting and discussing it.

Research Methods and Materials

Research Methodology:

The essential drive of this research is to examine the alertness of parents towards online safety use, as well as cybersecurity. More particularly, it determines the awareness among parents towards safe online surfing on www.cert.sa. The dependent variables consist of different items in a questionnaire, such as: demographic information, cybersecurity awareness, safely surfing on the Internet, authentication and password handling, family's privacy protection, computer cybersecurity practices, parents' greatest online fears, protecting family members from cyber threats, and cybersecurity initiatives by the government to combat cyber threats. The research questionnaire comprises of 33 items, as explained right after.

Research sample:

The research sample consists of 558 parents, 346 of them were males and 212 of them were females. Our sample of parents has the following education: 1) Bachelor's degree (58.24%), 2) Master's degree (17.38%), 3) Diploma (12.19%), 4) High School (5.56%), 5) Ph.D. (4.66%), 6) Lower than High School (1.25%), and others (0.72%). The 25–34 age group had the highest percentage of parents (36.92%), while the > 65 age group had the lowest percentage of parents (1.97%). According

to our findings, 79.21% of parents were < 44 years old. Table 1 illustrates the sample distribution (n=558).

Table 1: Demographic information

Statement	Group	Number	Percentage
Gender	Male	346	62.01
	Female	212	37.99
Academic qualification	Lower than High School	7	1.25
	High School	31	5.56
	Diploma	68	12.19
	Bachelor's degrees	325	58.24
	Master's degree	97	17.38
	Ph.D.	26	4.66
	Others	4	0.72
Statement	Group	Number	Percentage
Age	18-24	39	6.99
	25-34	206	36.92
	35-44	197	35.30
	45-54	81	14.52
	55-64	24	4.30
	65+	11	1.97

Research tool:

We reviewed several studies related to the topic of the research and designed a scale to achieve its purposes. Primary data included demographic information, phrases to measure cybersecurity awareness, and methods of protecting students from internet threats.

Part One: Demographic information: This part is to collect demographic information from the participants.

Part Two: Cybersecurity awareness and safely surfing on the Internet: This part included 5 items regarding measuring the general cybersecurity awareness of the parents.

Part Three: Authentication and password handling: This part included 3 items regarding dealing with passwords and authentication.

Part Four: Family's privacy protection: This part included 4 items about family members' privacy and personal information.

Part Five: Computer cybersecurity practices: This part included 6 items concerning securing computer devices.

Part Six: Parents' greatest online fears: This part included 6 items regarding some Internet threats and parents' fears.

Part Seven: Protecting family members from cyber threats: This part included 6 items concerning methods to protect families from Internet dangers.

Part Eight: Cybersecurity initiatives by the government to combat cyber threats: This part included 3 items about official methods to deal with cyber threats.

Face validity:

The scale was presented in its initial form to a group of specialists in cybersecurity to make observations about the appropriateness of the items of the questionnaire for research purposes. They were asked to modify, delete, or add what they thought would fit. After taking into account the opinions of specialists, some items were deleted, modified, and added in the initial form.

Construct validity:

Pearson correlation coefficient of construct validity ranged between 0.79% and 0.87, which are high values that confirm the validity and reliability of the tool in collecting study data.

Reliability of the questionnaire:

Cronbach's alpha coefficient to calculate the stability of the questionnaire axes ranged between 0.90 and 0.98, while the total stability of the study tool was 0.95. This clearly indicates that the study tool of the questionnaire has excellent reliability, confirming its validity for collecting study data.

Interpretation method:

To determine the range of the cells on a five-point Likert scale, the range (5-1=4) is calculated and divided by the largest value in the scale to get the length of the cell (4/5=0.80). Then, this value is added to the lowest value in the scale (the correct one), and the cell range became as presented in Table 2.

Table 2: Arithmetic mean values of response criteria

Standard response	Arithmetic mean value
Very low	From 1 to less than 1.80
Low	From 1.80 to less than 2.60
Medium	From 2.60 to less than 3.40
High	From 3.40 to less than 4.20
Very high	From 4.20 to 5

Research Results:

The results of the questionnaire were summarized in the form of frequencies and percentages to draw trendlines on the cybersecurity awareness level among parents.

Cybersecurity awareness and safely surfing on the Internet:

Table 3. Cybersecurity awareness and safely surfing on the Internet

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I avoid opening any link from unknown people	F	176	255	81	28	18	3.97	0.9760	5
		%	31.54%	45.70%	14.52%	5.02%	3.23%			
2	I make sure to not open any anonymous email	F	221	230	66	31	10	4.11	0.9416	2
		%	39.61%	41.22%	11.83%	5.56%	1.79%			
3	I make sure to use a safe Internet browser	F	202	246	69	30	11	4.07	0.9352	3
		%	36.20%	44.09%	12.37%	5.38%	1.97%			
4	I am very careful when connecting to public networks	F	217	242	70	21	8	4.15	0.8799	1
		%	38.89%	43.37%	12.54%	3.76%	1.43%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
5	I check links that appear to me to be malicious	F	198	248	75	23	14	4.06	0.9368	4
		%	35.48%	44.44%	13.44%	4.12%	2.51%			

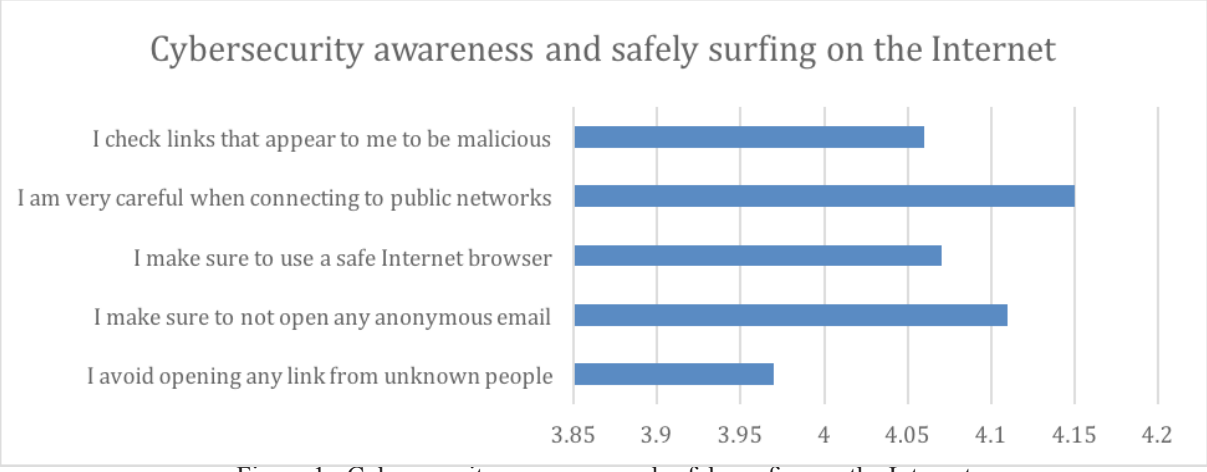

Figure 1 : Cybersecurity awareness and safely surfing on the Internet

Looking at Table 3, it is clear from the arithmetic averages of the items related to the degree of cybersecurity awareness and safely surfing on the Internet that parents have a very high level of cybersecurity awareness for most of the items, and a high one for the other items, where the arithmetic means ranged between 3.97 and 4.15. It was found that the item "I am very careful when connecting to public networks" got the highest arithmetic mean, while the item "I avoid opening any link from unknown people" got the lowest one as shown in Figure 1. The general average in the field of awareness of parents with cybersecurity from their point of view was 4.07, which is a high score on a five-point Likert scale. This indicates the high level of cybersecurity awareness parents have when browsing and surfing the Internet.

Table 4. Authentication and passwords handling

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I choose a strong password that contains a combination of letters, numbers and symbols	F	201	251	75	26	5	4.11	0.8671	1
		%	36.02%	44.98%	13.44%	4.66%	0.90%			
2	I use a two-factor authentication (password-fingerprint)	F	187	277	49	36	9	4.07	0.9071	2
		%	33.51%	49.64%	8.78%	6.45%	1.61%			
3	I take care of changing the passwords for accessing Internet services every once in a while	F	177	259	69	36	17	3.97	0.9870	3
		%	31.72%	46.42%	12.37%	6.45%	3.05%			

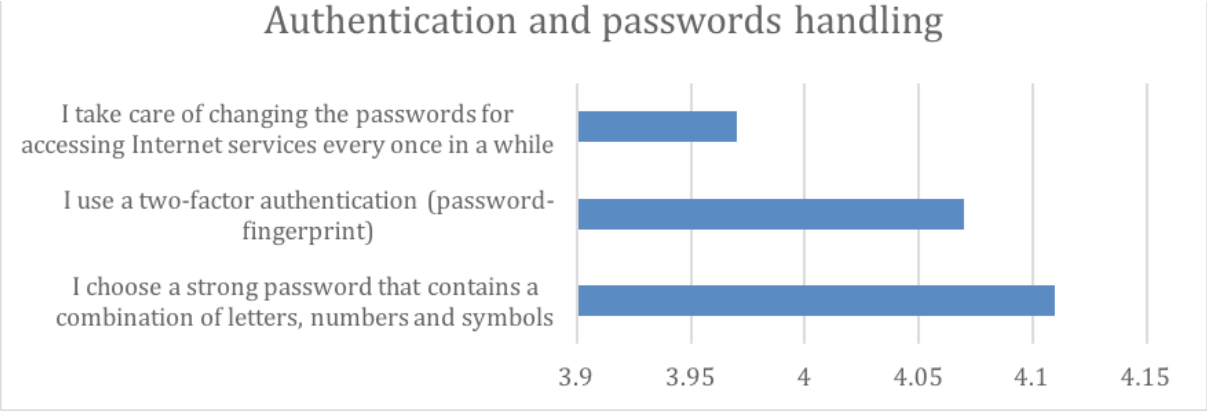

Figure 2: Authentication and passwords handling

Looking at Table 4, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about authentication and passwords handling show that they have a very high level of cybersecurity awareness for most of the items, and high for the other items, where the arithmetic means ranged between 3.97 and 4.11. It was found that the item "I choose a strong password that contains a combination of letters, numbers and symbols" got the highest arithmetic mean, while the item "I take care of changing the passwords for accessing Internet services every once in a while" got the lowest arithmetic average (i.e., 3.97) as shown in Figure 2. The general average in the field of cybersecurity awareness of parents from their point of view is 4.05, which is a high average on a five-point Likert scale. This indicates the high level of parents' awareness about authentication and passwords.

Family's privacy protection

Table 5: Family's privacy protection

\	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I avoid sending my personal information via text message or email	F	170	255	84	29	20	3.94	0.9920	5
		%	30.47%	45.70%	15.05%	5.20%	3.58%			
2	I am careful when sharing sensitive information with others using the privacy settings of online services	F	233	220	65	23	17	4.13	0.9791	1
		%	41.76%	39.43%	11.65%	4.12%	3.05%			
3	I remove subscription of any targeted advertising to protect my personal and financial data	F	166	253	92	28	19	3.93	0.9830	6
		%	29.75%	45.34%	16.49%	5.02%	3.41%			
4	I avoid revealing any personal or family data while surfing the Internet	F	201	241	71	27	18	4.04	0.9857	2
		%	36.02%	43.19%	12.72%	4.84%	3.23%			

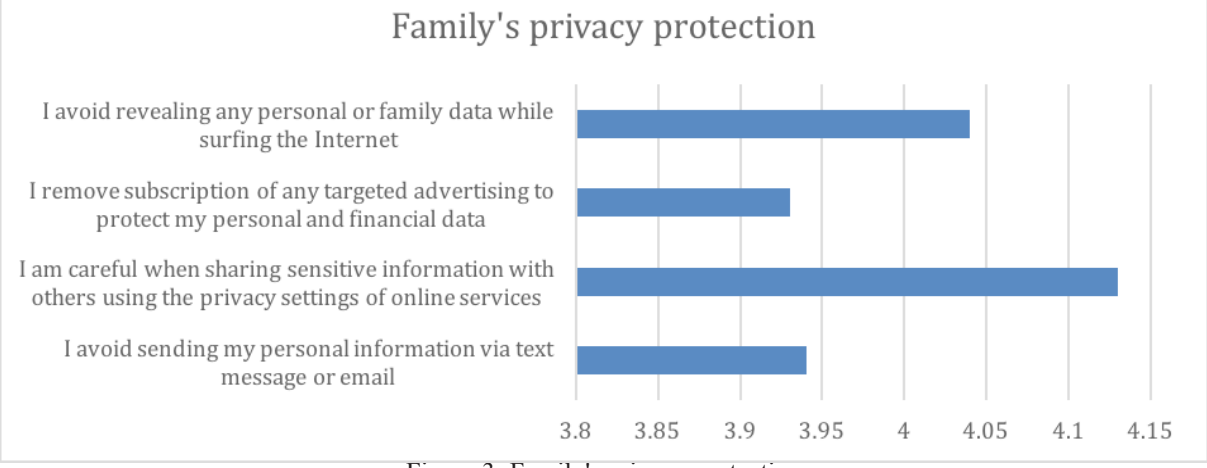

Figure 3: Family's privacy protection

Looking at Table 5, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about family's privacy protection showed that they have a very high level of cybersecurity awareness for most of the items, and high for the other items, where the arithmetic means ranged between 3.94 and 4.13 as shown in Figure 3. It was found that the item "I am careful when sharing sensitive information with others using the privacy settings of online services" got the highest arithmetic mean (i.e. 4.13), while the item "I remove subscription of any targeted advertising to protect my personal and financial data" got the lowest arithmetic averages (i.e. 3.93) The general average in the field of cybersecurity awareness of parents from their point of view was 4.01, which is a high score on a five-point Likert scale. This indicates the high level of parents' awareness about privacy.

Computer cybersecurity practices

Table 6. Computer cybersecurity practices

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I make sure to download safe updates and software	F	181	243	81	30	23	3.95	1.0270	2
		%	32.44%	43.55%	14.52%	5.38%	4.12%			
2	I make sure to use anti-virus programs	F	240	242	59	9	8	4.25	0.8176	1
		%	43.01%	43.37%	10.57%	1.61%	1.43%			
3	I back up the data stored on my device by making a backup on the cloud	F	160	255	80	30	33	3.86	1.0768	3
		%	28.67%	45.70%	14.34%	5.38%	5.91%			
4	I make sure that my computer is properly turned off in case I lose any data or information	F	152	239	99	48	20	3.82	1.0413	4
		%	27.24%	42.83%	17.74%	8.60%	3.58%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
5	I change the settings of my device regularly to prevent the Wi-Fi network from being hacked	F	140	245	97	39	37	3.74	1.1112	5
		%	25.09%	43.91%	17.38%	6.99%	6.63%			
6	I make sure to modify the access services to my location in the applications installed on my device	F	109	190	112	92	55	3.37	1.2440	6
		%	19.53%	34.05%	20.07%	16.49%	9.86%			

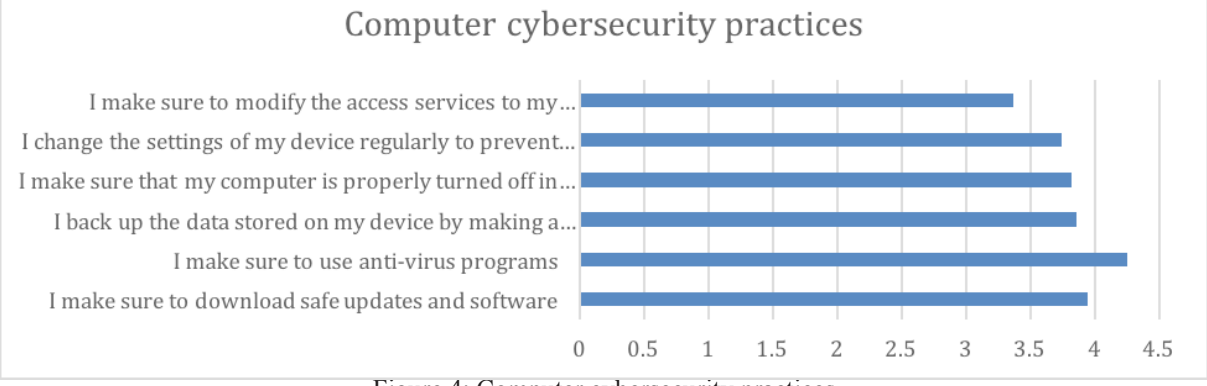

Figure 4: Computer cybersecurity practices

Looking at Table 6, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about computer cybersecurity practices showed that they have a very high level of cybersecurity awareness for most of the items, and a high level for the other items, where the arithmetic means ranged between 3.37 and 4.25 as shown in figure 4. It was found that the item "I make sure to use anti-virus programs" got the highest arithmetic mean, while the item "I make sure to modify the access services to my location in the applications installed on my device" got the lowest arithmetic average. The general average in the field of awareness of parents with cybersecurity from their point of view was 3.83, which is a high average on a five-point Likert scale. This indicates the high level of parents' awareness about the security of computers and devices.

Parents' greatest online fears:

Table 7. The greatest parents' online fears

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	be a victim of cyberbullying	F	171	230	102	29	26	3.88	1.0507	4
		%	30.65%	41.22%	18.28%	5.20%	4.66%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
2	have their privacy broken	F	261	246	29	13	9	4.32	0.8101	1
		%	46.77%	44.09%	5.20%	2.33%	1.61%			
3	be exposed to inappropriate content	F	272	215	29	28	14	4.26	0.9487	2
		%	48.75%	38.53%	5.20%	5.02%	2.51%			
4	be a victim of identity theft	F	158	251	90	41	18	3.88	1.0078	5
		%	28.32%	44.98%	16.13%	7.35%	3.23%			
5	learn or imitate inapporpriate behavior	F	231	223	72	21	11	4.15	0.9219	3
		%	41.40%	39.96%	12.90%	3.76%	1.97%			
6	be a victim of phishing attack	F	128	267	110	28	25	3.80	0.9956	6
		%	22.94%	47.85%	19.71%	5.02%	4.48%			

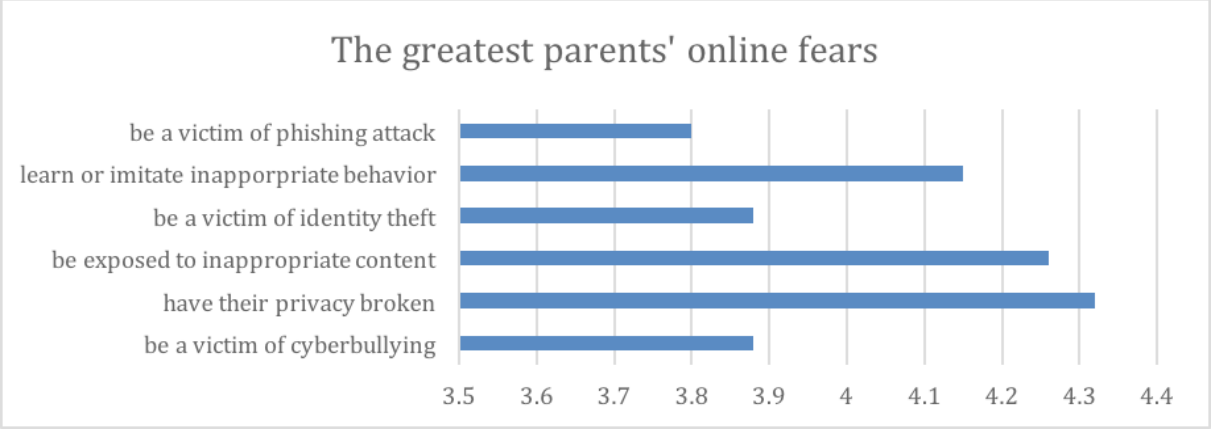

Figure 5: The greatest parents' online fears

Looking at Table 7, it is clear from the arithmetic averages of the items related to the degree of the greatest parents' online fears, that results showed that they have a very high level of worry for most of the items, and high for the other items, where the arithmetic means ranged between 3.80 and 4.32 as shown in figure 5. It was found that the item "I worry for my family members to have their privacy broken" got the highest arithmetic mean, which is very high on a five-point Likert scale. Furthermore, the mean for the item "be exposed to inappropriate content" was 4.26, which is very high on the Likert scale, while the item "I worry for my family members to be a victim of a phishing attack" got the lowest arithmetic average. The general average in cyber threats that make parents worry from their point of view is 4.05, which is a high average on a five-point Likert scale, and this indicates a high level of worry about cyber threats.

Protecting family members from cyber threats:

Table 8. Protecting family members from cyber threats

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I increase my family awareness of the dangers of malicious links when surfing the Internet	F	205	262	64	18	9	4.14	0.8591	5
		%	36.74%	46.95%	11.47%	3.23%	1.61%			
2	I train them to surf safely on the Internet	F	219	221	82	26	10	4.10	0.9375	6
		%	39.25%	39.61%	14.70%	4.66%	1.79%			
3	I educate them about some of the problems caused by using the Internet for long periods	F	249	215	51	27	16	4.17	0.9805	3
		%	44.62%	38.53%	9.14%	4.84%	2.87%			
4	I encourage them to integrate into social life and not get busy with virtual life	F	231	258	39	19	11	4.22	0.8671	1
		%	41.40%	46.24%	6.99%	3.41%	1.97%			
5	I encourage my family to use safe and reliable sources for information	F	221	231	81	21	4	4.15	0.8566	4
		%	39.61%	41.40%	14.52%	3.76%	0.72%			
6	I share with my family warning alerts from banks and authorities	F	241	220	62	32	3	4.19	0.8866	2
			43.19%	39.43%	11.11%	5.73%	0.54%			

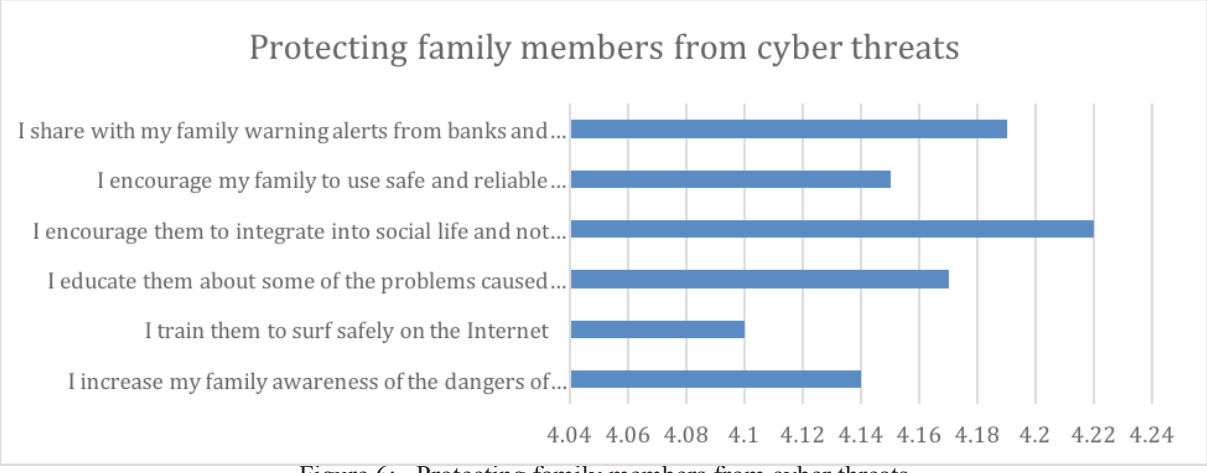

Figure 6: . Protecting family members from cyber threats

Looking at Table 8, it is clear from the arithmetic averages of the items related to the points of view of parents about protecting family members from cyber threats that they have a very high level of cybersecurity awareness for most of the items, and a high level for the other items, where the arithmetic means ranged between 4.10 and 4.22 as shown in figure 6. It was found that the item "I encourage them to integrate into social life and not get busy with virtual life online" got the highest arith-

metic mean, which is very high on a five-point Likert scale," while the item "I train them to surfing safely on the Internet" got the lowest arithmetic averages. The general average in the field of cybersecurity awareness of parents from their point of view is 4.16, which is a high average on a five-point Likert scale. This indicates a high level of awareness of parents about how they protect their family members from cyber threats.

Cybersecurity initiatives by the government to combat cyber threats:

Table 9. Cybersecurity initiatives by the government to combat cyber threats

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	When a cyber crime happens, I report to the service provided by the public security department via absher system.	F	246	209	47	34	22	4.12	1.0546	1
		%	44.09%	37.46%	8.42%	6.09%	3.94%			
2	I encourage my family to know about the Saudi anti cyber crime law.	F	130	252	106	65	5	3.78	0.9613	2
		%	23.30%	45.16%	19.00%	11.65%	0.90%			
3	I encourage my family to learn from www.cert.sa	F	95	98	209	97	59	3.13	1.1995	3
		%	17.03%	17.56%	37.46%	17.38%	10.57%			

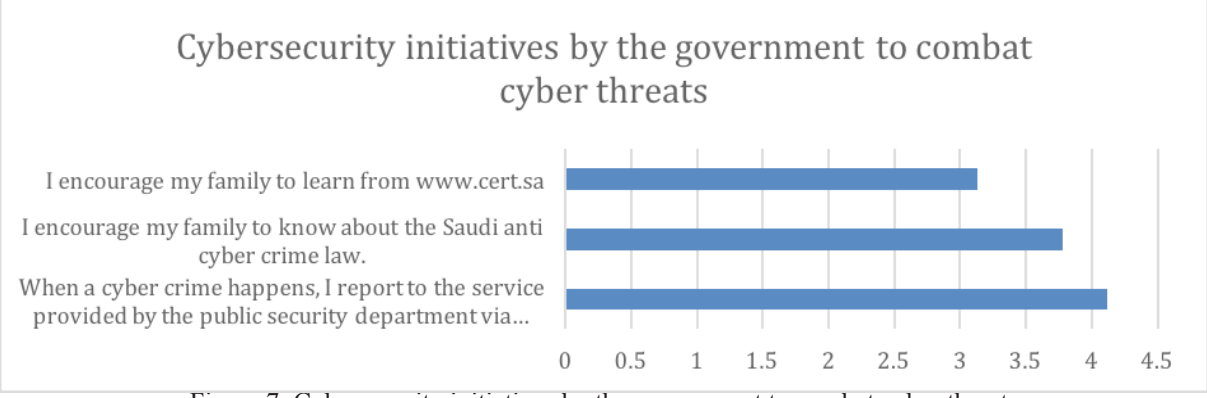

Figure 7: Cybersecurity initiatives by the government to combat cyber threats

Looking at Table 9, it is clear from the arithmetic averages of the items related to the degree of cybersecurity awareness of parents regarding cybersecurity initiatives by the government to combat cyber threats that they have a very high level of cybersecurity awareness for most of the items, and a high level for the other items, where the arithmetic means ranged between 3.13 and 4.12 as shown in figure 7. It was found that the item "When a cyber crime happens, I report to the service provided by the public security department via Absher system" got the highest arithmetic mean (4.12), which is high on the Likert scale, while the item "I encourage my family to learn from www.cert.sa" got the lowest arithmetic average, which is medium on the Likert

scale. The general average in the field of cybersecurity awareness of parents from their point of view is 3.68, which is a high average on a five-point Likert scale. This indicates the high level of parents' awareness about educating their family members about the official sources and organization to fight cyber crimes.

Discussion

Results showed that the highest awareness was regarding the protection of family members from cyber threats, with a mean score of 4.16. This indicates that parents are concerned about the safety of their family members. The second highest awareness was on cybersecurity awareness and surfing safely on the Internet with a mean score of 4.07. This means that the respondents consider cybersecurity when they actively use the Internet. Both items authentication and passwords handling, and parents' greatest online fears came in the third place with a mean score of 4.05. Passwords are changed when forgotten, using other verification methods. The fourth place is taken by family's privacy protection with a mean of 4.01. Parents want their family's private photos and data not to be shared without their consent. The fifth section was computer cybersecurity practices, with a mean of 3.83. Parents take average measures to keep themselves and their family members safe from eminent cyber threats. Finally, the last section was about cybersecurity initiatives taken by the government to combat cyber threats, with a mean score of 3.68. Therefore, many recommendations can be made.

Recommendations:

The recommendations with regard to cybersecurity awareness among parents can be stated as follows:

Spreading a culture of cybersecurity awareness among parents to look after their family members and protect them from all kinds of internet threats.

Preparing technical awareness programs aimed at media awareness campaigns to protect families from the internet threats, and taking security measures and precautions against the dangers of electronic attacks.

Including methods and strategies to protect family members from Internet dangers, and cybersecurity concepts in courses and curricula at all educational levels, with the need to employ terminology that serves each age group.

Conclusion

The current descriptive study aimed to investigate the extent to which parents are aware of cybersecurity in Saudi Arabia. Previous studies have revealed the importance and some major aspects of cybersecurity in today's information era. Moreover, parents are older than their children, and they may not keep up with the rapid technological changes in this digital era. In this regard, a sample of 558 parents, including 346 males and 212 females, was addressed by an online survey. The descriptive statistics in the forms of frequencies, percentages, mean scores, and standard deviations revealed that parents are, to a large extent, aware of the existence of cyber threats by willing to protect their

family members from cyberattacks like phishing, hacking and even cyberbullying. However, this knowledge needs to be put into practice by taking concrete measures by parents and governmental bodies. Time constraints and sample size can be overcome in previous studies by having longitudinal studies rather than cross-sectional studies. In general, it is important that parents and stakeholders be aware of the importance of cybersecurity, as well as practical strategies to protect themselves and their family members from cyber threats and cyber attacks.

References

[1] Nurunnabi, M., 2017. Transformation from an oil-based economy to a knowledge-based economy in Saudi Arabia: the direction of Saudi vision 2030. Journal of the Knowledge Economy, 8(2), pp.536-564. doi: 10.1007/s13132-017-0479-8.

[2] Quadri, A. and Khan, M.K., 2019. Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present and future. pp. 1–22, 2019, [Online]. Available at: https://www.researchgate.net/publication/331009167%0A

[3] Alashwali, E. and Alashwali, F., 2022. Saudi parents' privacy concerns about their children's smart device applications. International Journal of Child-Computer Interaction, 33, p.100486.

[4] Quayyum, F., Bueie, J., Cruzes, D.S., Jaccheri, L. and Vidal, J.C.T., 2021, September. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In Proceedings of the Conference on Information Technology for Social Good (pp. 236-241).pp. 236–241. doi: 10.1145/3462203.3475900.

[5] Al-Naser, A.E., Bushager, A. and Al-Junaid, H., 2019, March. Parents' awareness and readiness for smart devices' cybersecurity. In 2nd Smart Cities Symposium (SCS 2019) (pp. 1-7). IET.

[6] Gasior, R. M. 2010. "Parental awareness of cyber bullying," 2010. [Online]. Available: http://csus-dspace.calstate.edu/xmlui/handle/10211.9/119

[7] Muir, K. and Joinson, A., 2020. An exploratory study into the negotiation of cyber-security within the family home. Frontiers in Psychology, 11, p. 424. doi: 10.3389/fpsyg.2020.00424.

[8] Quayyum, F., Cruzes, D.S. and Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, p.100343. doi: 10.1016/j.ijcci.2021.100343.

[9] Nayci, Ö. 2021. Examination of Digital Parenting Awareness of the Primary School Students' Parents during the COVID-19 Pandemic. Pegem Journal of Education and Instruction, 11(2), pp.58-71.

[10] Pangrazio, L., 2021. Apps that help parents protect kids from cybercrime may be unsafe too. Parenting for a Digital Future. [Online]. Available: https://blogs.lse.ac.uk/parenting4digitalfuture/2021/05/12/parent-control-apps/

[11] Schemer, C., Masur, P.K., Geiß, S.,

Müller, P. and Schäfer, S., 2021. The impact of internet and social media use on well-being: A longitudinal analysis of adolescents across nine years. Journal of Computer-Mediated Communication, 26(1), pp.1-21. doi: 10.1093/jcmc/zmaa014.

[12] Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A., 2019. Cyber security education is as essential as "the three R's". Heliyon, 5(12), p.e02855. doi: 10.1016/j.heliyon.2019.e02855.

[13] Lo Cricchio, M.G., Palladino, B.E., Eleftheriou, A., Nocentini, A. and Menesini, E., 2021. Parental mediation strategies and their role on youths' online privacy disclosure and protection: A systematic review. European Psychologist, 27(2), pp. 116–130, 2021, doi: 10.1027/1016-9040/a000450.

[14] Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S. and Jambari, D.I., 2019. Parental awareness on cyber threats using social media. Jurnal Komunikasi: Malaysian Journal of Communication, 35(2), pp.485-498. doi: 10.17576/JKMJC-2019-3502-29.

[15] AlShabibi, A. and Al-Suqri, M., 2021, December. Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. In 2021 22nd International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE. doi: 10.1109/ACIT53391.2021.9677117.

[16] Glavind, K.L., 2021. Essays on Smartphones' Effects on Attention and Behavior (Doctoral dissertation, University of Copenhagen). doi: 10.1016/j.jheale-co.2019.102274.

[17] Elgharnah, K.G.E. and Ozdamli, F., 2020. Determining parents' level of awareness about safe internet use. World Journal on Educational Technology: Current Issues, 12(4), pp.290-300.doi: 10.18844/wjet.v12i4.5182.

[18] International Telecommunication Union, 2020. "Global Cybersecurity Index (GCI)," ITU Publications. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (accessed Mar. 22, 2022).

[19] Qian, Y., Ye, F. and Chen, H.H., 2022. Basic network security concepts. 1st ed., Wiley-IEEE Press, 2022, pp. 13–25. doi: 10.1002/9781119244400.ch2.

[20] Edwards, N., Kiser, S.B. and Haynes, J.B., 2020. Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability. Journal of Strategic Innovation and Sustainability, 15(4), pp.10-14. doi: 10.33423/jsis.v15i4.2956.

[21] Rawal, S. 2020. "Pros and cons of internet usage among children research papers," Pharma Innov. J., 9(10), pp. 482–484, 2020, Available at: http://www.thepharmajournal.com

[22] Othman, R.B., Rahim, K.F., binti Kamarulzaman, R.A., Amat, D.W. and Yahya, K., 2018. Literature review on internet benefits, risks and issues: a case study for cyber parenting in Malaysia. Recent Trends in Science, Technology, Management and Social Development, p.88. doi: 10.26480/mecj.02.2019.12.14.

[23] Abdulhameed, R.S., 2021. Crimes of threats and cyber extortion through social media: a comparative study. Review of International Geographical Education Online, 11(12), pp.1022-1033.

[24] Georgiadou, A., Mouzakitis, S. and Askounis, D., 2021. Detecting insider threat via a cyber-security culture framework. Journal of Computer Information Systems, pp.1-11. doi: 10.1080/08874417.2021.1903367.

[25] Kurniasanti, K.S., Assandi, P., Ismail, R.I., Nasrun, M.W.S. and Wiguna, T., 2019. Internet addiction: a new addiction?. Medical Journal of Indonesia, 28(1), pp.82-91.

[26] Helsper, E.J. and Smahel, D., 2020. Excessive internet use by young Europeans: psychological vulnerability and digital literacy?. Information, Communication & Society, 23(9), pp.1255-1273. doi: 10.1080/1369118X.2018.1563203.

[27] Cahyo, S.D., Al Fariz, A.B. and Lestari, C.A., 2020. Does internet usage frequency give impact to student's academic performance?. Indonesian Journal of Educational Assessment, 3(1), pp.16-23. doi: 10.26499/ijea.v3i1.57.

[28] Dyer, T., 2018. The effects of social media on children. Dalhousie Journal of Interdisciplinary Management 14(2018).

[29] Woods, N. and Siponen, M., 2018. Too many passwords? How understanding our memory can increase password memorability. International Journal of Human-Computer Studies, 111, pp.36-48. doi: 10.1016/j.ijhcs.2017.11.002.

[30] Alruwaili, A., 2019. A review of the impact of training on cybersecurity awareness. International Journal of Advanced Research in Computer Science, 10(5), pp. 1–3, 2019, doi: 10.26483/ijarcs.v10i5.6476.

[31] Murn, L., 2021. Data Safety and Cybersecurity. Digital Transformation of the Laboratory: A Practical Guide to the Connected Lab, pp.85-100. doi: 10.1002/9783527825042.ch4.

[32] Akinde, O.K., Ilori, A.O., Afolayan, A.O. and Adewuyi, O.B., 2021. Review of Computer Malware: Detection and Preventive Strategies. Int. J. Comput. Sci. Inf. Secur.(IJCSIS), 19, p.49.

[33] Al-Dahshan, Khalil J. A. and Al-Fuwaihi, H. A. K. (2010). "Digital citizenship is an introduction to help our children live in the digital age", Journal of Psychological and Educational Research, 30(4), pp. 1-42.

[34] Al Shamsi, A.,2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. Int. J. Inf. Technol. Lang. Stud, 3(2), pp. 8-29.

[35] Gogus, A, and Yücel S., 2019. Privacy perception and information technology utilization of high school students. Heliyon, 5(5)

A Novel Classifier for Cyber Attack Detection System in Industrial Internet of Things

Fathe Jeribi
College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia - Email: fjeribi@jazanu.edu.sa

Abstract

The usage of the Internet of Things (IoT) conception in the industrial sector along with applications is referred to as the Industrial Internet of Things (IIoT). Various applications have been subsumed in the IIoT. Nevertheless, cybercriminals mostly target these systems. Thus, here, a novel methodology of Cyber Attack Detection (CAD) system has been proposed in IIoT to overcome the aforementioned issue. UNSW-NB2015 and DS2OS are the two IIoT datasets utilized in this work. Initially, in both datasets, the missing values are replaced; subsequently, the feature extraction is performed. Next, by utilizing Poisson Distribution-based Naked Mole Rat Optimization Algorithm (PD-NMROA), the significant features are selected as of both datasets. After that, by employing MaHalanobis distance-based K-Means (MaH-KMeans) algorithm, the features extracted as of the datasets are normalized along with clustered. Eventually, to classify the data, the clustered features are inputted to the TanSwish - Restricted Boltzmann Dense Machines (TS-RBDMs). The experiential outcomes displayed that the proposed methodology obtained higher efficacy in contrast to the prevailing systems.

Keywords:
Poisson Distribution-based Naked Mole Rat Optimization Algorithm (PD-NMROA, MaHalanobis distance-based K-Means algorithm (MaH-KMeans), TanSwish - Restricted Boltzmann Dense Machines (TS-RBDMs), feature scaling, deep learning.

Introduction

Recently, the establishment of the IIoT has been brought about by the development in the industrial field by amalgamating the IoT, industrial system, along with cloud computing [1]. Acquiring the benefits of IoT technology in Industrial Control Systems (ICSs) is the major idea behind IIoT [2]. In the industrial process, to abate the human factor encumbrance and deal with the complicated industrial system process along with communications amongst them effectively, the ICS is utilized [3]. From several sensors, larger amounts of data can be gathered via IIoT for utilization all over the world. Retail, healthcare, transport, and automotive are several industries in which these applications are employed [4]. IIoT increases productivity, effectiveness, and operational efficiency significantly in numerous industries [5]. In general, cyber operations along with their effects are constrained to the cyber dimension in the conventional Information and Technology (IT) systems; however, special effects of normal operations outdo the limitations of the physical realm in IIoT [6]. To store along with to analyze big data engendered by the

IoT as well as IIoT systems, numerous data management, and security tools have been deployed in the cloud [7, 8]. The IIoT permits higher productivity; nevertheless, an attack on the infrastructure might be disastrous if it is not secured; thus, leading to an immense loss [9]. The development of IDS along with its security solutions brought about IIoT; however, to verify IIoT system requirements, these solutions have to be analyzed, checked, along with tuned utilizing labelled datasets; thus, espousing it in a real-world environment is highly challenging [10]. Thus, for the CAD system, a novel TS-RBDMS classifier is proposed in IIoT.

Application of Artificial Intelligence/Machine Learning in Cyber Security

Artificial Intelligence can be applied to security systems as a way to reduce cyber security threats. Here, a machine learns from the input data and makes a future prediction. It is utilized in email filters to sort out spam, banking software for detecting unusual transactions, internet search engines, websites for making personalized recommendations, and numerous apps on our phones like voice recognition. For cybersecurity, ML has become a significant technology. With ML, the patterns can be analyzed by cybersecurity, and learn from them to help in preventing similar attacks and respond to changing behaviour.

In the process of detecting cyber-attacks in IIoT, several benefits have been provided by the prevailing models; even then, there are certain uncertainties in those models; the drawbacks in the existing methodologies are enlisted below.

- There occurs exponential progression in computing times along with other complexities owing to the number of nodes and layers that augment the network structure.
- The huge cyber-attack classification problem, which evolved in the face of a real network application environment, is not addressed effectually by the prevailing system. Numerous classification tasks would result in lesser accuracy owing to the dynamic growth of datasets.
- Owing to higher energy consumption, time complexity, along with deprived algorithm design, there is a deficiency in QoS with energy efficiency.

Thus, for detecting cyber-attacks in IIoT, a novel TS-RBDMS classifier is proposed in this work. The proposed technique's major contributions and their significant are enlisted further:

- PD-NMROA is utilized for selecting the optimal features. This overcomes the problem of generating the same probability values.
- MaH-KMeans is proposed for clustering the features with non-convex shapes.
- TS-RBDMs are proposed to overcome the overfitting problem and reduce computation time.

The data are collected as of the datasets initially; then, they are pre-processed for replacing the missing values. After that, the features are extracted from the pre-processed data. Now, by utilizing PD-NMROA, the optimal features are selected.

Then, the selected features are scaled and then clustered by utilizing MaH-KMeans. Lastly, for classifying whether the data is attacked or non-attacked, TS-RBDMs are utilized.

The rest of the paper is organized as follows: the related works regarding the proposed model are reviewed in section 2; the proposed methodology is explicated in section 3; the results and discussion is demonstrated in section 4; lastly, section 5 offers conclusions and future work.

Literature Review

Zil e. Huma et al. [11] presented a Hybrid Deep Random Neural Network (HDRaNN) aimed atCADin the IIoT. The applications of DRaNN, as well as Multilayer Perceptron (MLP), were utilized by the HDRaNN. The experimental outcomes displayed the presented model's accuracy. Nevertheless, owing to Deep Learning (DL) ability, the developed model's computation time is high.

Shahid latif et al. [12] developed a lightweight Random Neural Network (RaNN)-centric prediction model. Attacks had been detected precisely by the presented RaNN model. The experiential outcomes demonstrated that the model attained a higher accuracy. However, merely limited attacks were deemed by this system.

Shahid Latif et al. [13] illustrated a DRaNN-centric scheme intended for intrusion detection in IIoT. For classifying the varied sorts of attacks, the DRaNN was employed. The evaluation outcomes exhibited that the presented methodology possessed a higher attack detection rate. Nevertheless, the system had a higher complexity.

Muna AL-Hawawreh et al. [14] suggested an anomaly detection mechanism meant for Internet ICSs (IICSs) grounded on DL models. The execution of a consecutive training process utilizing a deep auto-encoder was enclosed in this model. The experiential outcomes displayed that when analogized with the prevailing methodologies, the presented one achieved a higher detection rate along with a lower False Positive Rate (FPR). Nevertheless, owing to the NN's narrow waist structure, the model had a higher training time.

Radhakrishna Vangipuram et al. [15] developed a machine learning strategy aimed at imputation as well as anomaly detection in an IoT environment. The imputed datasets acquired by utilizing K-Means, F-Kmeans, and developed imputation methodologies were considered to perform classification. The experiential outcomes displayed that in contrast to the conventional classifiers, the presented model's performance was far better. However, the system had a higher computation cost.

Di Wu et al [16] recommended a Long Short-Term Memory (LSTM)-Gauss-NBayes model, which was a synergy of the LSTM Neural Network (LSTM-NN) and the Gaussian Bayes model for outlier detection in IIoT. In this, to detect the prediction error, the presented LSTM model was utilized. The experimental results demonstrated that optimistic results were obtained by this model. Nevertheless, more memory was utilized by this model

to train.

Tran Viet Khoa et al. [17] developed a collaborative learning-centric Intrusion Detection System (IDS). To classify the packets into normal and abnormal behaviors, the Deep Belief Network (DBN) was utilized. The experiential outcomes displayed that when analogized with traditional machine learning methodologies, the presented model attained a better performance. However, for a smaller number of data, the DBN was not appropriate.

Faezeh Farivar et al. [18] recommended a model to determine along with to reimburse for attacks hurled in the forward link of nonlinear Cyber-Physical Systems (CPSs) utilizing the intelligent variable structure control. For estimating the attack, Neural Network (NN) estimator was utilized. The simulation outcomes proved the developed system's efficacy. Nevertheless, the system had higher training time owing to NN's narrow waist structure.

Yanmiao Li et al. [19] illustrated a DL model for intrusion detection utilizing a multi-Convolutional Neural Network (multi-CNN) fusion methodology. For classification, the CNN was presented into the IDS by utilizing the flow data visualization model. The experimental outcomes that the presented system possessed a higher accuracy of multi-CNN. However, owing to the existence of a vanishing gradient problem in CNN, the data was learned gradually by the developed methodology.

Muna AL-Hawawreh and Elena Sitnikova [20] presented a detection system grounded on the stacked Variational Auto-Encoder (VAE) with a fully connected NN. The latent structure of system activities was learned by the VAE with a fully connected NN; in addition, it exposed the ransomware behavior. The outcomes displayed that a superior detection rate was attained by the presented model in contrast to the prevailing methodologies. However, as a result of the auto encoder's blurry characteristics, an accurate output was not provided by the system.

Proposed Cyber Attack Detection Method

For effective detection along with classification of attack or non-attack, a novel TS-RBDM Classifier has been proposed in this paper. Here, initially, the features are extracted. Next, as of extracted features, the significant features are selected. After that, for the classification of attacks or non-attacks, the features being selected are inputted into the TS-RBDM Classifier. Figure 1 exhibits the block diagram of the proposed methodology.

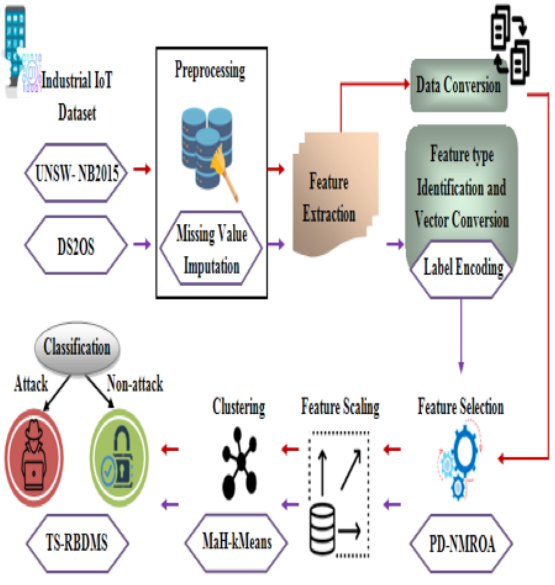

Fig. 1. Block Diagram of the Proposed Methodology

UNSW-NB2015 and DS2OS are the datasets utilized by the proposed CAD system. Here, owing to the non-existence of values in those datasets, the missing value imputation is executed. To retain most data of the dataset, the missing data is replaced with certain substitute values by performing the imputation process. Let the UNSW-NB2015 data set be U . In this, the missing value is substituted with the same attribute values that are signified in the dataset. It is formulated as:

$$\hbar_i^{mi} \in U = \hbar_i \leftrightarrow U_{sameatt} \quad (1)$$

Where, the missing value and output of the missing value are specified as $\hbar_i$ and $\hbar_i^{mi}$, the same attribute value in the dataset is notated as $U_{sameatt}$.

Let the DS2OS dataset be D . Here, a few values are not assigned. Additionally, these columns are substituted with certain meaningful value λ_i^{mi} , which is expressed as:

$$\lambda_i^{mi} \in D \to \delta(\lambda_i) \quad (2)$$

Where, the replacement function is symbolized as δ , and the column that represents the True, False, Twenty, and None are substituted with 1.0, 0.0, 20.0, and 0.0, correspondingly. The data as of both datasets U_{pre} and D_{pre} are obtained following the completion of pre-processing.

Feature extraction

More information about the dataset can be obtained swiftly with the aid of feature extraction (attributes extraction). Therefore, from U_{pre} , protocol, service state, standard mean, deviation mean, et cetera are the key attributes being extracted. The extracted attributes $f_n \in U_{pre}$ are expressed as:

$$f_n^{U_{pre}} = \{f_1^{U_{pre}}, f_2^{U_{pre}}, f_3^{U_{pre}}, \ldots\ldots f_N^{U_{pre}}\} \quad (3)$$

In this process, from D_{pre} , the attributes like address, source ID, destination, type, et cetera are extracted; eventually, the output $f_n^{D_{pre}}$ is attained.

Data conversion

In this, as the strings are extant in the dataset, the extracted attributes $f_n^{U_{pre}}$ are transmuted into numbers. Moreover, those strings are not processed in the classifier. Thus, the strings are converted into numbers. In the dataset, the numbers are assigned for every single string to perform this conversion $f_{i(con)}^{U_{pre}}$. It is modelled as:

$$f_{i(con)}^{U_{pre}} = \Delta\left(f_i^{U_{pre}}\right) \quad (4)$$

Where, the conversion function is represented as Δ .

Feature type identification and vector conversion

Here, the feature type is detected as whether it is a string or vector in $f_n^{D_{pre}}$. If the feature is detected as a string then the string features are partitioned; in addition, they are transmuted into the vector format by encoding. The process of transmuting the labels into numeric by assigning the numeral values to strings in alphabetical order is termed label encoding. It is formulated as:

$$f_{n(con)}^{D_{pre}} = S\left(f_i^{D_{pre}}\right) \quad (5)$$

Where, the vector conversion's output is specified as $f_{n(con)}^{D_{pre}}$, the state is signified as S, which illustrates the numerals.

Feature selection

In this, by utilizing the PD-NMROA, the features are selected as of $f_n^{U_{pre}}$. Naked mole rats' behavioral characteristics are the major concept behind the NMROA. Regarding the breeding probability, the breeder group is selected; here, the uniform distribution random process is utilized to perform initialization. Betwixt the ranges with the same probability, the population is created. In the initialization step, the Poisson Distribution model is replaced to overcome the problem of such generation of the same probability values in the prevailing algorithm.

(a) Population initialization

Firstly, the NMR's population is engendered randomly in *d* dimensional vector where the features being extracted are regarded as a number of NMR; furthermore, by utilizing the Poisson Distribution system, every single NMR is initialized as:

$$f_{uv}^{U_{pre}} = \frac{e^{-\ell} * \ell^{n\left(f_n^{U_{pre}}\right)}}{n\left(f_n^{U_{pre}}\right)} \tag{6}$$

Where, the u^{th} NMR in v^{th} dimension is specified as $f_{uv}^{U_{pre}}$, the number of NMRs is signified as $n\left(f_n^{U_{pre}}\right)$, and the average number of $f_n^{U_{pre}}$ occurrences of is notated as $\ell^{n\left(f_n^{U_{pre}}\right)}$.

(b) Calculating fitness value

Regarding the classifier's accuracy, the objective function along with its fitness value is computed after initializing the population. It is measured as:

$$\wp_n = \Gamma\left(f_{(uv)}^{U_{pre}}\right) \tag{7}$$

Where, the output of the n^{th} fitness function of th number of NMR is symbolized as $\wp_n$, and the fitness function is represented as Γ. The population is further partitioned into breeder and worker concerning the fitness value; moreover, the queen (q) is also estimated.

(c) Worker group

Here, by enhancing their fitness, NMR workers attempt to turn into breeders to mate with the queen. Subsequently, regarding its own experience along with local information, the NMR's new solution is generated; in addition, for the new solution, the fitness value is computed. Next, the new solution is forwarded to the breeder group. The new solution will be accepted if it is better than the preceding solution. Or else, it will be continued with the previous solution. Here, the new solution is spawned as:

$$\omega_u(I+1) f_{uv}^{U_{pre}} = \omega_u(I) + \alpha\left(\omega_x(I) - \omega_y(I)\right) \tag{8}$$

Where, the u^{th} worker in $(I+1)^{th}$ iteration is specified as $\omega_u(I+1)$, the u^{th} worker in I^{th} iteration is indicated as $\omega_u(I)$, the uniform distribution in the range of $[0,1]$ is denoted as a, and the random solutions from the worker's group are represented as $\omega_x(I)$ and $\omega_y(I)$.

(d) Breeder group

Every single breeder NMR in this breeder

group attempts to update its position with an intention to stay as a breeder, additionally, to be selected as the breeder for mating. Regarding the breeding probability, the breeder NMRs are updated in terms of the overall best in the range of $[0,1]$. The breeder will be sent to the worker's group if its NMR is not capable to ameliorate its fitness. The breeders update their position as:

$$B_u(I+1)f_{uv}^{U_{pre}} = (1-\alpha)B_u(I) + \alpha(q - B_u(I)) \quad (9)$$

Where, the u^{th} breeder in $(I+1)^{th}$ iteration is notated as $B_u(I+1)$, and the u^{th} breeder in I^{th} iteration is illustrated as $B_u(I)$.
Until satisfying the termination condition, the whole search procedure will be continued iteratively. Next, the significant features are selected just like the best breeder selected utilizing the PD-NMROA. It is modelled as:

$$f_{n(sel)}^{U_{pre}} = \{f_{1(sel)}^{U_{pre}}, f_{2(sel)}^{U_{pre}}, f_{3(sel)}^{U_{pre}}, \ldots\ldots f_{N(sel)}^{U_{pre}}\} \quad (10)$$

Where, the number of selected features is specified as $f_{n(sel)}^{U_{pre}}$. In the same manner, by utilizing the same algorithm that is utilized for the feature selection in the UNSW-NB2015 dataset, the features are extracted $f_n^{D_{pre}}$; consequently, the selected features' output in the DS2OS dataset $f_{n(sel)}^{D_{pre}}$ is obtained.

Feature scaling

The range of variables in the selected features is extremely varied; so to unify feature ranges in data, a mechanism is utilized, which is termed the feature-scaling model. Therefore, the proposed model in which the features within the range are normalized utilizing robust scaling for the UNSW-NB2015 dataset $f_{n(nor)}^{U_{pre}}$ is formulated as:

$$f_{n(nor)}^{U_{pre}} = \frac{f_{i(sel)}^{U_{pre}} - \left(f_{i(sel)}^{U_{pre}}\right)^*}{\Psi} \quad (11)$$

Where, the median of $f_{n(nor)}^{U_{pre}}$ is defined as $\left(f_{i(sel)}^{U_{pre}}\right)^*$, and the Inter Quartile Range is notated as Ψ. Similarly, the features are normalized for $f_{n(sel)}^{D_{pre}}$ and the output $f_{n(nor)}^{D_{pre}}$ is attained. 80% of the normalized features are utilized for training whereas the remaining 20% are utilized for testing.

Clustering

By utilizing the MaH-KMeans, the features $f_{n(nor)}^{U_{pre}}$ are clustered with regard to protocol, state, id, et cetera following the normalization process. The K Means segmentation is the technique of vector quantization; the major intention of this model is to partition the number of features into ϕ clusters where every single feature corresponds to the cluster with the nearest mean.
(i) Selecting the number of clusters, (ii) Initializing centroids, (iii) Assigning features to the nearest value, and (iv) Reinitializing centroids are the steps undergone by the algorithm for segmenting the scaled features. Generally, the basic Euclidean distance is utilized for the partitioning of features in clustering. Nevertheless, for the detection of clusters with non-convex shapes, this model is not appropriate. Here, the model is replaced with the MaHalanobis distance technique. The steps in MaH-KMeans are:

- The number of clusters, which is estimated by their centroids, is selected.

The centroid is the cluster's center. However, primarily, the feature's exact center is not known. Thus, to define every single cluster, the centroids C_ϕ can be selected randomly as:

$$C_\phi = \{C_1, C_2, C_3, \ldots\ldots C_N\} \quad (12)$$

- The feature $f_{i(nor)}^{U_{pre}}$ is assigned to the closest centroid.
- The distance betwixt the assigned feature and centroid is computed utilizing the MaHalanobis distance strategy. It is expressed as,

$$\Phi^2 = \left(f_{i(nor)}^{U_{pre}} - C_\phi\right)^T * m^{-1} * \left(f_{i(nor)}^{U_{pre}} - C_\phi\right) \quad (13)$$

Where, the MaHalanobis distance technique's output is specified as Φ^2, and the inverse covariance matrix of C_ϕ is symbolized as m^{-1}.

- A cluster is chosen for features where the distance betwixt the feature and centroid is minimum.
- By computing the average of all the data points of that cluster, the centroids are reinitialized.

$$C_\phi = \frac{1}{n\left(f_{n(nor)}^{U_{pre}}\right)} \sum f_{n(nor)}^{U_{pre}} \quad (14)$$

Where, the number of features is denoted as $n\left(f_{n(nor)}^{U_{pre}}\right)$.

This process is repeated until no alterations occur in clusters. The clustered output $\aleph_n^{U_{pre}} \in f_{n(nor)}^{U_{pre}}$ is attained via this process. Likewise, based on source id, type, address, et cetera, the features presented in $f_{n(nor)}^{D_{pre}}$ are clustered by employing the same process; furthermore, the output $\aleph_n^{D_{pre}} \in f_{n(nor)}^{D_{pre}}$ is acquired. The pseudo-code of MaH-KMeans is:

Input: Normalized features $f_{n(nor)}^{U_{pre}}$

Output: clustered features $\aleph_n^{U_{pre}} \in f_{n(nor)}^{U_{pre}}$

Begin

Initialize C_ϕ, Φ^2 and $n\left(f_{n(nor)}^{U_{pre}}\right)$

While $(\phi = 1)$

Select number of centroids

Assign feature to the closest centroid

For each feature, **do**

Compute distance Φ^2

End for

Reinitialize centroids

End while

Return $\aleph_n^{U_{pre}} \in f_{n(nor)}^{U_{pre}}$

Classification

In this, to classify whether the data is attacked or non-attacked, the clustered features $\aleph_n^{U_{pre}}$ are inputted into the TS-RBDMs. In the context of unsupervised learning, the Restricted Boltzmann Machine (RBM), a latent-variable generative model, is utilized most frequently. It comprises hidden H_g as well as visible units ε_k and contains a weight matrix in the size of $l \times z$, which is associated betwixt visible and hidden units. It has no output layer. However, the prevailing methodologies are integrated with some additional layers like MLP, drop layer, and so on; thus, resulting in a higher computation time along with an overfitting problem. Thus, a dense layer is proposed in this work to address this issue; this layer compensates for all the characteristics of the aforementioned layers. Figure 2 exhibits the architecture of TS-RBDMs.

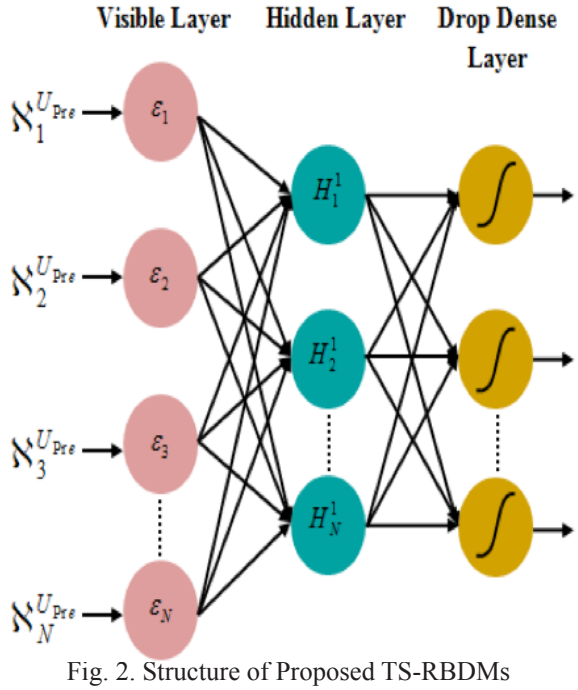

Fig. 2. Structure of Proposed TS-RBDMs

Primarily, with the input features $\aleph_n^{U_{pre}}$, the TS-RBDMs' first layer is pre-trained. By means of the energy function, the TS-RBDMs' learning process is performed. The energy function $E(\varepsilon, H)$ is proffered as:

$$E(\varepsilon,H)=-\sum_k a_k\varepsilon_k-\sum_g b_g H_g-\sum_k\sum_g \varepsilon_k W_{k,g}H_g \qquad (15)$$

Where, the bias values are represented as a_k and b_g, the element weight is specified as $w_{k,g}$,and the number of units is notated as k,g.

The $E(\varepsilon, H)$ is formulated in the matrix representation as:

$$E(\varepsilon,H)=a^T\varepsilon-b^T H-\varepsilon^T WH \qquad (16)$$

The first hidden layer's output is inputted into the subsequent hidden layer after obtaining all the parameters of the first hidden layer. Next, the '2' hidden layers are deemed as new TS-RBDMs. Similarly, by updating the bias along with weight values continuously, TS-RBDMs' every single layer is trained separately. The weight and bias values of the first hidden layer's visible unit are updated as:

$$H^1(\varepsilon_k)=\chi(a_k+\sum_{k,g} W_{k,g}\varepsilon_k(\aleph_n^{U_{pre}})) \qquad (17)$$

Where, the TanSwish activation function in the drop dense layer is specified as χ ; here, every single neuron gets input as of all the neurons of the preceding layer; moreover, they are changed into a single output. Therefore, in this work, the overfitting problem is prevented. The TanSwish activation function is expressed as:

$$\chi=\frac{\aleph_n^{U_{pre}}\left(e^{\aleph_n^{U_{pre}}}-e^{-\aleph_n^{U_{pre}}}\right)}{1+e^{-\aleph_n^{U_{pre}}}\left(e^{\aleph_n^{U_{pre}}}+e^{-\aleph_n^{U_{pre}}}\right)} \qquad (18)$$

After that, the subsequent hidden layer's visible unit is fed with the output being computed. The output is achieved by the continuous updation along with training till the last layer of TS-RBDMs; subsequently, the attacked or non-attacked data in the IIoT system is retrieved. Furthermore, to predict whether the data is attacked or non-attacked, the same process is proceeded for $\aleph_n^{D_{pre}}$.

Result and Discussion

Here, to analyze the proposed methodology's performance, various experiments were performed.

The data used in the proposed work is obtained from UNSW-NB15 and DS2OS datasets. The proposed model is executed in PYTHON.

Dataset description

- UNSW-NB15
  It is a network intrusion dataset. Information pertinent to Denial of Service (DoS), raw network packets, worms, Backdoors, and Fuzzers attacks is included in this dataset. With multiple attack records, it is separated into training and testing datasets. The number of records in the training set is 175,341 records, whereas in the testing set are 82,332 records from the different types, attack and normal. Argus and Bro-IDS tools extracted a total of 49 features comprising packet-centric and flow-centric features from the raw network packets [22]. Packet-based features are extracted from the packet header along with its payload. Conversely, flow-centered features are generated utilizing the sequencing of packets, from a source to a destination, traveling in the network.
- DS2OS
  Information attained as of network traces is included in this dataset. This data is employed for the evaluation of different anomalies in the network. Here, from numerous organizations conducting varying services, the information is obtained. The dataset encompasses a total of 357952 samples with 10017 anomalous and 347935 normal values [23]. It contains 13 features and '7' various sorts of attacks like malicious operations, wrong setup, scan, denial of service, malicious control, spying, along with data type probing attacks.

Performance analysis for UNSW-NB15 dataset

Here, regarding feature selection, classification accuracy, along with clustering time, the proposed CAD model's performance is assessed.

Performance evaluation of proposed PD-NMROA

Naked Mole Rat Optimization Algorithm (NMROA), Whale Optimization Algorithm (WOA), Crow Search Algorithm (CSA), and Fish Swarm Optimization (FSO) Algorithm are the prevailing methodologies with which the proposed PD-NMROA is analogized regarding fitness vs.iteration.

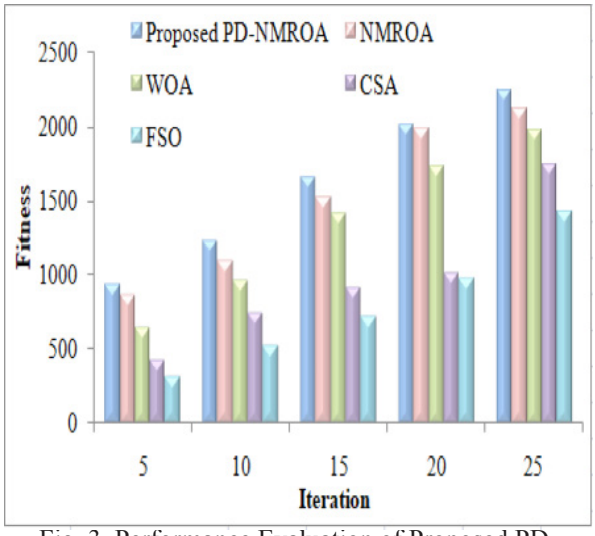

Fig. 3. Performance Evaluation of Proposed PD-NMROA

As per figure 3, it is evident that the proposed model's fitness value increases with the increase in the number of iterations. In the proposed model, for the varying number of iterations like 5, 10, and 25, the fitness values obtained are 948, 1235, and 2245, respectively; however, the reduced fitness values attained by the prevailing WOA are 653 (5), 970 (10), and so on. In

the same manner, only lower range values are obtained by the other prevailing NMROA, CSA, and FSO methodologies. Thus, it is proved that in contrast to the prevailing methodologies, the proposed one attained a higher performance.

Performance evaluation of proposed MaH-Kmeans

Here, regarding clustering time, the proposed model's performance is analogized with the prevailing KMeans (KM), Birch, Fuzzy C Means (FCM), and Mean Shift (MS) methodologies.

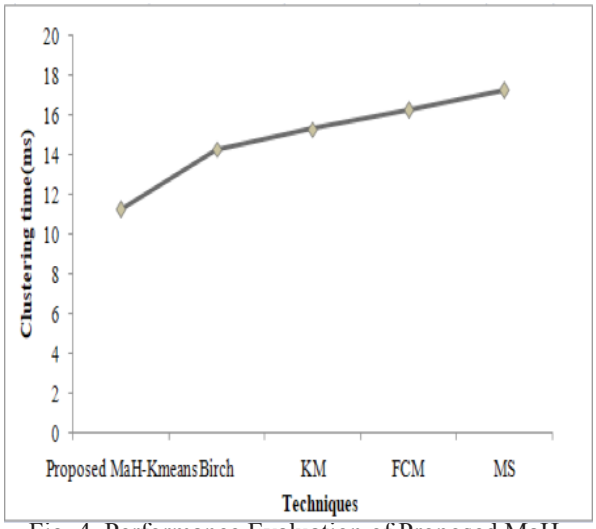

Fig. 4. Performance Evaluation of Proposed MaH-KMeans

Regarding clustering time, the proposed model's performance is evaluated in figure 4. It is evident that a lower clustering time of 11.2365ms was attained by the proposed MaH-Kmeans whereas the clustering time obtained by the prevailing Birch, KM, FCM, and MS methodologies are 14.2563ms, 15.2896ms, 16.2358ms, and 17.2356ms, correspondingly, which are higher than that of the proposed model. Consequently, it is concluded that when analogized with the prevailing methodologies, the proposed model is highly secure as well as faster.

Superiority measure of proposed TS-RBDMS

Here, DRaNN [13], DAE-DFFNN (Deep Auto-Encoder-Deep Feed Forward Neural Network) [14], and HDRaNN [11] are conventional methodologies with which the proposed TS-RBDMS is analogized regarding the metrics like Accuracy.

Table 1: Comparative analysis of proposed TS-RBDMS

Techniques	Accuracy (%)
Proposed TS-RBDMS	99.68
DRaNN [13]	99.54
DAE-DFFNN [14]	92.48
HDRaNN [11]	90.21
DAE-DFFNN [21]	98.9

With regard to the accuracy, the proposed TS-RBDMS is analogized with other prevailing methodologies and is tabulated in table1. The proposed model attained the highest accuracy of 99.68% whereas the least accuracy of 90.21% was obtained by the conventional HDRaNN mechanism. Similarly, the performance metrics differ for other classifiers also. Thus, it is evident that better performance was achieved by the proposed model than the prevailing methodologies.

Table 2 depicts the comparative analysis of the proposed and the conventional systems regarding precision, recall, and f-measure. The precision, recall, and f-measure attained by the proposed approach are 99.86%, 99.55%, and 99.54%,

Table 2: Comparative analysis of the proposed model in terms of precision, recall, and f-measure

Techniques/ Metrics	Precision (%)	Recall (%)	F-Measure (%)
Proposed TS-RBDMs	99.86	99.55	99.54
HDRaNN [11]	99.07	98.98	99.02
DAE-DFFNN [21]	99.8	99.6	96.7

correspondingly, which are higher than the prevailing approaches, namely HDRaNN and DAE-DFFNN. Thus, it is concluded that the proposed model is more efficient in attack detection in IIoT.

Performance analysis for DS2OS dataset

In this section, the proposed methodology's performance is assessed concerning feature selection, clustering time, along with classification accuracy.

Performance evaluation of proposed PD-NMROA

The proposed model is analogized with the prevailing methodologies regarding fitness vs. iteration in figure 5.

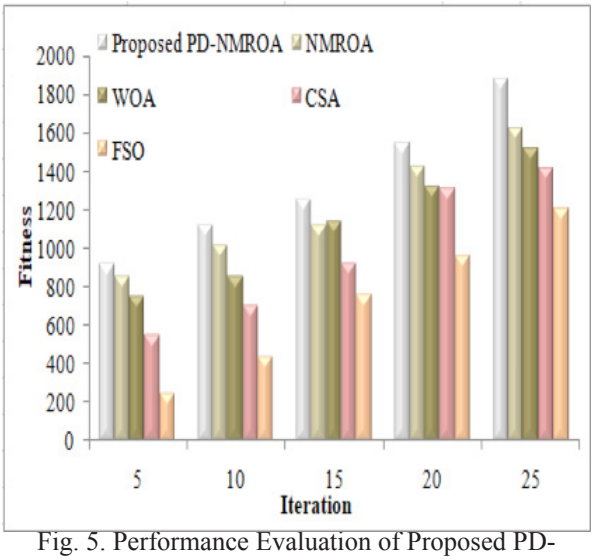

Fig. 5. Performance Evaluation of Proposed PD-NMROA

Figure 5 demonstrates that a higher fitness value was obtained by the proposed model in contrast to existing methodologies. For 5 iterations, a fitness value of 920 is acquired by the proposed PD-NMROA; conversely, for the same number of iterations, the conventional WOA obtained 850 fitness values. Similarly, the fitness values differ for the other conventional models also. Therefore, the proposed model outshines the existing methodologies.

Performance evaluation of proposed MaH-Kmeans

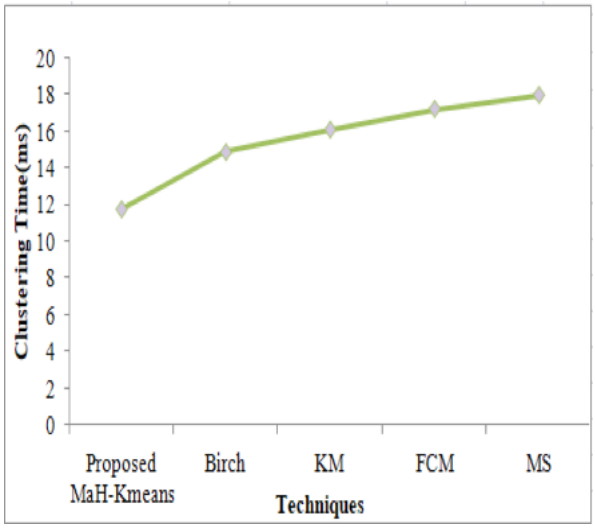

Fig. 6. Performance Evaluation of Proposed MaH-Kmeans

Figure 6 exhibits the superiority measure of the proposed model with regard to clustering time. Here, the proposed MaH-Kmeans attained a clustering time of 11.7892ms, which is lower than the clustering time of 14.8914ms obtained by the prevailing Kmeans model. In the same manner, the clustering time varies for the other methodologies also. Therefore, it is

evident that when analogized with the prevailing methodologies, the proposed model achieved better performance.

Superiority Measure of proposed TS-RBDMS

Here, concerning the accuracy metric, the proposed TS-RBDMS's performance is compared with other prevailing algorithms like RaNN [12], and HDRaNN [11].

Table 3: Comparative analysis of proposed TS-RBDMS based on the accuracy (%)

Techniques	Accuracy (%)
Proposed TS-RBDMS	99.70
HDRaNN [11]	98
RaNN [12]	99.20

Table 3 compares the accuracy of the proposed TS-RBDMS with existing works like HDRaNN and RaNN. The model having higher accuracy will be the best model. In accordance with this, the accuracy achieved by the proposed model was 99.70% whereas the accuracy values attained by the prevailing models are HDRaNN (98%), and RaNN (99.20%). Therefore, in contrast to the traditional models, the proposed one achieved better performance.

Regarding precision, recall, and f-measure, the performance analysis of the proposed and the prevailing models are represented in table 4. The proposed model attains a precision of 99.74%, recall of 99.66%, and f-measure of 99.67%, which are higher when analogized with the prevailing techniques like HDRaNN and RaNN. The outcomes exhibited that the proposed mechanism displays better performance than the conventional frameworks in attack detection.

Table 4: Comparative analysis of the proposed model in terms of precision, recall, and f-measure

Techniques/ Metrics	Precision	Recall	F-Measure
Proposed TS-RBDMs	99.74	99.66	99.67
HDRaNN [11]	98.25	98.36	98.3
RaNN [12]	99.08	99.16	99.04

Figure 7 displays the computational complexity of the proposed TS-RBDMs. The best training and testing accuracies of the proposed model are achieved at 99.85% and 99.70%, correspondingly. Similarly, the best training and testing accuracies of DNNBoT are achieved at 90.71% and 90.54%, respectively [24]. Likewise, the best training and testing accuracies of PCCNN are 99.34% and 98.64%, respectively [25]. On comparing these values, the proposed model shows better performance in the detection of attacks in IIoT.

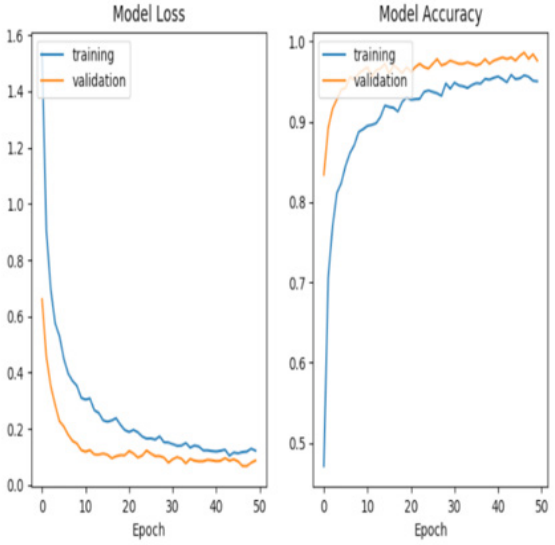

Fig. 7. Computational Complexity of Proposed TS-RBDMs

Conclusion

To detect attacks in IIoT, a novel TS-RBDMS model has been proposed in this work. (i) feature selection, (ii) clustering, and (iii) classification are the operations undergone by the system. After that, the experimental evaluation is performed; here, to validate the proposed model's efficacy, the performance along with a comparative analysis of the proposed is done in comparison with the prevailing methodologies regarding certain performance metrics. Several uncertainties along with attacks are recognized accurately by the proposed model. For the evaluation, UNSW-NB15 and DS2OS datasets are utilized. In this, the proposed TS-RBDMS attained an accuracy of 99.68% for UNSW-NB15 and 99.70% accuracy for DS2OS datasets, in that order. Therefore, to detect cyber-attacks in IIoT, major support was provided by the proposed framework. But the model shows low energy efficiency in real-time data sensing time. So, the work may concentrate on the data security process for non-attacked data, and energy efficiency will be concentrated on real-time data sensing time in the future.

Conflict of Interest

None

References

1. Xinghua Li, Mengfan Xu, Pandi Vijayakumar, Neeraj Kumar and Ximeng Liu, "Detection of low-frequency and multi-stage attacks in industrial internet", IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 8820-8831, 2020.
2. Maede Zolanvari, Marcio A Teixeira, Lav Gupta, Khaled M Khan and Raj Jain, "Machine learning based network vulnerability analysis of industrial internet of things", EEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, 2018.
3. Gamal Eldin I Selim, EZZ El-Din Hemdan, Ahmed M Shehata, Nawal A El-Fishawy, "Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms", Multimedia Tools and Applications, vol. 80, no. 8, pp. 12619-12640, 2021.
4. Muna Al-Hawawreh, Elena Sitnikova and Neda Aboutorab, "X-IIoTID a connectivity- and device-agnostic intrusion dataset for industrial internet of things", IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3962-3977, 2021.
5. Sharmistha Nayak, Nurzaman Ahmed and Sudip Misra, "Deep learning-based reliable routing attack detection mechanism for industrial internet of things", Ad Hoc Networks, vol. 123, pp. 1-11, 2021.
6. Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha and Reza M Parizi, "An ensemble deep learning-based cyber-attack detection in industrial control system", IEEE Access, vol. 8, pp. 83965-83973, 2017.
7. Bela Genge, Piroska Haller and Calin

Enachescu, "Anomaly detection in aging industrial internet of things", IEEE Access, vol. 4, pp. 1-14, 2016.

8. Truong Thu Huong, Ta Phuong Bacb, Dao Minh Longa, Tran Duc Luonga, Nguyen Minh Dana, Le Anh Quanga, Le Thanh Conga, Bui Doan Thanga and Kim Phuc Tran, "Detecting cyberattacks using anomaly detection in industrial control systems: A Federated Learning approach", Computers in Industry, vol. 132, no. 7, pp. 1-16, 2021.
9. Mohamed Abdel-Basset, Victor Chang, Hossam Hawash, Ripon K Chakrabortty and Michael Ryanmn, "Deep-IFS intrusion detection approach for IIoT traffic in fog environment", IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7704-7715, 2020.
10. Yash Shah and Shamik Sengupta, "A survey on classification of cyber-attacks on IoT and IIoT devices", 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, 28-31 October 2020, New York, NY, USA, 2020.
11. Zil E Huma, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani and Fatmah Baothman, "A hybrid deep random neural network for cyberattack detection in the industrial internet of things", IEEE Access, vol. 9, pp. 55595-55605, 2021.
12. Shahid Latif, Zhuo Zou, Zeba Idrees and Jawad Ahmad, "A novel attack detection scheme for the industrial internet of things using a lightweight random neural network", IEEE Access, vol. 8, pp. 89337- 89351, 2020.
13. Shahid Latif, Zeba Idrees, Zhuo Zou and Jawad Ahmad, "DRaNN a deep random neural network model for intrusion detection in industrial IoT", International Conference on UK-China Emerging Technologies, IEEE, 20-21 August 2020, Glasgow, UK, 2020.
14. Muna AL-Hawawreh, Nour Moustafa and Elena Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models", Journal of Information Security and Applications, vol. 41, pp. 1-11, 2018.
15. Radhakrishna Vangipuram, Rajesh Kumar Gunupudi, Veereswara Kumar Puligadda and Janaki Vinjamuri, "A machine learning approach for imputation and anomaly detection in IoT environment", Expert Systems, vol. 37, no. 5, pp. 1-16, 2020.
16. Di Wu, Zhongkai Jiang, Xiaofeng Xie, Xuetao Wei, Weiren Yu and Renfa Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT", IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5244-5253, 2019.
17. Tran Viet Khoa, Yuris Mulya Saputra, Dinh Thai Hoang, Nguyen Linh Trung, Diep N Nguyen, Nguyen Viet Ha and Eryk Dutkiewicz "Collaborative learning model for cyberattack detection systems in IoT industry 4.0", Wire-

less Communications and Networking Conference, 25-28 May 2020, Seoul, Korea, 2020.

18. Faezeh Farivar, Mohammad Sayad Haghighi, Alireza Jolfaei and Mamoun Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber physical systems and industrial IoT", IEEE Transactions on Industrial Informatics, vol. 16, no. 4, pp. 2716-2725, 2019.
19. Yanmiao Li, Yingying Xu, Zhi Liu, Haixia Hou, Yushuo Zheng and Yang Xin, Yuefeng Zhao and Lizhen Cui, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion", Measurement, vol. 154, no. 2, pp. 1-27, 2019.
20. Muna AL-Hawawreh and Elena Sitnikova, "Industrial internet of things based Ransomware detection using stacked variational neural network", 3rd International Conference on Big Data and Internet of Things, 22-24 August 2019, Melbourn, Australia, 2019.
21. Joseph Bamidele Awotunde, Chinmay Chakraborty and Abidemi Emmanuel Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection" Wirel. Commun. Mob. Comput., vol. 2021, 2021, doi: 10.1155/2021/7154587.
22. Nour Moustafa and Jill Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)" 2015 Mil. Commun. Inf. Syst. Conf. MilCIS 2015 - Proc., 2015, doi: 10.1109/MilCIS.2015.7348942.
23. Zil E. Huma, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani and Fatmah Baothman "A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things" IEEE Access, vol. 9, pp. 55595–55605, 2021, doi: 10.1109/ACCESS.2021.3071766.
24. Mohd Anul Haq, Mohd Abdul Rahim Khan, "Dnnbot: Deep neural network-based botnet detection and classification" Comput. Mater. Contin., vol. 71, no. 1, pp. 1729–1750, 2022, doi: 10.32604/cmc.2022.020938.
25. Mohd Anul Haq, Mohd Abdul Rahim Khan and Talal AL-Harbi, "Development of pccnn-based network intrusion detection system for edge computing" Comput. Mater. Contin., vol. 71, no. 1, pp. 1769–1788, 2022, doi: 10.32604/cmc.2022.018708.

Journal of Engineering and Applied Sciences (JEAS)

- **Effects of Vibration Intervention on Grip Strength and Endurance Time of Young College Students.**

  Abdulelah M. Ali.

- **Parents' Awareness of Cybersecurity.**

  Abdulrahman Abdullah Alghamdi.

- **A Novel Classifier for Cyber Attack Detection System in Industrial Internet of Things.**

  Fathe Jeribi.

شركة مطابع جامعة المجمعة
Majmaah University Press Co.
0540010909