International Journal of Computer Applications Technology and Research
Volume 9–Issue 11, 287-294, 2020, ISSN:-2319–8656

Image Modification using Text with GANs

Fenil Doshi
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Parth Doshi
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Jimit Gandhi
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Khushmann Dwivedi
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Dr. Ramchandra Mangrulkar
Dwarkadas J. Sanghvi College of Engineering
Mumbai, India

Abstract: This paper works towards finding an effective solution for the task of image feature manipulation using natural language commands. The authors aim to modify the relevant features of an image using a natural language description of the target image, such that the irrelevant features are not modified. Majority of the research in this domain focuses on generating completely new images using natural language description, and the few methodologies which attempt manipulation of existing images super in a number of aspects such as modification of irrelevant features or the aesthetic quality of the generated image. The authors propose an architecture that combines the best components of existing techniques to create an effective system to solve the stated task. The proposed architecture generates images at a high resolution to maintain the aesthetic quality of the image and ensures that the irrelevant content of the original image is not affected. The authors present a qualitative and quantitative analysis of the system as compared to the existing baselines and demonstrate the system for a relevant application such as virtual trial of clothes.

Keywords: Language-Based Image Editing (LBIE), Generative Adversarial Networks, Text Adaptive Discriminator, Feature Wise Linear Transformation, Bilinear Residual Layer

1. INTRODUCTION

Images have become an inseparable part of everyone's lives. With the widespread usage of images, the need for instant manipulation of images based on user requirements has grown at the same time. There are several existing solutions, but these tools are highly advanced and not easy to use for an amateur. For example, if a person wishes to see how they would look in a particular set of clothes, they should not have to use highly complicated and advanced tools. In such a scenario, being able to use textual descriptions or natural language commands would be the easiest way out.

The authors of this paper propose a model to solve this problem by combining features from several different architectures and applying it on a very common application such as the virtual trial of clothes. The focus of this paper is to manipulate various characteristics of an existing image using textual descriptions through the use of generative models.

The rest of the paper is organized as follows: Section 2 gives a brief summary of all the work undertaken relevant to the problem statement, Section 3 proposes a novel approach to tackle the problem and Section 4 explains the implementation of the proposed model. This is followed by Section 5 that discusses the results obtained. Finally, Section 6 gives a possible Future Scope and Section 7 provides a conclusion for the paper.

2. LITERATURE REVIEW

Majority of the existing research closely related to the task focuses on the creation of new images based on a textual description. The recent push in research in this domain can be attributed to the success of generative architectures such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAE).

Goodfellow et al. [4] were the first ones to introduce the idea of Generative Adversarial Networks (GANs). Previous work in the field of creating images by estimating the probabilistic distribution of data included using Variational Autoencoders (VAE). They trained two processes simultaneously with opposing loss functions (adversarial loss)- (i) A Generator G that captures the distribution of data and (ii) A Discriminator D that tries to distinguish between generated and data samples. Another variant of GANs - Conditional GANs was proposed by Mirza et al. [11]. They introduced a new model - a conditional version of GANs - where the Generator is conditioned on some external feature to generate the sample.

GANs and Conditional GANs have been used in several architectures for the generation of images from random noise vectors (latent space). These architectures have focused on generating entirely new images from random noise vectors conditioned on some variable. For example, Riviere et al. [14] focus on the creation of entirely original images which are inspired by an image which is fed as the conditioning variable, while Wang et al. [16] propose an architecture for the generation of photo-realistic high resolution images from semantic label maps using Conditional GANs. While these architectures provide an interesting insight into how conditional GANs can be effectively used for generation of new images based on some condition, these do not focus on manipulation of existing images based on user interaction.

Zhu et al. [22] present an interesting solution, in which users can manipulate images using sketching tools normally available in painting applications. However, it uses manipulation of latent space vectors, and the results are not always predictable or generated as per the user's intention. The approach suggested by Lample et al. [8] reconstructed images by extracting the information of the values of attributes of the image directly in the latent space. Instead of using natural language, they used sliding knobs to modify specific attributes of the image.

He et al. [6] present another architecture involving manipulation of the original images using latent space vectors. It proposes an architecture where an attribute classification constraint is applied directly on the generated image to check whether the desired features have been modified or not, while style controllers are used to control the amount of attribute editing. It is an improvement over the Fader Networks proposed in [8], but does not take into account any textual description of the image, which leads us to look at architectures related to text-to-image synthesis.

One of the seminal papers in this domain, Reed et al. [13] propose an architecture for generation of low-resolution images from a descriptive image caption. The need for high resolution images is satisfied by stacking multiple GANs, as proposed in [19][20]. Spatial attention is introduced in this task by Xu et al. in the approach proposed in [18], which uses an attention module to automatically select word level conditions for generating different parts of the image. It also uses multiple generators to generate images at different resolutions and scales. However, these architectures cannot be used directly for manipulation of existing images, as these are focused on text-to-image synthesis.

The problem statement mainly focuses on this architecture where the conditioning parameter is a natural language description on which the image needs to be modified. Over the years, there have been many proposed models that particularly focus on this type of problem. This conditioning parameter can either control the latent space (Latent Space GANs) or the generator network in GANs (Conditional GANs). This paper looks into the latter architecture in more detail.

Shinagawa et al. [15] manipulated the latent space vector of the original image using the embedded vector of the natural language command. They constructed a neural network that handled image vectors in latent space to transform the source vector to the target vector by using the vector of instruction.

Dong et al. [2] experimented with a standard conditional GAN architecture where the image was encoded with encoder network, then fused together with representations of text from a text encoder network by concatenating both representations, followed by a decoder network that generated the required image. A simple sentence-level discriminator would provide feedback to the generator about the correctness of the generated image.

Nam et al. [12] used a novel approach of TAGAN (Text adaptive generative adversarial networks) and modified the discriminator architecture in order to make it more adaptive to the editing text. Previously, the works focused on single sentence-level discriminators. In TAGAN, these sentence-level discriminator is split into multiple local word-level discriminator which are then aggregated with text attention. This ensures fine-grained training feedback to the generator which then only modifies text-relevant content of the image. The experimental results of this architecture gave state of the art performance and outperformed existing methods.

Concatenation of features, as done in [2], was not the most efficient way to fuse together the image and text representations. Hence, Gunel et al. [5] used a FiLMedGAN architecture where the generator used Feature-wise linear transformations in order to combine the image and text representations. This significantly reduced the parameter space without any loss in the accuracy. Moreover, Mao et al. [10] introduced a new fusing module - BRL layers (Bilinear Residual Layers) to provide richer representations than linear models by learning second order interaction. The experimental results show that these models outperform the aforementioned models when the editing required is much more complex.

Language-based Image editing (LBIE) has been used in a various number of applications where the architectures are tweaked catering to the specific application in context.

Zhou et al. [21] used Conditional GAN architecture to modify a person's pose and other visual attributes using a natural language description. The architecture consists of two systems, namely a pose inference system to infer the pose that text refers and an image generation network that transfers the pose and attributes from text to the input image to output the required image.

G□nel et al. [5] used the FiLMedGAN architecture in order to edit the out of the person in the input image based on textual descriptions. This has various applications in the fashion industry.

El-Nouby et al. [3] extends the work done on Conditional GANs by presenting a recurrent image generation model which takes the generated image up to the current step and the natural language based instruction into account for the generation of a new image. This presents an architecture for iterative editing, which is based on conversational dialogue between the user and the system.

3. PROPOSED MODEL

The authors of this paper propose a new architecture of GANs where the fusing layer in Generator is BRL layer as discussed in [10] and the Discriminator is Text Adaptive Discriminator as proposed in [2]. Both of these techniques are tried independently but have never been examined simultaneously.

For the task, the authors propose the following model - Let input be <x, t, t'>where <x>represents the input image to be modified, <t>represents the positive text that correctly describes the image and <t'>represents negative text according to which <x>has to be manipulated to produce image <x'>where <t'>is a positive text for image <x'>. The generator objective is to produce image <x'>whereas the discriminator objective is to discriminate between <x> and <x'> (Output 1 for <x>i.e. Real image from dataset and 0 for <x'> i.e. generate fake image not from dataset.

Here,

$$< x'>= G (< x >, < t'>) = dec (brl (enc (< x >), w (< t' >))) \quad (1)$$

where G = Generator function, dec = Decoder Network, brl = Bilinear Residual Layer for fusing image and text representation, enc = Encoder network for Image <x>, w = representation of text <t'>

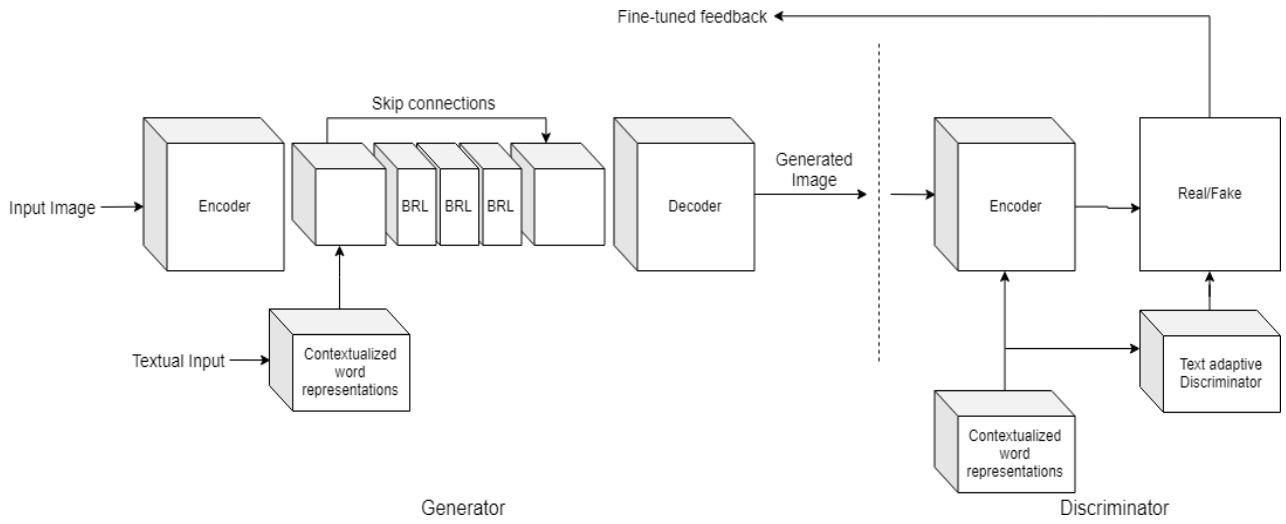

Fig. 1. Proposed Architecture

The generator loss function is given by –

$$LG = [\log(D(x)) + \lambda_1 * \log(D(G(x, t'), t'))] + \lambda_2 * L_{rec} \quad (2)$$

where Lrec = Recreational loss to preserve the text-irrelevant contents of the original image, λ_1 = weight to control the importance assigned to the discriminator's ability to correctly identify a true image and description pair, λ_2 = weight of recreational loss and D = Discriminator network as defined below.

At the discriminator end, the discriminator takes in the text and the image and provides feedback to the generator. This is done by considering output from many word-level local discriminators for each visual attribute. The text-adaptive discriminator takes in input as <x, t, t'>and tries to produce 1(real) for D (<x, t>) and D (<x>). Similarly, it tries to output 0 (fake) for D (<x, t'>) and D (G (<x, t'>)). That is, the discriminator tries to classify the generated image as well as original image on negative text as fake samples whereas original image on positive text as positive sample.

Thus, the discriminator objective is to minimize the following loss function –

$$LD = \log(D(x)) + \lambda_1 * (\log(D(x, t) + \log(1 - D(x, t')))) + \log(1 - D(G(x, t'))) \quad (3)$$

Hence, the proposed GAN structure adversarially tries to minimize both these losses to produce the output image <x'>which is conditioned on the given text <t'>.

4. IMPLEMENTATION

Algorithms and Methods Used

Fasttext Embeddings[1][7]: The user provided text is represented in a mathematical format using Word Embeddings. The authors used pretrained Fasttext embeddings for this part. Each word is represented as a vector in a 300- dimensional space. These embeddings use character level information while training and hence, can handle rare words more efficiently.
One of the major drawbacks of these embeddings is the high memory requirement as it breaks down the text into n-grams to incorporate words that are not seen while training.

Bilinear Residual Layer (BRL)[10]: The conditioning of two features in a generative network is generally accomplished by concatenation of both the feature vectors or using FiLM (Feature-wise Linear Modulation). This could have been easily done with concatenating the image encodings and word embeddings.

However, the interaction that follows between the two vectors in not deep and complex interactions cannot emerge with

simple concatenation. This is due to the fact that the concatenation or FiLM is a simple linear transformation of the features over the conditioning features.

The authors apply a more complex bilinear transformation using BRL which learns second order interaction and provides richer representation.

Using BRL, the output feature will be given as –

$$I_o = I_f * W * I_c \quad (4)$$

where I_o = Output feature, I_f = the feature that is being conditioned (here, image representation), I_c = the conditioning feature (here, text representation) and W = learnable weight matrix.

The authors chose the weight matrix to be of low rank (Hence, low rank bilinear residual) and decompose it into two matrices of that lower rank in order to relax the computations.

Generative Adversarial Networks (GANs) [4]: Generative Adversarial Networks comprises two networks - Generator and Discriminator. Both are trained on opposite tasks with opposing

loss functions (Hence, Adversarial). Generators try to approximate (mimic) the probability distribution of input space (from the dataset) and Discriminator tries to distinguish between the two distributions (approximated and real distribution).

The authors use a variant of GANs known as conditional GANs where the generation of data samples is conditioned on some external feature. The data samples are images and the conditioning feature is a natural description of the required image.

The generator and discriminator architectures need to be modified accordingly as discussed above while formulating the loss functions.

Generators - The Generator network consists of Encoder network, Fusing Network and Decoder Network. The Encoder network is a series of Convolutions, Pooling and Batch Normalization layers. The Fusing Network uses Residual layers and BRL layers (as discussed above). The Decoder Network takes in the fused vector and upsamples it using Transposed Convolutions and unpooling layers along with Batch Normalization.

Discriminators - The Discriminator is made up of several local discriminators which are created using Recurrent neural networks with Gated Recurrent Unit (GRU) cells and then attention is applied over them. More details will be followed in the next section.

Both the Generators and Discriminator network are trained using ReLU activation functions with dropout regularization to avoid overfitting. The loss functions of the networks are mentioned above.

Text Adaptive Discriminators [6]: In order to consider the effect of each word on the text, the idea is to have word-level discriminators. The generator will then receive a combined feedback from each `N' discriminator where `N' is the number of words in text.

The final classification decision to distinguish between whether the image is fake (from generator) or real (from dataset) comes via taking attention on the output vector of each of the local discriminators. This would ensure to give relatively less importance to insignificant words such as `the', `under', etc. and more importance to the words that de ne the change such as `red blouse', `green shirt', `blue jacket', etc. After considering the weighted sum using attention, the final output is then calculated.

4.2 Experimentation and Training

Datasets and Creating Training Samples: The training was performed on two datasets –

Caltech-UCSD Birds 200 [17]: It consists of 11,788 images of birds in their natural habitat along with their captions. Each of the images is associated with 10 different captions that de ne the image. The authors select any of these captions randomly.
The total images are divided into 200 classes. The authors aim to modify the body and color of the birds based on the textual description.

DeepFashion: Fashion Image Synthesis Dataset [9] [23]: There are a total 78,979 images of fashion outfits along with The training set pairs were created by –

1. The image and its caption formed the pair <x, t>which was fed to the Discriminator in order to output 1 (Real).

2. The image and a random caption from some other image was chosen to form the pair <x, t'>. The true label for Discriminator for such a pair would be
0 (Fake). The Generator was fed the pair <x, t'>to create a new fake image <x'> (Generated Fake Sample conditioned on text <t'>). Additionally, <x'>was compared with <x>for computing Reconstruction loss in order to preserve the background.

3. The new pair of <x', t'>was also fed to Discriminator and Discriminator was trained to output 0 (Fake) for such an input pair. Simultaneously, Generator was trained to get an output 1 (Real) from the Discriminator.

Training Setup: After generating the training samples, Generator and Discriminator were trained consequently one after the other. While updating the weights of the Generator, the corresponding gradients of Discriminator were not updated. Similarly, the Generator was not used while training the Discriminator.

The samples were fed in the batch size of 32 to the model. The model was trained on CUB dataset for 600 epochs while the DeepFashion dataset was trained for 220 epochs because of the difference in size of datasets. It was observed that there was no considerable decrease in loss and not much improvement of the model in its performance.

The model was trained on a single core GPU (RTX 2080 Ti) with 18.3 TFLOPS with 64 GB storage RAM. The machine was rented on Vast.ai and was trained for 2.5 days for training the Birds model and for 4-5 days for training the Fashion Synthesis model.

5. RESULTS AND DISCUSSION

5.1 Analysis on CUB Dataset

To analyse the results of the model, the authors first trained the model on the CUB-200 dataset [17]. To test, images and input texts were randomly selected and first they were run on the TAGAN model proposed by Nam et al. [12]. Then, the same pairs of images and text were tested on the model and the results were collated together. Some results are visible in Fig. 2. The authors' model is referred to as Model 1 and the TAGAN Model [12] is referred to as Model 2.

Because of the absence of some uniform universal metric to analyze the efficacy of the results, the authors chose to perform comparative analysis.

In the comparative analysis, the authors showed the original image, the input text and the output image of both the TAGAN model as well as the authors' model. After observing these three

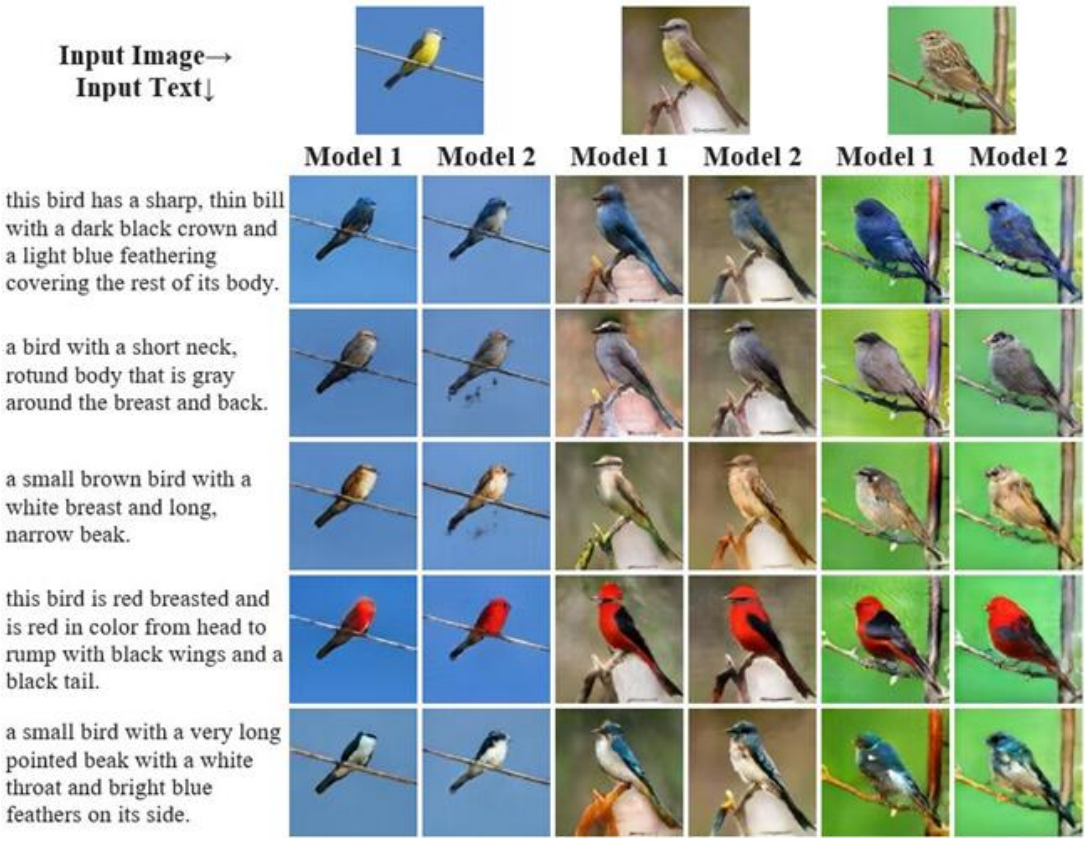

Fig. 2. Results obtained on the CUB-200 Dataset

images, the volunteers were asked to choose which model performed better in the following characteristics:

1. Which model was successfully able to edit the image according to the textual description?
2. Which model preserved the background of the image?
3. In which model is the bird distinguishable naturally?

The choices of the volunteers for each of these questions were recorded and then analyzed. Fig. 3 shows the pie chart for responses of the questions asked.

As can be seen from the pie chart, 56.5% volunteers found Model 1 to successfully edit the image according to the textual description, as opposed to 32.4% for Model 2. Further, according to 56.5% of the volunteers, the bird was naturally distinguishable in the output of Model 1, remarkably more than the 32.4% of Model 2. However, the background of the image was preserved in a more effective way by Model 2, as 46.3% chose Model 2 and only 44.4% chose Model 1. The number of responses for each question can be seen from Fig 4.

Hence, from this extensive comparative analysis, the authors conclude that their model (Model 1) outperforms Nam et. al's model [12] (Model 2) in two of the three metrics analysed by the authors. That is, their model successfully performs the task of editing the image according to the text better and the output image of the bird is more distinguishable in their model. However, Nam et. al's model still preserves the background of the image in a better way than the model proposed by the authors.

This suggests that the BRL layer does increase the interaction between the text and image which consequently leads to better and focussed editing of the image. However, it might be the case that the reconstruction error is overwhelmed by this and the model focuses much more on editing the image and less on preserving the background.

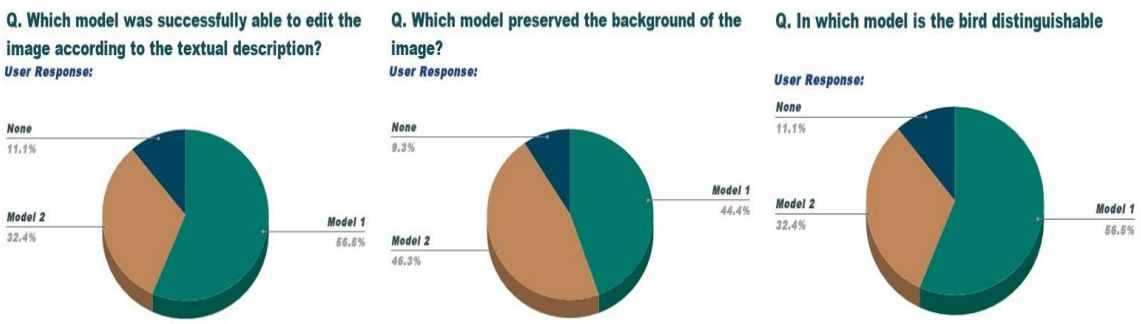

Fig. 3. Pie chart for responses to the questions

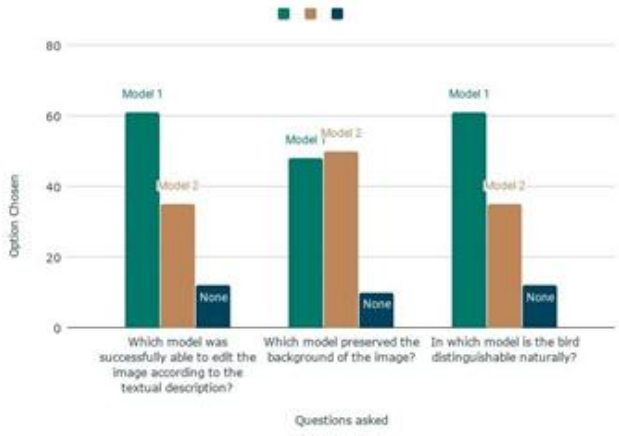

Fig. 4. Bar Graph displaying choices chosen by volunteers

5.2 Analysis on DeepFashion Dataset

After performing analysis on the CUB-200 dataset, the authors trained their model on the DeepFashion dataset [9] [23]. The model was then tested by randomly selecting images and input statements and collating the results together. Fig. 5 shows some of the results obtained.

Due to the absence of a quantitative metric to judge the accuracy of the model on the DeepFashion dataset, the author's decided to perform qualitative analysis. In this, the chosen volunteers were given the input image, input text and the output and were asked to rate the image manipulation for the following metrics:

1. Was the model successfully able to edit the input image based on the given textual description?
2. Did the model preserve the background of the image (features such as face, hair, etc.)?
3. How good is the naturalness of the image and does the image look similar to a person?

The volunteers were asked to rate the image manipulation on a scale of 1-5 where 1 signifies the most erroneous conversion whereas 5 signifies the most accurate conversion. The results were collected and can be understood by Fig 6.

Hence, the volunteers gave an average score of 3.79/5 to the model's accuracy in successfully editing the input image based on the given textual description. They gave an average score of 3.61/5 to the model for preserving the background of the image and an average score of 3.03 to the model for maintaining the naturalness of the image.

Fig. 5. Results obtained on the DeepFashion Dataset

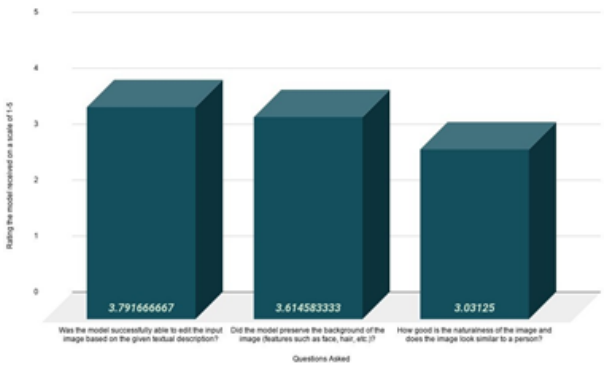

Fig. 6. Average results for the questions asked on the DeepFashion Dataset

Hence, while the model performs considerably well in performing the task of image manipulation based on the input text, it sometimes does not preserve the features of the women in the images. The hair, the accessories like watches, hats, sunglasses, etc. sometimes get altered or disappear completely. Another area where the model lacks slightly is preserving the naturalness of the image. Sometimes the face in the output image fails to be naturally identified as a human face. However, given the complexity of the human body and human faces, the model performs considerably well in retaining the overall posture of the body and effectively performs manipulation on the dresses.

6. FUTURE SCOPE

There are many directions that can be taken for furthering this work. One direction is the trial implementation of a prototype in a real shop, thus testing the system against real-world noisy data. Another direction is to improve the size and quality of images generated through the use of deeper neural networks, requiring massive computational resources.

7. CONCLUSION

Thus the architecture combines the best features of existing architectures and can be used in the fashion domain for virtual trial of clothes. The architecture overcomes the drawbacks of the existing approaches of image manipulation and makes it easier for an amateur to use textual descriptions to convert an existing image into the desired version.

The results show that the model generates better results than the baseline models that the authors have based it on. The model

combines the best features of different models and allows high-quality results to be generated with accurate modifications as per the user requirements.

8. References

1. Bojanowski, P., Grave, E., Joulin, A., Mikolov, T.: Enriching word vectors with subword information. Transactions of the Association for Computational Linguistics 5, 135-146 (2017).

   https://doi.org/10.1162/tacl a 00051, https://www.aclweb.org/anthology/Q17-1010

2. Dong, H., Yu, S., Wu, C., Guo, Y.: Semantic image synthesis via adversarial learning. In: Proceedings of the IEEE International Conference on Computer Vision. pp. 5706-5714 (2017)

3. El-Nouby, A., Sharma, S., Schulz, H., Hjelm, D., Asri, L.E., Kahou, S.E., Bengio, Y., Taylor, G.W.: Tell, draw, and repeat: Generating and modifying images based on continual linguistic instruction. In: Proceedings of the IEEE International Conference on Computer Vision. pp. 10304-10312 (2019)

4. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative adversarial nets. In: Advances in neural information processing systems. pp. 2672-2680 (2014)

5. G□unel, M., Erdem, E., Erdem, A.: Language guided fashion image manipulation with feature-wise transformations. arXiv preprint arXiv:1808.04000 (2018)

6. He, Z., Zuo, W., Kan, M., Shan, S., Chen, X.: Attgan: Facial attribute editing by only changing what you want. IEEE Transactions on Image Processing 28(11), 5464-5478 (2019)

7. Joulin, A., Grave, E., Bojanowski, P., Mikolov, T.: Bag of tricks for e cient text classication. In: Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers. pp. 427-431. Association for Computational Linguistics, Valencia, Spain (Apr 2017),

   https://www.aclweb.org/anthology/E17-2068

8. Lample, G., Zeghidour, N., Usunier, N., Bordes, A., Denoyer, L., Ranzato, M.: Fader networks: Manipulating images by sliding attributes. In: Advances in neural information processing systems. pp. 5967-5976 (2017)

9. Liu, Z., Luo, P., Qiu, S., Wang, X., Tang, X.: Deepfashion: Powering robust clothes recognition and retrieval with rich annotations. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (June 2016)

10. Mao, X., Chen, Y., Li, Y., Xiong, T., He, Y., Xue, H.: Bilinear representation for language-based image editing using conditional generative adversarial networks.

    In: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). pp. 2047-2051. IEEE (2019)

11. Mirza, M., Osindero, S.: Conditional generative adversarial nets. arXiv preprint arXiv:1411.1784 (2014)

12. Nam, S., Kim, Y., Kim, S.J.: Text-adaptive generative adversarial networks: Manipulating images with natural language. In: Advances in neural information processing systems. pp. 42-51 (2018)

13. Reed, S., Akata, Z., Yan, X., Logeswaran, L., Schiele, B., Lee, H.: Generative adversarial text to image synthesis. arXiv preprint arXiv:1605.05396 (2016)

14. Riviere, M., Teytaud, O., Rapin, J., LeCun, Y., Couprie, C.: Inspirational adversarial image generation. arXiv preprint arXiv:1906.11661 (2019)

15. Shinagawa, S., Yoshino, K., Sakti, S., Suzuki, Y., Nakamura, S.: Interactive image manipulation with natural language instruction commands. arXiv preprint arXiv:1802.08645 (2018)

16. Wang, T.C., Liu, M.Y., Zhu, J.Y., Tao, A., Kautz, J., Catanzaro, B.: Highresolution image synthesis and semantic manipulation with conditional gans. In:Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 8798-8807 (2018)

17. Welinder, P., Branson, S., Mita, T., Wah, C., Schro, F., Belongie, S., Perona, P.: Caltech-ucsd birds 200 (2010)

18. Xu, T., Zhang, P., Huang, Q., Zhang, H., Gan, Z., Huang, X., He, X.: Attngan: Fine-grained text to image generation with attentional generative adversarial networks.

    In: Proceedings of the IEEE conference on computer vision and pattern recognition. pp. 1316-1324 (2018)

19. Zhang, H., Xu, T., Li, H., Zhang, S., Wang, X., Huang, X., Metaxas, D.N.: Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks.

    In: Proceedings of the IEEE international conference on computer vision. pp. 5907-5915 (2017)

20. Zhang, H., Xu, T., Li, H., Zhang, S., Wang, X., Huang, X., Metaxas, D.N.: Stackgan++: Realistic image synthesis with stacked generative adversarial networks. IEEE transactions on pattern analysis and machine intelligence 41(8), 1947-1962 (2018)

21. Zhou, X., Huang, S., Li, B., Li, Y., Li, J., Zhang, Z.: Text guided person image synthesis. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 3663-3672 (2019)

22. Zhu, J.Y., Krahenbuhl, P., Shechtman, E., Efros, A.A.: Generative visual manipulation on the natural image manifold. In: European conference on computer vision.

    pp. 597-613. Springer (2016)

23. Zhu, S., Fidler, S., Urtasun, R., Lin, D., Loy, C.C.: Be your own prada: Fashion synthesis with structural coherence. In: International Conference on Compute

    Vision (ICCV) (October 2017)

International Journal of Computer Applications Technology and Research
Volume 9–Issue 11, 295-298, 2020, ISSN:-2319–8656

Measuring E-Readiness of Students of Public Universities in Kenya for Digital Learning during the COVID 19 Pandemic and Beyond - A Survey of the Cooperative University of Kenya

Duncan Nyale
School of Computing and Mathematics
The Cooperative University of Kenya
Nairobi, Kenya

Abstract: The main purpose of this paper is to assess the e-capacity of the students of The Cooperative University of Kenya to access and use digital platforms of learning at present and beyond. The need for this urgent study is occasioned by the impact of COVID 19 which has stopped on campus learning at all institutions in Kenya; thus necessitating an urgent shift towards digital learning for all students to mitigate against delays that will otherwise have adversely affected their graduation schedules. Three main variables derived from the Harvard Center for International Development (CID) and Asia-Pacific Economic Cooperation (APEC) models - Human skills, Infrastructure and Connectivity - were used to craft the evaluation criteria. The results show that (74.87%) of the respondents can access LMS via smart phones not computers which insinuates that Mobile Learning (m-Learning) is the most effective digital learning model that can be adopted by the University in the short term to quickly mitigate against the effects of the lack of face to face learning occasioned by social distancing guidelines due to COVID 19.

Keywords: ICT: - Information and Communications Technology, LMS: - Learning Management System, CUK: - Cooperative University of Kenya, COVID 19: - Corona Virus Disease 2019

1. INTRODUCTION

The disruption of the world order by the COVID 19 pandemic has not spared institutions of higher learning. An abrupt interruption of face to face learning has created a very urgent need to incorporate all on campus students to e-learning platforms. This was unprecedented and therefore no plans were in place to do this. It is therefore important to gauge the capacity of the main stakeholders of the institutions (students) to adopt this mode of training effective immediately. This paper aimed to do just that by running a quick survey to ascertain the e-readiness of the Cooperative University of Kenya students currently in session during the pandemic to quickly adopt and shift to the e-learning mode of education as soon as possible to minimize the disruption to their learning during the pandemic period and beyond.

The university already has a running LMS which mainly services students in the Institute of Open, Distance and e-Learning (I-oDEL). The system is also used to run select common courses for on Campus students. However, it must be noted that a full scale migration to full e-learning mode has never been envisaged before making this abrupt need even more challenging.

E-Readiness can be defined as the degree to which a community is prepared to participate in the digital age (Networked World). A high level of e-readiness also contributes positively towards the realizations of an institutional goal (Kashorda & Waema, 2014). E-Readiness assessment is meant to guide evolution efforts by providing benchmarks for comparison and gauging progress (Zaied, Khairalla & Al-Rashed, 2007).

The results of this survey should go a long way towards informing the university of not only the current e-readiness of its students but also help in the decision, planning and rolling out of a full scope e-learning mode of training in the short, mid and long term.

This is more so due to the rapid rate of internet penetration throughout the world and Kenya in particular, coupled with dramatic advances in uses of information technology in business, industry, government and even education which makes it inevitable that there is likely to be a paradigm shift in the way university teaching, learning and assessment is done and very soon too considering the acceleration that has and still is being occasion by the COVID 19 pandemic.

2. OBJECTIVES

The goals of the study were:

a) To assess the e-preparedness of CUK students for digital learning
b) To analyze and gauge digital infrastructure and connectivity capacity of CUK students
c) To identify the key issues that need to be addressed in order to achieve the highest level of e-readiness
d) To create a base for the university to plan and roll out e-Learning to all its students not only in the short term (pandemic period) but also in the long term.

3. METHODOLOGY

The population of the research comprised of the entire active under graduate students duly registered and active on the university portal.

The research instrument used for gathering information from the respondents was a questionnaire. The Google form method was used where the questionnaire was uploaded on the website then the respondents were invited to fill in the form through their email addresses and through official WhatsApp class groups.

4. DATA ANALYSIS AND PRESENTATION

Some 1058 respondents filled the online questionnaire. Therefore, the findings presented in this section were based on the responded instruments; the analysis is as follows:

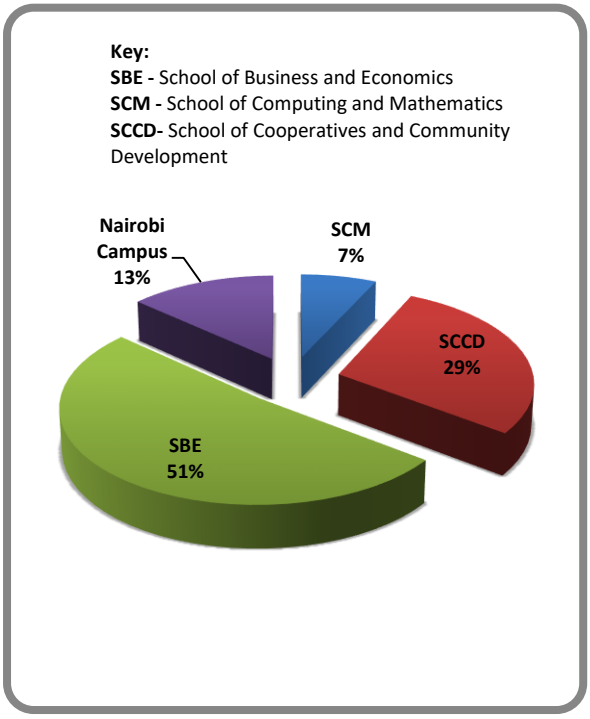

Figure 1. Analysis by School

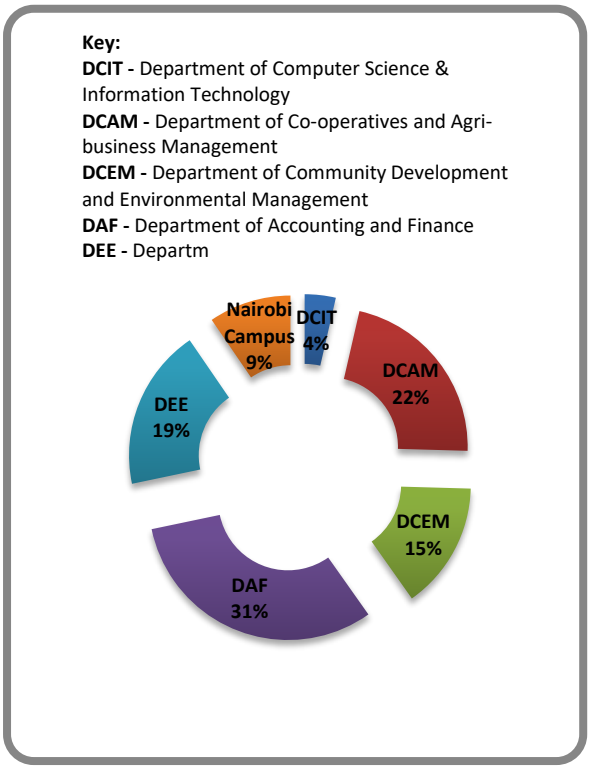

Figure 2. Analysis by Department

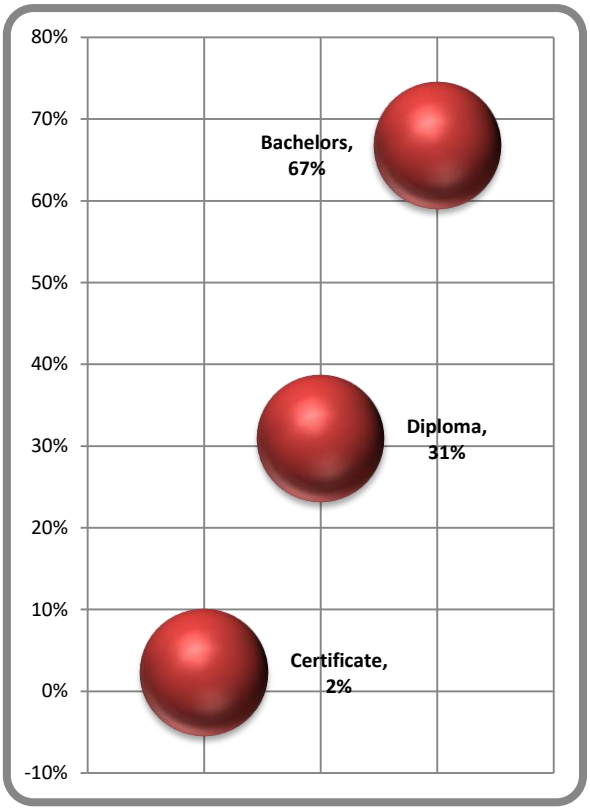

Figure 3. Analysis by Level of Study

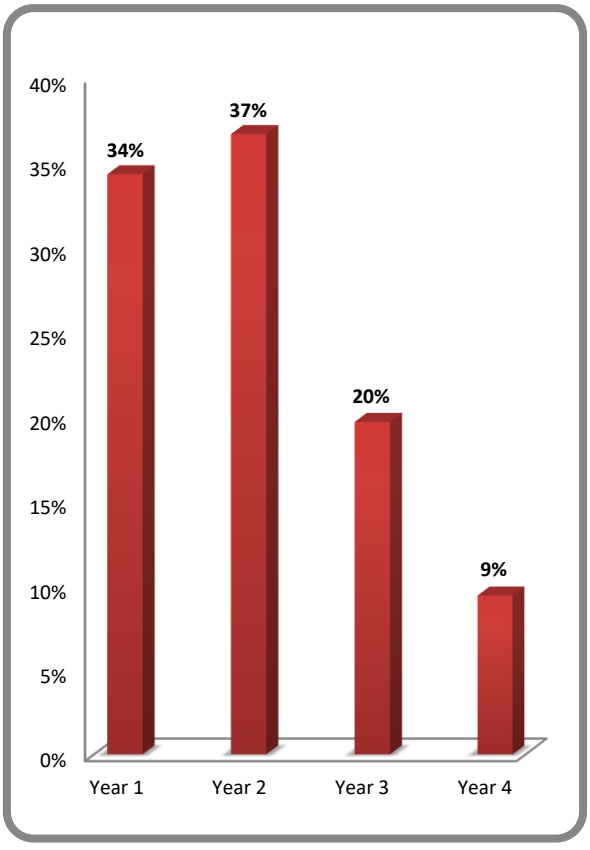

Figure 4. Analysis by Year of Study

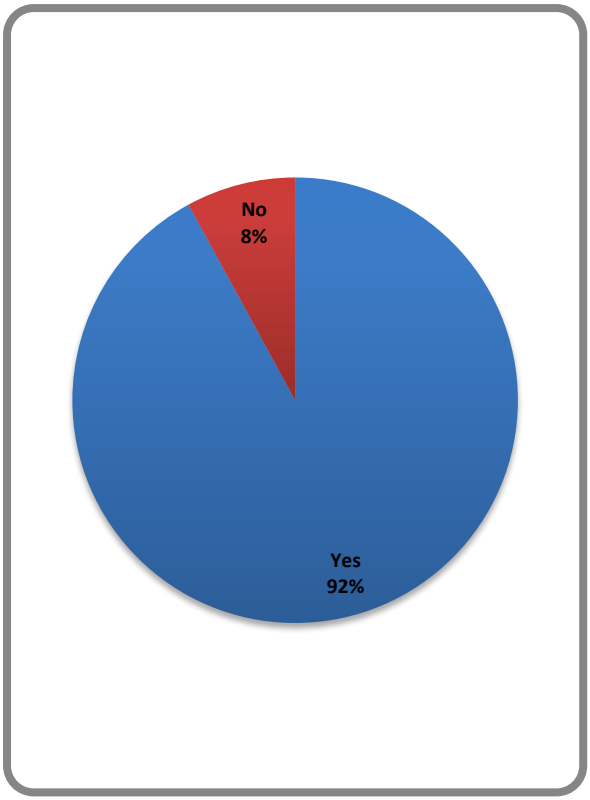

Figure 5. Percentage (%) of respondents who have prior interaction with digital learning platforms

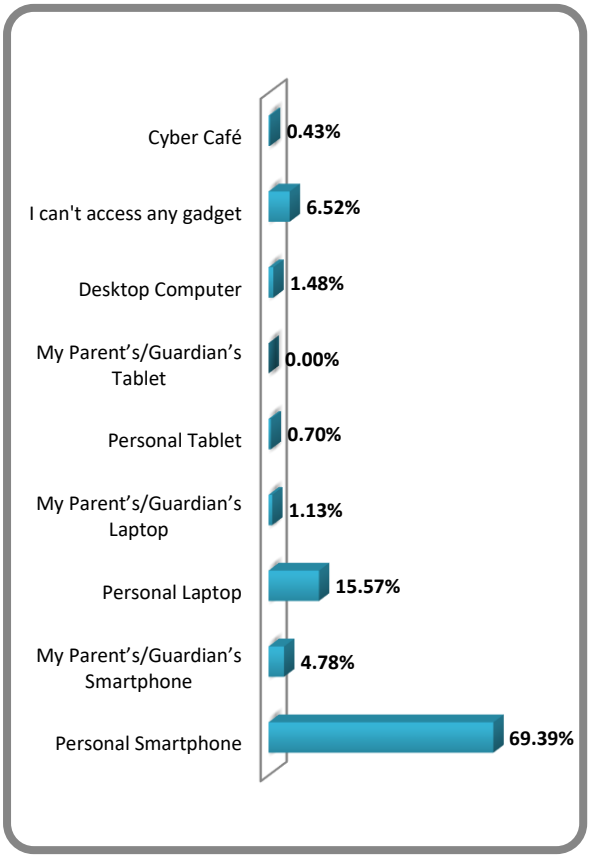

Figure 6. Analysis by Digital Gadget Access

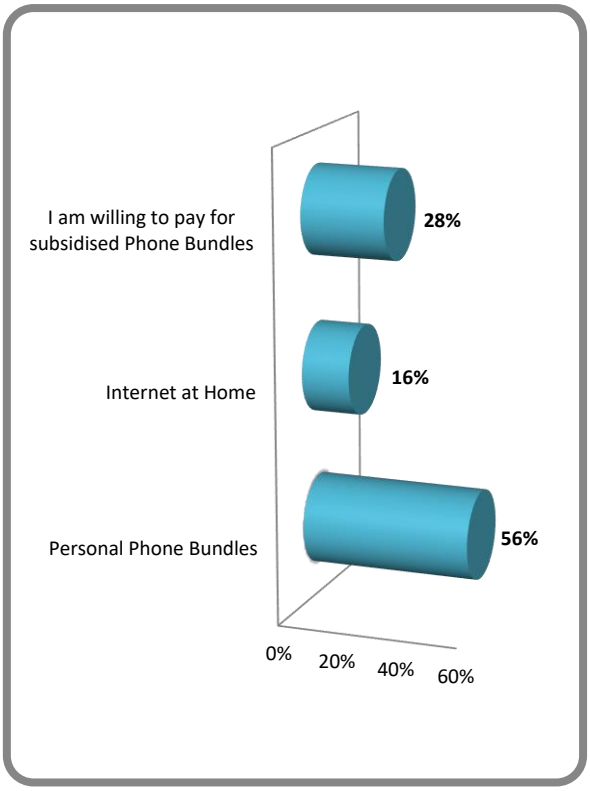

Figure 7. Analysis by Internet Connectivity Capacity

5. SUMMARY OF FINDINGS

- Majority of students have access to Smartphones and/or tablets (74.87%) compared to 18.79% who can access Desktops and Laptops
- A significant 6.52% of the respondents do not have access to any digital gadget usable for digital learning
- 85.66% of the students reported to have personal dedicated digital devices; which means a significant number of the remaining depend on communal, shared or borrowed resources.
- 92% of respondents reported to having prior interaction with digital learning platforms
- Only 16% of respondents have internet connectivity at home meaning most students will rely on smartphone internet.
- The majority of respondents were Bachelor's degree students (67%).

6. CONCLUSION

The conclusion of this research reveals that although most students have had prior interaction with digital online platforms, more is needed to ensure its application will be a success. As is, not all students are fully e-ready to adopt this mode of learning, although this is more so due to infrastructural deficiencies rather than a lack of technical capacity considering their previous experience with digital delivery of academic content. More investment is therefore required to boost capacity in infrastructure, training and support to needy

students otherwise some students will be left out and thereby require intervention measures later on to ensure their academic cycle is completed which will beat the core purpose of this anticipated migration to full digital learning during this pandemic and beyond. That being said, the findings reveal that immediate migration to digital learning is a feasible option for the University.

7. RECOMMENDATIONS

- Mobile Learning (m-Learning) is the most feasible option for the University to adopt in the short term considering the findings above.
- Infrastructural support is needed to ensure all students will be able to access this mode of study. More so for those without access to any digital gadgets.
- Regular capacity building as regards digital learning should be adopted for all university stakeholders

8. REFERENCES

[1] Kashorda, M., & Waema, T. (2014). E-Readiness survey of Kenyan Universities (2013) report. Nairobi: Kenya Education Network

[2] Readiness for the Networked World (2001-2002; and 2002-2003) Online. (http://www.weforum.org/gitr) available at www.readinessguide.org

[3] Zaied, A. N. H., Khairalla, F. A., & Al-Rashed, W. (2007). Assessing e-Readiness in the Arab Countries: Perceptions towards ICT Environment in Public Organizations in the State of Kuwait. Electronic Journal of E-government, 5(1).

International Journal of Computer Applications Technology and Research
Volume 9–Issue 11, 299-302, 2020, ISSN:-2319–8656

Underwater Image Enhancement Using Histogram Equalization and Color Correction

Reza Bagus Acintyasakti
Depertment of Electrical Engineering
University of Brawijaya
Malang, East Java, Indonesia

Rahmadwati
Depertment of Electrical Engineering
University of Brawijaya
Malang, East Java, Indonesia

Panca Mudjirahardjo
Depertment of Electrical Engineering
University of Brawijaya
Malang, East Java, Indonesia

Abstract: This research provides instructions for improve underwater image quality using histogram equalization and color correction. Images processing plays important role, the image does not only provide effects that make an image better but also must be able to improve quality of the image itself. The performance of each method is calculated by finding the Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

Keywords: underwater images, image enhancement, histogram equalization, color correction, MSE, PSNR.

1. INTRODUCTION

Underwater images is an underwater photo-taking process and is performed not only by SCUBA (Self-Contained Underwater Breathing Apparatus) but can also be done with a camera that dives underwater and is operated from the surface. The results of the documentation obtained are not as clear when compared to the documentation obtained on the mainland. There are several factors that affect the quality of underwater imagery. First, the absorption of light in water and the spread of light that alters the flow of light by small particles in the environment in the water have a limited impact on visibility during shooting. Second, the absorption and scattering effect is not only caused by the water itself but also for other components such as dissolved organic matter or small observable floating particles. The visibility range can be improved by artificial lighting but due to these absorption and scattering factors, artificial lighting tends to illuminate objects in a less uniform way, resulting in bright spots in the center of the image and poor lighting around them. This absorption and spread affects the seven color elements that sunlight has. The seven color elements of sunlight have different abilities in penetrating water. Purple and blue wavelengths are the most efficient in the spread of light. Therefore, if documentation is done in deeper waters then what is obtained is a blue color that increasingly dominates[2]. This is why it is necessary to improve the quality of underwater images.

Image processing can be utilized to improve the quality of underwater images. Several studies have been conducted to improve underwater images, such as researchers[3] stating that the use of gamma correction can improve dark image. The goal is to process an image so that the result is more suitable than the original image to be applied to a more specialized application. Researchers [4] analyzed systems that could perform underwater images improvements by applying RGB-HSI color model stretching methods and homomorphic filtering. The results showed optimum values in PSNR and MSE, depending on the combination of parameters. The selection of underwater image repair methods should be considered for accuracy in order to know the maximum results of the study. As in digital image repair research using Histogram Equalization (HE)[5]. The use of the method is one of the very effective techniques used in improving the entire detail of imagery and texture. The histogram equalization method is also one of the most efficient techniques for reducing missmatch between training results and test data results. The study [6] mentions the use of histogram equalization methods is considered easy due to simplicity and has relatively better performance in almost all types of images and is also able to increase images contrast. The method used by [7] for color correction in underwater images using Markov Random Field (MRF) increases color, contrast, and brightness of underwater images. The advantage of the MRF method is that it only requires a small set of patch images to color and correct images with depleted colors.

2. METHOD

2.1 Input Image

The initial process of this application is process the underwater images into the program. The image data used is an underwater image with RGB level with .jpg format. Image resolution size used is 500x300 pixels. The underwater image will be shown in Figure. 1.

Figure. 1. Underwater image

2.2 Histogram of Colored Image

Histogram of colored image is created for each RGB channel (red, green, and blue). A histogram is a graph that displays the color distribution of a scene according to the number of each color [3]. The histogram graph arranges the pixels into 256 levels of brightness in the range of 0 (dark) to 255 (white) and stacks them according to their respective brightness, meaning there are 254 gray levels between the ranges 0 - 255.

2.3 Histogram Equalization

One of the image enhancement processes in this research is Histogram Equalization. Important information about the content of digital images can be known by creating an image histogram. An image histogram is a graph that illustrates the spread of pixel intensity values from an image or a specific part of an image. The purpose of histogram equalization is to change the image so that the output image has a flatter histogram. Histogram equalization can be calculated using the following equations:

$$S_k = \frac{(n_G - 1)}{n} \sum_{j=0}^{k} n_{r_j}$$

With:

n_G : the number of grey level images = L
n : the total number of image pixels
k : $(0, 1, \ldots, n_G - 1)$
n_{r_j} : the number of pixel tha have a gray degree of $r_j = n_i$.

2.4 Markov Random Field (MRF)

The MRF method studies the relationship between each image and the corresponding color. This method uses a multi-scale representation of the corrected color and the original image built a probabilistic enhancement algorithm. The parameters of the MRF model are learned from the most possible color assignment of each pixel. This method allows the system to adjust the color recovery algorithm to real-time conditions at the time of shooting. Specifically, MRF models studied the relationship between color images and depleted images. Color correction can be modeled as sample functions of the stochastic process based on the Gibbs distribution shown in the following equations:

$$P(X = x) = \frac{1}{Z(\beta)} \exp\left(-\beta E(x)\right)$$

The color value is set for each pixel of the image input by describing the surrounding structure using a training image patch. The MRF method uses representations between corrected imagery and bluish colors to establish the probability of algorithms that can increase colors in underwater images.

3. RESULTS

3.1 Histogram Equalization of Colored Image

Important information about the content of digital images can be known by creating an image histogram. An image histogram is a graph that illustrates the spread of pixel intensity values from an image or a specific part of an image. From a histogram can be known the relative frequency of occurrence of each grayish level value in the image. Since the degree of grayness has 256 degrees (0-255), the histogram will state the number of occurrences of each value of 0-255. It starts by input an underwater image. Furthermore, a histogram will be obtained in each channel of red, green, and blue. Histogram equalization results are necessary to improve the quality of underwater images. An example of the histogram display of each color channel is shown in Figure. 2.

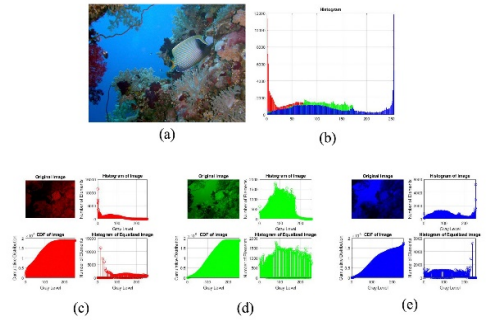

Figure. 2. Underwater image that showing the histogram of each RGB color channel: (a) the oringinal image, (b) histogram of original image, (c) the histogram of red channel, green channel (d), and blue channel (e)

The results of the colored image histogram equalization are displayed in Figure. 3.

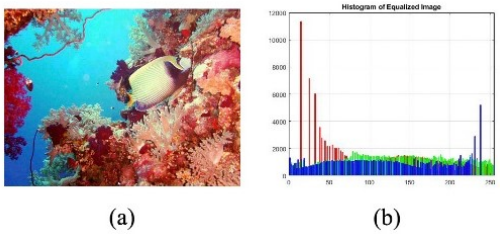

Figure. 3. The results of underwater image histogram equalization: (a) equalized image, (b) histogram of equalized image

From the images above, it can be seen that the output image of the histogram spread is more evenly distributed than the input image. With a more even distribution of histograms, the distribution of grayscale values will increase so that the output image will look brighter and the details will be more visible.

3.2 Color Correction of Underwater Images Using Markov Random Field

Measuring the difference between a depleted image (original image) and ground truth (an image with a equalized histogram) is essential for obtaining quality results, especially when there are dominant blue and green colors such as in underwater imagery. Color information can be determined, created, and visualized by different color spaces [7]. This method uses CIELab color space. This color space model has an advantage of being close to the human vision system. CIELab color space conversion is a method that used to determine compatibility functions and evaluate the performance of the Markov Random Field method. This algorithm uses pixel-based synthesis, which is that one pixel value can be estimated at a time. CIELab color space is shown in Figure. 4.

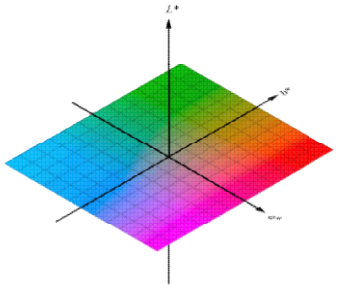

Figure. 4. CIELab color space

The conversion from RGB to CIELab can be done with the following equations.

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0.412453 & 0.357580 & 0.180423 \\ 0.212671 & 0.715160 & 0.072169 \\ 0.019334 & 0.119193 & 0.950227 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

$$L^* = 116 f\left(\frac{Y}{Y_n}\right) - 16$$

$$a^* = 500\left[f\left(\frac{X}{X_n}\right) - f\left(\frac{Y}{Y_n}\right)\right]$$

$$b^* = 200\left[f\left(\frac{Y}{Y_n}\right) - f\left(\frac{Z}{Z_n}\right)\right]$$

With:

$$f\,q = \begin{cases} q^{\frac{1}{3}} & if\ q > 0{,}008856 \\ 7{,}787q & therefor \end{cases},$$

L* : brightness level
(a*, b*) : chromatization point.

It starts by input a depleted image as an original image and equalized image as a ground truth. Divide the depleted image and equalized image into several patches measuring 50x50 pixels. To be able to distinguish between objects in an image, patches are taken from parts of the image with varying pixel values. The image is divided into several patches so that the image patches that will be corrected to color become overlapping. Next, convert the patch into the CIELab color space. The parts of the patches will represent the overall color change of the image so that it will be an image with corrected image. Fig. 6. shows Markov Random Field color correction process by converting RGB color to CIELab.

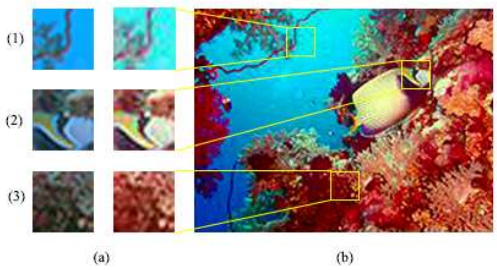

Figure. 5. (a) image patches used as ground truth, and (b) image with color correction

From Figure. 5, it can be seen that the image with color correction looks more contrast, the discontinuig on the edges of the object is maintained so as to avoid excessive image refining. Also, there are no overly contrast color changes that cause unrealistic image.

3.3 Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR)

The analysis method in this research using performance evaluation techniques by looking for MSE (Mean Square Error) and PSNR (Peak Signal-to-Noise Ratio) values. In digital images, there is a standard measurement of image quality error. The capability of an image quality improvement method is calculated using MSE and PSNR. The ability of the method of improving image quality can also be measured by visual techniques by looking at the image of the results and comparing them with the original image, however, the results of measurement of each person's visual techniques may vary. PSNR is a calculation that determines the value of a resulting image. The PSNR value is determined by the size or small value of the MSE that occurs in the image [8]. MSE and PSNR are formulated with the following equations

$$MSE = \left(\frac{1}{mn}\right)\sum_{i=1}^{m}\sum_{j=1}^{n}[u(i,j) - v(i,j)]^2$$

$$PSNR = 20Log_{10}\left(\frac{m \times n \times L^2}{\sum_{ij}[u(i,j) - v(i,j)]^2}\right)$$

With
L : maximum gray level value
m and n : rows and columns
$u(i,j)$: original image color value
$v(i,j)$: the image color value obtained from filtering result.

The first step to knowing the value of PSNR and MSE is to equate the image size between the original image, equalized image and the image with color correction. The output size of the specified image has 6 lines. Figure. 6. shows the image before and after resized

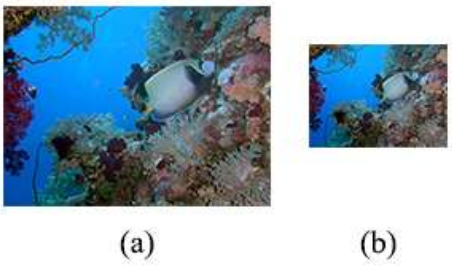

Figure. 6. (a) image before resizing, and (b) image after resizing

Calculation result of MSE and PSNR image value is shown in Figure. 7. and Table I.

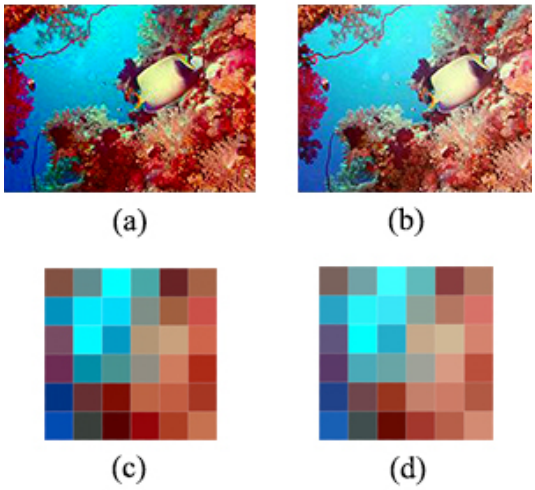

Figure. 7. (a) equalized image, (b) color corrected image, (c) and (d) are resized image of (a) and (b)

Table 1. MSE And PSNR Value

	Equalized Image	Corrected Image
MSE	143.5	51.83
PSNR	30.14	43.93

4. CONCLUSION

Low-quality images, such as underwater images, can be enhanced by histogram equalization. All pixels must be evenly distributed across the range of existing values, so that the histogram equalization can change the output image to have a flatter histogram and the information in the underwater image is more clearly visible. In color images, histogram equalization is applied to each channel and then each result is recombined. Color correction and image enhancement, especially underwater images contains many distortions that appear and are difficult to use simple methods. The MRF method uses a small number of required image patches as an example of a corrected image of a depleted image. There are several factors that affect the quality of the results, such as the adequate amount of information as input and statistical consistency of the underwater images. MSE and PSNR values between equalized image can be higher than image with color correction, and vice versa. This is affected by the lack of information on red, green, and blue color values in the underwater image so that the output image is noise.

5. REFERENCES

[1] Harahap, B. (2018). "Implementasi Metode Retinex Untuk Meningkatkan Kualitas Citra Underwater". Medan: *E-Journal*. [Online] Available: http://ejurnal.stmik-budidarma.ac.id

[2] Sudhakar, M. & Janaki Meena, M. "Underwater Image Enhancement using Conventional Techniques with Quality Metrics". *IJITEE*. 2019. 242.

[3] Hendrawan, A., Andono, P. N., Susanto. "Analisa Peningkatan Kualitas Citra Bawah Air Berbasis Koreksi Gamma dan Histogram Equalization". Jurnal Transformatika. Semarang: Universitas Semarang & Universitas Dian Nuswantoro. 2016.

[4] Norrochim, S., Wirayuda, T., & Violina, S. "Analisis Perbaikan Citra Underwater Menggunakan Metode Stretching Model Warna RGB-HSI dan Homomorphic Filtering". *Tugas Akhir.* Bandung: Universitas Telkom. 2011.

[5] Cheng, H.D. & Shi, X.J. "A Simple And Effective Histogram Equalization Approach To Image Enhancement". *Digital Signal Processing* 14(2), 2004, 158-170.

[6] Ibrahim, H. & Sia, K.P. "Brightness Preserving Dynamic Histogram Equalization For Image Contrast Enhancement". *IEEE*. 2007. Vol. 53.

[7] Torres-Mendez, L. & Dudek, G. "Color Correction of Underwater Images for Aquatic Robot Inspection". Montreal: Centre for Intelligent Machines, McGill University. 2005.

[8] Wirayasa, A. *Pengertian MSE & PSNR Pada Citra*. 2014. [Online]. Available: https://www.ketutrare.com/

International Journal of Computer Applications Technology and Research
Volume 9–Issue 11, 303-310, 2020, ISSN:-2319–8656

Adoption of Bring Your Own Device: Challenges and Risks in Higher Learning Institutions in Kenya

Oonge, O. Samuel
Department of Information Technology,
Maseno University Kenya
Kisumu, Kenya

Muhambe, T. Mukisa
Department of Information Technology,
Maseno University Kenya
Kisumu, Kenya

Ratemo, M. Cyprian
School of Computing,
Kisii University Kenya,
Kisii, Kenya

Abstract: In the digital world, consumerization of Information Technology has motivated individuals to privately acquire the latest mobile technology devices to access the organization/institution networks to perform their formal duties, a phenomenon also known as bring your own device (BYOD). The popularity of BYOD in learning institutions has been accelerated by perceived benefits of work flexibility, increased productivity and efficiency, dynamic student and employee preferences and technology trends and advancements. It has been noted however, that BYOD adoption compromises the general security of organizational information resources. This paper explores the challenges and risk factors of BYOD adoption in higher learning institutions and recommends mitigation strategies for the same.

Keywords: Bring your own device (BYOD), Risks, Security, point to point (P2P), Mobile Device Management (MDM) Mobile Application Management (MAM) and Identity Access Management (IAM).

1. INTRODUCTION

Information Technology (IT) has progressed from being a commodity service provider to a means for achieving greater efficiency and productivity [1]. The growth of IT adoption has been driven by the need for efficiency in operations, increased dependency on information for strategic and evidence-based decision making, online digital platform learning, the need to secure institutions information resources, and the growing phenomenon of collaboration between the institutions and other entities. The growth in uptake of mobile devices has greatly contributed to the use of information technology in enterprises. There is also a growth in the use of personal devices to execute enterprise applications and access data or information to perform their work related activities, a phenomenon known as Bring Your Own Device (BYOD), gradually becoming the norm. [2][3][4].

Studies [5][6] have established that powerful mobile operating systems, with capability to handle enterprise level applications, coupled with growing use of mobile internet connectivity provide advanced device capabilities allowing individuals to access information wherever they are and at whatever time. These devices, combined with business applications hosted in cloud-based environment means that organizational data and information or institutions learning resources are available to users no matter where, when or which devices they access the corporate networks with [7], which has led to increased access flexibility and availability of corporate information [8], hence increased efficiency and productivity.

Fortinet, [9] established that academic institutions' networks continue to be a favorite playground for cybercriminals because of their openness nature when it comes to information sharing. The report also highlighted the upsurge of attacks in these BYOD environments because of the users' cutting edge technologies and strategies, not forgetting pushing hard against network restrictions that make them employ workarounds to access information when in need. According to this report, in 2018, academic institutions had posted 13% of information security breaches compared to all other sectors in the United States of America (USA) resulting to a compromise of over 32 million records. Oregon University also suffered a breach that resulted in exposing students and their respective families' data. The PII of 636 students were compromised because of a BYOD user being compromised through a phishing email. The victims of this attack were majorly those who had interacted through email with the attack victim [10]

In [11] global risk management survey, cyber risk was ranked as the first risk facing academic institutions in Africa and is likely going to remain on top. In its 2016 report, [11] reported that the University of Limpopo's website was brought down, leaking exam papers and the details of over 18,000 students. The perpetrator also leaked login details for the University's intranet. This was suspected to be an insider with a BYOD device [10]

1.1 Objective of the Study

This study explores the challenges and risk factors that face higher learning institutions' information resources due to BYOD adoption and proposes mitigation strategies to counter the challenges and improve information security.

1.2 BYOD in Higher Learning Institutions

Institutions of higher learning have contributed towards the growth of the BYOD phenomenon. [12] revealed that "ownership and use" of mobile devices by higher education learners were on the ascendency. Cisco Networks [12] in their survey indicate that 85% of education institutions have allowed some form of BYOD on their institutions networks, a trend confirmed by the Bradford Networks global survey [13]. A survey by [14] on the use of personal devices established that 92% of students used laptops, 68% tablets, 44%, smart phones while 16% used e-readers for academic purposes. In another survey, [13] found that 85% of higher education institutions in US and UK, allow students, faculty and non-academic staff to access the institution's network using personally-owned mobile devices and predicted that by 2019, 90% of learning institutions would support BYOD [16], while

the institutions that do not allow BYOD would receive ongoing requests to use personal devices on their networks [13].

Several factors have been identified as driving forces behind adoption of BYOD in the university. The higher learning institutions have allowed their employees and students to use their own devices for personal and official purposes on the same infrastructure instead of them maintaining a separate, work-dedicated device [17]. It is argued that this has been fuelled primarily by the limited budgets for purchasing computers for these institutions, dynamic employee preferences and technological trends and advancements that has spiked the number of smartphones and tablets on the network.

[18] argues that one of the main reasons for the sudden shift towards BYOD by institutions is students' determination to use their personal devices to access institutions and other information regardless of the institutions security policies in place. The students believe that it is their right to use their own devices within their institutions [19] , and will intentionally break any anti-BYOD policies introduced [20] [21] [22] established that students and staff prefer the use of education apps on their mobile devices to more efficiently handle their tasks, while using the same device to interact on social media, access cloud based storage and entertainment.

Currently, the world has experiencing significant economic and learning disruptions due to the effects of the Corona Virus (COVID-19) pandemic. COVID19 resulted in halting of most face to face interaction, with more emphasis being put on the online learning's as well as online transaction for most of the university activities. Higher learning institutions as indicated by national media houses have encouraged learning from home necessitating the use of BYOD to access course materials and examinations. This has accelerated the adoption of working from home, and made it necessary for employees and students to access learning and work-related applications from their personal devices.

While 95% of institutions allow the use of BYOD devices in the workplace in some way, two out of three employees use their personal devices at work, regardless of the company's BYOD policies. That means some employees are using their personal devices to access organization networks and applications irrespective of the policies in place.

Meanwhile, despite the institutions striving to establish and continually improve information security controls to adequately protect sensitive data and comply with a variety of laws and regulations [23] [1], note that this task has become difficult to achieve due to overdependence on BYOD. According to [24], organisations are struggling to manage remote workers' use of phones and other mobile devices. 52% of the respondents on the same survey indicated that personal mobile devices on the network were very challenging to protect from cyber threats. The institutions are tasked with balancing the expectations of users, reaping the benefits of mobile devices and applications, while protecting the Confidentiality, Integrity, and Availability (CIA) of the institutions' information [25]. [4] pointed out that attacks directed towards this information are on the rise.

2. METHODOLOGY

A survey was carried out across 3 Kenyan public universities that permit BYOD. A sample of 400 users was used in the study as recommended by [26]. The sample consisted of technical staff; Senior ICT administrators, covering system, network and operations and maintenance. In this category, the respondents were purposively selected and interviewed. The second category of respondents were other users; consisting of students, lecturers and non-academic staff who were randomly selected to participate in the study through a survey. It was a requirement for a user to have one or more years of BYOD experience to fill the questionnaire.

A mixed method research design was adopted allowing both qualitative and quantitative approaches [27] [28]. A five point structured Likert scale questionnaire was constructed based on comprehensive literature review. The questionnaire was sent out to four hundred (400) email addresses belonging to participants who included lecturers, non-teaching (administration) staff and students out of which three hundred and eightynine (389) responses were received representing approximately 97% response rate. The questionnaire was administered using google forms assuming high computer literacy among the respondents. A semi-structured interview schedule was also used to obtain precise but relevant BYOD risks and challenges information from the selected eleven (11) senior ICT administrators [28][29]. A qualitative and descriptive analysis of data was done to assist in establishing the challenges and risks experienced due to BYOD adoption within higher learning institutions.

2.1 Demographics

The participating universities were coded as U1, U2, and U3 representing university 1, university 2 and university 3 respectively. Out of the 389 responses received university U1 had a majority of respondents with 162 followed by university U3 with 126 respondents while university U2 had 101 respondents. Majority of the respondents were students representing 60%, lecturers 27% while non-academic staffs represented 13% of the respondents. The non-academic staff category comprised of ICT administrators, other administrative staff and top management cadre. Three ICT administrators were randomly selected and interviewed from U2 and U3 while five respondents were interviewed from U1 university for being an established and more populous university. There was 100% response rate for interviews.

2.2 Results and discussion

To identify the challenges and risk factors for BYOD adoption within higher learning institutions, a questionnaire and interview schedule containing nine questions were administered to the respondents. The responses for the questions were as follows;

2.2.1 Does your institution allow students and staff to use their own mobile devices on the institutions network?

The question was meant to establish whether BYOD adoption is in place in the respondent's institution. All the respondents were positive on this question. As indicated by one of the administrators

> *"The university has allowed own mobile devices into the institution hooking them up on the institutions network in order improve mobility and ease of information and academic material access by the students and researchers*".

This indicated that out of the three selected universities, none prohibits the use of BYOD on the institution's network, a confirmation that BYOD has been adopted to enhance student motivation and learning in higher learning institutions as also established by [30] [31] [32]

2.2.2 Do the ICT administrators control who to connect to the institution's network?

This question was meant to establish if there were any information security controls implemented to detect and deter any unauthorized access. Out of the 100 respondents, more than half (75%) denied knowledge of any implemented security controls that controls who connects to the network. 15% of the respondents slightly agreed while 10% strongly agreed of their administrators knowing who connects to the network.

Institutions of higher learning promote a culture of openness in order to promote access to information and learning materials therefore, they have a habit of using either one or two layers of security. Similarly, researchers, lecturers and students are committed to sharing information through collaboration, inside and outside the university, in order to facilitate their discoveries irrespective of information security policy flouting. These sentiments were also echoed by [33] [34] [35].

BYOD adoption overwhelms the universities' security teams since there is a lot of difficulty in controlling what the owners of the devices do with them. Since the institutions' focus is on getting users connected to ease learning, research and entertainment, this has deteriorated the general security of the network making it vulnerable to attacks and becoming easy targets or where targets anchor to launch attack against other targets [4].

2.2.3 Does your own mobile device have an active antivirus and a genuine operating system?

This question was meant to establish the security level of devices that constantly connect to the institution's network. The analysis revealed a sad state of operation since 83% of respondents had never protected their mobile devices, 11% of the respondents have an antivirus installed but not updated while only 6% had an updated antivirus. It was noted that 2% of the respondents used open source operating systems while 76% of the respondents used inactivated proprietary software. Variations in operating systems and physical platforms was encountered (e.g. Apple's iOS, Android, and windows mobile) on the institution's network posing a unique security challenge to IT resources, since every producer has customized security tools for their device. Getting the learning institution to implement all the security tools for different devices is a big challenge. [36] [37] also highlights on the security risk posed by variations of applications with different levels of trust installed on the varied devices.

2.2.4 Are there any security challenges that have come up by allowing BYOD in your institutions?

This open question to the respondents granted them an opportunity to list all challenges that they have experienced because of BYOD adoption in their respective universities. The responses were varied but classified in major topics as follows; Bandwidth constraints (8%), exposure of institution information to attacks (39%), device and data losses (13%), data ownership problems (25%), and spreading of malware (15%). With an increasing reliance on BYOD new and emerging software threats that target them specifically have also been on the rise. Viruses, for example, can infect one cellular phone and then spread to other devices via the network. Threats such as bluejacking and bluesnarfing where actual theft of data from Bluetooth enabled devices (including both mobile phones and laptops): contact lists, phonebooks, images are also on the rise.

Varied use of mobile devices within the organization network is likely to allow viruses and malware infections to proliferate the network, hence, exposing the institutions to information security incidents. [36][38] [39]; [40]. As pointed out by [41], protecting devices from infection of malware and viruses is a big challenge. A network admin in one of the institutions said; *"At our learning institution, blocking access to restricted applications is a challenge. Users exchange information through social media sites and share conference facilities using the institution's network. During this sharing, sometimes, institutions accounts are used".*

As much as staff and students may want to be secure while using institutions information [43] controlling downloaded information on BYOD devices is a challenge [39] because downloaded data can easily be accessed by friends who borrow the gadget. This introduces third party individuals or organization to the network who may try to gain unauthorized access to organizations' information depending hence, introducing a bridge to confidentiality [39] [45] [41] Likewise, users who grant permissions such as push notifications create another security loophole which enables installation of malicious applications onto the network [6]

Generally, as [47] puts it, there is a challenge in accounting for network access by BYOD devices for both students and staff and hence, protecting these devices from malware and viruses' infection is almost impossible. As one of the information security administrators reported,

"The learning institutions is not able to account for every device and its security status, this is because there is a big challenge to monitor who accesses these devices and what they do with them while connected on the network."

[41] suggest that theft and loss of mobile devices is rampant within learning institutions. These loses expose the institutions' information to CIA breaches (e.g. emails, financial information). Stolen information can also be used by malicious attackers to blackmail the victims especially if the gadget contained personal private information too. Users are the enemy within the organization. [43] argues that a bigger risk to institution's information is the insider. Insider threats emerge when an employee bypasses BYOD security controls to gain access to unauthorized areas. According to [4], curious and naughty students have always found themselves trying out their new learned skills on the institution's network. This activity is usually attempted remotely using their own gadgets with the help of open source hacking tools. This has brought down websites and corrupted information which would have been minimal without BYOD.

2.2.5 Are there any efforts from the institution's side to assist deal with the identified challenges?

The researcher sought to know whether the universities had put any measurer(s) to address the negative impact(s) brought by BYOD. 75% of the respondents indicated NO measurer(s)

implemented while a mere 25% were positive about security controls implementation. For the positive response participants, it was noted that the main information security controls implemented included user authentication, system firewalls and antivirus software. NIST 800-30 guideline of information security recommend a layered approach to information security, which implies that the measures implemented in these environments were inadequate to fight against the challenges brought about by BYOD.

2.2.6 In the past six months, did you ever experience any information security attack(s) as a result of adopting BYOD within your institution?

The researcher sought to find out the recent and frequent attacks experienced on the university's information systems as a result of adopting BYOD. This was an open ended question posed to both questionnaire and interview respondents. The analysis indicated a high magnitude of malware attacks at 43% while student hackers who consistently tried to bring down websites and /or access the university's sensitive information followed closely at 40%. Theft of devices was at 10% while Denial of Service (DoS) attacks staggered at 7%.

With the introduction of BYOD in campus, young exploratory students always access inappropriate sites on the Internet, often engaging in illegal downloads from P2P, frequently visiting malware-infected sites and downloading questionable applications using personally owned devices on the institutions network with minimal oversight from the IT staff. As [48] puts it, these students are intelligent, curious, daring to use new tools and consistent in exploring the network. Their intrusive nature increases attacks on the network since their gadgets are not well protected

According to [49] the amount of malware for mobile devices keeps growing. Every quarter 1.5 to 2 million new malware variants are discovered. As of the end of 2019, there were over 30 million malware variants in total.

2.2.7 Do you receive any training from your institution on how to effectively protect yourself and the institution's information resources from attacks?

This question sought to establish whether BYOD users had been sensitized on security attacks and protection while using their devices on the university network. 58.5% of the respondents revealed that there was no form of training conducted with most of users citing major challenges on the use of the learning management system. The remaining percentage of respondents who acknowledged some form of training were university staff. Majority of users (71%) indicated their inadequacy in terms of user and technical skills when it comes to the use of ICT for Educational purposes. Due to limited budgets assigned to ICT improvement within institutions, users have been encouraged to acquire their own devices for use to keep up with the large number of students admitted in the universities. In the bid to achieve institutional objectives, institutions have invested in ICT infrastructure which includes allowing for Internet connectivity to other devices [50][51] but not training and awareness needs.

Respondents confirmed that despite the rampant BYOD security challenges and attacks within the campuses, there has been minimal training and sensitization on information security for users. Significant efforts have majorly been directed to policy and technical implementations. Statistics also indicate inadequate knowledge on information security for both staff and students despite the sophisticated BYOD device ownership. These condition calls for the need for capacity building for staff and running sensitization programs for students to improve the security of the information system with BYOD adoption in mind.

2.2.8 If attacked, is your institution able to continue with daily operations?

This question was posed to the ICT administrators because they are the ones in-charge of business continuity plans. Only 36% or 4 of the 11 respondents acknowledged having business continuity plans in place. This means that in case of an attack, most of the learning institutions are not be able to serve their clients and may not even continue operating because of loss of information and other resources.

University employees handle extremely sensitive details about students, staff members, research data and patients from institutions' clinics and hospitals. Use of personal digital devices in such environment requires that the organs meet compliance regulations of the information entrusted to the institution, backups of such data is paramount however efforts to comply with this goal has been hampered by the limited resources at hand, since the security teams tend to be perennially understaffed and underfunded. Given the kind of information acquired and stored by these institutions, this may be a very serious oversight. Continuity plans such as backing up data and having other redundant sites are crucial to every institution.

2.2.9 State any efforts and future plans by your institution to deal with other identified security challenges not currently addressed?

This question sought information from ICT administrators and management about the institution's commitment towards securing the information systems. Responses received pointed at improving the ICT infrastructure by increasing funding. This will ensure the learning institutions are able to implement adequate security controls. Training needs towards information security for both staff and students was highlighted. Policies, guidelines and procedures were also mentioned and management was keen on ensuring their implementation.

Higher learning institutions provide a wide range of information resources that attract hackers and other cyber criminals. BYOD adoption among these institutions has exposed student, staff and institution's information to major cyberattacks due to inadequate security controls. With the implementation of "traditional security controls" which include firewalls, antivirus and IDS, BYOD attacks have been on the rise because of their varied sources. Major information security challenges such as bandwidth inadequacy, information attacks due to malware, device losses and Denial of Service (DOS) attacks have been on the rise despite little security control implementation. Information gathered from this research reflect poor adoption of BYOD within these institutions; there has been neither sensitization and training for the users nor existent business continuity plans as outlined in [52] documentation.

3. PROPOSED INFORMATION SECURITY CONTROLS FOR A BYOD ENVIRONMENT

Information security controls are mitigation strategies implemented by an organization to detect, deter or correct attacks directed to the organization information system resources [53] The selection of information security controls plays a major role in ensuring business continuity in any information system environment.

Legacy information security strategies implemented in any computer networked environment usually involve physical, technical and administrative mitigation strategies which usually detect, deter and/or correct the security breach at hand of which are inadequate for the BYOD environment [54].

Due to the limited ICT infrastructure budgets, higher learning institutions' policy on information security allows the deployment of 'baseline' security measures, which has led to a continued increase in the number of security breaches. Literature indicate that over 60% of learning institutions have employed traditional security countermeasures which include anti-virus software, firewalls, anti-spyware software, virtual private networks (VPN's), vulnerability/patch management, encryption, and Intrusion Detection Systems [55] [56]. This has however not deterred the frequent BYOD targeted attacks due to increased internal and external activities.

[57] on recommendations for mitigation strategies in a BYOD environment start by proposing a unique security strategy for BYOD since it is "a project initiated by the users but not the organization" therefore posing unforeseen challenges. The authors state the importance of treating BYOD risks and challenges differently because most institutions have found themselves in them without much control. To secure information resources in a BYOD environment, simplicity with effectiveness should be combined.

3.1 BYOD Policy

A policy specifies an organization's security posture, defines and allocates functions and responsibilities, grants authority to security professionals, and identifies the incident response processes and procedures [58]. A BYOD policy should therefore be a well thought document that specify who, what, when, why and how of accessing, using, modifying and sharing information resources and educate employees on the best practice of data security.

A policy elaborates matters concerning eligibility, allowed devices, service availability, rollout, cost sharing, security, acceptable use, support and maintenance [59]. A BYOD policy according to [10] may cover Mobile Device Management(MDM), Mobile Application Management (MAM) and Identity Access Management (IAM). These three address the mobile device, mobile application and user access security strategies. MDM outlines the protocols for accessing data from within and remote locations, the applications manager monitors what application to be run on the mobile devices while IAM highlights user authentication. Mobile device management (MDM) solutions offer a balance between total control for employers and total freedom for employees, offering the ability to deploy, secure, and integrate devices into a network and then monitor and manage those devices centrally. Updating of BYOD devices and patching application systems, vulnerability checking to probe possible or potential weak points in the security infrastructure using "red teaming" or "penetration testing." Is another step towards prevention [60][61]; [62]; [63].

BYOD policy should be audited and tested regularly protect while serving the interests of both the user and information resources. The BYOD security specifies punishment of employees that fail to adhere to policy statements. The policy should also include and enhanced education and training program to inform students and staff of institutional policies and guidelines of using BYOD devices in order to make information security efforts more effective [64]

Encryption

Encryption addresses the security for data both at rest and in transit. Encryption technologies scramble data so that only people with the decryption keys can have access. Encryption can be applied in organizational emails, VPNs, passwords and even webpages. Encryption protects sensitive information from unauthorized people.

Encrypting information in transit within the BYOD environment prevent unauthorised access and hence enhances integrity and confidentiality [65] [66].

Risk assessment

Identifying the risks, threats and challenges that present themselves in a BYOD environment helps in alleviating these threats. A risk assessment will help in identifying assets and registration of devices that are allowed to access the network for easy authentication of the devices [58].

Risk assessment will help in identifying sensitive ICT resources that need limited access so that technological and human aspects of security are employed to protect them [67] [10]. also recommends in-depth risk assessment using methodologies such as ISO 27005 and NIST SP 800-30 to help determine appropriate controls for BYOD environments.

Remote Management and Surveillance

Loss of physical ICT storage devices are rampant in a BYOD environment. These devices mostly contain sensitive and private institutional information. Remote switching off and wiping of the devices should be made possible to protect the organizations' information [69].

Remote login should be restricted to a few individuals. SSO should never be allowed especially to individuals logging in remotely.

Surveillance involve monitoring of the security environment aimed at developing situational awareness to adapt to fast-changing BYOD circumstances and mobile threats [70]. Surveillance typically uses information generated from strategically placed 'sensors' augmented with visualization tools to increase security managers' understand ability of the situation [70] [69] [72]. Information collected is typically sourced from systems and applications software [73] including intrusion detection systems that report on the number of attacks, degree of attack propagation, and type of attack [70].

3.2 Other Information Security Control Strategies

Many more actions can be done to help protect information in a BYOD environment. Additional strategies include; consider implementing Enterprise Content Management (ECM) system, beware of vendor access, achieving compliance, WI-FI management/network segmentation, avoiding storage of sensitive information on mobile devices, having adequate technical support for ICT services, abandoning legacy systems, keeping track of inventory and containerization which separates the attacker and/or attacked area from other (unaffected) areas [75].

4. CONCLUSION

This study sought to identify the information security challenges and risks in higher learning institutions due to BYOD adoption. The study also proposes recommendations for information security controls in this environment. According to the respondents' views,

BYOD adoption is on the rise and has become inseparable part of today's academic and organizational system. Despite the convenience, BYOD is accompanied with lots of challenges and risks to institutional information resources.

In order to support and make BYOD adoption more beneficial, there is need for institutions to enhance their network infrastructure by implementing adequate security controls to counter the risks introduced on the network which can only be possible through top management support for these activities. It can also be noted that although insiders pose the biggest challenge to information systems security, implemented controls should embrace simplicity to users and security to technology. To sensitize users on the need to stay safe, regular training and awareness campaigns should be done. System audits are also crucial in establishing the weaknesses an information system. Top management should help in all these activities by taking information security as a key component and function of management. Structured approach to security implementation can be realized through formation of information security team adequately advice and protect the institution's resources

5. RECOMMENDATIONS FOR FURTHER RESEARCH

Due to the dynamic nature of BYOD within higher learning institutions, there is need to constantly identify the organization's sensitive information resources' security and highlight the needs for improving the same. Risk assessment as mentioned in the review is one of the best security control to secure a BYOD ecosystem. Further research is therefore recommended to develop a standard information security risk assessment model that will be used to identify threats and vulnerabilities within the BYOD academic environment. This will help prioritize security of sensitive areas because of the limited budgets allocated to ICT services within the learning

6. ACKNOWLEDGMENT

I would like to express my deep and sincere gratitude to my research supervisors Dr, Muhambe, T. Mukisa and Dr, Makiya, C. Ratemo for providing invaluable guidance throughout this research and my family for their support and valuable prayers during the time of writing this paper

7. REFERENCES

[1]. Van Leeuwen, D. 2014. "Bring Your Own Software," Network Security (3), pp.12-13.

[2]. Marcus, J. 2015. Is BYOD Trend Fading. Technivorz. Retrieved from https://technivorz.com/is-byod-trend-fading.

[3]. Gartner. 2013. Employees to Supply Their Own Device for Work Purposes. Retrieved May 28, 2020, from Gartner: http://www.gartner.com/newsroom/id/2466615

[4]. Khan Rahat Afreen. (2014). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 233-236.

[5]. Michael E. Whitman, Herbert J. Mattord. 2011. Cengage Learning, Jan 1, 2011 - Computers - 656 pages.

[6]. Armando A, G. Costa, A. Verderame, and A. Merlo, 2014. "Securing the 'bring your own device' paradigm," Computer, vol. 47, no. 6, pp. 48–56, 2014.

[7]. Power, D. 2012. BYOD: is Bring your own Devise" good for enterprise business. sprout.

[8]. Beckett, P. 2014. BYOD – popular and problematic. Network Security, 7-9.

[9]. Neo Sesinye 2018. Cyberattacks on educational institutions n the rise. Retrieved from https://www.itnewsafrica.com/2018/10/cyber-attacks-on-educational-institutions-on-the-rise on 12/7/2020

[10]. Brook Chris, 2020. The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. Retrieved from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating 2/11/2020

[11]. Cisco. 2012b. Cisco Bring Your Own Device. Retrieved May 21, 2020, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unifi ed_Access/byoddg.html

[12]. Cisco. 2012a. BYOD Security Challenges in Education: Protect the Network, Information, and Students. Retrieved march 22, 2020, from https://www.cisco.com/web/strategy/docs/gov/security_challenges.pdf

[13]. Bradford Networks. 2013. The impact of BYOD in education. Retrieved August 27, 2020, from http://th-ebooks.s3.amazonaws.com/The_Impact_of_BYOD_in_Education.pdf

[14]. ISDecisions (n.d). Network security in Universities, Colleges and Schools. Retrieved from https://www.isdecisions.com/blog/it-management/network-security-in-universities-colleges-and-schools/ on 21/10/2020

[16]. Thomas, S. M. 2014. Bring your own Devise. Benefits, risks and control techniques, pp. 1-6.

[17]. Gimenez, O., & Wang. 2015. Remote Mobile Screen (RMS): an approach for secure BYOD environments. *CSE Conference and Workshop Papers*, (p. 238). Nebrasca.

[18]. Negrea, S. 2015. *BYOD boundaries on campus*. Retrieved october 11, 2020, from UB University Business: https://www.universitybusiness.com/article/byod-boundaries-campus

[19]. Fortinet 2018. Top Cybersecurity Threats Active in the Education Sector Today – and Why You Should Care. Retrieved from https://www.csoonline.com/article/3250862/top-

cybersecurity-exploits-active-in-the-education-sector-today-and-why-you-should-care.html on 21october 2020

[20]. Ounza, J. E., Liyala, S., & Ogara, S. 2018. Emerging Security Challenges due to Bring Your Own Device Adoption: A Survey of Universities in Kenya. *International Journal of Science and Research (IJSR)*, 345-350.

[21]. Brian, T. 2013. *The security implication of BYOD*. Network Security, , 12-13.

[22]. Stavert, B. 2013. Bring your own device (BYOD) in schools. NSW Department of Education and Communities

[23]. Koh, E. B., Oh, J., & Im, C. 2014. A Study on Security Threats and Dynamic Access Control Technology for BYOD, Smart-work Environment. International Multi-conference of Engineers and Computer Scientists, 2, pp. 1-6. Hong Kong.

[24]. Brian, T. (2013). The security implication of BYOD. Network Security, , 12-13.

[25]. Kang D, Oh J, and C. Im, 2013. "A study on abnormal behavior detection in BYOD environment," Int. J. Env. Ecol. Geol. Geophys. Eng., vol. 7, no. 12, pp. 612–615

[26]. Israel, Glenn D. 1992. Sampling the Evidence of Extension Program Impact. Program Evaluation and Organizational Development, IFAS, University of Florida

[27]. Wilknison, D., & Birmingham, P. 2003. Using Research Instruments: A Guide for Researchers. Psychology Press.

[28]. Elizabeth A Buchanan Erin E Hvizdak 2009. Online Survey Tools: Ethical and Methodological Concerns of Human Research Ethics Committees. Journal of Empirical Research on Human Research Ethics 4(2):37-48.

[29]. Chris Brook 2020. The ultimate guide to BYOD security: overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. Retrieved on 21/10/2020 from https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

[30]. Shneiderman, B., & Plaisant, C. 2005. Designing the User Interface. Chapter 14.5: Information Visualization (pp. 580–603). Boston: Pearson

[31]. Akin-Adetoro, Kabanda 2015, Contextualizing BYOD in SMEs in developing countries. Proceedings of the **2015** Annual Research …, **2015** - dl.acm.org.

[32]. Attewell, J. 2005. Mobile technologies and learning: A technology update and m-learning project summary. London: Learning and Skills Development Agency http://www.lsneducation.org.uk/user/order.aspx?code=041923&src=XOWB

[33] French, A. M., Guo , C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). Communications of the Association for Information Systems, 10, 192-197.

[34] Gessner, D., Girao, G., & Li, W. (2013). Towards a User Friendly Security enhensing BYODSolution,. Nec Tech J, 7, 113.

[35]. H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, 2015. Predictive, Probabilistic Cyber Security Modeling Language," in *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 626-639, doi: 10.1109/TDSC.2014.2382574

[36]. Coleman, L., and B. Purcell. 2015. Data breaches in higher education. Journal of Business Cases and Applications. 15: 1–7

[37]. Gajar P, A. Ghosh A, and. Rai S, 2013."Bring your own device (byod): Security risks and mitigating strategies," J. Global Res. Comput. Sci., vol. 4, no. 4, pp. 62–70,

[38]. A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner 2011. A survey of mobile malware in the wild. In Proc. of ACM Worksgop on Security and Privacy in Smartphones and Mobile Devices (SPSM), pages 3– 14,

[39]. Francis A. Kwansa, Katerina Berezina, Cihan Cobanoglu, Brian L. Miller, 2012. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth International Journal of Contemporary Hospitality Management ISSN: 0959-6119,

[40] Eilertson EE, Ertoz L, Kumar V 2004. MINDS: A New Approach to the Information Security Process. Paper presented at the 24th Army Science Conference, Dec.

[41]. Shumate T, Ketel M- 2014. 2014 - Bring your own device: Benefits, risks and control techniques, ieeexplore.ieee.org;

[42]. Wang Y, Wei J., and Vangury K. 2014, "Bring your own device security issues and challenges," in Proc. IEEE 11th Consumer Communications and Networking Conference (CCNC), Jan. 2014, pp. 80–85.

[43]. Lampson BW 2004. Computer Security in the Real World. Computer 37 (6):37-46

[44]. Potts, M. 2012. The state of information security. Network Security, 2012, 9-11. doi:10.1016/S1353-4858(12)70064-8

[45]. A. Armando, R. Carbone, L. Compagna, &Lt 2014 SATMC: A SAT-Based Model Checker for Security-Critical Systems", In the Proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014), pp. 31--45, Springer, France, April 2014

[49]. Kumari, Debbarma and Shyam 2015. Security Problems in Campus Network and Its Solutions , www.researchgate.net › publication › 224771078_Security_problems_in_campus_network_and_its_solutions.

[50]. McAfee Labs. 2018a. *McAfee Labs Threats Report, December 2018*. Santa Clara, CA: McAfee Labs.

[51]. Gikas, J., & Grant, M.M. 2013. Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones and social media. The Internet& Higher Education, 19(1), 18-26.

[52]. Salaway G, Caruso JB. 2007. The ECAR study of undergraduate students and information technology, : key findings. At: www.educause.edu/library/EKF0706. Accessed: June 26, 2009

[53]. ISO/IEC 27001, 2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html accessed on 21/10/2020

[54]. Souppaya m, Scarfone K (2015) - NIST special publication, - telehealthtechnology.org

[55]. Stanford Musarurwa, Attlee M. Gamundani and Fungai Bhunu Shava 2019. An Assessment of BYOD Control in Higher Learning Institutions A Namibian Perspective. ResearchGate.

[56]. Richardson, J. T. E. 2011. "Eta Squared and Partial Eta Squared as Measures of Effect Size in Educational Research." *Educational Research Review* 6: 135–147

[57]. Debar H, Tombini E 2005. Accurate Detection of HTTP Attack Traces in Web Server Logs. Paper presented at the European Institute for Computer Antivirus Research (EICAR) 2005 Conf. Best Paper, Saint Julians, Malta, Apr

[58]. Hamill JT, Deckro RF, Kloeber-Jr. JM 2005. Evaluating Information Assurance Strategies. Decision Support Systems 39:463-484

[59]. Park S, Ruighaver AB, Maynard SB, Ahmad A 2011 Towards Understanding Deterrence: Information Security Managers' Perspective. Paper presented at the International Conference on IT Convergence and Security 2011, Suwon, Korea,

[60]. Franklin, Onyechere and Ismail, Mohamed 2015. The future of BYOD in organizations and higher institution of learning. International Journal of Information Systems and Engineering VL – 3

[61]. Forcht KA 1994. Computer Security Management. Boyd and Fraser, Danvers, MA

[62]. Arce I, McGraw G 2004. Why Attacking Systems Is a Good Idea. IEEE Security & Privacy 2 (4):17-19

[63]. Evans S, Kyle DH, Piorkowski J, Wallner J 2004. Risk-Based Systems Security Engineering: Stopping Attacks with Intention. IEEE Security & Privacy 2 (6):59-62

[64]. Ray HT, Raghunath, Kantubhukta HR 2005. Toward an Automated Attack Model for Red Teams. IEEE Security & Privacy 3 (4):18-25

[65]. Graham D 2003. It's All About Authentication. SANS Institute,

[66]. Dunn TS 1982. Methodology for the Optimization of Resources in the Detection of Computer Fraud. University of Arizona

[67]. Kankanhalli A, Teo H-H, Tan BCY, Wei K-K 2003. An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23:139-154

[68]. Liu S, Sullivan J, Ormaner J 2001. A Practical Approach to Enterprise IT Security. IEEE IT Professional 3 (5):35-42

[69]. Klete H (ed) 1975. Some Minimum Requirements for Legal Sanctioning Systems with Special Emphasis on Detection. Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington, D.C.

[70]. Brand RL 1990. Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery, CERT, Pittsburgh, Pa., June 1990.

[71]. Doyle J, Kohane I, Long W, Shrobe H, Szolovits P 2001. Agile Monitoring for Cyber Defense. Paper presented at the 2001 DARPA Information Survivability Conference & Exposition II (DISCEX '01).

[72]. Ohno K, Kike HK, Koizumi K 2005 IPMatrix: An Effective Visualization Framework for Cyber Threat Monitoring. Paper presented at the Ninth Int'l Conf. on Information Visualisation (IV5), London, England,

[73]. CSSP 2009. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-InDepth Strategies. Control Systems Security Program, National Cyber Security Division, Department of Homeland Security,

[74]. Dourish P, Redmiles D 2002. An Approach to Usable Security Based on Event Monitoring and Visualization. Paper presented at the 2002 Workshop on New Security Paradigms, Virginia Beach, Virginia, USA, Sep.

[75]. Grance T, Kent K, Kim B 2004. Computer Security Incident Handling Guide (trans: Computer Security Division ITL). NIST Special Publication. National Institute of Standards and Technology, Gaithersburg, MD