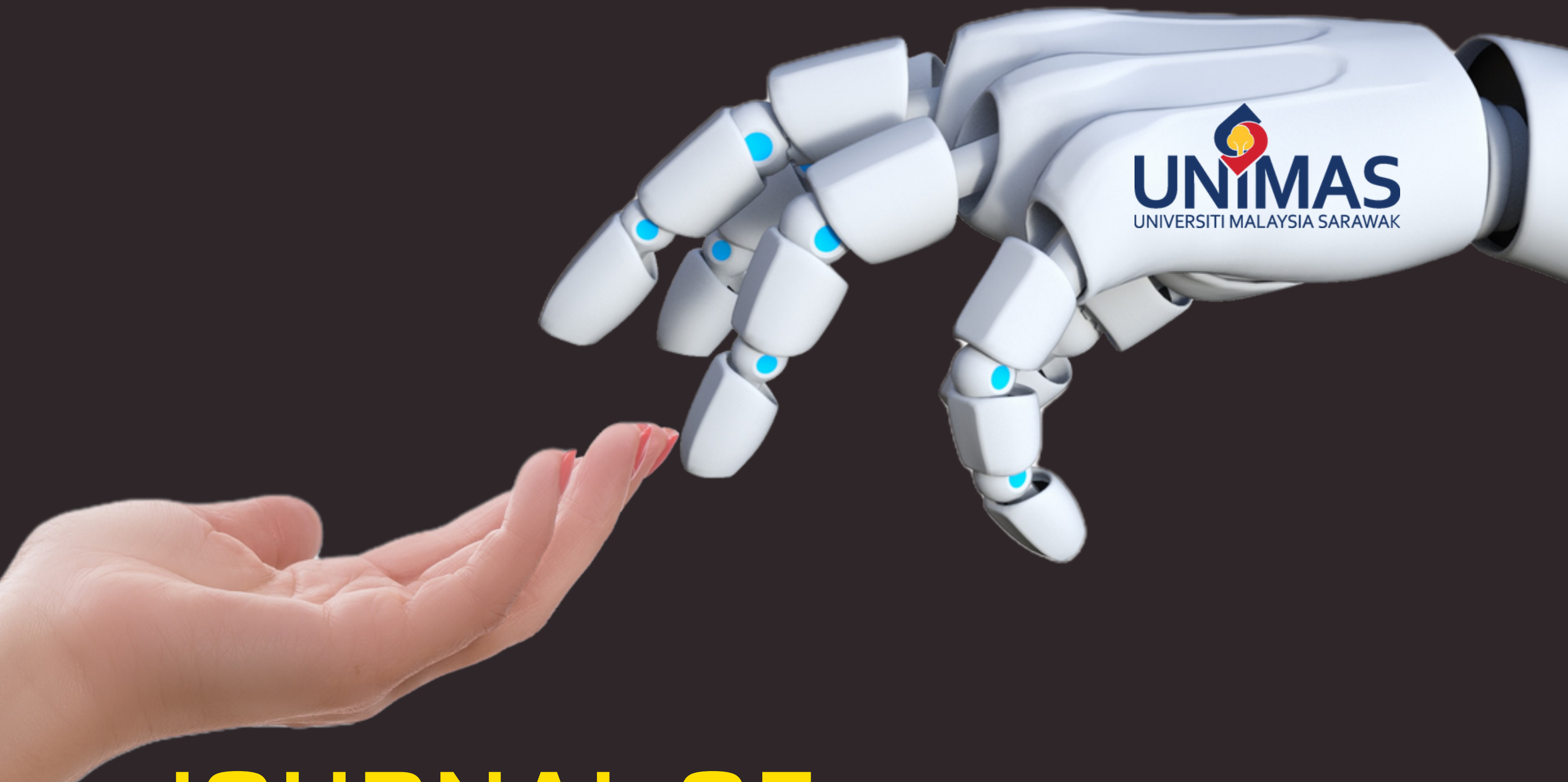


UNIMAS
UNIVERSITI MALAYSIA SARAWAK

JOURNAL OF COMPUTING AND SOCIAL INFORMATICS

FACULTY OF COMPUTER SCIENCE AND
INFORMATION TECHNOLOGY

UNIVERSITI MALAYSIA SARAWAK

eISSN 2821-3777
9772821377005

Editorial Committee

Advisory Board

Reviewers

Journal of Computing and Social Informatics

The Journal of Computing and Social Informatics (JCSI) is an international peer-reviewed publication that focuses on the emerging areas of Computer Science and the overarching impact of technologies on all aspects of our life at societal level. This journal serves as a platform to promote the exchange of ideas with researchers around the world.

Articles can be submitted via *www.jcsi.unimas.my*

Assoc Prof Dr Chiew Kang Leng

Chief Editor
Journal of Computing and Social Informatics
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
94300 Kota Samarahan
Sarawak, Malaysia

Contents

A Three-Tier Model for Intrusions Classification on a Computer Network

Sunday Samuel Olofintuyi

Department of Computer Science, College of Natural and Applied Science, Achievers University, Owo, Ondo State, Nigeria.

email: Olofintuyi.sundaysamuel@gmail.com

Received: 24 December 2022 | Accepted: 22 May 2023 | Early access: 22 Jun 2023

Abstract - *Activities of cyber attackers are on the rampage; this is because there is an increase in the usage of computer related applications. Attackers have caused reputational and economic damages to network administrators, companies and industries based on the information they have stolen. To curb all these activities, a formidable Intrusion Detection System (IDS) is needed to guide against all the numerous cyber-attacks. The research work solely aimed at reducing the accessibility of cyber threats by bringing its operations to as minimal as possible because of the adverse effects they have had in the past. This research proposed a three-tier IDS which classifies the various attacks into their various groups. The proposed model consists of Bayes Network (BN), Support Vector Machine (SVM), and Artificial Neural Network (ANN). NLS KDD 99 dataset was used for simulating the proposed three-tier IDS in the WEKA environment. The effectiveness and efficiency of the proposed model was based on recall, precision, and accuracy. The proposed three-tier model gave the following results: recall: 0.993; precision: 0.979; accuracy: 0.986.*

Keywords: Classification, Intrusion Detection System, Cyber-attacks, Machine Learning, Cyber Security.

1 Introduction

The advent of Internet of Things (IoT) has generated more activities of cyber-attacks on the network and the tremendous usage of computer applications by user has also increase cyber threats on a computer network. Companies, industries, and various sectors of the economy have suffered a serious setback because of the devastating effects of cyber-threats. Also, measures have been put in place by companies, industries, research institutes, government, and network administrators to curb all these cyber-attacks but all effort seem not enough (Olofintuyi, 2021). In 2010, there were about 50 million malwares, and in less than 3 years, the number of malwares has increased to about 100 million. Unexpectedly, by the year 2019, the number of malwares have skyrocketed to about 900 million cyber threats (Sarker et al., 2020). Morgan (2021) predicted in his work that by the year 2021, the global crime rate will cost about $6 trillion USD and $10.5 trillion by the year 2025. Recently, First America records that about 900 million records were compromised and the account of American Medical Collection Agency (AMCA) was hacked and the attackers were able to gain access to their account and record for almost a year (Hao et al., 2020). Hardware and software firewalls, user's authentication and data encryption are some of the mechanisms that have been adopted to curb the activities of intruders. Unfortunately, all these mechanisms seem not robust enough for effective and efficient guidance against these cyber-threats (Mohammadi et al., 2019). For instance, a firewall only gives signal when communication takes place between two or more networks, but it doesn't give any signal for any form of internal attacks. With this, a more secure, robust, and accurate Machine Learning (ML) based IDS is needed for the safety of the system. IDS is a system that detects inconsistencies, attacks, irregularities, infectious activities, and any form of abnormalities on a network such as Root to Local (R2L), Denial of Service (DoS), User to Root (U2R) and probe (Olofintuyi & Omotehinwa, 2021). IDS is also suitable for classifying the various threats into their respective classes using either Machine Learning or statistical methods. The following metrics: True Negative (TN), False Negative (FN), True Positive (TP) and False Positive (FP) were used to evaluate the aforementioned algorithms. Obtaining optimum results for all the metrics at the same time seem impossible because each metric is dependent on each other. The big challenge comes in when striking the balance between them (Hao et al., 2020). The various classes of threats can be identified and grouped into their various classes by a data driven IDS. This is possible when IDS analyzes the patterns in the cyber threat and then categorizes them into various classes. ML algorithms are needed to build data driven IDS. However, different ML predicts based on their context hence, each algorithm classifies threats on the network to different groups based on their context (Alqahtani et al., 2020). Based on the pertinent reasons, a three layers model has been proposed for classifying the dataset into threats and benign to reduce the false negative and overall increase the accuracy. Efficiency and effectiveness of the proposed three-tier model is evaluated based on Recall, Precision, and Accuracy. The next section discusses the review of literature, methodology used, result obtained and conclusion.

2 Literature Review

Activities of cyber threats differ on the computer network because of this: an IDS system is needed to classify each threat to their respective classes (Stallings, 2003). Generally, IDS can be broadly classified into two types which are Anomaly Based Intrusion Detection System (AIDS) and Signature Intrusion Detection System (SIDS) (Lin et al., 2013). AIDS detects threats based on the new pattern established by the system. AIDS generates a new model with a new pattern which is capable of detecting any unknown threat (Buczak & Guven, 2016). Operation of SIDS is quite different from AIDS. SIDS classifies threats based on known patterns. SIDS cross checks the pattern of the threat on the network against the patterns of the event known and then classifies each activity to their respective groups. SIDS is effective and efficient when it comes to classifying known attacks but it is ineffective at classifying unknown attacks. A good example of SIDS is an expert system developed in mid-1960 (Liao, 2005). Machine learning and statistical methods have been the major approaches used for classifying threats under the anomaly-based intrusion detection system. Operation of statistical methods is based on assumption whether a particular situation is normal or abnormal. Also, there is inconsistency in the assumption made with the statistical method and because of this, the parameters are not easily determined (Zhao, 2020). Machine learning algorithms such as Support Vector Machine (SVM) (Shams & Rizaner, 2018), ANN (Olofintuyi et al., 2019) BN (Sarker et al., 2020) and clustering (Lin & Ke, 2015) have played a vital role in IDS but there are some loopholes in their operation and this is not far-fetched from the fact that each classifier predicts base on their context (Sarker, 2019; Olofintuyi & Olajubu, 2021).

Vapnik and Corinna (1995) were the first to propose SVM, and since then, many other researchers have used it for threat classification on the computer network. Aslahi- Shahri (2006) proposed a hybrid model of support vector machine and genetic algorithm for threat detection on the network. KDD99 dataset was used for model simulation and an accuracy of 97.3% was derived. Also, to solve the problem of low detection rate, Pozi et al., (2016) proposed a hybridized approach for classifying threats. The hybridized model consists of SVM and genetic programming and accuracy of 89.28% was achieved. Horng et al., (2011) presented a novel hybridized model which consisted of SVM and hierarchical clustering. KDD99 dataset was also used and an accuracy of 95.7% was achieved.

Another powerful machine learning algorithm used is Decision Tree (DT). DT uses a sequence of decisions to classify events into their respective classes. DT adopts a tree-like approach for classification. Rahman et al., (2010) uses DT for threats classification on the computer network; KDD99 dataset was also used for model simulation and an accuracy of 98% was derived. Sahn and Mehtre (2015) also used J48 for threats classification; Kyoto 2006+ dataset was used for model simulation. After the experiment, 97.2% accuracy was achieved.

Gang (2010) achieved 96.71% accuracy on NSL-KDD data using neural network and clustering algorithms. Also, Mansour et al., (2012) presented a recurrent neural network for intrusion detection; the performance evaluation was based on KDD dataset and an accuracy of 94.1% was obtained. Long Short Term Memory Recurrent Neural Network (LSTM-RNN) was proposed by Jihyun et al. (2016); LSTM-RNN was used to classify the event on the network and 93.93% accuracy was achieved using the KDD dataset.

3 Methodology

A sequential three-tier model is proposed because a single classifier is limited when it comes to detecting the entire negatives. The proposed workflow was adopted to reduce the False Negative (FN) and then improve the overall accuracy. Also, it was adopted to know the effectiveness of increasing classifiers on the network. NLS-KDD 99 dataset was used in model building and simulation in Waikato Environment for Knowledge and Analysis (WEKA). The three-tier model consists of Bayesian Network (BN), Support Vector Machine (SVM), and Artificial Neural Network (ANN). Firstly, NSL-KDD 99 is fed into the proposed model, BN classifies the event as either threats or benign. Benign from the first classifier are reclassified to detect the false positive and false negative and overall improve the accuracy. Once classified as threat, the administrator tagged such traffic as threat. But we are more concern about the benign because there are still some elements of threats in it. This is so because of the weakness of the classifiers. This approach is adopted because of the context of each machine learning algorithm; bearing in mind that FN must be at the minimal level to protect the network administrator. The benign output is forwarded to SVM which also classifies the event into threat or benign. The output from SVM is fed into ANN. At this stage, ANN re-classifies the threats and benign to reduce the FN in the dataset. Figure 1 depicts the flowchart for the proposed model.

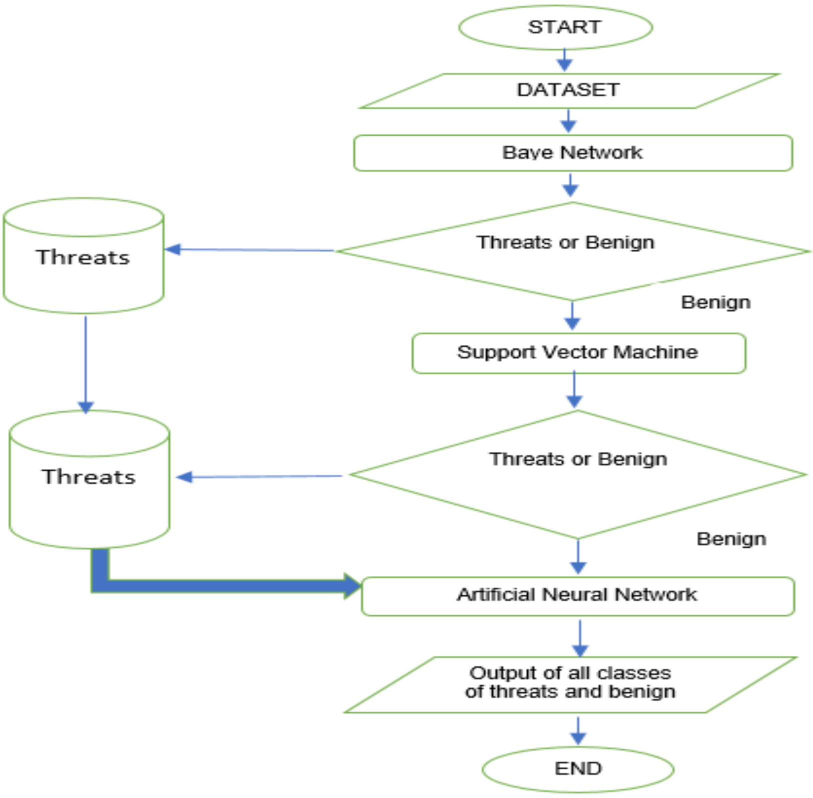


Figure 1: Flowchart of a Three-Tier Model

3.1 Dataset

NSL KDD 99 dataset was obtained online, the dataset is an extract from KDD99 dataset. NSL KDD99 dataset does not contain any redundant and irrelevant features. The dataset has forty-one (41) attributes and the dataset has five classes which are; DoS, Probe, U2R, R2L and benign. Table 1 depicts the forty-one features of the dataset used.

DOS: DoS is the first group of threats considered in this research work. The aim of this threat is to shut down the network so that intended users which are legitimate will not have access to it. Traffic is used to flood the target to get this task accomplished. Examples include SYN Flood, Ping of death, Back, Land, Process table, Mail tomb and Apache 2.

Probe: The first line of action of the probe is to obtain vital information from the network after which it launches its attacks. Examples include Mscan, Nmap, Satan, saint and Ipsweep.

Root to Local: The system becomes vulnerable when packets of data are sent by the attackers and the end user accepts it. Examples include Xlock, Dictionary, Imap, FTP Write and Guest.

User to Root: U2R gained access to the system in disguise to be legitimate users. These groups of threat explore the vulnerabilities of the system once they have gained access to the system. Examples include Perl, Xtem, Loadmodule and Fdformat.

Table 1: The forty-one features of the dataset

No	Feature name	Types	NO	Feature Name	Types	NO	Feature name	Types
1	Duration	Continuous	15	Su_attempted	Continuous	29	Same_srv_rate	Continuous
2	Protocol type	Symbolic	16	Num_root	Continuous	30	Diff_srv_rate	Continuous
3	service	Symbolic	17	Num_file creation	Continuous	31	Srv_diff_host_rate	Continuous
4	Flag	Symbolic	18	Num_shell	Continuous	32	Dst_host_count	Continuous
5	Scr_bytes	Continuous	19	Num_access file	Continuous	33	Dst_host_srv_count	Continuous
6	Dst_bytes	Continuous	20	Num_outbound_ cmds	Continuous	34	Dst_host_same_srv_rate	Continuous
7	Land	Symbolic	21	Is_host_login	Symbolic	35	Dst_host_diff_srv_rate	Continuous
8	Wrong fragment	Continuous	22	Is_guest_login	Symbolic	36	Dst_host_same_src_port_rate	Continuous
9	Urgent	Continuous	23	count	Continuous	37	Dst_host_srv_diff_host_rate	Continuous
10	Hot	Continuous	24	Srv_count	Continuous	38	Dst_host_serror_rate	Continuous
11	Num_failed login	Continuous	25	Serror_rate	Continuous	39	Dst_host_srv_rate	Continuous
12	Logged_in	Symbolic	26	Srv_serror_rate	Continuous	40	Dst_host_srv_serror_rate	Symbolic
13	Num_compropmised	Continuous	27	Rerror_rate	Continuous	41	Dst_host_serror_rate	Symbolic
14	Root_shell	Continuous	28	Srv_rerror_rate	Continuous			

3.2 Bayes Network (BN)

BN is the first algorithm used on the three-tier model. NSL-KDD 99 dataset was fed into the algorithm, and the algorithm then classifies the dataset into two categories as either threat or benign. Threats are malicious activities that aim to intrude into the network and steal vital information while benign are activities that are not harmful to the computer network.

3.3 Support Vector Machine (SVM)

This algorithm classifies the output from the BN. Although BN has classified the output as benign, because of the different content of how each algorithm classifies, SVM is used to re-classify the output again as either threat or benign. SVM classifies each point in the space into various categories using a hyper-plane.

3.4 Artificial Neural Network (ANN)

ANN is the third algorithm used to classify the dataset into threat or benign. ANN has basically three components which are the input, hidden, and output layers. Output from SVM and database of threats serves as input into the input layer of ANN. The hidden layer performs its operation by using sigmoid activation function. The output layer classifies each group into their respective classes as depicted in Table 2.

Table 2: Threat/Benign classification based on their group

S/N	Attacks/Benign	Different attacks	Output
i	Denial of service attack	Mail bomb, Ping of death, Land, SYN, Process table Flood, Back and Land.	00001
ii	Root to local	Xlock, Guest, Dictionary, write, Imap and FTP	00010
iii	User to root	Xterm, Fdformat, Loadmodule and Perl.	00100
iv	Probes	Mscan, Saint, Ipsweep, Satan and Nmap	01000
v	Benign		10000

3.5 Performance Evaluation

The proposed three-tier model was validated after experimental simulation with the following metrics:
False Positive: This classifies events that are negative as positive wrongly.
False Negative: This metric misclassifies positive events as negative.
True Positive: Report events that are positive correctly
True Negative: Report events that are negative correctly
Recall: Completeness and quantity of the model are being measured by this parameter. Equation 1 depicts the formula for recall.

$$Recall = \frac{TP}{TP+FN} \tag{1}$$

Precision: This described the exactness and quality of the proposed model. Equation 2 depicts the formula for precision.

$$Precision = \tag{2}$$

Accuracy: This described the effectiveness of the proposed model. Equation 3 depicts the formula for accuracy.

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN} \tag{3}$$

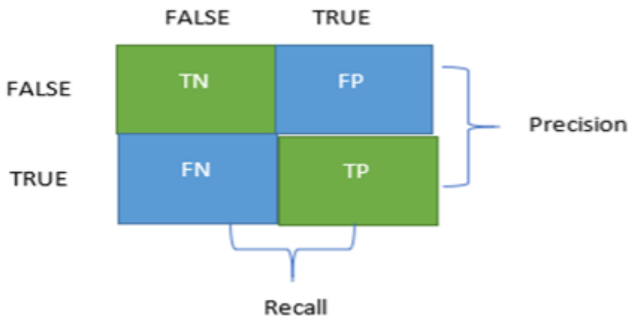


Figure 2: Confusion matrix for evaluation

3.6 Experimental Setup

The whole experiment was carried out in a WEKA environment. The dataset (NSL-KDD 99) used has no redundant and irrelevant features because it is an extract from KDD 99 dataset. The dataset was firstly saved in CSV format and later converted to arff format. This is done because that is the format WEKA recognizes in order to accept the dataset for simulation. 10-fold cross validation was applied during simulation, where the dataset was partitioned into ten samples. 9 of the samples were used for model training while the remaining one was used for testing. Finally, the performance of the three-tier model was based on how the model was able to correctly classify instances. In the experimental setup, three different classifiers were selected and combined so that we can produce low FN. In adding a new classifier to the first, we carefully select a model that produces low FP and FN so that we will be able to achieve a low overall FN for the three-tier model. By adding new classifiers, we expect that each added classifier should improve on the limitation of the first and overall improve the accuracy. The proposed model adopts three classification steps. Firstly, the model was created and classification was done by the models. In the training phase, 10-fold cross validation was used to avoid overfitting and the best model was selected based on the turning parameters. Immediately after the training phase, the classification begins. For each of the classifier, the testing data is fed into it. The intention of the researcher is to reduce FN by detecting the negatives from each benign classified. The positive output from BN is forwarded as input into SVM. Also, the positive output from SVM is fed into ANN which does the final classification.

4 Results and Discussion

The first algorithm used for classification in the first layer is BN. The algorithm correctly classified 50,588 instances and wrongly classified 8689 instances. The following results were obtained from the first layer after simulation: recall: 0.790; precision: 0.871; accuracy: 0.8534. For the second layer, SVM algorithm was used, and it classified 58119 instances correctly and 1158 incorrectly. The following results were obtained from the second layer: recall: 0.978; precision 0.978, accuracy: 0.9804. ANN was used for the third layer and 58505 instances were correctly classified while 772 were incorrectly classified. The following results were obtained for the third layer: recall: 0.993; precision: 0.979; accuracy: 0.9869.

From Table 3, the first layer (BN) produced an FN of 5599 instances and an accuracy of 85.34% which is not too satisfactory for an administrator. And because of this, another classifier (SVM) was introduced which reduced the FN drastically to 579 instances and produced an accuracy of 98.04 %. To further improve the FN and accuracy, another classifier (ANN) was used, and the final FN gave 193 instances while 98.69 % accuracy was achieved. This shows that using a combination of classifiers can drastically improve the FN and accuracy as compared to a single classifier. The three-tier model reduces the FN from 5599 instance for the first layer to 579 instances in the second layer and 193 instances in the third layer of the model. It is suspected that the difference in the FN between the first layer and the second layer is 5020 instances. This is suspected to be so because the first layer actually does the classification as threat or benign. It is benign that is passed to the second classifier to check and reclassify if there is other malicious traffic in the benign so that it can reclassify. Finally, ANN does the final classification and gave an improvement of 386 FN as compared to the second layer and 5406 FN as compared to the first layer. Table 3 depicts the results of the different three layers. From the table, layer 3 of the model gave a better accuracy compared to the respective two layers. Figure 3 depicts the bar chart of the three-tier model.

Table 3: Evaluation Table for the three-tier model

Layers	Instances	TN	TP	FN	FP	Recall	Precision	Accuracy
Layer 1	59,277	29543	21045	5599	3090	0.7902	0.8712	0.8534
Layer 2	59,277	32054	26065	579	579	0.9781	0.9781	0.9804
Layer 3	59,277	32054	26451	193	579	0.9933	0.9792	0.9869

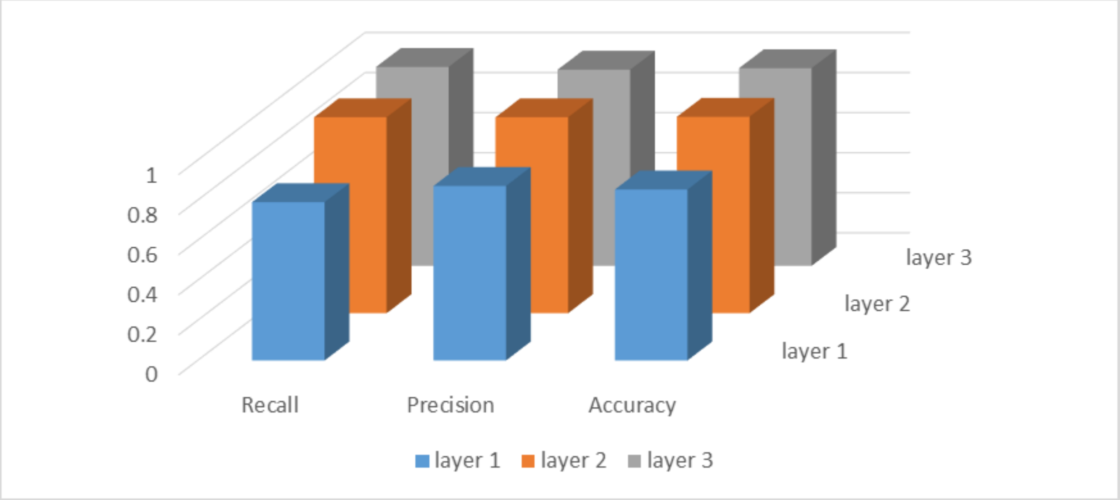


Figure 3: Chart to depict the evaluation results for the three-tier model

5 Conclusions

Detection rate of each algorithm differs and this is based on the context of each of the algorithms. Also, there are various categories of cyber-attacks on the network which some of them have outplayed some of the mechanisms put in place to curb them. It is with this reason, that the study proposed a three-tier model. The proposed three-tier model will reduce activities of threats in companies, industries, IT offices and government parastatal if fully deployed. Finally, the proposed model gave 97.92% precision, 99.33% recall. And 98.69% accuracy.

References

Alqahtani, H., Sarker, I. H., Asra K., Syed Md. Minhaz, H., Sheikh I., & Sohrab H. (2020). Cyber Intrusion Detection Using Machine Learning Classification Techniques. *Springer Nature Singapore*, CCIS 1235, pp. 121–131.

Aslahi-Shahri, M. (2016). A hybrid method consisting of genetic algorithm and support vector machine for intrusion detection system. *Neural computing and applications*, 27(6):1669-1676.

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE* Communications Surveys and Tutorials.

Chen, Y. H., Horng, S. J., & Su, M., Y. (2011). A novel intrusion detection system based on hierarchical clustering and support vector machines. *Expert systems with Applications*, 38(1):306-313

Gang, M. (2010). A new approach to intrusion detection using artificial neural networks and fuzzy clustering. *Expert systems with applications*, 37:9.

Harbi, N., Rahman, C. M. & Farid, D. M (2010). Attacks classification in adaptive intrusion detection using decision tree. *World academy of science, engineering and technology*, 39:86-90.

Hao, Z., Feng, Y., Koide, H. & Sakurai, K. (2020). A sequential detection method for intrusion detection system based on artificial neural networks. *International Journal of Networking and Computing*, 10:213-226

Liao, S H. (2005). Expert system methodologies and applications|. A decade review from 1995 to 2004. *Expert systems with applications*, 28(1):93-103.

Lin, C. H., Liao, H. J., & Lin, Y. C. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16-24.

Lin, W. C. & Ke, S. W. (2015). An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based system.

Mohammadi, S., Mirvaziri H., Ghazizadeh-Ahsaee, M. & Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Application*, 44:80-88

Morgan, S (2021). Cyberwarfare in the suite. Cyber security magazine. Publish by cybersecurity ventures.

Mustapha, N., Pozi, M., & Sulaiman, M. (2016). Improving anomalous rare attack detection rate for intrusion detection system using support vector machine and genetic programming. *Neural Processing Letters*.

Olofintuyi, S.S. (2021). Cyber Situation Awareness Perception Model for Computer Network. *International journal of advanced computer science and application*. 12(1):392-397.

Olofintuyi, S.S. & Olajubu, E.A (2021). Supervised Machine Learning Algorithms for Cyber-Threats Detection in the Perception Phase of a Situation Awareness Model. *International Journal of Information Processing and Communication*, 11(2): 61-74.

Olofintuyi, S.S. & Omotehinwa, T.O. (2021). Performance Evaluation of Supervised Ensemble Cyber Situation Perception Models for Computer Network. *Computing, Information Systems, Development Informatics and Allied Research Journal*. 11(2):1-14.

Olofintuyi, S.S., Omotehinwa, T. O., Odukoya, O.H. & Olajubu, E. A. (2019). Performance comparison of threat classification models for cyber-situation awareness. Proceedings of the OAU Faculty of Technology Conference, 305-309.

Ozgur, A. & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. Peer Preprints, 4.

Sahu, S. & Mehtre, B. M. (2015). Network intrusion detection system using J48 decision tree[c]. International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2023-2026.

Sarker, H. Abushark. Y., Alsolami, F. & Khan, A. (2020). Intrudtree: a machine learning-based cyber security intrusion detection model. Symmetry, 12:754-761.

Sarker, H. (2019). A machine learning based robust prediction model for real-life mobile phone data. Internet of Things, 5:180-193.

Shams, E. A., & Rizaner, A. A. (2018). A novel support vector machine-based intrusion detection system for mobile ad hoc networks. Wireless Networks.

Stallings W. (2003). Cryptography and network security: principles and practices.

Thu, H. L., Kim, J., & Kim, J. (2016). Long short term memory recurrent neural network classifier for intrusion detection. 2016 International Conference on Platform Technology and Service (PlatCon).

Vladimir, V. & Corinna, C. (1995). Support-vector networks. Machine learning, 20(3):273-297.

Zahra, J., Mansour, S., & Ali, F. (2012). Intrusion detection using reduced-size recurrent neural network based on feature grouping. Neural Computing and Applications, 21:6.

Zhao, H., Feng, Y., Koide, H., & Sakurai, K. (2020). A sequential detection method for intrusion detection system based on artificial neural networks. *International Journal of Networking and Computing*, 10:213-226.

Facial Recognition Technology on Attendance Tracking

1*Shalin Binti Shaheezam Khan, 2Hamimah Ujir, 3Muhammad Quazy Bin Razali and 4Sarfiza Binti Othman@Osman

1,2,3,4Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: 1*shalinshaheezamkhan@gmail.com, 2uhamimah@unimas.my, 3jiejierezalius@gmail.com, 4osarfiza@unimas.my

**Corresponding author*

Received: 18 March 2023 | Accepted: 22 June 2023 | Early access: 29 August 2023

Abstract - *Numerous airports have opted to replace traditional check-in systems with advanced Attendance Tracking technology that incorporates face recognition. This paper presents the findings of a research study conducted among individuals aged 20 to 60, currently employed in either government or private sectors. The results shed light on the respondents' attitudes towards and acceptance of this advanced technology, as well as its effectiveness. Technology Acceptance Model (TAM) is implied together with Perceived System Quality (PSQ) in this study. Perceived ease of use (PEOU), perceived usefulness (PU), attitude (ATT), behavioral intention to use (BI), and actual system use are also included in measuring the effect. The outcomes of this investigation indicate a wide acceptance of this technology, particularly in the context of attendance tracking systems. The respondents demonstrate a favorable attitude towards the integration of face recognition technology in various aspects of their lives. The survey encompasses several key components, namely demographic information, awareness of facial recognition technology, and perceptions of system quality. These results provide insights into the viability and acceptance of face recognition technology, validating its potential implementation in attendance tracking systems.*

Keywords: Attendance Tracking, Facial Recognition Technology, Acceptance Status, Threats, User Behavior.

1 Introduction

Biometric identification technology employs a continuous image frame from a video source or a digital image to identify or authenticate a person. It is mainly focused on use case that may individually identify a person by suggesting patterns from facial data and is also known as biometric artificial intelligence (AI). An efficient identity management system is necessary for the successful implementation of an attendance management system. Additionally, the fields of machine learning and computer graphics are becoming interested in facial recognition. Face recognition using image processing to recognize and extract facial traits such as the nose, mouth, and eyes is known as feature-based face recognition. Apart from face recognition, facial expression technology is also a form of biometric technology. This technology is capable of recognizing facial expressions as well as the intensity of those expressions (Alicia et al., 2017). In comparison to other solutions, biometric ones require almost minimal user effort because the technology is steadily developing into a universal biometric approach. Among other methods, face recognition is a more precise and effective technology that lowers the possibility of proxy attendance (Kar et al., 2012). However, this application as mentioned by He et al., (2020) as heterogeneous face recognition allows you to use computer vision and machine learning to find the best match between a user's facial features and available images of people. It can be used in a variety of applications, including registrations at events or in stores that require the user to show their face, or for login and other secure access procedures where facial verification is required. Finally, facial recognition is entirely non-intrusive, protecting the user from any viruses that might be present in a system with many users (Okokpuie et al., 2017). In most cases, the static face recognition result depends on the facial characteristics of the algorithm's processing, but in practical applications, such as traffic control and security, this will also influence the face recognition system according to real-time use. In a face recognition system using a static face recognition algorithm and hardware, we should not only carry out the static test of the algorithm but also carry out dynamic test algorithms on actual faces (He et al., 2020).

Facial recognition technology is a biometric recognition based on human face data. The facial recognition software is built on machine learning for identifying people, where the number of times that a person is checked and compared (the scanning time) will be small. Facial recognition technology is applied for many fields such as cashless payment, identification, ticketing, and security applications. By using this technology, employers can improve efficiency while reducing costs of time and training by eliminating error. Face recognition technology has both potential benefits and drawbacks. The positive attributes of this technology include being able to accurately track criminals or victims of crimes by recognizing their faces, verifying identity, or even in cases of identification such as corporate access. Face recognition can also be used for fraud detection when checking bank statements or other documents. However, problems arise from these uses as well; for instance, privacy implications on the part of individuals who are tracked via their facial features make it difficult for them to live freely and peacefully when these points are logged into databases that contain sensitive information about their identities and activities. System quality issues relate to how a system works, with the result that an organization achieves a certain standard. The perceived system quality (PQS) has been employed in this study to gather data and information from users. Perceived system quality (PQS) has been used in this study's survey to gather information and data from the study's target user. This survey was applied on a high-tech research platform to receive answers from the target user. This survey address user's judgment and evaluation of facial recognition technology in terms of their perceived system quality (PSQ), which can help us understand how important user's perception of quality is before they make a selection or decision on whether or not they want to use facial recognition technology.

As the use of face recognition expands, keeping an accurate attendance record becomes a challenge. Facial recognition helps to reduce the cost associated with timekeeping and attendance tracking by providing a quick, reliable and accurate method of tracking employees as well as access control for equipment or facilities that require proof of authorization. In context, the current time and attendance tracking system is currently used by most companies as a primary medium for tracking the attendance of workers. The global facial recognition market was valued at USD 3.78 billion in 2020 and is expected to reach USD 10.2 billion by 2028, rising at a compound annual growth rate (CAGR) of 15.92% from 2021 to 2028, according to data provided by (Aaron Raj, 2021). There has been a tremendous increase in demand for facial recognition systems in Malaysia. The market for these systems is expected to reach USD 8.5 billion by 2025, according to the author of this report. This will lead to a decent work environment, as well as positive economic growth for an organization (Aaron Raj, 2021).

The use of face recognition in Malaysia will affect users' privacy. Some companies are considering this technology but there are some organizations that are still questioning its advantages and disadvantages, especially the possibility of data breaches. There will be a possibility that this technology will lead to data vulnerabilities. A hacker may be able to access the data, and this would lead to a data breach. Based on a (Air Asia, 2018), Air Asia Group has introduced "FACES," a facial recognition feature which allows passengers to check in with their airline. As part of its stated vision of collaborative technology, Malaysia Airports Holding Bhd. has started rolling out this authentication process at Kuala Lumpur International Airport Terminal 1 and 2. This works by taking a 5-second video via the airport's integrated security cameras, which can be found throughout the airport. Once completed, all facial details will be sent back to the airlines through various forms of surveillance such as CCTV cameras, sensors, and facial recognition devices (Facial Recognition Market, 2018). This research paper also concluded that for this new way forward, we must ensure that privacy is taken into consideration before implementing any form of surveillance technology in airports.

The following are the study's research questions: [1] What is the technology-acceptance status of each organization? and [2] How does facial recognition technology give a huge impact on Malaysia's working system? To address the objectives, the following are the objectives: [1] Assess the technology acceptance status in Malaysia; [2] To evaluate the benefits and impact of this technology in Malaysia working system.

This research is built specifically for employed workers with at least 3 months of working experience in Malaysia. They may work in the public or private sectors. Real-time attendance monitoring and recording are made possible by facial recognition technology. The database will be instantly updated with the workers' attendance information, including their clock-in and clock-out times. This information is critical for an organization's efficiency and cost control, but existing technologies are not very accurate in monitoring accurate attendance records. This advanced technology will improve efficiency as well as accuracy of management, while it will also detect faces of workers to process the attendance record directly based on their time of detection.

This paper presents findings from the survey conducted on the acceptance for attendance tracking using facial recognition technology among the workers in Malaysia. Section 2 describes the related works in this field. We present data collection, data pre-processing, and our framework in Section 3, followed by the experiment setting, results, and analysis in Section 4. Finally, the conclusions are drawn.

2 Literature Review

Article Alhussain et al., (2010) analyses the results of exploratory research on government employees' reactions to the adoption of biometric verification at work in Saudi Arabia. It suggested that researching the elements that influence employees' acceptance of new technology will aid biometric technology adoption in other e-government applications. The relevant data were gathered using a combination of surveys and interviews. The findings of this study reveal a large digital and cultural divide between employees' technical awareness and management's chosen authentication options. The managers' need to evaluate their duties for closing these gapsis reflected in a lack of faith in technology, its potential for misuse, and management motives. It became clear that overcoming employee resistance to biometric deployment is a critical challenge.

According to Brömme et al., (2013), biometric technology has been demonstrated to be dependable and secure in the field. In their work, the results of a comprehensive survey on social acceptance of biometric technologies in Germany are presented. A total of 140 people participated in the survey, providing a representative investigation of residents' attitudes regarding biometric technologies. According to the survey, despite numerous deployments on large-scale systems, biometric applications raise privacy concerns, resulting in arguments over the social and ethical acceptance of biometrics reaching new heights.

Article Zhang et al., (2019) explain factors that affect the use of facial-recognition payments by the Chinese consumer. This paper explains how the nature of the facial-recognition payment system was chosen as an independent element in this paper's model. In this study, four important independent characteristics were chosen based on other experts' research on the willingness to accept new technologies. Perceived usefulness was used as a final dependent variable after being used as an intermediate variable. The openness attribute was chosen as the moderating variable in this study to investigate the impact of consumers' characteristics on behavioral preferences. Consumers' personalities will impact their willingness to adopt new items and technology, according to the theory. To explore customers' willingness to accept new technologies, several studies combine a personality model and a technological acceptance model. In this strategy, transparency has a big impact. Openness has a significant influence on this model. Personality traits also have a strong effect on perceived utility and perceived ease of use, and the latter has considerable effects on behavioral intention to use the product, according to this article itself.

Different from Venkatesan et al., (2021) which explain and proposed the security to secure online payment through facial recognition and proxy detection with the help of TripleDES encryption. It presented a two-step authentication method for online transactions conducted via mobile devices. The major benefit is to makes use of proxy detection, which is implemented in image processing and will increase security during online transactions. The Face Net method is the proposed algorithm for face verification in this study. This approach embeds 128 face feature points and uses a Support Vector Machine (SVM) to include the proxy. The 128 feature points are computed using a triple loss function, and the features of each person's face will be classified using an SVM that maps the input into high-dimensional feature spaces. Face detection and recognition, SVM classifier, proxy detection, and encryption of the unique id created during the Face Net technique are the four primary stages in the proposed work. As we can see from both works, it focuses on payment using face recognition and securing the payment using face recognition. Article Zhang et al., (2019) explain the Chinese people's acceptance of using facial-recognition payment while another article proposed the secured framework to secure the payment used by this technology.

Article (Wang, 2021) describes how face recognition is used in national law enforcement and contrasts commercial applications in China and the US. In terms of the number of cameras per 100 persons, the United States is ranked 1, followed by China. It elaborates on the law enforcement government or agencies that monitor the public and mentions surveillance in using this technology which is already common in the world (Wang, 2021). Both China and the United States are working to develop the face recognition law system. Conflict between law enforcement agencies and the privacy concerns associated with facial recognition cannot be avoided by strict state regulation or law enforcement. The variety of applications for facial recognition, prevailing legal standards, and regional variations should all be taken into consideration. It should also be mindful of how face recognition and other forms of artificial intelligence are changing how society governs and what constitutes a person's right to privacy. The public's consciousness is also supporting policy change and responsiveness of the state power organization as education, global rational thinking, and individual self-consciousness improve. After the commercialization and wide-scale implementation of such systems, they increasingly encountered privacy issues, particularly due to concerns about racial biases in recognition techniques and the lack of legal framework for oversight on this technology's deployment (Liu et al., 2021). This is due to the privacy, public acceptance, and prejudice have been the main topics of discussion in the public about the response to facial recognition technology. As the privacy issue arise, this technology will be one topic will be debate by the public to ensure their privacy secured by the law.

Article Katsanis et al., (2021) created two questionnaires from paper to get the public's opinions on the usage of face photographs and facial recognition technology in healthcare and health-related studies in the US. Facial imaging and facial recognition technologies are being used more and more in the health care industry to precisely match patients, provide touch-free appointment check-in, and help with the diagnosis of some medical disorders. One survey instrument examined six different biometrics, such as facial images and DNA, and how they are used in a variety of societal contexts, such as healthcare and research, while the other examined the use of facial imaging, facial recognition technology, and related data practices specifically in health and research contexts. The results show that while the majority of research participants might feel comfortable using facial images and facial recognition technologies in healthcare and health-related research, a significant number of them expressed concern for the privacy of their own face-based data, much like how people feel about the privacy of their DNA and their medical records. It is necessary to take an advanced approach to face-based data applications in healthcare and health-related research, taking into account storage protection strategies and usage contexts.

The influence of body-worn video (BWV) on police observation, note-taking, investigative analysis, report-writing, and court-ready evidence is examined in this article (Bowling et al., 2019). It describes the technology's operation and considers how it may be used for regulatory, investigative, and probative purposes. The findings indicates that BWV cameras and analytics like facial recognition are revolutionizing enforcement tasks. Real-time facial recognition is possible with the newest BWV version. This will provide police access to a person's criminal history, any outstanding warrants, and other data. It may also be used to track where and when the police make contact with a specific person. It is obvious that BWV is automating a number of certain front-line policing jobs. A wide range of human activities are becoming automated at the same time as crime control is changing, and the police will need to adapt to a society that is much more mechanized. This study focused on the development of automated policing more broadly as a background thread and the foreground thread of BWV as a specialized technology. When taking into account the quick development of police robots and drones that utilize the same mobile video technology, vehicle number plate and person recognition analytics, and reporting capabilities discussed in this study, the impacts of these changes become more significant. The technological capabilities of police robots will be far more advanced to those of current technology, including continuous recording by several cameras that provide 360-degree vision in low and no-light conditions, thermal imaging, and the capacity to store many weeks' worth of video data. The implementation of video cameras into police uniforms allows a chance to consider public knowledge and attitudes of automated policing as well as the regulatory procedures needed to control it. It also gives an idea of how police robots will operate. The rising automation of fundamental police functions suggests a broad study agenda for social scientists and legal theorists that is concerned with issues surrounding the interaction of humans and machines in policing, law enforcement, and criminal justice.

In order to evaluate the application of biometrics at airports and pinpoint the difficulties encountered, this article evaluates the Biometric Exit Programme (Khan et al., 2021). An evaluation of Dublin Airport's face recognition boarding gates and Entry Exit Programme has been conducted. The benefits and difficulties of utilizing biometric technology at airport border controls are discussed in this article, with a specific focus on the U.S. CBP's Biometric Entry-Exit Programme. Long wait times at U.S. ports of entry demonstrated the need for improved operational efficiency. It was obvious that a biometric system was required in addition to the legal prerequisites for biometric implementation. The long wait times point to congested spaces and long lines, neither of which are ideal in a pandemic environment. As a result, researcher are aware of the significance of biometrics at border control and airport security checkpoints since they are touch less, speed up processing times, and minimize crowding. Both the face recognition boarding trial and the entry-exit programme at the US preclearance facilities at Dublin Airport were inspected and examined in order to find problems and gauge accuracy. Results indicated that the overall rate remained high even with an increase in the number of passengers. Results from the biometric e-gate study run in cooperation with American Airlines revealed a significant reduction in the time needed to board passengers using facial recognition. To get a deeper understanding of the difficulties and problems faced, industry specialists in charge of biometric programme, including CBP's entrance departure programme, were interviewed. Pilot testing at U.S. airports revealed that, in order to maintain punctual aircraft departures, airline authorities had to return to conventional boarding procedures due to a lack of CBP agents and a reduction in authorized boarding time. To meet operational expectations, such as quick passenger processing, timely aircraft departure performance, and minimizing inefficiencies brought on by system outages, a reliable network connection must be built. Algorithms must be continuously improved to increase match rates that take both age and quality into account. By simplifying the procedure and removing congestion in the passenger flow, this can provide increased operational effectiveness and user satisfaction. The development of an enforcement system will guarantee that the biometric procedure is used consistently in every circumstance. As the research has shown, a lot of tourists worry about their privacy, mostly because they are unaware of the issues. They will be more willing for cooperation if they are aware of the advantages that come with it. The respondents noted that the biometric technologies maintain privacy. For instance, instead of being delivered as the actual picture, templates which a collection of encrypted binary digits that can't be decoded back into the original image instead serve as security.

Airport technology is being created in several forms to provide travelers with a smoother, faster, safer, and more effective process (Negri et al., 2019). Through a discrete choice model, specifically the binomial logit, this research explores the possibility of using biometric technology in check-in procedures—technology that is non-existent in Brazilian airports. 82.94% of passengers said they would use this new technology, according to research that used a database of 760 passengers who had been surveyed at three separate airports in Brazil. The goal of this study is to examine the probability that airport technologies, more specifically biometric technology for the check-in process, will be used during the study phase. It is important for the airport operator to understand how much these investments could improve the overall quality of service because introducing new technologies might be expensive in terms of initial investment. Another questionable issue is whether it is desirable for the operator to perform studies before the insertion of the technology in order to identify whether the passenger has a tendency to use it or not, given the quick technological advancement at airports. Due to the technology's insertion and the user's refusal to accept it, it may result in interruptions that were not anticipated given the technology, including excessive queuing. It was important to develop an experimental design connected to the technique of stated preference in order to react to the study's purpose. International Airport of So Paulo/Guarulhos, International Airport of Campinas/Viracopos, and Airport of So Paulo/Congonhas were the airports where the questionnaires were administered. To create a more thorough analysis of the context of Brazilian airport travelers, data from the three airports were obtained. The three airports under study are also among the ten busiest in Brazil in terms of both annual passenger volume and aircraft traffic. It was determined that there is a high likelihood that travelers will use biometric technologies for the check-in process. The results of the complete data set represent a usage rate of 82.94% of the technology. The results of the analysis were then confirmed for each passenger profile, including those who were travelling for leisure or business, as well as for different age groups, income levels, and genders. Additionally, this research may be useful to industrial designers when they negotiate with airport operators and select equipment features that will be more acceptable to passengers. Faster equipment, stronger operating systems, and pleasing display designs are preferred by travelers. In light of passengers' preferences for using the airport technologies under study, this research offers a contribution to the scholarly literature as well as a contribution to the airport operator.

Article Zaharia et al., (2018) discusses developments in airport digitization, the framework for implementing total airport management, and the modifications to airport management brought about by new implementation strategies. As part of their analysis of the technological difficulties brought on by the equipment needed for the digital transformation of Romania's Henri Coandă Airport, the researchers also make suggestions for the check-in area, security, customs control, departure control, and passenger assistance services. Finally, the effects of applying the suggested technology, particularly on the passenger experience, will be assessed. The two issues that are highlighted are boarding and border control. The border control section of Henri Coandă International Airport consists of 13 counters, each with two checkpoints, according to the Bucharest National Airport Company (CNAB). It is possible to suggest replacing half of these control points with biometric passage gates in order to improve the airport's capacity for processing passengers. Because they would only be accessible to travelers from the EU with biometric passports, researcher decided to replace only half of these checkpoints. The hypothesis put forth by the researcher takes into consideration a bordering control zone with 13 traditional checkpoints and 13 biometric entry gates. In this instance, deploying biometric technologies based on facial recognition will result in an increase of about 62.5% in processing capacity. According to the researchers' research, the longest waits, the worst internet connections, and the need to stay informed about boarding times or potential gate changes are the most inconveniences that travelers face in the boarding area. Passengers typically stay at the boarding area for 30 minutes. Boarding time can be cut in half by employing an automatic boarding system. For the purposes of this case study, the most popular types of aircraft at Henri Coandă Airport—which average 150 passengers every flight—will be used as a point of reference. In the near future, HCIA will use automatic gates as the norm because of their greater throughput rate. This will also reduce aircraft stopovers, allowing for an increase in aircraft movements. Nevertheless, only one or two of the boarding gates in the terminal would now benefit from this technology. The study discusses the changes in ITC, education, training, and marketing management, with social responsibility in management serving as a strong pillar. It also gives a general trend on operational management on airports, with a focus on HCIA. The airport under study is required to come up with and implement ways of accommodating the increasing number of passengers due to the demand on the Romanian air transport market. Although the development of a new terminal is an option considered by HCIA, the directorates suggested in the paper involve embracing new technologies for the automation of specific air transport processes. In their analysis of the HCIA survey, the researchers found a gap between management and technology, showing a very low level of digitization and proving that employees is not prepared to handle the difficulties of emerging technologies. Furthermore, the study's assessment of the organizational cultures of all market participants revealed a significant impact on the efficiency of operations, impacting advancement and impacting the level of digitalization. The researchers believe it is crucial for HCIA to have a digitization department since technology advancement in aviation ensures a rise in efficiency, opening up new perspectives on the nature of operations management. The development of the managerial directions suggested in the current article is intended to optimize airport operations and modify them in accordance with emerging air traffic and technical trends.

The design and implementation of a smart attendance system are presented in this project (Pawar et al., 2020). System is built with an automated attendance system that considers about the employee's efforts, acknowledges his or her work, and discretely records the employee's presence at the gate and when the employee exits the gate. This information is then stored in the database, making it easier and less expensive for the employee to attend work. Due to its effectiveness, this approach that reduces costs and saves time generates a significant profit for the company. This project records attendance using the face recognition method while using personnel records. The proposed system application is operational during business hours for the company. The system's camera (a computer programme) will be installed at the door so that it can be used to scan people's faces as they enter the building. The application then records the image and transmits it to the processing part. The application's processing part can identify the employee's face. Finally, if the employee is present, the application marks the information. Employees are marked as absent for the day if the application does not recognize them, meaning they are not present. Automated attendance management systems guarantee precise timekeeping and reduce the unavoidable, expensive errors associated with manual data entering. As a result, reliable performance and payroll figures are provided thanks to this data. The significance of proposed system are the time and effort saved and the accuracy of the data contribute to the efficient use of resources, which increases productivity and raises profits. The workflow for payrolls, leaves, and performance reviews can be made easier by an integrated attendance management system, which may provide strong data transparency. Automation of notifications and alerts allows the manager to quickly approve requests for early departure, overtime without the need for further discussion. Real-time tracking can be made by cloud-based attendance management, which also offers automatic payroll processing inputs.

In paper Taibat et al., (2021), a standard electronic attendance system is developed employing facial recognition technology to analyse and compute faces made up of Eigen vectors. In order to improve quality and risk management, the face recognition is developed applying the Principal Component Analysis (PCA) algorithm and Rapid Application Development (RAD). By automating the process, this paper serves as an ideal solution for the lengthy, time-consuming, and tiresome methods of manually recording and monitoring staff attendance in an organisation. To increase the effectiveness of attendance monitoring and management, it implements automatic attendance through face detection and identification. The system will include two modules, one of which is the face detector and is used to take pictures of employees' faces. This module functions as a camera programme that saves JPEG images of employee faces in a folder. The second module matches facial (faces) photographs of employees that have already been taken and stored in a folder using a desktop application, marks or indicates it on the attendance register, and then stores the results in a database for further research. The benefits of employing time attendance systems go beyond keeping track of logged, compensated time and guaranteeing that insurance requirements are met; the most notable benefit is the increased financial value it offers to the company. An organisation can reduce its payroll costs by up to 20% by automating the attendance record. The organizational system improves efficiency by reducing the effort of manual entry, automatically generating daily employee hours worked and other benefits into the payroll system, and preventing staff from sharing data. Researchers took things a step further by looking at how face recognition can address the distressing problems with manual attendance methods. Based on the information in this paper, it was determined that implementing an E-attendance system in businesses and organisations will not only remove the difficulties that human resources face but will also create a dynamic, efficient, and flexible environment that will improve attendance. Compared to conventional attendance systems, e-attendance systems are more effective since they protect both employees and employers from common errors including fabricating inputs and improperly recording data. From the description above, it can be inferred that a system has been designed to replace a manual and unreliable system that is reliable, secure, quick, and efficient. The management of attendance and leaves will improve with the use of this system. Time will be saved, less work will need to be done by the administration, and electronic equipment will take the place of stationery. Consequently, a system with predetermined outcomes has been created.

Due to the rapid increase in travelers around the world, a quick automated biometric solution has been put up to meet airports' future border control needs (Del Rio et al., 2016). Automated border control (ABC) systems take care of the issues presented on by this expansion, like crowding at electronic gates (e-gates) or delays in scheduled arrival times. Most of the ABC systems seen in airports in the European/Schengen regions will use various modalities, including face, fingerprint, or iris recognition. It was chosen to integrate facial recognition in all second generation passports because it is the technology that travelers find to be the most acceptable. For useful performance and efficiency, face recognition systems installed in small kiosks within the e-gates need high quality facial photos. For these systems, accurate facial recognition algorithms are also necessary. These algorithms should be invariant to non-idealities, such as changes in stance and expression, occlusions, and changes in lighting. The most significant face recognition algorithms discussed in the literature that can be used to ABC e-gates and are invariant to these non-idealities are reviewed in this study. There is a comparison of the most popular ABC e-gates situated at the various airports. To conclude, an experimental evaluation of a face recognition system under halogen, white LEDs, NIR, and fluorescence illumination was provided. This system's design is quite similar to that of the Barajas Airport ABC system. Halogen illumination is superior to all the other different illumination configurations analyzed, according to a test using a 144-subject database. LED illumination is second, and may be more appropriate in real operation conditions due to power consumption, heat dissipation, and user convenience. The results that were presented might be applied to the real scenario because there are no major differences between the real system and the proposed prototype.

3 Method

3.1 Research Model and Hypotheses

The following model was developed based on the previously given theoretical notions and constructs. This research model was created following the prior studies, which means that the pieces were chosen for their high relevance. Figure 1 shows the research model on user acceptance which is based on TAM model. The following are the hypotheses used in this study:
H1: Perceived ease of use (PEOU) is correlated with behavioral intention (BI) to use the Attendance Tracking using Facial Recognition Technology
H2: The perceived usefulness (PU) of using the Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology.
H3: The perceived reliability of using the Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology.
H4: The perceived quality of using the Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology.

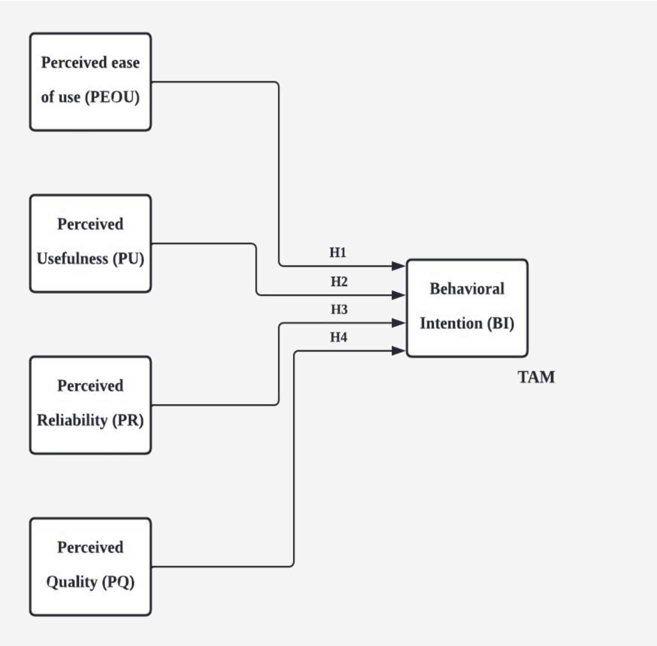

Perceived ease of use (PEOU)
Perceived Usefulness (PU)
Perceived Reliability (PR)
Perceived Quality (PQ)
H1
H2
H3
H4
Behavioral Intention (BI)
TAM

Figure 1: Research model on user acceptance

3.2 Method

This study has been conducted by using a cross-sectional and survey-based research design to investigate the relationship between facial recognition technology and the acceptance status among workers in Malaysia. An online survey was conducted among working adults from February 2022 to April 2022 using an online survey platform. The online survey link, with a brief description of the objective of the study, was shared through the well-known social media app WhatsApp. The inclusion criteria for respondents were as follows: (1) participants must be aged between 20-60 years old; (2) participants must be employed with at least 3-months of experience working in anyof the government or private sectors.

The survey contains a list of questions that will be asked by using the Likert scale where each item is scored on a 5-point Likert scale. Each participant is asked to rate the question given and list it from most unlikely (score 1) to most likely (score 5) which will influence the research. Participants will also be asked to reveal their age and working background. The perceived quality system is applied in this survey to see thoroughly the acceptance of this technology. From the survey, we examine the distribution for each factor in terms of age groups, working sectors, and economic background.

3.3 Survey

In this section, the questions from previous studies are employed, as they have undergone scrutiny to ensure their reliability and validity. Table 1 shows question distribution and also the source of the question.

Table 1: Types and number of questions in the survey

Types of Questions	**Number of Questions**
Socio-demographics	2
Facial Recognition Awareness	4
Perceived Usefulness	3
Perceived Ease of Use	3
Perceived Reliability	5
Perceived Quality	3

Table 2: Questions from the existing surveys

Constructs	**Items**	**Source**
Perceived Usefulness (PU)	• This system would make it easier to identify oneself. • Biometric technologies provide a significant benefit to my organization. • Biometric technologies are reliable	F. D. Davis, (1989) D. R. Lease, (2005)
Perceived Ease of Use (PEOU)	• Is it easy to use this system? • Do you find the verification fast? • Are you ready to use this biometric system in future?	M. El-Abed et al., (2012)
Perceived Reliability (PR)	• Do you think that the use of this technology in your workplace means that employers mistrust employees? • Does this technology threats your privacy? • Personal information identified by this technology will be strictly protected and will not be leaked. • When using this technology, the public’s right to know needs to be guaranteed. • In your opinion, is the system used can be easily attacked?	T. Alhussain et al., (2010) K. L. Ritchie et al., (2021) Y. Yang et al., (2021)
Perceived Quality (PQ)	• Do you think this technology is equally accurate with different races of faces? • How accurate do you think facial recognition technology is? • I would recommend biometric technologies in my organization.	K. L. Ritchie et al., (2021)

4 Result and Discussion

4.1 Results

4.1.1 Respondents Demographic Variable

Table 3: Respondents by Demographic Factors

Variable	Category	Total	
		Frequency	Percentage (%)
Age Group (Years)	20 to 30 years	68	63.6
	31 to 40 years	12	11.2
	41 to 50 years	13	12.1
	51 to 60 years	14	13.1
Total		107	100
Working Sector	Public sector	48	47.5
	Private Sector	44	43.6
	Public-private sector	9	8.9
Total		101	100

Table 3 presents overview of the demographic characteristics, including age, occupation, and other relevant factors, in the initial section. The first section of the survey questionnaire pertains to the respondents' demographics. For the 108 participants in this study, the demographic variables considered are (i) age groups and (ii) working sectors. Table 3 provides a summary of the respondents' demographic profile. The age group with the largest number of respondents' falls within the range of 20 to 30 years old, and the public sector exhibits slightly higher representation compared to the private sector, with a marginal difference of four individuals.

4.1.2 Respondents Familiarity of Attendance Tracking System and Facial Recognition Technology

Table 4: Familiarity of attendance tracking system and facial recognition technology

Variable	Category	Total	
		Frequency	Percentage (%)
Familiarity with attendance tracking	Yes	71	66.4
	No	36	33.6
Total		107	100
Current attendance system in your organization	Manual key-in record	17	16.3
	Punch card system	46	44.2
	Biometric recognition system	41	39.4
Total		104	100
Familiarity with facial recognition technology	Yes	82	76.6
	No	25	23.4
Total		100	100
Experience using facial recognition technology	Yes	73	68.2
	No	34	31.8
Total		107	100

The second part of the survey question is the familiarity with the attendance tracking system and facial recognition technology of the respondents. Table 4 illustrates a summary of the respondents regarding the familiarity with the attendance tracking system and facial recognition technology of the respondents. This demonstrates the respondents' familiarity with using attendance monitoring systems inside their firms as well as the actual attendance system respondents used within organizations. We can see that most system that is still be using are the punch card system which it is slightly different from biometric technology. Other than that, from this part, we can see the familiarity of the respondent with biometric technology specifically facial recognition technology. As a result, most of the respondents were familiar and experienced using facial recognition technology. In Malaysia, this technology has been introduced along with the rapid development of biometric technology as some large companies such as AirAsia, Malaysia Airport Berhad (MAHB), and others introducing this technology to be used at the airport for a better experience and efficiency (KLIA to use, 2021). Thus, this technology will give more impact on daily life routine and will be used rapidly under high development and research.

4.1.3 Analysis of Measurement Model

4.1.3.1 Perceived Usefulness

Figure 2 illustrates a summary of the respondents' perceived usefulness variables. Most respondents agree that the system would make it easier to identify oneself, whereas 6.5% disagree and strongly disagree with it. Other than that, respondents highly agree with the reliability of biometric technologies. As biometric technologies provide a significant benefit to the organization, the highest respondent agrees as this technology will give a huge impact on their organization.

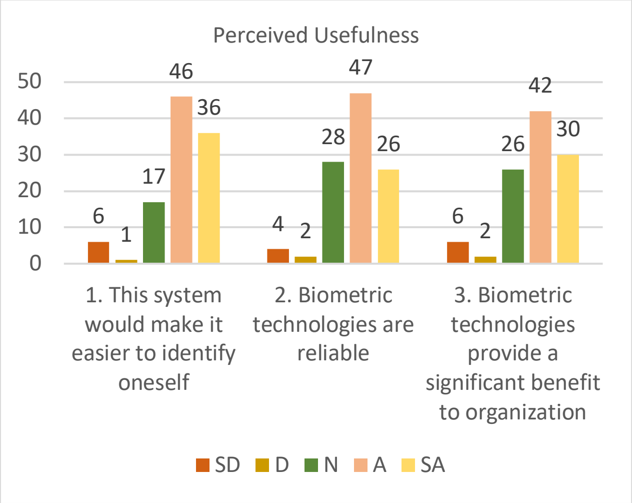
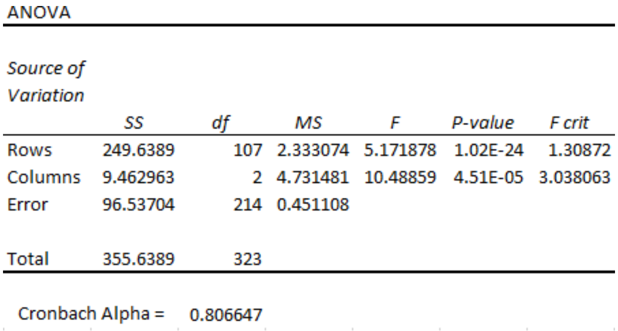


Figure 2: Perceived Usefulness Scores

Table 5: Perceived Usefulness Mean and Standard Deviation of Respondents

Variables	Mean	Mean^2	Standard Deviation
This system would make it easier to identify oneself	3.990566	16.9717	3.602934
Biometric technologies are reliable	3.831776	15.57009	3.426123
Biometric technologies provide a significant benefit toorganization	3.830189	15.75472	3.453191



ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Rows	249.6389	107	2.333074	5.171878	1.02E-24	1.30872
Columns	9.462963	2	4.731481	10.48859	4.51E-05	3.038063
Error	96.53704	214	0.451108			
Total	355.6389	323				

Cronbach Alpha = 0.806647

Figure 3: Reliability for Perceived Usefulness

4.1.3.2 Perceived Ease of Use

Figure 4 illustrates a summary of the respondents' perceived ease of use variables. Most of the respondents agree that it will be easy to use the system. Other than that, the respondent highly agrees with the fast verification by this technology as it will only use face- recognition to detect faces. The highest respondent agrees to use this biometric system in the future in daily life and organization. This led to this technology acceptance by the respondents being highly acceptable thus acceptance status is higher.

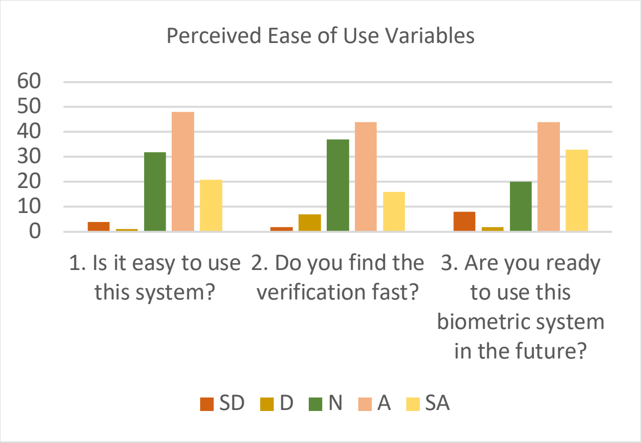
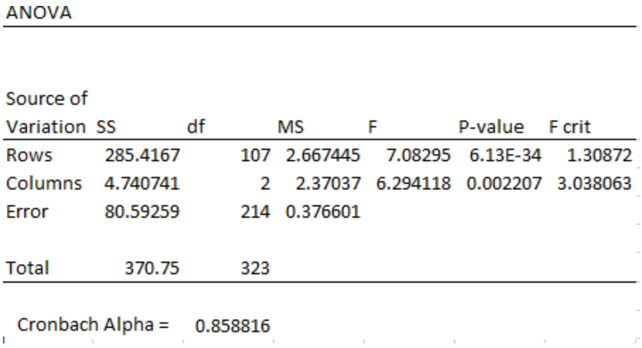


Figure 4: Perceived Ease of Use Variables Scores

Table 6: Perceived Ease of Use Mean and Standard Deviation of Respondents

Variables	Mean	Mean^2	Standard Deviation
Is it easy to use this system?	3.764151	14.99057	3.350584
Do you find the verification fast?	3.613208	13.83962	3.197877
Are you ready to use this biometric system in the future?	3.859813	16.1215	3.501668



ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Rows	285.4167	107	2.667445	7.08295	6.13E-34	1.30872
Columns	4.740741	2	2.37037	6.294118	0.002207	3.038063
Error	80.59259	214	0.376601			
Total	370.75	323				

Cronbach Alpha = 0.858816

Figure 5: Reliability for Perceived Ease of Use

4.1.3.3 Perceived Reliability

Figure 6 illustrates a summary of the respondents' PR variables. Most respondents feel neutral when comes to the usage of this technology in your workplace means that employers mistrust employees. Other than that, the respondent also feels neutral when comes to privacy issues on this technology. The highest respondent agrees that personal information identified by this technology will be strictly protected and will not be leaked. Besides, most respondents agree that when using this technology, the public's right to know needs to be guaranteed. Most of the respondents feel neutral when comes to the systembeing attacked.

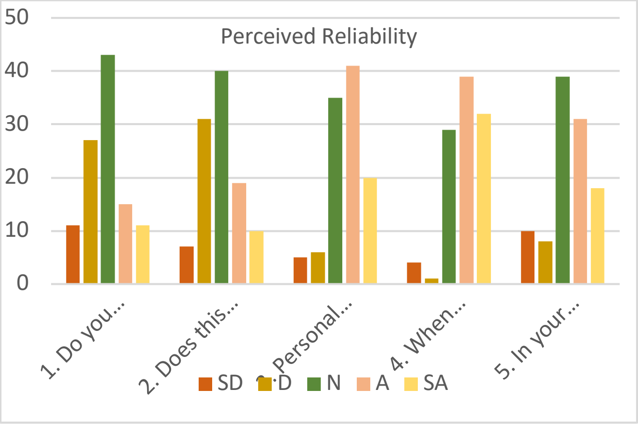
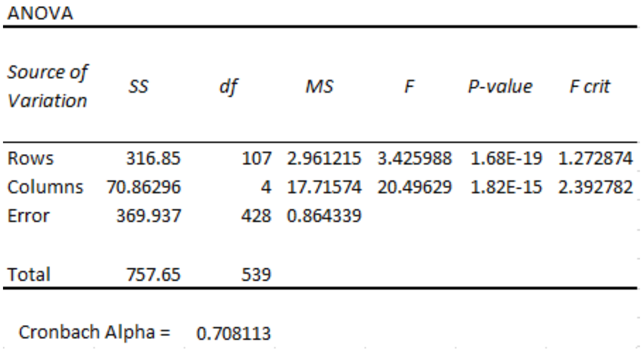


Figure 6: Perceived Reliability Variables Scores

Table 7: Perceived Reliability Mean and Standard Deviation of Respondents

Variables	Mean	Mean^2	Standard Deviation
Do you think that the use of this technology in your workplace means that employers mistrust employees?	2.88785	9.542056	2.579575
Does this technology threats your privacy?	2.943925	9.766355	2.611978
Personal information identified by this technology will bestrictly protected and will not be leaked	3.607477	14.01869	3.226641
When using this technology, the publics right to knowneeds to be guaranteed	3.895238	16.12381	3.496937
In your opinion, is the system used can be easily attacked?	3.367925	12.63208	3.043707



ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Rows	316.85	107	2.961215	3.425988	1.68E-19	1.272874
Columns	70.86296	4	17.71574	20.49629	1.82E-15	2.392782
Error	369.937	428	0.864339			
Total	757.65	539				

Cronbach Alpha = 0.708113

Figure 7: Reliability for Perceived Reliability

4.1.3.4 Perceived Quality

Figure 8 illustrates a summary of the respondents' perceived quality variables. Most respondents feel neutral when comes to the accuracy of this technology to equally accurate with different races of faces. Other than that, respondents felt neutral and slightly high than agreeing when comes to the accuracy of this facial recognition technology. The highest respondent agrees to recommend biometric technologies in their organization.

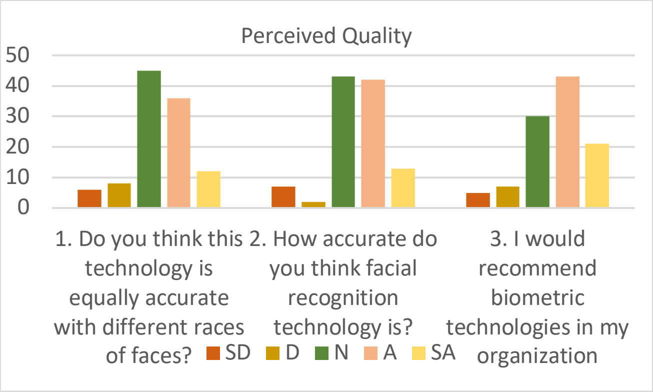
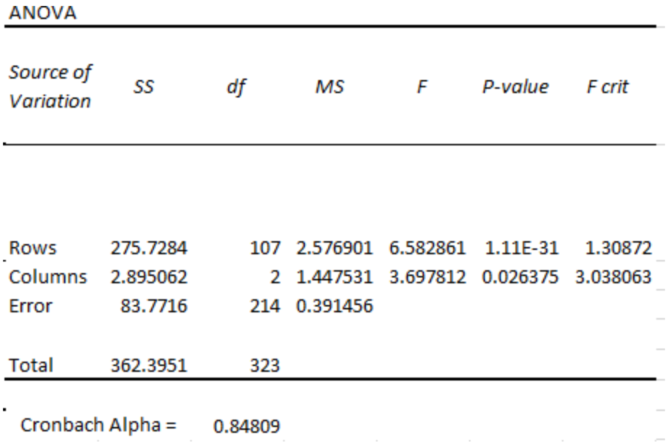


Figure 8: Perceived Quality

Table 8: Perceived Reliability Mean and Standard Deviation of Respondents

Variables	Mean	Mean^2	Standard Deviation
Do you think this technology is equally accurate with different races of faces?	3.373832	12.3271	2.992202
How accurate do you think facial recognition technology is?	3.485981	13.07477	3.096576
I would recommend biometric technologies in my organization	3.641509	14.30189	3.265023



ANOVA

Source of Variation	*SS*	*df*	*MS*	*F*	*P-value*	*F crit*
Rows	275.7284	107	2.576901	6.582861	1.11E-31	1.30872
Columns	2.895062	2	1.447531	3.697812	0.026375	3.038063
Error	83.7716	214	0.391456			
Total	362.3951	323				

Cronbach Alpha = 0.84809

Figure 9: Reliability for Perceived Quality

We categorized the age groups and sectors of respondents working into subgroups as shown in the Table.1 Age ranged from 20 to 60 but we divided it into 4 sub-groups including (20-30), (31-40), (41-50), and (51-60). And then count their percentage by the frequency of each group which gave us a total percentage of 100%. The working sector has three subgroups which are the private sector (43.6%), public sector (47.5%), and public-private sector (8.9%). This percentage shows that the public sector has a high percentage as compared to the other.

Figure 2 represents a summary of respondents' perceived usefulness variable. It explains that the respondents highly agree with the reliability of this biometric technique. This fact provides a huge benefit to the organization. By looking at the minor details of the research questions we observed that 34% of respondents seemed strongly agree with the fact that this technology is easier to identify. 24.3% of respondents showed that the biometric system is quite reliable whereas 3.7% seemed to disagree with this statement. 28.3% of them stated that this new technology is providing great benefit to the organization. While discussing the use of this system we observed that 19.8% of respondents claimed that this system is easy to use and only 3.8 seemed to disagree. 30.8% were those who are strongly motivated to use this system in the future. When we were concerned about the privacy of the workers 9.3% agreed that their privacy has disturbed. Whereas 17% of respondents said that they think that this system can be easily attacked. 12.1% responded that this facial recognition is accurate. 19.8% of respondents stated that they would highly recommend using this system in all organizations whereas 4.7% disagreed with this. These results show that the majority of the employees seem satisfied with the technology but some are not agree with the use of this technology.

Table 9: Results of Measurement Model Assessment

Construct	Factor Loading	Cronbach's alpha	CR	AVE
Preceived Usefulness				
Item 1	0.039	0.806	0.004	0.001
Item 2	0.038			
Item 3	0.038			
Perceived Ease of Use				
Item 1	0.037	0.858	0.006	0.002
Item 2	0.061			
Item 3	0.038			
Perceived Reliability				
Item 1	0.028	0.708	0.005	0.001
Item 2	0.029			
Item 3	0.036			
Item 4	0.038			
Item 5	0.033			
Perceived Quality				
Item 1	0.033	0.848	0.004	0.001
Item 2	0.034			
Item 3	0.036			

Table 10: Discriminant validity assessment using Fornell-Larcker criterion

Fornell-Larcker Criterion	Construct	(1)	(2)	(3)	(4)
	PU	0.0316			
	PEOU	0.032	0.044		
	PR	0.002	0.026	0.0316	
	PQ	0.063	0.045	0.003	0.0316

4.2 Discussion

There was a total of 108 respondents in this study. There are three research questions, three objectives and four hypotheses used as guidance. The first hypothesis is perceived ease of use (PEOU) is correlated with behavioural intention (BI) to use Attendance Tracking using Facial Recognition Technology. As we can see from PEOU variables, most of the respondents agree with the three questions that have been listed. On this, we can conclude that the hypothesis is accepted. The second hypothesis, which is the perceived usefulness (PU) of using Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology. As we can see from PU variables, most of the respondents agree with the three questions that have been listed. It explains that the respondents highly agree with the reliability of this biometric technique. These findings show that most of respondents have been using biometric technique in some sector and trust that the system is efficient and reliable where it does not bring harm to the user. As biometric is not widely used in some sector, this show that respondents aware with security of data on this technology and believe their privacy will not be breach. On this, we can conclude that the hypothesis is accepted. The third hypothesis, the perceived reliability of using the Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology. In this part, a few more questions have been asked to know the status of the respondents if there is a lack of the system. Out of 3 questions, most of the respondents choosing on the neutral side, and in 2 questions most of the respondents agree. This shows the neutral side which is slightly higher and most of the respondents are aware of the implication of the system. From this, we can see that the hypotheses are still accepted as a smaller number of respondents do not agree with the implication. The last hypothesis is perceived quality of using the Attendance Tracking by Facial Recognition Technology will have a positive impact on an individual's behavioral intention (BI) to use the technology. In two questions, most of the respondents chose the neutral side and in 1 question most of the respondents agree. This shows the neutral side which is slightly higher. From this, we can see that the hypotheses are still accepted as a smaller number of respondents do not agree. To analyses the data collected from the survey, the frequency and the percentage of respondents who responded to each question were recorded. As we can see from the result itself, when comes to perceived usefulness and perceived ease of use, most respondents agree, and this shows that it is efficient and should be implemented. But when comes to PR and PQ, respondents tend to answer on the neutral part, but higher on agree rather than disagree, we can conclude that respondents still felt unsure but some of them agree on the reliability of this technology.

As a result, the hypotheses are still accepted and most of the respondents agree on using this technology not only for attendance tracking but also in daily life. When comes to acceptance in daily life, we can be sure that respondents involved in this study, are willing to accept this technology in their daily life. This shows rapid advancement of this technology will increase as the net worth of this technology has been increasing daily. Thus, it will impact the working sector and the efficiency of the working system in Malaysia.

5 Conclusions

This paper includes a summary review of studies related to attendance tracking based on facial recognition systems. In this paper, we have discussed the technology acceptance status in Malaysia and user behaviour toward this technology. Every researcher has their approach to recognizing faces from the database or video and many products have been developed on this facial recognition technology. This study presents the result of a questionnaire study among individuals targeting with at least 100 participants who are currently working in government or private sectors with the aged at least 20 years old to a maximum 60 years old. From the data that have been collected, the acceptance status of this technology is higher. These findings indicate the respondents' status on this technology system and the acceptance among the workers and also the efficiency of the system when it is implemented in the organization. The results of this study show the acceptance of this technology. Data collected from the survey have been analysed where the percentage of respondents for each question recorded. As we can see perceived usefulness and perceived ease of use have been higher among respondents choosing to agree.

As it is perceived reliable, the respondents still feel neutral and the same goes for perceived quality. As stated from data itself, the findings show for perceived usefulness, respondents' acceptance on this technology is positive where they believe that the system will ease them, also this technology is reliable in term of security and usefulness and it will help provide a great impact to organization. When discuss on perceived of ease of use, shown that this technology will help them in term of efficiency and respondents are ready to accept this technology in future. Perceived reliability shown neutral things on mistrust of employer, threats on privacy and attack on the system. On this part, it show that respondents need guarantee and secured law that their data is secured when use this technology. Perceived quality indicates that respondents are not sure with the accuracy of this technology on different races and accuracy of this technology. This show that the technology need to have an high accuracy when implemented.The limitation of this study is the method of selecting respondents as it was limited to those who are currently working and employed. As this technology which is facial recognition is not widely used in attendance tracking on working environment, it was limited for those who are working in any sector to be in part of the survey. This research has specify on attendance tracking system by using facial recognition where it has to follow the condition to be currently working and employed. Furthermore, if it is general, the result will be slightly different and the status can be seen as the question will not be limited to employ workers. For future work, the research can be improved by not only implement facial recognition technology in working attendance tracking system, but also in university or school attendance where it will be more efficient and convenience. As the data collection can be spread with working person and student, it will give more respondents so will have various and possibly higher differences of each answer on the survey.

References

Alhussain, T., & Drew, S. (2010). Employees' Perceptions of Biometric Technology Adoption in E-Government. International Journal of E-adoption, vol. 2, no. 1, pp. 59–71, Jan. 2010, doi: 10.4018/jea.2010010105. Available: https://doi.org/10.4018/jea.2010010105

Alicia, C. C. Y., Hamimah,U., & Irwandi, H. (2017). 3D facial Expression Intensity Measurement Analysis. Proceedings of the 6th International Conference on Computing and Informatics, ICOCI 2017, Jan. 2017, http://repo.uum.edu.my/22793/

Air Asia introduces F.A.C.E.S facial recognition system to ease boarding process. Borneo Post Online, Feb. 2018, https://www.theborneopost.com/2018/02/07/air-asia-introduces-f-a-c-e-s-facial-recognition-system-to-ease-boarding-process/

Bowling, B., & Iyer, S.V. (2019). Automated policing: the case of body-worn video. International Journal of Law in Context, vol. 15, no. 2, pp. 140–161, Jun. 2019, doi: 10.1017/s1744552319000089. Available: https://doi.org/10.1017/s1744552319000089

Brömme, A., Busch, C., "BIOSIG 2013" Proceedings – International Conference of the Biometrics Special Interest Group, 04-06, September 2013 Darmstadt, Germany, ISBN 978-3-88579-606-0

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. Management Information Systems Quarterly, vol. 13, no. 3, p. 319, Sep. 1989, doi: 10.2307/249008. Available: https://doi.org/10.2307/249008

Del Rio, J. S., Moctezuma, D., Conde, C., De Diego, I. M. & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. Computers & Security, vol. 62, pp. 49–72, Sep. 2016, doi: 10.1016/j.cose.2016.07.001. Available: https://doi.org/10.1016/j.cose.2016.07.001

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2012). Evaluation of biometric systems: a study of users' acceptance and satisfaction. International Journal of Biometrics, vol. 4, no. 3, p. 265, Jan. 2012, doi: 10.1504/ijbm.2012.047644. Available: https://doi.org/10.1504/ijbm.2012.047644

Facial Recognition Market size worth $ 10.2 Billion, Globally, by 2028 at 15.92% CAGR: Verified Market Research®." https://www.prnewswire.com/, Oct. 14, 2021. Available: https://www.prnewswire.com/news-releases/facial-recognition-market-size-worth--10-2-billion-globally-by-2028-at-15-92-cagr-verified-market-research-301400457.html

He, R., Cao, J., Song, L., Sun, Z., & Tan, T. (2020). Adversarial Cross-Spectral Face Completion for NIR-VIS Face Recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 5, pp. 1025–1037, May 2020, doi: 10.1109/tpami.2019.2961900. Available: https://doi.org/10.1109/tpami.2019.2961900

Kar, N., Debbarma, M. K., Saha, A., & Pal, D. R. (2012). Study of Implementing Automated Attendance System Using Face Recognition Technique. International Journal of Computer and Communication Engineering, pp. 100–103, Jan. 2012, doi: 10.7763/ijcce.2012.v1.28. Available: https://doi.org/10.7763/ijcce.2012.v1.28

Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J. D., Evans, B. J., Lee, M. K., Anderton, J., Weinberg, S. M., & Wagner, J. K. (2021). A survey of U.S. public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. ProQuest, e0257923. https://doi.org/10.1371/journal.pone.0257923

Khan, N. N. & Efthymiou, M. (2021). The Use of Biometric Technology at Airports: The Case of Customs and Border Protection (CBP). International Journal of Information Management Data Insights, vol. 1, no. 2, p. 100049, Nov. 2021, doi: 10.1016/j.jjimei.2021.100049. Available: https://doi.org/10.1016/j.jjimei.2021.100049

KLIA to use facial recognition in place of boarding pass. The Star, Jan. 18, 2021. https://www.thestar.com.my/business/business-news/2021/01/19/klia-to-use-facial-recognition-in-place-of-boarding-pass

Lease, D. R. (2005). Factors Influencing the Adoption of Biometric Security Technologies by Decision Making Information Technology and Security Managers. Oct. 01, 2005. http://hdl.handle.net/10919/71576

Liu, T., Yang, B., Geng, Y., & Du, S. (2021). Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology. Frontiers in Psychology, vol. 12, Dec. 2021, doi: 10.3389/fpsyg.2021.809736. Available: https://doi.org/10.3389/fpsyg.2021.809736

Negri, N. A. R., Borille, G. M. R. & Falcão, V. A. (2019). Acceptance of Biometric Technology in Airport Check-In. Journal of Air Transport Management, vol. 81, p. 101720, Oct. 2019, doi: 10.1016/j.jairtraman.2019.101720. Available: https://doi.org/10.1016/j.jairtraman.2019.101720

Okokpujie, K.O., Noma-Osaghae, E., John, S., Grace, K.A., & Okokpujie, I.P. (2017). A Face Recognition Attendance System with GSM Notification. Doi: 10.1109/nigercon.2017.8281895. Available: https://doi.org/10.1109/nigercon.2017.8281895

Owayjan, M, Dergham, A., Haber, G., & Abdo, E. (2019). Face Recognition Security System. ResearchGate, Dec. 2013, https://www.researchgate.net/publication/259027363_Face_Recognition_Security_System

Pawar, A. S., Patil,S. S., Rai, K, A., & Bauskar, R. (2020). Automated Attendance System Using Facial Recognition. International Research Journal of Engineering and Technology (IRJET), vol. 07, no. 03 March 2020, pp. 2701–2704, Mar. 2020.

Raj, A. (2021). Increasing demand for facial recognition system technology in Malaysia. https://techwireasia.com/, Oct. 14, 2021. https://techwireasia.com/2021/10/increasing-demand-for-facial-recognition-system-technology-in-malaysia/

Ramachandran, V., Princy, B.A., Ambeth Kumar, V.D., Raghuraman, M., Gupta, M., Kumar, A., Kumar, A., & Khan, A. K. (2021). Secure online payment through facial recognition and proxy detection with the help of TripleDES encryption. Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 8, pp. 2195–2205, Nov. 2021, doi: 10.1080/09720529.2021.2011096. Available: https://doi.org/10.1080/09720529.2021.2011096

Ritchie, K.L., Cartledge, C., Growns, B.,Yan,A., Wang, Y., Guo, K., Kramer, R.S.S, Edmond, G. Martire, K.A., Roque, M, S., & White, D. (2021). "Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world," PLOS ONE, vol. 16, no. 10, p. e0258241, Oct. 2021, doi: 10.1371/journal.pone.0258241. Available: https://doi.org/10.1371/journal.pone.0258241

Taibat, A. O., & Agboizebeta, I. A. (2021). Standard Electronic Attendance System with Facial Recognition. International Research Journal of Modernization in Engineering Technology and Science, vol. 03, no. 11 November 2021, Nov. 2021.

Wang, L. (2021). Face Recognition in Law Enforcement: A Comparative Analysis of China and the United States. Open Journal of Social Sciences, Jan. 2021, doi: 10.4236/jss.2021.910036. Available: https://doi.org/10.4236/jss.2021.910036

Yang, H & Han, X. (2020). Face Recognition Attendance System Based on Real-Time Video Processing. IEEE Access, vol. 8, pp. 159143–159150, Jan. 2020, doi: 10.1109/access.2020.3007205. Available: https://doi.org/10.1109/access.2020.3007205

Yang, Y., Yin, D., Easa, S. M., & Liu, J. (2021). Attitudes toward Applying Facial Recognition Technology for Red-Light Running by E-Bikers: A Case Study in Fuzhou, China. Applied Sciences, vol. 12, no. 1, p. 211, Dec. 2021, doi: 10.3390/app12010211. Available: https://doi.org/10.3390/app12010211

Zaharia., S & Pietreanu, C.V. (2018). Challenges in airport digital transformation. Transportation Research Procedia, vol. 35, pp. 90–99, Jan. 2018, doi: 10.1016/j.trpro.2018.12.016. Available: https://doi.org/10.1016/j.trpro.2018.12.016

Zhang, W & Kang, M.H (2019). Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers. IEEE Access, vol. 7, pp. 154360–154374, Jan. 2019, doi: 10.1109/access.2019.2927705. Available: https://doi.org/10.1109/access.2019.2927705