BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research

Volume 3 | Issue 4 | October 2021 | ISSN 2630-5151（Online）

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Editor-in-Chief

Editorial Board Members

Volume 3 Issue 4 • October 2021 • ISSN 2630-5151 (Online)

Journal of Computer Science Research

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 3 | Issue 4 | October 2021 | Page1-50
Journal of Computer Science Research

Contents

Articles

Review

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Emoji Essence: Detecting User Emotional Response on Visual Centre Field with Emoticons

Fatima Isiaka[1*] Zainab Adamu[2]

1. Department of Computer Science, Nasarawa State University, Keffi, Nigeria
2. Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

ARTICLE INFO

Article history
Received: 16 August 2021
Accepted: 7 September 2021
Published Online: 18 September 2021

Keywords:
Emotion emblem
Emoticons
Visual expression
Area of interest
Ergonomics
User interaction
Web interface

ABSTRACT

User experience is understood in so many ways, like a one on one interaction (subjective views), online surveys and questionnaires. This is simply so get the user's implicit response, this paper demonstrates the underlying user emotion on a particular interface such as the webpage visual content based on the context of familiarisation to convey users' emotion on the interface using emoji, we integrated physiological readings and eye movement behaviour to convey user emotion on the visual centre field of a web interface. The physiological reading is synchronised with the eye tracker to obtain correlating user interaction, and emoticons are used as a form of emotion conveyance on the interface. The eye movement prediction is obtained through a control system's loop and is represented by different color display of gaze points (GT) that detects a particular user's emotion on the webpage interface. These are interpreted by the emoticons. Result shows synchronised readings which correlates to area of interests (AOI) of the webpage and user emotion. These are prototypical instances of authentic user response execution for a computer interface and to easily identify user response without user subjective response for better and easy design decisions.

1. Introduction

Users subjective response doesn't allow for authentic response when asked about their user experience. They prefer to give a straight forward answer simply because they don't want to reveal inappropriate views such as expressing their low opinion of an interface. Users' emotional response is the best form of conveying positive or negative authentic response to a computer interface. Computer interface is mostly used as a form of user friendly computer interaction between the user and the system. They are mostly designed to suit the purpose of an underlying assignment. Its design should be configured to suit 10 the ergonomically characterised requirements of the user. To obtain an astute user response and opinion, physiological response are normally used as a metric for users' authentic response. Authentic responses are required for an enhanced design decision, such as to build an enhanced user interface that is free of stress and a lot more of adaptive physiological ambience of the user. Also for the 15 designers, an astute opinion of the user might not be obtained from direct user communication [1,11,13] but from the interface itself by easily transmitting user emotion on the AOI. One of the most important user attributes is the user behaviour which is communicated

**Corresponding Author:*
Fatima Isiaka,
Department of Computer Science, Nasarawa State University, Keffi, Nigeria;
Email: fatima.isiaka@outlook.com

 DOI: https://doi.org/10.30564/jcsr.v3i4.3577

from the eyes or eye movement behaviour on the interface. The eye tracker is used to measure eye movement behaviour 20 and pupil dilation on an interface. The eyes not only convey a particular information but also an underlying user emotion which is expressed through pupil dilation. Integrating user physiological response (UPR) and user eye movement behaviour (EMB) can give an underlying user response that interprets user opinion of an interface in a high-level instance. Using emoticons is one of the means of expressing user emotion and response in so many ways. It can represent when a person is sad, happy or extremely excited. In this paper, emoticons are used to express user emotion through EMB and UPR. These emoticons are the most voiced language digitally. It is used here to represent users' emotional response to webpage interface based on EMB and UPR integration and prediction 30 through a control system. The user emotional response is represented here as stress, neutral and relaxed mood.

Objectives

Based on the discussion above, the objectives of this paper are to:

- conduct a thorough literature review.
- design a method for predicting users' EMB on visual centre field of a webpage interface.
- illustrate methods of conveying emoticons on visual interface.
- identify correlates of EMB and UPR on webpage interface.

One of the most basic user interface is the web interface used to control basic information that interprets an organisation's hierarchy, activity and research 40 database. Its design must suit the users' profile and user friendly authentication. Conveying user emotion on interface is a novel area which is presently a static state of the art investigation on user interface designed expressed using emoticons. The proceeding section discusses recent work on user behaviour, computer user interface through UPR and EMB and expression of emotion through emoticons on AOI.

2. Literature Review

In user experience, the user behaviour towards a particular interface can be interpreted through the use of eye tracker which stores the users' information for analysis. The EMB is recorded with the pupil dilation. EMB contains fixations points (FP) and saccades connected through scan-path, this represents the trajectories (paths) of the eyes when scanning the visual field and viewing for analysing visual information. Its predictions interprets emotional response through the pupil dilation [3,5,7,9]. With the increasing number of human computer interaction technology, the natural interactive products are now more 55 valued by more people. The visual sense is the most important method of channelling information and most research are more focussed on the measurement of the eye movement [4,3]. The interaction of eyes with machines have a very wide prospect such as including the pluses and minuses of available control systems written by [4,8,10], that puts forth design principle, system concept and 60 state of change model of eyes interaction from consideration of user-centred design principle. The system simplifies measurement process by focussing on fast tracking and accurate eye movement and calibration using context information to reduce interaction. Physiological measures when used with eye tracking interprets authentic user emotion and despite many challenges. Numerous HCI researches have utilised the use of physiological data to observe user interactions in ways that would have seemed impossible [20-22]. It demonstrates the common theme of using the technique to collect real-time observations of a particularly task in progress, as opposed to some subjective and post-test response. A study by [2] used three different traffic control interfaces with three different task complexity levels to investigate the possibility of using a skin conductance response as a metric for cognitive load. The participants used gestured-based and multimodal speech and gesture interfaces to complete tasks. The analysis show that from five participants indications where shown that average response levels were the lowest of the multimodal interface, which is followed by speech and gesture interface whose overall response increased with task complexity. This provides evidence for the utility of using SCR to indicate cognitive loads [12,14,17]. These SCR peaks were found to be correlated with stressful or frustrating events, with response decreasing overtime. These peaks were also correlated with other major events that were otherwise thought to be cognitively challenging such as reading instructions and completing tasks. While this method proved significant this paper tends to tackle this process by correlating the task performance, eye movement and SCR correlates to convey the user emotion on the task allocated AOI using emoticons. There is not much research conducted in this area of HCI field so far [15,16,18]. Emoticons express the user expression or language in hidden ways understood by user and examiner. Current studies [23] examines the influence of social context on the use of emoticons in internet communication. Students responded to short internet chats such as a task-oriented

DOI: https://doi.org/10.30564/jcsr.v3i4.3577

vs socio-emotional and valence of the context task which either conveys positive 90 or negative emotion which were manipulated in the charts. The results showed that the participants used more of the emoticons in socio-emotional than in the task-oriented social contexts. And also participants are more positive emoticons in positive contexts and negative emoticons in the negative emoticons in the negative contexts. This is also similar to correlated user interactions with 95 physiological response to interpret user behaviour and emotions. The basic contribution here is conveying user emotions on the interface with these emoticons by conducting a study on user interaction with a webpage interface and predicting user eye movement behaviour synchronised with physiological responses. This is one of the novel method we intend to base our analysis on in this paper as 100 discussed in the proceeding section.

3. Materials and Methods

An experimental study was conducted with six participants, all adults (three females and three males) aged between 32-45 from different work background such as computer and internet oriented environment and a manual and less-internet oriented environment, each asked to interact with a webpage.

An eye movement data generated for a single participant in a given time interval can generated thousands of eye movement behaviour patterns that includes gaze points, saccades, fixation duration, pupil dilation and also hand movement such as the number of clicks per second and the object or area of interest.

Six participants were chosen because this would generate data that would amount to a 100,000 within 10 minutes interval for the purpose of a pilot study. The participants were approached during their free time with the request to fill a participant's agreement form that confirms their consent to the study.

The participants were given 1 to 2 minutes to interact with a Yahoo webpage with four (AOI) containing picture, video and text content dated back to 2014 saved in an eye tracker archive. They sat in-front of the eye tracker and were asked to browse through the webpage interface to locate any content that caught their interest at first glance. Their eye movement and pupil dilation were recorded after calibration. This set the eye positions to the middle and four corners of the webpage cartesian plane. A SCR measure was attached to their wrist to get their physiological readings. The setting was from the start time of interaction with the webpage interface to end of the session. The recorded data from the eye tracker and SCR were collected for analysis.

Emotion Emblem

Three different types of emoticons were used to represent the emotional response of the user, which were classified as "stress", "relaxed" and "neutral" mood. The overall emotion is set to appear at the centre visual field of the webpage. Other emoticons can appear at the upper and lower part of the visual field. The emoticons were novel design constructed from spherical coordinates that uses compact logic in Java to differentiate when the body (face) smiles, slightly stressed, or in a neutral mood. The numbers 1-3 are used as the default value during running time. The 3D emoticon is mapped to the cartesian plane of the webpage using the eye movement predictions of the fixation points generated from the eye tracker.

4. Analysis

The eye movement predictions were generated by a control system loop, using discrete time-variation instance to predict the gaze point with different color shades matching mood fluctuations that indicates user responses corresponding to spikes in the SCR. The correlates of the EMB and UPR to webpage contents is determined by time synchronisation of the measuring sensors (Eye tracker and SCR sensor) used in the study. Error in time synchronisation will be dealt with in length in future prospects.

The stress emotions were correlated with the optimal local maxima of SCR response signal while neutral and relaxed mood were correlated to the average and low local minima of the response. Each emoticon was used to map out these points on the webpage vertical plane with co-ordinates of a web browser on a desktop view. Using the eye tracker settings, fixations points were set as the co-ordinates of gaze point on a vertical plane. This process is stretch mapped to each participant's response emotion and the corresponding emojis. The emoticons were set to false for unhappy face when the local maxima is detected and mapped to the fixation points on the webpage.

5. Results

The emotional expression of a user as it happens at a certain point in time in an interaction, is a function of underlying emotions and display rules specifying what kind of expressions are appropriate in a given situation. Here the eye movement and pupil dilation is one of the basic features of interpreting underlying emotions, because there are a lot of cognitive workload and expression during brain activity as the user tries to comprehend the visual field placed in-front of them. The overall emotional expression is summarised to a single

 DOI: https://doi.org/10.30564/jcsr.v3i4.3577

emoticon and conveyed on the visual interface. Lots of fixations are sighted on the AOI for the first visual contact between the eyes and the middle of the main screen. The first participant's gaze point is first located on the picture content in AOI 1 (Figure 1a), the eye movement predictions were displayed around AOI 1 of the webpage. This participant's overall expression was classified as "relaxed" and "Neutral" at the centre of the visual field (Figure 1b) and he also happens to be unfamiliar with the webpage's content. Bother emoticons came out as neutral. The time interval of interest between the SCR and pupil dilation is between 10 to 20 seconds corresponding to the 160 maximum local minima.

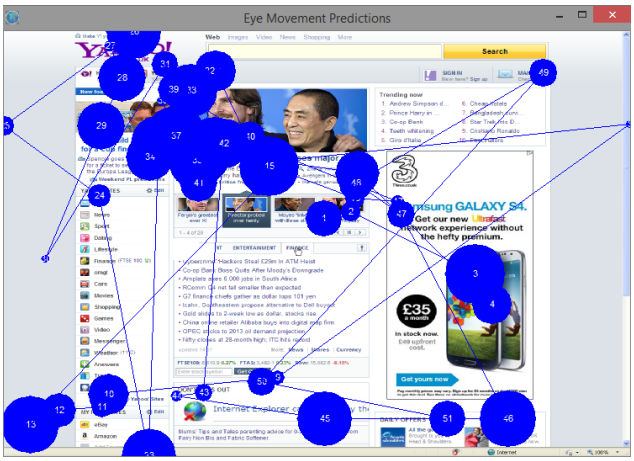

Figure 1a. User 1 original Eye movement behaviour

Figure 1b. User 1 Predicted gaze points and overall response.

In most cases, the visual acuity decreases rapidly when the eye movements sway away from the center of the visual field to other locations of the field. The eye movement generates less fixation points if a particular participant is relaxed and comfortable (familiar) with the visual web interface (Figure 2a). The second participant's overall emotion is summarised as "relaxed", "not happy" and "stressed" at the upper corner and the middle of the visual field during her session with first eye contact on the picture content that contains human features on "AOI-1".

Figure 2a. User 2 original eye movement behaviour.

Figure 2b. User 2 Predicted gaze points and overall emotion expression.

Participant 4 and 6 generated fixations which were summarised as "relaxed", "stressed" and a "neutral" mood, with the centre visual field having stress faced emoticon for participant 4. Few of the predicted fixations also slightly correlates to its original co-ordinate on the webpage cartesian plain. The effects of color on user visual interaction and general arousal indicate that visual attention correlates to physiological effects on human body and influences emotions, feelings and mode. These colors are used to display different eye fixations on the visual webpage (Figure 4).

Figure 3a shows that between 9 to 30 seconds and 30 to 40 seconds into the session, there were changes in emotional response which correlates to eye movement

DOI: https://doi.org/10.30564/jcsr.v3i4.3577

Figure 3a. User 3 original eye movement behaviour.

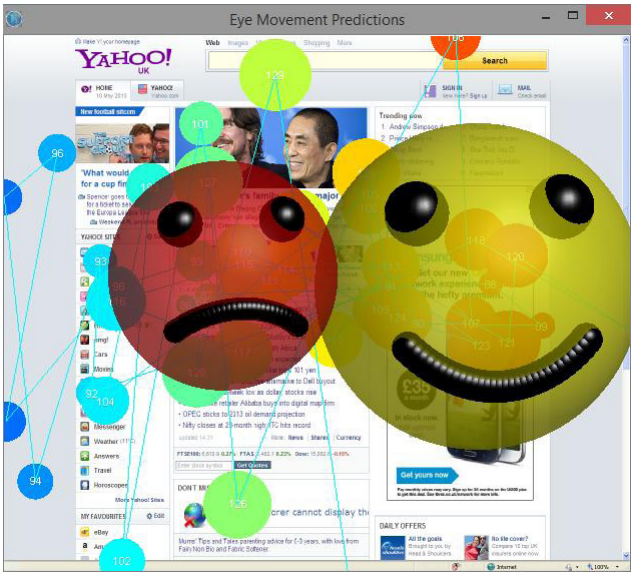

Figure 3b. User 3 Predicted gaze point and overall emotion expression.

behaviour running between picture contents and text contents. The predicted fixation points lie below the lower section of the webpage which is represented by AOI 3 and 4. The participant general response is termed as "relaxed" and "stressed" and also familiar with the webpage's contents. In the real sense, changes or consecutive spikes in pupil dilation don't necessarily mean the participant is stressed but could also mean excitement or happy mood. Visual attention is also known to correlate with divided attention in a complex visual field.

The fifth participant's original eye movement behaviour (Figure 5a) reveals that attention can be subjected to the middle of a visual field at first gaze, as demonstration by

Figure 4a. User 4 original eye movement behaviour

Figure 4b. User 4 Predicted gaze point and overall emotion expression.

the amount of eye fixation between AOI-3 and AOI-4 of the webpage interface, just like that of participant 4, the fixation points were mostly in AOI-4 (left lower corner of the webpage). The predicted eye movement conveyed a neutral mood at the centre of the visual field between these AOIs and a relaxed face with not happy expression (Figure 5b). The number of interval of interest was two (0-20 and 40-50) seconds into the interaction section. Though the participant could not tell between which web content to start with but settled for the middle of the page.

The size of the emojis depends on the extent of the emotional expression e.g. if a particular user expressed intense unfamiliarity to the webpage layout and content the size of the emoji is increased (Figure 6b), just like when a user gazed for a long moment on a particular point in the visual field, the gaze point becomes enlarged,

DOI: https://doi.org/10.30564/jcsr.v3i4.3577

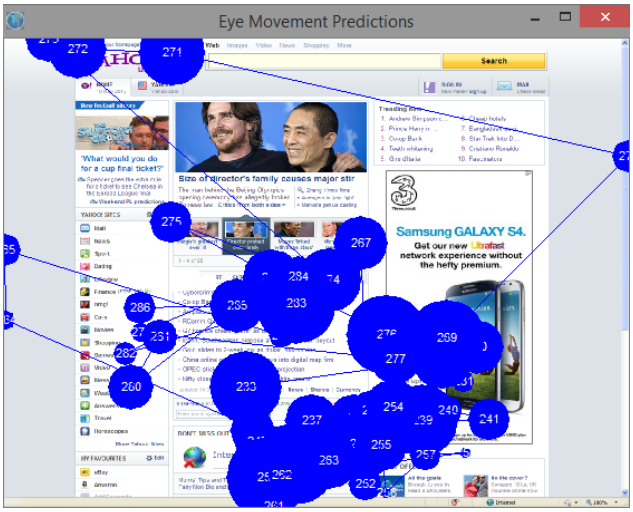

Figure 5a. User 5 original eye movement behaviour.

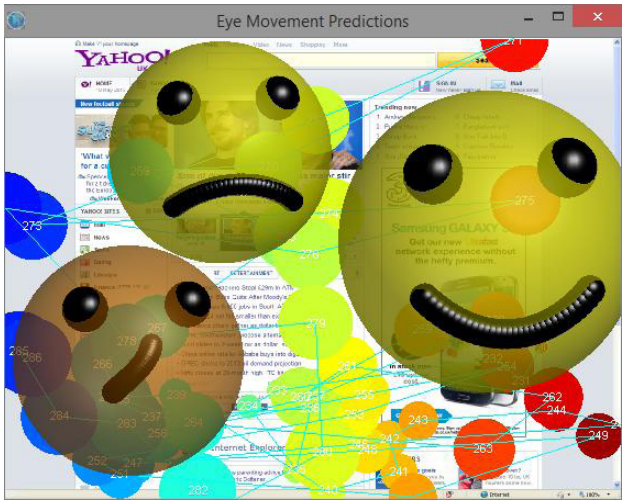

Figure 5b. User 5 Predicted gaze point and overall emotion expression.

the larger the gaze point the intense the look. EMB are mostly seem to correlate with predicted gaze points (Figure 6a). In this session the fixations are mostly located at the AOI-1 section (picture content) of the page, this AOI also contained the predicted eye movement response. The interval of interest in the pupil dilation lies between 10, 30 to 50 seconds into the session. This matches the eye movement. As noted, emotions are often instantaneous and may be unconscious, so investigations should not be limited to self-report gaze points [17] and single physiological measurement but must measure affective responses with a variety of tools. The combination of generated and self-report provides richer insight into emotions. The result of the analysis above is just a conceptualize framework demonstrated for the purpose of developing a high-level prototypical model of a window oriented human computer interface design and development that would ease a complex rule for design decision. Other works [17,22] in the field have been known to produce similar but very distinct outcome.

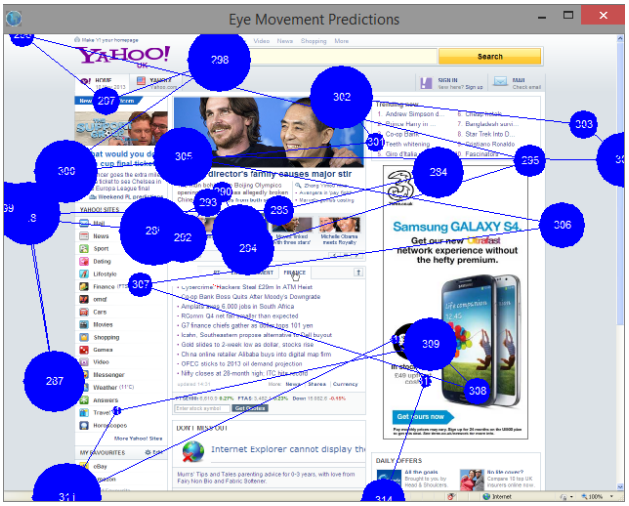

Figure 6a. User 6 original eye movement behaviour.

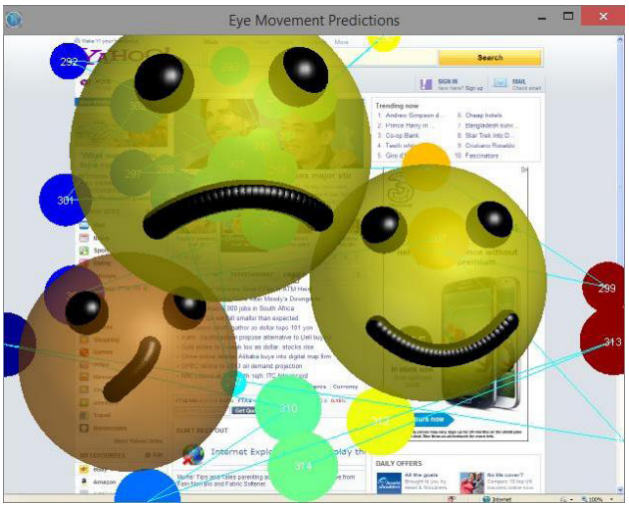

Figure 6b. User 6 Predicted gaze point and overall emotion expression.

6. Conclusions

This paper demonstrates emoticon essence that replaces user subjective response, by conveying user emotion expression to the centre visual field of a webpage interface, the conveying of emoticons that represents user expression on a webpage interface is a relatively new topic in the field of user interaction. This particular study contributes to a new line of analysis on the expression of emotions and the use of emoticons to convey user emotion. The effects of color on user visual interaction and general arousal indicates that visual attention

DOI: https://doi.org/10.30564/jcsr.v3i4.3577

correlates to physiological effects on human body and influences emotions, feelings and mode. These colors are used to display different eye fixations on the visual webpage. The paper also puts forward the eye movement interaction design with an eye control system that predicts the gaze points used to summarise the overall user emotion during interaction. These possibilities influences other novel approaches such as using emoticons to locate a particular coordinate on an interface that triggered the elicited emotion and also the use of emoticons to unveil underlying visual expression. This could also be embed in an eye tracker by using emoticons to represent user response during interaction.

References

[1] Huang, Y., Gursoy, D., Zhang, M., Nunkoo, R., and Shi, S. Interactivity in online chat: Conversational cues and visual cues in the service recovery process. *International Journal of Information Management* (2021), 60, 102360.

[2] Jonathan Lazar, Harry Hochheiser, Measuring the Human, Measuring the Human, Research Methods in *Human Computer Interaction*, (2017), 23, 230 34-56.

[3] Isiaka, Fatima. Modelling stress levels based on physiological responses to web contents, *Sheffield Hallam University*, (2017).

[4] Fang Zhi-Gang, Kong Xiang Zong and Xu Jie. Design of Eye Movement Interactive Interface and Example Development; *Information Technology Journal: Asian Network for Scientific Information*, (2013), 1981-1987.

[5] Goldberg, J. H., and Kotval, X. P. Computer interface evaluation using eye movements: methods and constructs. *International journal of industrial ergonomics*, (1999), 24(6), 631-645. 18.

[6] Iáñez, E., Azorin, J. M., and Perez-Vidal, C. Using eye movement to control a computer: A design for a lightweight electro-oculogram electrode array and computer interface. *PloS one*, (2013), 8(7), e67099.

[7] Kim, K. N., and Ramakrishna, R. S. Vision-based eye-gaze tracking for human computer interface. *In IEEE SMC'99 Conference Proceedings. IEEE International Conference on Systems, Man, and Cybernetics* (Cat. No. 245 99CH37028) (1999), Vol. 2, pp. 324-329.

[8] Jacob, R. J. What you look at is what you get: eye movement-based interaction techniques. *In Proceedings of the SIGCHI conference on Human factors in computing systems*, (1990), 11-18.

[9] Ding, Q., Tong, K., and Li, G. (2006, January). Development of an EOG 250 (electro-oculography) based human-computer interface. *In 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, (2005), pp. 6829-6831.

[10] Deng, L. Y., Hsu, C. L., Lin, T. C., Tuan, J. S., and Chang, S. M. EOG-based Human-Computer Interface system development. *Expert Systems with Applications*, (2010), 37(4), 3337-3343.

[11] Lv, Z., Wu, X. P., Li, M., and Zhang, D. A novel eye movement detection algorithm for EOG driven human computer interface. *Pattern Recognition Letters*, (2010), 31(9), 1041-1047.

[12] Gu, X., Cao, Z., Jolfaei, A., Xu, P., Wu, D., Jung, T. P., and Lin, C. T. 260 EEG-based brain-computer interfaces (BCIs): A survey of recent studies on signal sensing technologies and computational intelligence approaches and their applications. *IEEE/ACM transactions on computational biology and bioinformatics*, (2021).

[13] Juhola, M., Zhang, Y., and Rasku, J. (2013). Biometric verification of a subject through eye movements. *Computers in biology and medicine*, 43(1), 42-50. 19.

[14] Tecce, J. J., Gips, J., Olivieri, C. P., Pok, L. J., and Consiglio, M. R. Eye movement control of computer functions. *International Journal of Psychophysiology*, 29(3), 319-325. 270.

[15] Triadi, T., Wijayanto, I., and Hadiyoso, S. Electrooculogram (EOG) based Mouse Cursor Controller Using the Continuous Wavelet Transform and Statistic Features. *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*, (2021), 12(1), 53-61.

[16] Zamora, M., Toth, R., Morgante, F., Ottaway, J., Gillbe, T., Martin, S. and Denison, T. DyNeuMo Mk-1: Design and Pilot Validation of an Investigational Motion-Adaptive Neurostimulator with Integrated Chronotherapy. *bioRxiv*, (2020), 19-29.

[17] Prendinger, H., Mori, J., and Ishizuka, M. (2005). Using human physiology to evaluate subtle expressivity of a virtual quizmaster in a mathematical game. *International journal of human-computer studies*, (2005), 62(2), 231-245.

[18] Chocarro, R., Corti˜nas, M., and Marcos-Mat´as, G. Teachers' attitudes towards chatbots in education: a technology acceptance model approach considering the effect of social language, bot proactiveness, and users' characteristics. *Educational Studies*, (2021), 1-19.

[19] Jin, Y., Deng, Y., Gong, J., Wan, X., Gao, G., and Wang, Q. OYaYa: A Desktop Robot Enabling Multimodal Interaction with Emotions. *In 26th International Conference on Intelligent User Interfaces*,

 DOI: https://doi.org/10.30564/jcsr.v3i4.3577

(2021), pp. 55-57.

[20] Fraoua, K. E. (2021, July). How to Asses Empathy During Online Classes. In *International Conference on Human-Computer Interaction, Springer, Cham*, (2021), 427-436.

[21] Huang, A. H., Yen, D. C., and Zhang, X. Exploring the potential effects of emoticons. *Information and Management*, 45(7), 466-473.

[22] K., Suzuki, I., Iijima, R., Sarcar, S., and Ochiai, Y. EmojiCam: Emoji295 Assisted Video Communication System Leveraging Facial Expressions. *In International Conference on Human-Computer Interaction*, (2021), (pp. 611-625).

[23] Daantje Derks , Arjan E.R. Bos, Jasper von Grumbkow. Emoticons and social interaction on the Internet: the importance of social context, *Computers in Human Behavior, Elsevier*, 23 (2007) 842-849.

DOI: https://doi.org/10.30564/jcsr.v3i4.3577

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Quick Quantum Circuit Simulation

Daniel Evans*

Pace University, New York, United States

ARTICLE INFO

Article history
Received: 15 August 2021
Accepted: 9 September 2021
Published Online: 18 September 2021

Keywords:
Quantum
Computing
Circuit
Simulation
Education
Software

ABSTRACT

Quick Quantum Circuit Simulation (QQCS) is a software system for computing the result of a quantum circuit using a notation that derives directly from the circuit, expressed in a single input line. Quantum circuits begin with an initial quantum state of one or more qubits, which are the quantum analog to classical bits. The initial state is modified by a sequence of quantum gates, quantum machine language instructions, to get the final state. Measurements are made of the final state and displayed as a classical binary result. Measurements are postponed to the end of the circuit because a quantum state collapses when measured and produces probabilistic results, a consequence of quantum uncertainty. A circuit may be run many times on a quantum computer to refine the probabilistic result. Mathematically, quantum states are 2^n-dimensional vectors over the complex number field, where n is the number of qubits. A gate is a $2^n \times 2^n$ unitary matrix of complex values. Matrix multiplication models the application of a gate to a quantum state. QQCS is a mathematical rendering of each step of a quantum algorithm represented as a circuit, and as such, can present a trace of the quantum state of the circuit after each gate, compute gate equivalents for each circuit step, and perform measurements at any point in the circuit without state collapse. Output displays are in vector coefficients or Dirac bra-ket notation. It is an easy-to-use educational tool for students new to quantum computing.

1. Introduction

The beginning quantum computing student immediately confronts the steep hurdle of the mathematics of complex vector spaces needed to understand the basics. While there are new languages and extensive systems available to aid quantum computations, they add to the learning curve. Quantum algorithms are presented as circuits or gate sequences, and one wants to know several things that are not immediately available in quantum programming systems. First, a trace of the quantum state after each circuit gate is convenient. A display of the gate equivalent at any point in the circuit is also desirable. Measures of the quantum probabilities, without state collapse, are helpful. All this information is available in a circuit simulation. A circuit simulation is not a quantum computer simulation. It is a mathematical rendering of each step of a quantum algorithm described by a sequence of gate operations on an initial quantum state and rendered by the software system described in this paper, Quick Quantum Circuit Simulation (QQCS). The system allows a student to quickly construct a circuit using a linear notation motivated by the circuits themselves and acquire the information to analyze an algorithm without the need for extensive computation.

As an example of the operation of QQCS, consider

**Corresponding Author:*
Daniel Evans,
Pace University, New York, United States;
Email: de36804p@pace.edu

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

the circuit in Figure 1 [1,2] which is a sequence of basic one- and two-qubits gates that together implement a more complicated gate known as a controlled Hadamard gate.

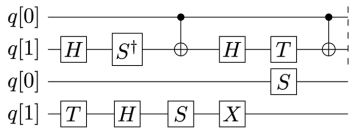

Figure 1. A Controlled Hadamard Gate Sequence

In an interactive QQCS session, the user enters the circuit in a single QQCS statement on one line, shown in Listing 1, and the result is immediately displayed after the Enter key.

```
(1)[1] :_H :_Sa :Cx :_H :_T :Cx :_T :_H :_S :_X :S_
[0.7+0.7i  0          0          0
 0         0.7+0.7i   0          0
 0         0          0.5+0.5i   0.5+0.5i
 0         0          0.5+0.5i   -0.5-0.5i]
```

Listing 1. QQCS Linear Notation, Input and Output for the Controlled-H Gate Sequence of Figure 1

Listing 1 Explanation

(1) The user enters the full gate sequence. A gate is introduced by a colon (:) followed by a mnemonic for the common name of the gate, H for Hadamard, Sa for S-gate adjoint ($\pi/2$ phase gate inverse), Cx for controlled-X, and so forth. The underscore character (_) is used to position the gate in the circuit, and to represent a qubit line with no gate (an implied identity gate). In Figure 1, all the gates one-qubit gates except for the two-qubit Cx gates at step 3 and step 6 of the circuit.

The following output display is the final gate matrix result. Since $e^{i\pi/4} = \cos(\pi/4) + i\sin(\pi/4) = 0.7 + 0.7i$, the result is equivalent to

$$e^{i\pi/4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

a controlled-Hadamard gate with a global phase factor of $e^{i\pi/4}$.

In this QQCS statement, there is no initial quantum state, so the output display represents the gate equivalent, the complex matrix that is the controlled-Hadamard gate, the product of eleven 4×4 matrix multiplications. The quantum computing student who is using QQCS as a study tool, can quickly see and dissect the operation of any circuit encountered in a textbook. Supporting software for quantum programming education is important [3]. QQCS provides a simple tool that does not detract from the primary learning task.

2. Related Work

For an extensive review of quantum programming, see the article "Quantum Programming Languages" [4]. The following references are selected as systems in which results close to those of QQCS could be obtained. In a few cases, they are explicitly compared to QQCS.

One of the most well-known quantum computing resources is IBM's Quantum Experience [2] public web site. IBM supports the open-source software QISKit [5], a set of Python libraries which allow one to write quantum programs (circuits) in a language called Open Quantum Assembly Language (QASM), the language used to program the real quantum computers available through the website. QISKit can submit to the website or simulate locally the operation of QASM. In QISKit, the circuit of Figure 1 would be written as shown in Listing 2.

```
def ctl_h():
    qs = QuantumRegister(2, 'qs')
    cr = ClassicalRegister(2, 'cr')
    ckt = QuantumCircuit(qs, cr)
    # initialization to |11>
    ckt.x(qs[0])
    ckt.x(qs[1])
    # end init
    ckt.h(qs[1])
    ckt.sdg(qs[1])
    ckt.cx(qs[0], qs[1])
    ckt.h(qs[1])
    ckt.t(qs[1])
    ckt.cx(qs[0], qs[1])
    ckt.t(qs[1])
    ckt.h(qs[1])
    ckt.s(qs[1])
    ckt.x(qs[1])
    ckt.s(qs[0])
    ckt.measure(qs, cr)
    return ckt
```

Listing 2. QISKit Controlled-Hadamard

This circuit would be run using the 'qasm_backend' executor for 100 shots and would output a result that would provide counts for each probabilistic result that would show approximately half the shots producing the value 10 and half the shots producing 11. These reflect

1 Program output has been edited to accommodate the needs of publication.

DOI: https://doi.org/10.30564/jcsr.v3i4.3567

the actual mathematical result $\mathrm{CtlH}(|11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$, so one could assume that the sequence of gates was equivalent to a controlled-Hadamard gate.

Listing 3 shows the controlled-Hadamard computation expressed in QuTIP-qip [6], the Quantum Toolbox in Python component for quantum information processing. The component has a circuit simulator, and the computation looks very much like QISKit. It has facilities to display the equivalent matrix, shown at the end of the listing. Compare this to Listing 1. QuTIP is an extensive package going far beyond circuit simulation and is an excellent tool for the advanced quantum computing student, worthy of study on its own.

```
def sdg_gate2():
    # S adjoint gate
    mat = np.array([[1., 0],
                    [0, -1.j]])
    return Qobj(mat, dims=[[2], [2]])
def ctl_h():
    q = QubitCircuit(2, reverse_states=False)
    q.user_gates = {'SDG': sdg_gate2}
    q.add_gate('SNOT', targets=[1])
    q.add_gate('SDG', targets=[1])
    q.add_gate("CNOT", controls=[0], targets=[1])
    q.add_gate('SNOT', targets=[1])
    q.add_gate('T', targets=[1])
    q.add_gate("CNOT", controls=[0], targets=[1])
    q.add_gate('T', targets=[1])
    q.add_gate('SNOT', targets=[1])
    q.add_gate('S', targets=[1])
    q.add_gate('X', targets=[1])
    q.add_gate('S', targets=[0])
    return q
Quantum object: dims = [[2, 2], [2, 2]],
shape = (4, 4), type = oper, isherm = False
Qobj data =
[[ 0.7+0.7j  0. +0.j   0.  +0.j   0.  +0.j  ]
 [ 0. +0.j   0.7+0.7j  0.  +0.j   0.  +0.j  ]
 [ 0. +0.j   0. +0.j   0.5 +0.5j  0.5 +0.5j ]
 [ 0. +0.j   0. +0.j   0.5 +0.5j -0.5 -0.5j ]]
```

Listing 3. QuTIP-qip Controlled-Hadamard

The language Q# [7] was used as a teaching tool, described in "Teaching Quantum Computing through a Practical Software-driven Approach: Experience Report" [3]. A Q# implementation of the controlled-Hadamard computation would look very much like Listing 2 and Listing 3. It provides another approach but is an additional learning burden.

Although quantum computing is a relatively new computer science subfield, there are many software systems to aid in quantum computation, most of which are open source. ProjectQ [8] is a compiler framework capable of targeting various types of hardware, containing a high-performance simulator with emulation capabilities, based on a Python-embedded domain-specific language. Toqito [9] is a Python library for studying various objects in quantum information, states, channels, and measurements. QuNetSim [10] is a quantum network simulation framework. Interlin-q [11] is a simulation platform for simulating distributed quantum algorithms. Cirq [12] is a Python library for writing, manipulating, and optimizing quantum circuits and running them against quantum computers and simulators. QRAND [13] is a smart quantum random number generator for arbitrary probability distributions, which operates by providing a multiplatform NumPy adapter interface. Qrack [14] is a GPU-accelerated HPC quantum computer simulator framework. Pulser [15] is a Python library for programming neutral-atom quantum devices at the pulse level. QCOR [16] is a quantum-retargetable compiler platform providing language extensions for both C++ and Python that allows programmers to express quantum code as stand-alone kernel functions. XACC [17] is a service-oriented, system-level software infrastructure in C++ promoting an extensible API for the typical quantum-classical programming, compilation, and execution workflow. Yao [18] is a framework that aims to empower quantum information research with software tools in the Julia programming language. Quantify [19] is a Python-based data acquisition platform focused on quantum computing and solid-state physics experiments.

3. QQCS

3.1 Quantum Circuits, Briefly

Quantum programs are often constructed and displayed as quantum circuit diagrams. As shown in Figure 1, circuit diagrams are stacked horizontal lines with various connections between them. Each horizontal line represents a qubit. A line is also called a wire, but it is only a wire conceptually. The qubit it represents may be physically realized in several different ways by a quantum computer. The lines are read from left to right corresponding to the sequential execution of the circuit and are best thought of as representing movement in time. Elements that are vertically aligned in the circuit are considered to happen simultaneously. Gates are labeled rectangles, named for the type of gate. Measurement sets a classical bit from a qubit. Measurement is indicated in a quantum circuit by a meter symbol, and usually appears at the end of the circuit. The double wire exiting a meter indicates that the line now carries a classical bit, not a qubit. There are

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

a small number of additional conventions. A controlled gate, such as a controlled NOT, has a control qubit and a target qubit, and is represented not by a rectangle but by a vertical line from the control qubit, indicated by the black dot at the line intersection, to the target qubit, indicated by the $\oplus$ at the intersection. The third and sixth gates in Figure 1 are controlled NOT gates, with controls on line 0 and targets on line 1. A Toffoli gate, a three-qubit controlled gate with two controls and one target, is represented the same way; the control intersections have black dots, and the target intersection has a $\oplus$. A Toffoli gate is shown in Figure 4c.

3.2 Gate Linear Notation

A quantum circuit is a sequence of gates, and as the number of qubits increases, the options for placing and connecting the gates increases, too. Most gate placements, however, are of only a few varieties. The simulation's available gates are one-qubit gates named with one and two letter abbreviations, which are then augmented with prefixes and suffixes describing their positions within the circuit. Additional conventions provide for multiple gates in a single time slice, and for arbitrary control and target lines anywhere within a ten-qubit circuit. The full syntax is shown in Appendix A.

The basic gate names are shown in Table 1 [20,21].

In the linear notation, a gate name is preceded by a colon (:) character.

3.3 Rotational Gates

All the rotational gates specify the angle parameters as factors of π radians, with π implicit. Thus, Rx(.5) is an X-axis rotation of $\pi/2$ radians, or 90 degrees. The parameter range for all angles is (0,4).

The U gate may have one, two, or three parameters: i) $U(\lambda) = U(0,0,\lambda)$, ii) $U(\phi,\lambda) = U(\pi/2,\phi,\lambda)$, or iii) $U(\theta,\phi,\lambda)$. The three-parameter version implements the general unitary matrix:

$$\begin{pmatrix} e^{-i(\phi+\lambda)/2}\cos(\theta/2) & -e^{-i(\phi-\lambda)/2}\sin(\theta/2) \\ e^{i(\phi-\lambda)/2}\sin(\theta/2) & e^{i(\phi+\lambda)/2}\cos(\theta/2) \end{pmatrix}$$

The Rx(θ) gate is equivalent to $U(\theta,-\pi/2,\pi/2)$.

The Ry(θ) gate is equivalent to $U(\theta,0,0)$.

The Rz(λ) gate is equivalent to $U(0,0,\lambda)$.

An alternate general unitary definition is available, invoked by the -u command line flag, or the $ualt comment flag. The alternate definition differs only by a phase factor from the default definition above, but it can simplify the elements of some rotational gates. The definition is:

$$\begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i(\phi+\lambda)}\cos(\theta/2) \end{pmatrix}$$

Table 1. The Basic 1-, 2-, and 3-qubit Gate Names

Names	Gate Description
1-Qubit	
H	Hadamard gate
I	Identity gate
_	ungated lines (implied Identity)
Kp(θ)	Phase gate (universal set) [21]
Rp(θ)	Rotation gate (universal set) [21]
Rx(θ)	Pauli X rotation gate
Ry(θ)	Pauli Y rotation gate
Rz(θ)	Pauli Z rotation gate
S	S gate ($\pi/2$ phase gate)
Sa	S adjoint
T	π gate ($\pi/4$ phase gate)
Ta	T adjoint
Tp(θ)	Phase rotation gate (universal set) [21]
U(θ,ϕ,λ)	Universal one-, two-, or three-parameter rotation gate
X	Pauli X gate
Y	Pauli Y gate
Z	Pauli Z gate (π phase gate)
2-Qubit	
C	general CNOT (used with a 2-digit control suffix)
Cx	CNOT with control qubit *q* and target qubit *q+1*
Cr	reverse CNOT with control qubit *q+1* and target qubit *q*
Sw	General swap (used with a 2-digit control suffix)
3-Qubit	
Tf	general Toffoli gate (used with a numerical suffix)
Fr	general Fredkin gate (used with a numerical suffix)
n-Qubit	
Im	Mean Inversion (used with 1-digit size suffix)
Qf	Quantum Fourier Transform (used with 1-digit size suffix)
Qa	QFT adjoint (used with 1-digit size suffix)

3.4 Oracles

Table 2. Oracles

Oracles	specified with 1-digit size suffix, and optional parameters
Ob	Bernstein-Vazirani
Od	Deutsch-Jozsa
Os	Simon
Og	Grover

Oracles are available for the well-known algorithms of Deutsch, Deutsch and Josza, Bernstein and Vazirani, Simon, and Grover.

The oracles are specified with the syntax :Ox(p)n.

DOI: https://doi.org/10.30564/jcsr.v3i4.3567

x is set to *d* for Deutsch and Deutsch-Josza, which are distinguished by their qubit size, *b* for Bernstein-Vazirani, *s* for Simon, and *g* for Grover. The optional parameter *p* is specific to the oracle and determines whether the oracle will implement a random function or a function determined by the parameter. The *n* suffix is the qubit size and must be specified. The qubit size includes any ancilla qubits.

:Od2 is considered the Deutsch oracle, and any larger qubit size is the Deutsch-Josza oracle. Both algorithms use a single ancilla qubit, and the random function is either a constant or balanced binary function of domain size *n-1*. If the optional parameter is specified, a value of 0 generates a constant function whose values are all 0. A value of 1 generates a constant function whose values are all 1. Any other value generates a balanced function.

:Obn is the Bernstein-Vazirani oracle. The algorithm uses a single ancilla qubit, and the function implements a hidden binary string of size *n-1*. If the optional parameter is specified, it determines the hidden string and should be a value between 0 and $2^n - 1$.

:Osn is the Simon oracle. The algorithm uses *n/2* ancilla qubits, and the function implements a binary string of size *n/2* representing the "period" [22] of the function, which is discovered by the Simon algorithm. If the optional parameter is specified, it determines the "period" and should be a value between 0 and $2^{n/2} - 1$.

:Ogn is the Grover oracle. The oracle randomly selects one basis vector from its n-qubit input and changes its phase to the opposite sign. If the optional parameter is specified, it determines the basis vector to be changed and should be a value between *0* and $2^n - 1$.

3.5 Permutation Gates

Permutation gates are matrices with a single 1 in each row and column and 0's in all other elements. The CNOT gate is a typical permutation gate. When applied to a quantum state, permutation gates shift the amplitudes from one basis vector to another. A permutation gate is specified with the syntax :P(pair, ...)n. Each pair is syntactically real number, but it is interpreted as a pair of integers separated by a period. The *n* suffix is the qubit size of the gate. The integers in a pair must be in the domain $0 \text{ to } 2^n - 1$. For example, the number 2.6 is taken as the pair 2→6, referencing the basis vectors $|010\rangle$ and $|110\rangle$. The gate :P(2.6,6.4,4.2)4 will cycle the amplitudes of three basis vectors in a four-qubit circuit. A two-qubit CNOT gate is equivalent to the permutation specification :P(2.3,3.2)2. The QQCS specification of a large permutation gate is tedious. The simplest way to use one is to specify it once and assign it to a custom gate, then reuse the custom gate as needed.

3.6 Positioning and Replicating Gates

When a gate is positioned in a circuit, it may have qubit lines above and/or below on which there are no gates. The Identity gate is implied when no gate is specified. To indicate this, QQCS uses an underscore (_), repeated once for each ungated qubit line. If the gate is replicated on several circuit lines, the gate name can be repeated, or the replication can be abbreviated with a digit. :H_ is a Hadamard gate on qubit 0, with no gate on qubit 1. To place the Hadamard gate on qubit line 1, use :_H. See Figure 2. The _ can be repeated as many times as needed. :_____H is a one-qubit Hadamard gate on line 5 of a six-qubit circuit. :____H_ moves the Hadamard gate up to line 4.

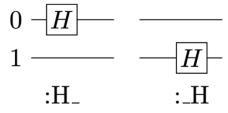

Figure 2. Gate Positioning

To place a gate across multiple qubit lines, follow its name with a digit replicator suffix. To transform a $|0000\rangle$ initial value in a four-qubit circuit to a balanced superposition, use :HHHH or :H4 as a four-qubit Hadamard gate on lines 0 through 3, shown in Figure 3a. The replicator suffix is applicable only to one-qubit gates.

In instances where several gates appear on non-adjacent qubit lines, and are therefore executed simultaneously, the gates can be listed in sequence. If there are implied identity gates between some gates, use one or more underscores. To put an X-gate on lines 1 and 3 of a four-qubit circuit, use :_X_X, as shown in Figure 3b.

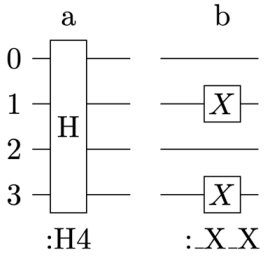

Figure 3. Positioning in a 4-Qubit Circuit

3.7 Controlled Gate Names

Qubit line numbers on a controlled gate can be relative to the span of the gate, or absolute.

For relative line numbers, the span of a gate is the difference between the minimum and maximum control/target lines plus one. Reading left to right, controls occur

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

first, then the target, each as a single digit. As an example, the control suffix 02 has a span of 3 *(2-0+1=3)* lines and indicates a control on relative line 0 and a target on relative line 2.

Ungated prefixes and suffixes are used, as in all other gates, to position the gate vertically in the circuit. Lines within the span that are not control or target lines are ungated by implication.

To place controlled gates in a circuit, start as if the gate were placed at line 0, then identify the controls and the target, in that order. A controlled NOT gate with a three-qubit span with the control on line 2 and the target on line 0 is :C20. To reverse the control and target, use :C02. See Figure 4. If the gate needs to be positioned within a larger qubit circuit, use leading underscores to shift it. The control and target numbers are with relative to the span of the gate, not the number of qubit lines in the circuit. This means that if the gate spans 4 qubits, the lines within the span are referenced from 0 to 3, regardless of the position. The controlled NOT gate :_C02 is shown in Figure 4b. The common names :Cx (equivalent to :C01) and :Cr (equivalent to :C10) are also available for CNOT and reverse CNOT gates with a span of 2.

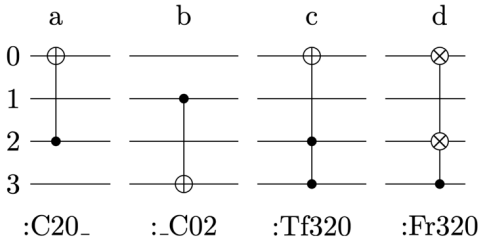

Figure 4. Controlled Gate Linear Notation

Gates that involve two or more control lines and one target, or one control and two targets, will have three (or more) digits following the gate name, in the order (control1, control2, target), or (control, target1, target2), as shown in Figure 4c and 4d. Again, the control and target line numbers are relative to the span.

Any of the built-in one-qubit gates can be supplied with a 2-digit control suffix to add a control line to the gate. See Figure 5 showing a three-qubit quantum Fourier equivalent circuit [20,22], using several different controlled gate forms. The final gate is a swap between lines 0 and 2.

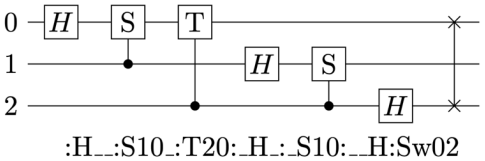

Figure 5. 3-qubit Quantum Fourier Transform

With an absolute suffix, the control and target digits indicate the actual lines of the circuit. No leading _'s are needed for positioning. Trailing _'s may still be needed to indicate the full qubit size of the gate. Either absolute or relative notation may be used.

A Toffoli gate may have more than two control qubits.

3.8 Display

A circuit simulation display starts with the initial value if it is a quantum state and ends with the resulting quantum state at the end of the circuit. By default, both displays are row vectors. Internally, quantum states are column vectors, but they are transposed for linear display. To see the balanced superposition result of a Hadamard gate across three qubits, enter the circuit sequence in Listing 4 and press *Enter*. The result is shown following the entry[2].

```
(1)   |000>:H3
[1  0   0  0  0  0  0  0]       H3
[ 0.354   0.354  0.354  0.354
0.354  0.354  0.354  0.354 ]
```

Listing 4. Balanced Superposition

Listing 4 Explanation

(1) The user enters a three-qubit initial value, and the three-qubit Hadamard gate. The following output display is the initial value as a transposed vector, the gate sequence, and the final quantum state, which shows the balanced superposition.

If the gate sequence does not start with an initial value, the display is an empty initial value and the ending gate matrix. The ending matrix is the matrix product of all the gates in the circuit. In Listing 5, there is only a single two-qubit Hadamard gate.

```
(1)  :H2
[ ]  H2  [
0.5     0.5     0.5     0.5
0.5    -0.5     0.5    -0.5
0.5     0.5    -0.5    -0.5
0.5       -0.5    -0.5     0.5]
```

Listing 5. 2-Qubit Hadamard Gate

Listing 5 Explanation

(1) The user enters a two-qubit Hadamard gate. The following output display is the gate itself.

2 In Listings, line wraps and indentation are artificial for format purposes

DOI: https://doi.org/10.30564/jcsr.v3i4.3567

3.9 Comments

An input comment is anything following a '#' character to the end of the line. A comment is also searched for switch specifications beginning with the character '$'. Keywords following the '$' set or unset internal options, most of which correspond to command line flags.

3.10 Measurement

If simple quantum state display is not sufficient, the results can also be measured and displayed. Measuring produces a probability display for each non-zero basis vector component of the result. Measurement is specified by the M pseudo-gate. M is not an actual gate, but it can be placed anywhere in the circuit gate sequence just as if it were a gate. Unlike measurement in an actual quantum computer, measurement in the simulation does not collapse the quantum state. It is designed for trace purposes. It can occur in a circuit any number of times. If the measurement is only to be applied to some subset of the qubits, specify it exactly as if M were a gate, with underscore prefixes, suffixes, infixes. The controlled-H sequence of Figure 1 is shown with three additional measuring points in Listing 6.

```
(1) |10>:_H:M_:_Sa:Cx:_H:M_:_T
:Cx:_T:_H:_S:_X:S_:M2
M1={1:1}
M2={1:1}
M3={10:0.5, 11:0.5}
[0 0 1 0] _H _Sa Cx _H _T Cx _T _H
_S _X S_ [0 0 0.5+0.5i 0.5+0.5i]
```

Listing 6. Measurement

Listing 6 Explanation

(1) The gate sequence has internal two measurements for qubit line 0, and a full measurement of both lines as the final gate.

[M1] The output of the first measurement, measuring only the first qubit, shows a probability of 1 for the qubit value 1.

[M2] The output of the second measurement also shows a probability of 1 for the qubit value 1.

[M3] The final measurement shows a probability of .5 for each of $|10\rangle$ and $|11\rangle$.

[last] The output is the initial state, the gate sequence, and the final quantum state.

Note that the first two measurements only measure the qubit on line 0. The last measurement, at the end, is for both qubits. The measurement outputs are sequentially numbered so they can be distinguished, and the results are enclosed in braces indicating that it is not a quantum state. The measurement output is a list of measurement outcomes and the probability of each. Even when measuring fewer qubits than are in the circuit, the probabilities will always add to one. The final measurement in Listing 6 shows the probabilities, but the final quantum state shows that the probabilities arise from interesting basis coefficients.

3.11 Initial Values

Quantum circuits are generally assumed to start with an initial value of $|0\rangle_n$ where n is the number of qubits. QQCS uses the presence or absence of an initial value to distinguish between displays. If an initial value is present at the beginning of a circuit, the ending display will be the ending quantum state. If there is no initial value, the ending display will be the equivalent gate matrix. An initial value syntactically is quantum state, a sum of basis kets with complex coefficients. Listing 7 shows four interactions with QQCS in which a Hadamard gate operates on initial values of $|0\rangle$, $|1\rangle$, $0.707|0\rangle + 0.707|1\rangle$, and $0.707|0\rangle - 0.707|1\rangle$. It is an illustration of measurement in the Hadamard basis.

```
(1) |0>:H
[1 0] H [0.707 0.707]
(2) |1>:H
[0 1] H [0.707 -0.707]
(3) 0.707|0>+0.707|1>:H
[0.707 0.707] H [1 0]
(4) 0.707|0>-0.707|1>:H
[0.707 -0.707] H [0 1]
```

Listing 7. Measurement in the Hadamard Basis

Listing 7 Explanation

(1) User enters $|0\rangle$ followed by a Hadamard gate. The output is the initial state $|0\rangle$ (as a transposed column vector), followed by the gate sequence, followed by the final state.

(2) The same sequence with an initial value of $|1\rangle$.

(3) The initial value is $1/\sqrt{2}(|0\rangle + |1\rangle)$, which is $|0\rangle$ in the Hadamard basis, as the following H transformation shows.

(4) Complete the example by showing $|1\rangle$ in the Hadamard basis.

3.12 Tensor Products

An initial value can be constructed from a tensor product. If more than one quantum state is entered as an

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

initial value and the states are parenthesized, a tensor product is implied. This is shown in Listing 8. As in all other QQCS interactions, the first value displayed is that of the first operand. The last value displayed is the result of the computation.

```
(1)  (|0>) (|1>)
[1  0]   [0  1  0  0]
(2)  (0.707|0>+0.707|1>)
(0.707|0>-0.707|1>)
[0.707   0.707]   [0.5  -0.5  0.5  -0.5]
(3)  (0.707|0>+0.707|1>)
(0.5|00>-0.5|01>+0.5|10>-0.5|11>)
[0.707   0.707]
[0.354    -0.353    0.354    -0.353
0.354     -0.353    0.354    -0.353]
```

Listing 8. Tensor Products

Listing 8 Explanation

(1) The tensor product $|0\rangle \otimes |1\rangle$

(2) The tensor product $1/\sqrt{2}(|0\rangle + |1\rangle) \otimes 1/\sqrt{2}(|0\rangle - |1\rangle)$

(3) The tensor product $1/\sqrt{2}(|0\rangle + |1\rangle) \otimes 1/2(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

3.13 Factoring

The Quantum Fourier Transform circuit in Figure 5 will display the matrix shown in Listing 9.

```
0.354   0.354          0.354       0.354          ...
0.354   0.25+0.25i     0.354i      -0.25+0.25i    ...
0.354   0.354i         -0.354      -0.354i        ...
0.354   -0.25+0.25i    -0.354i     0.25+0.25i     ...
0.354   -0.354         0.354       -0.354         ...
0.354   -0.25-0.25i    0.354i      0.25-0.25i     ...
0.354   -0.354i        -0.354      0.354i         ...
0.354   0.25-0.25i     -0.354i     -0.25-0.25i    ...
..
```

Listing 9. QFT With No Factoring

In texts [22], the n-qubit QFT is the matrix

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^{1} & \omega^{2} & \dots & \omega^{N-1} \\ 1 & \omega^{2} & \omega^{4} & \dots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

where $N = 2^n$ and ω is a primitive N'th root of unity.

By factoring out $\frac{1}{\sqrt{8}}$ (0.35355) using the suffix operator (/) at the end of the circuit, it is easier to see that the result of the circuit is the three-qubit QFT, as in Listing 10.

```
[2]  :H__:S10_:T20:_H_:_S10:__H
:C02:C20:C02/0.35355
1   1                  1          1                  ...
1   0.707+0.707i       1i         -0.707+0.707i      ...
1   1i                 -1         -1i                ...
1   -0.707+0.707i      -1i        0.707+0.707i       ...
1   -1                 1          -1                 ...
1   -0.707-0.707i      1i         0.707-0.707i       ...
1   -1i                -1         1i                 ...
1   0.707-0.707i       -1i        -0.707-0.707i      ...
..
```

Listing 10. QFT Factored

4. Examples

4.1 Oracles for the Grover Search

The two-qubit Grover Search tries to determine the phase encoding of the input quantum state. The algorithm uses a black box circuit, called an Oracle, to initially change the phase of one of the basis kets in a balanced superposition two-qubit quantum state. It then uses inversion to the mean to amplify the phase difference before a final measurement. Listing 11 shows four oracle gate sequences to change the phase of the input in each of the possible ways, that are alternatives to the built-in QQCS :Og gate.

```
(1)  |00>:H2:_H:C01:_H
[1  0  0  0]  H2 _H  C01  _H
[0.5  0.5  0.5  -0.5]
(2)  |00>:H2:S_:_H:C01:_H:S_
[1  0  0  0]  H2  S_  _H  C01 _H  S_
[0.5  0.5  -0.5  0.5]
(3)  |00>:H2:_S:_H:C01:_H:_S
[1  0  0  0]  H2  _S  _H  C01  _H  _S
[0.5  -0.5  0.5  0.5]
(4)  |00>:H2:Y2:_H:C01:_H:Y2
[1  0  0  0]  H2  Y2  _H  C01  _H  Y2
[-0.5  0.5  0.5  0.5]
```

Listing 11. Four Oracles For Grover Search

Listing 11 Explanation

(1) Change the phase of $|11\rangle$.

(2) Change the phase of $|10\rangle$

(3) Change the phase of $|01\rangle$.

(4) Change the phase of $|00\rangle$.

DOI: https://doi.org/10.30564/jcsr.v3i4.3567

4.2 Modular Arithmetic Subroutine

The implementation of Shor's algorithm[23] needs a subroutine circuit to compute $g(x) = (2x) \bmod 15$, from 1 to the modulus minus 1. Instead of a straightforward, and inefficient, implementation, the book presents a simple qubit swapping circuit based on the bit patterns of the modulo computation. Listing 12 shows the gates of the swap circuit assigned to name, ss, which then can be used like any other gate. The named gate is applied to the four-qubit values from $|0001\rangle$ to $|1110\rangle$. The result shows the resulting quantum state of each of the 16 inputs, which in each case is a single basis ket whose binary value equals that of the $g(x)$ calculation.

```
(1) #$rzeroes
(2)  ss:C03:C30:C03:C01__
:C10__:C01__:_C01_:_C10_:_C01_
[]  C03 C30 C03 C01__
C10__ C01__ _C01_ _C10_ _C01_=
1 . . . . . . . . . . . . . . .
. . . . . . . . 1 . . . . . . .
. 1 . . . . . . . . . . . . . .
. . . . . . . . . 1 . . . . . .
. . 1 . . . . . . . . . . . . .
. . . . . . . . . . 1 . . . . .
. . . 1 . . . . . . . . . . . .
. . . . . . . . . . . 1 . . . .
. . . . 1 . . . . . . . . . . .
. . . . . . . . . . . . 1 . . .
. . . . . 1 . . . . . . . . . .
. . . . . . . . . . . . . 1 . .
. . . . . . 1 . . . . . . . . .
. . . . . . . . . . . . . . 1 .
. . . . . . . 1 . . . . . . . .
. . . . . . . . . . . . . . . 1
(3)  |0001>:ss
[|0001>]
ss [|0010>]
(4) |0010>:ss
[|0010>]
ss [|0100>]
. . .
(9)  |0111>:ss
[|0111>]
ss [|1110>]
(10) |1000>:ss
[|1000>]
ss [|0001>]
(11)  |1001>:ss
[|1001>]
ss [|0011>]
. . .
(15)  |1101>:ss
[|1101>]
ss [|1011>]
(16)  |1110>:ss
[|1110>]
ss [|1101>]
```

Listing 12. Shor's Algorithm Subroutine

Listing 12 Explanation

(1) set a switch to display zeros as periods

(2) Assign the swap circuit to the custom gate name **ss.** The following display is the circuit's equivalent gate matrix.

(3) Invoke the :**ss** gate circuit on the initial value $|0001\rangle$. The output that follows displays the quantum state initial value in ket format, then the gate name, then the quantum state resulting from the execution of the gate, $|0010\rangle$ again in ket format.

(4) Shows that $|0010\rangle \mapsto |0100\rangle$.

(…) …

(16) Shows that $|1110\rangle \mapsto |1101\rangle$.

4.3 The Bernstein-Vazirani Oracle

The Bernstein-Vazirani algorithm [24] can be written in QQCS as shown in Listing 13.

```
(1)  | 0 0 0 1>:H4:Ob4:H3_:M3_
M1={010:1}
[ | 0 0 01>]  H4  Ob4  H3_
0.707|0100>-0.707|0101>
(2) |0001>:H4:Ob(3)4:H3_:M3_
M1={011:1}
[ | 0 0 0 1>]  H4  Ob(3) 4  H3_
0.707|0110>-0.707|0111>
```

Listing 13. The Bernstein-Vazirani Algorithm

Listing 13 Explanation

(1) the Bernstein-Vazirani circuit; the oracle generates a random hidden string, which the measure shows as 010.

(2) a version of the Bernstein-Vazirani circuit in which the oracle's hidden string is set by the parameter to 3; the measure shows 011.

5. Conclusions

QQCS is a simple linear notation for the simulation of quantum circuits. It is an educational tool that can be easily used by students new to Quantum Computing.

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

It provides automatic mathematical analysis of circuits by incorporating the matrix mathematics necessary to provide insight into circuit operation, and by displaying the details at each execution step, something not available from quantum computer execution.

Installation

QQCS is installed with the Node Package Manager. First, install NodeJS. Then, at the command line, enter:

npm install qqcs

To run, go to the node_modules directory, and enter:

node qqcs -or- node qqcs/qdesk.js

Use the command line switch -h to get help.

Acknowledgement

The circuit diagrams in this paper were constructed using the QPIC software package [25].

References

[1] A. Cross, L. Bishop, J. Smolin and J. and Gambetta, "Open Quantum Assembly Language," 2017. [Online]. Available: https://arxiv.org/pdf/1707.03429.pdf.

[2] IBM, "IBM Quantum Experience," 2019. [Online]. Available: http://quantumexperience.ng.bluemix.net/.

[3] M. Mykhailova and K. M. Svore, "Teaching Quantum Computing through a Practical Software-driven Approach: Experience Report," in SIGCSE '20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 2020.

[4] B. Heim, M. Soeken, S. Marshall, C. Granade, M. Roetteler, A. Geller, M. Troyer and K. Svore, "Quantum Programming Languages," Nat Rev Phys 2, pp. 709-722, 2020.

[5] QISKit, "The QISKit SDK for quantum software development," 2019. [Online]. Available: https://github.com/QISKit.

[6] QuTIP, "Quantum Toolbox In Python," 2019. [Online]. Available: http://qutip.org/.

[7] Microsoft, "The Q# User Guide," 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/quantum/user-guide/.

[8] D. S. Steiger, T. Häner and M. Troyer, "ProjectQ: An Open Source Software Framework for Quantum Computing," 2018. [Online]. Available: https://arxiv.org/abs/1612.08091.

[9] Toqito, "toqito - a Python library for studying various objects in quantum information: states, channels, and measurements," 2021. [Online]. Available: https://github.com/vprusso/toqito.

[10] QuNetSim, "QuNetSim -a quantum network simulation framework," 2021. [Online]. Available: https://github.com/tqsd/QuNetSim.

[11] Interlin-q, "Interlin-q - a simulation platform for distributed quantum algorithms," 2021. [Online]. Available: https://github.com/Interlin-q/Interlin-q.

[12] Cirq, "Cirq - a Python library for writing, manipulating, and optimizing quantum circuits and running them against quantum computers and simulators," 2021. [Online]. Available: https://github.com/quantumlib/cirq.

[13] QRAND, "QRAND - a smart quantum random number generator for arbitrary probability distributions," 2021. [Online]. Available: https://github.com/pedror-rivero/qrand.

[14] Qrack, "Qrack - a GPU-accelerated HPC quantum computer simulator framework," 2021. [Online]. Available: https://github.com/vm6502q/qrack.

[15] Pulser, "Pulser - a Python library for programming neutral-atom quantum devices at the pulse level," 2021. [Online]. Available: https://github.com/pasqal-io/Pulser.

[16] QCOR, "QCOR - a quantum-retargetable compiler platform providing language extensions for both C++ and Python that allows programmers to express quantum code as stand-alone kernel functions," 2021. [Online]. Available: https://github.com/ornl-qci/qcor.

[17] XACC, "XACC - a service-oriented, system-level software infrastructure in C++ promoting an extensible API for the typical quantum-classical programming, compilation, and execution workflow," 2021. [Online]. Available: https://github.com/eclipse/xacc.

[18] Yao, "Yao - a framework that aims to empower quantum information research with software tools in the Julia programming language," 2021. [Online]. Available: https://github.com/QuantumBFS/Yao.jl.

[19] Quantify, "Quantify - a Python based data acquisition platform focused on Quantum Computing and solid-state physics experiments," 2021. [Online]. Available: https://gitlab.com/quantify-os.

[20] M. A. Nielsen and I. L. and Chuang, Quantum Computation and Quantum Information 10th Anniversary Ed, New York: Cambridge University Press, 2010.

[21] E. Rieffel and W. Polak, Quantum Computing, A Gentle Introduction, Cambridge: MIT Press, 2011.

[22] R. S. Sutor, Dancing With Qubits, Birmingham: Packt Publishing, 2019.

[23] C. C. Moran, Mastering Quantum Computing with IBM QX, Birmingham: Packt Publishing, 2019.

[24] J. Abhijith and e. al, "Quantum Algorithm Implementations for Beginners," 2020. [Online]. Available: https://arxiv.org/pdf/1804.03719.pdf.

DOI: https://doi.org/10.30564/jcsr.v3i4.3567

[25] QPIC, "QPIC (2018) Creating quantum circuit diagrams in TikZ," 2018. [Online]. Available: https://github.com/qpic/qpic.

Appendix A

Linear Notation Syntax

Meta-symbols

::= is defined as
| alternative
e empty
'x' x is a grammar symbol, not a meta-symbol

Grammar

```
          Pgm   ::=  stmt  stmt-list  eof
    stmt-list   ::=  eol  stmt  stmt-list | e
         stmt   ::=  ident  gate-sequence |
                     initial-value  gate-sequence
initial-value   ::=  q-state | q-state-list | e
gate-sequence   ::=  g-seq-tail  g-factor
   g-seq-tail   ::=  : gates  g-seq-tail | e
     g-factor   ::=  / unop  Complex | e
  q-state-list  ::=  ( q-state )  q-state-list | e
      q-state   ::=  unop v-comp  p-state-tail
p-state-tail    ::=  addop v-comp  p-state-tail | e
        gates   ::=  full-gate  gates | e
    full-gate   ::=  gate  gate-suffix | ident
  gate-suffix   ::=  gate-angle  gate-repl
  gate-angle    ::=  ( unop Real reals ) | e
   gate-repl    ::=  integer | e
       reals    ::=  , unop Real reals | e
     v-comp     ::=  coeff ket
       coeff    ::=  Complex | e
         ket    ::=  '|' integer >
     Complex    ::=  complex | Real
        Real    ::=  real | integer
       addop    ::=  + | -
       unop     ::=  - | e
```

 DOI: https://doi.org/10.30564/jcsr.v3i4.3567

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Comparative Analysis of Scheduling Algorithms Performance in a Long Term Evolution Network

Bamidele Moses Kuboye*

Department of Information Technology, School of Computing, The Federal University of Technology, Akure, Nigeria

ARTICLE INFO

Article history
Received: 13 August 2021
Accepted: 14 September 2021
Published Online: 29 September 2021

Keywords:
Algorithms
LTE
Scheduling
Network
Performance

ABSTRACT

The advancement in cellular communications has enhanced the special attention given to the study of resource allocation schemes. This study is to enhance communications to attain efficiency and thereby offers fairness to all users in the face of congestion experienced anytime a new product is rolled out. The comparative analysis was done on the performance of Enhanced Proportional Fair, Qos-Aware Proportional Fair and Logarithmic rule scheduling algorithms in Long Term Evolution in this work. These algorithms were simulated using LTE system toolbox in MATLAB and their performances were compared using Throughput, Packet delay and Packet Loss Ratio. The results showed Qos-Aware Proportional Fair has a better performance in all the metrics used for the evaluation.

1. Introduction

The rapid growth of wireless broadband mobile communication is astronomical, as a result, Long Term Evolution (LTE) has been embraced by a lot of subscribers all over the world. The 3rd Generation Partnership Project (3GPP) developed LTE as an emerging wireless technology in the path of mobile broadband evolution. Long Term Evolution (LTE) was developed as an all IP network to achieve a higher data rate, low latency, scalable bandwidth and mobility as well as wide coverage [1]. The LTE network enhanced the data rate in other to provide the radio resources for various highly demanded services in other to give a level of satisfaction of Quality-of-Service (QoS) to all active subscribers. LTE uses Orthogonal Frequency Division Multiple Access (OFDMA), Single Carrier- Frequency Division Multiple Access (SC-FDMA) in the Downlink (DL) and Uplink (UL) respectively [2]. LTE supports up to 300 Mbps, 75 Mbps in the downlink and uplink for data transmission respectively using a bandwidth from 1.25 MHz to 20 MHz. These requirements meet the needs of diverse network operators with different bandwidth allocations to give support for different services to their subscribers [3,4].

Most of the services on LTE involve high-speed data, multimedia services and so on. It is the last effort to the provision of 4th generation (4G) radio network. The revolution towards 4G started with the UMTS 3G technologies increasing their data rates and improving network architecture to 3.5G with High Speed Packet Access (HSPA) and HSPA evolution. These networks moved into 4G LTE to attain data rates of 100Mbps, 50Mbps in DL and UL respectively [5,6]. LTE used the Radio Resource Management (RRM) to manage the

**Corresponding Author:*
Bamidele Moses Kuboye,
Department of Information Technology, School of Computing, The Federal University of Technology, Akure, Nigeria;
Email: bmkuboye@futa.edu.ng

DOI: https://doi.org/10.30564/jcsr.v3i4.3555

limited radio resources. Thus, improves the data rate and secure quality of service (QoS) provisioning. LTE downlink scheduling is a component of RRM responsible for the allocation of shared radio resources among their user equipment's (UEs) [4]. Furthermore, scheduling strategy plays a vital role in system performances such as throughput, delay, fairness, loss rate and so on. This paper described the features of LTE network that have direct impact on scheduling strategy in section 2. Section 3 described the related works on scheduling algorithms. Section 4 and 5 discussed the features QoS Aware Proportional Fair (QAPF), Exponential Proportional Fairness (EX/PF) and LOG rule and the performance metrics used for the simulation. In section 6, performance of QAPF, EX/PF and LOG rule scheduling algorithms were analyzed and compared.

2. LTE Architecture

The architecture of LTE is founded on flat, Internet Protocol (IP) requirements of 3GPP Technologies [2]. LTE system architecture is made up of Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and the Evolved Packet Core (EPC) as depicted in Figure 1 [7,8].

2.1 Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

The E-UTRAN controls the radio communications between the mobile and EPC [9]. The E-UTRAN is the access network has evolved-NodeBs (eNodeBs) and User Equipments (UEs). Also, it supports orthogonal frequency-division multiple access (OFDMA), Multiple Inputs and Multiple outputs (MIMO), management of the radio resources as well as security of transmitted data [3]. It is the base station that manages radio resources as used in GSM and has connection to the UEs where network air interface roles is performed [3,11,12]. As seen in Figure 1, LTE-Uu is the radio link between the UEs and eNodeB.

2.2 The Evolved Packet Core (EPC)

The EPC is the core network and enables exchange of data packets with the internet as well as UE while maintaining a given QoS [3]. EPC contains Home Subscriber Service (HSS), Policy Control and Charging Rules Function (PCRF), Mobility Management Entity (MME), P-GW and Serving Gateway (S-GW) [12]. The Home Subscriber Server (HSS) is the central database that contains information on the network operator's subscribers while Packet Data Network (PDN) Gateway (P-GW). Access point name (APN) identifies each data packet and the serving gateway (S-GW) forwards data between enodeB and the P-GW. The S1 interface is used to connect the eNodeB to EPC as seen in Figure 1. The MME controls signaling messages and HSS. Some of the other functions of EPC are Network access control, authentication, authorization, admission control, policy and charging enforcement, packet routing and transfer,

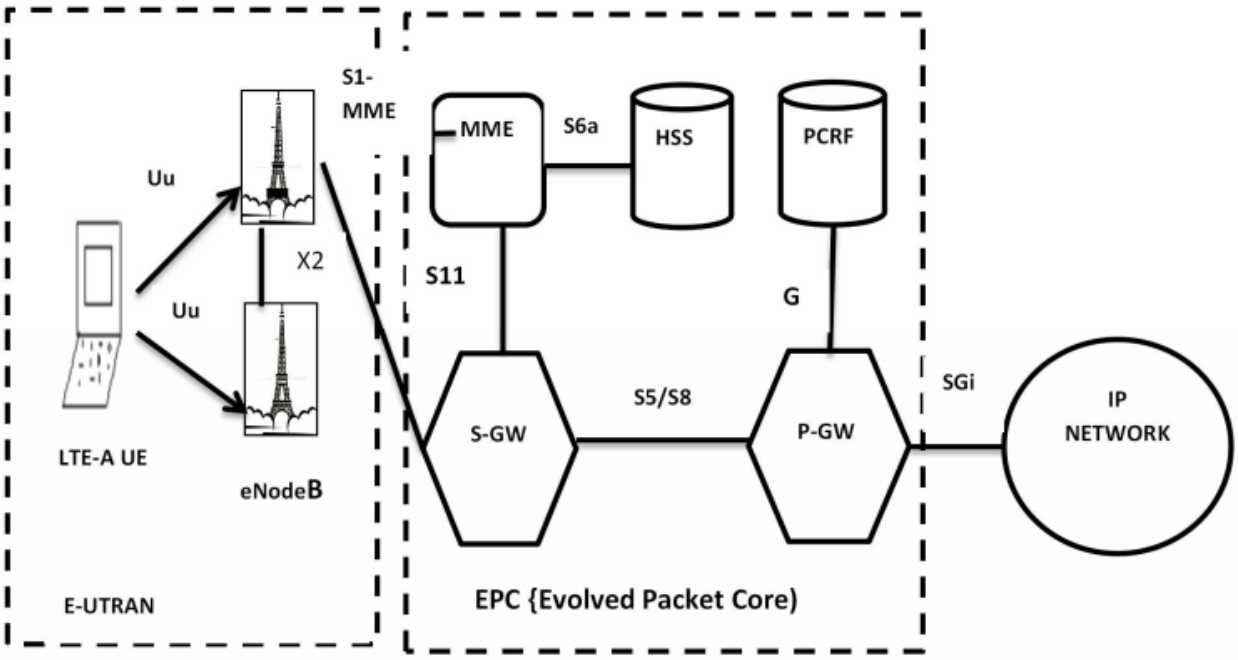

Figure 1. LTE Architecture [7].

 DOI: https://doi.org/10.30564/jcsr.v3i4.3555

security and others [8].

3. Related Works

The deployment of an appropriate scheduling algorithm will make wireless communications more effective. Also, determination of the appropriate algorithm that provides the optimal use in the face of scarcity of radio resources will be of great value. Some previous work done by authors on scheduling algorithms that have shown appreciable improvements in literature are discussed in this section. A proportional fair (PF) scheduling algorithm built on INS was proposed by Wang et al [13]. In the proposed scheme, the fairness was improved without passing high difficulty to the system. The results of the simulation showed that the proposed algorithm can efficiently increase the throughput of LTE users as well as improve the system fairness. QoS aware proportional fair (QAPF) downlink scheduler for LTE network was by Myo and Mon [14]. Its purpose was to optimize the use of available resources while maintaining QoS requirements of different classes of service in GBR and non-GBR. The algorithm when compared with Modified- Largest Weighted Delay First (MLWDF) and Exponential (EXP) rule shows that a lower packet loss rate can be maintained for nonGBR bearers. At the same time, GBR bearers will have a high performance in delay and packet loss rate. Sadiq et al [15] propounded a LOG rule algorithm, though similar to exponential (EXP) rule but uses logarithmic function on delay to calculate the scheduling parameters. It gave fairness to users when is in poor channel quality of service.

A new scheduling algorithm for downlink transmission in LTE was offered by Bechira et al [6]. This scheduler performance was evaluated and compared to Round Robin (RR), the opportunist Max rate and the Proportional Fair (PF) scheduler. The proposed algorithm improves the throughput in LTE system according to the simulation results. Elhadad et al [16] proposed Enhanced Proportional Fair (E-PF) Scheduling Algorithm for LTE in order to enhance the capacity of LTE and the proposed scheduler was compared with the original Proportional Fair. The results showed improvement in the capacity of the LTE and as well as fairness to the distribution of the resources among the users. Sudheep and Rebekka [17] presented a Proportional equal throughput (PET) scheduler using fair scheduling approach in LTE. This work modified Blind Equal Throughput (BET) algorithm and Proportional Equal Throughput (PET) algorithm emanated. The simulation showed that PET gives better fairness performances compared to BET without a significant decrease in system throughput.

An enhanced PF scheduling algorithm for LTE networks was proposed by de Oliveira et al [18]. The paper used the Latency-Rate (LR) server theory and system characteristics specified by the LTE standard for both theoretical and simulation investigations. The results show a better performance when compared with PF and MLWDF scheduler. Uyan and Gungor [19] examined performances of some algorithms using throughput and fairness and thereafter, proposed a new QoS-aware downlink scheduling algorithm (QuAS). The simulation shows an increase in the QoS-fairness and overall throughput of the edge users without producing a substantial degradation in the system throughput when compared with best CQI, PF, RR and Coordinated Multi Point (CoMP) structure with RR. Yaqoob et al [20] presented an enhanced EXPRULE (eEXPRULE) scheduling algorithm for real-time (RT) traffic in LTE network. The scheduler shows improvement on all the metrics used by most scheduler reviewed.

4. Scheduling Algorithms Used

Scheduling algorithm is not defined in LTE and various approaches have been presented to address this issue of scheduling algorithms [18,20]. Some results have shown some significant improvements in literature. Therefore, QAPF, EX/PF and LOG Rule are discussed for the purpose of this work:

4.1 QoS Aware Proportional Fair (QAPF)

QAPF is a downlink scheduler for LTE network proposed by Myo and Mon [14]. QAPF defines four MAC-QoS-traffic types as Voice over IP (VoIP), live video streaming, video streaming and e-mail as seen in Table 1. Firstly, QAPF differentiates different QoS classes by defining MAC bearer types as Guaranteed Bit Rate (GBR) and non-Guaranteed Bit Rate (nonGBR). GBR has Voice over Internet Protocol (VOIP), Live-video Streaming while nonGBR has video streaming and Email.

The QAPF directs the incoming IP packets into MAC QoS classes as shown Figure 2. Thereafter, the priority candidate lists are generated for the GBR and nonGBR bearer types in time domain (TD) scheduling. The TDS prioritized GBR and nonGBR using their Head of Line (HOL) delay. In GBR, the emergency bearers which have delayed closing to the maximum delay are first extracted.These extracted emergency bearers are sorted in descending order according to their delay. The priority for *nonGBR* $Pi_(t)$ bearer *i* at time *t*, is:

$$P_i(t) = argMax\left[w_i * \frac{r_i}{\bar{r}_i}\right] \quad (1)$$

DOI: https://doi.org/10.30564/jcsr.v3i4.3555

where, *wi* equals weight factor of nonGBR bearer i, *ri* equals instant throughput and is the average throughput for bearer *i*. The time average throughput of user is updated by the moving average as:

$$\bar{r}_i(t) = (1-a)\bar{r}_i(t-a) + ar_i(t) \quad (2)$$

where $a = \frac{2}{1+N}$ is scaling factor of *N* time period.

The frequency domain (FD) assigned physical resource blocks to each user according to the priority list. The motive is to guaranteeing the QoS requirements of different service classes while maintaining the fairness and maximizing the system throughput.

Table 1. CQI to MAC-QoS Class Mapping

Bearer Type	Traffic Type	Priority	Packet Delay Budget	Mac-QoS Class
GBR	VOIP	2	100ms	Class 1
	Live-video Streaming	4	150ms	Class 2
NonGBR	Video Streaming	7	300ms	Class 3
	Email	8	300ms	Class 4

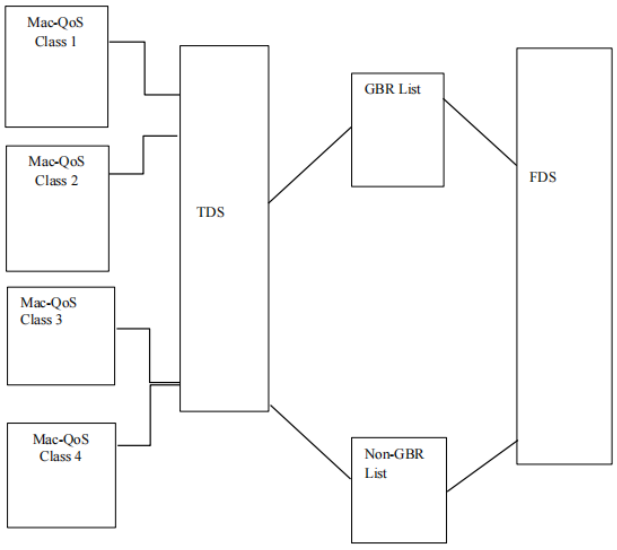

Figure 2. QAPF Mac-classes Framework [10]

4.2 Exponential Proportional Fairness (EX/PF) Scheduler

The EX/PF scheduling algorithm was proposed to give support to multiple traffic types so that Real-Time (RT) traffic will be prioritized over non-RT traffic [21]. Its metrics is calculated as follows:

$$W_{i,j} = \exp\left(\frac{\alpha_i D_{HoLi} - X}{1+\sqrt{X}9}\right)\frac{r_i(t)}{\bar{R}_i(t)} \quad (3)$$

where X is given as:

$$X = \frac{1}{N_{rt}} \sum_{i=1}^{N_{rt}} \alpha_i D_{HoLi} \quad (4)$$

N_{rt} denotes the number of active UEs for RT traffics, $\bar{R}_i(t)$ is the weight factor, is the previous average throughput of the user until time t while stands for the expected data-rate for the user i at time t, D_{HoLi} expresses the head of line (HOL) packet delay , that is, difference between the current time and arrival time of a packet [22,23].

4.3 Logarithm Rule Scheduling Algorithm

LOG rule algorithm balances QoS like delay and robustness. The algorithm allocates resources to users as EXP rule does with a prior knowledge of arrival and statistics of traffic channel [16].

$$\mathrm{LOG}_{rule} = max\left[b_i \log\left(c + \alpha_i D_{HoL,i}\right)\frac{r(t)}{\bar{R}_i(t)}\right] \quad (5)$$

where α_i, b_i and c are tunable parameters. Optimal parameters defined as

$b_i = \frac{1}{\frac{r(t)}{\bar{R}_i(t)}}$ and c = 1.1, $\alpha_i = \frac{5}{0.99 r_i}$ [22,23].

5. Performance Metrics

The following parameters where used:

Throughput *(th)* measures the rate of useful bits successfully transmitted through a network by a user per unit time. It uses Equation 6 for this:

$$Throughput = \frac{B}{Tsim} \quad (6)$$

where B is the total amount of bits received while *Tsim* false is the total simulation time.

Average packet delay experienced by UE is the arrival time between the packets in the Queue to their departure. The average delay of the ith flow can be expressed by using Equation (7) [7]:

$$D_i = \frac{1}{N}\sum_{j=0}^{N}\left[T_d(j) - T_s(j)\right] \quad (7)$$

where $T_s(j)s$ stands for the time when the j'th packet was transmitted from its source and N is the number of packets used.

Packet Loss Ratio (p) indicates the percentage of packets that missed their deadlines and is calculated as:

$$P = \left(\frac{P_{transmit} - P_{receive}}{P_{transmit}}\right) \times 100 \quad (8)$$

where $P_{transmit}$ false is total size of packets transmitted, while $P_{receive}$ false is the total size of packets arrived [22].

6. Results of the Simulation

In this section, the performance of QAPF, LOG-RULE and enhanced proportional fair (EX-PF) are compared. The LTE system toolbox in MATLAB is used using the

 DOI: https://doi.org/10.30564/jcsr.v3i4.3555

parameters stated in Table 2. The LTE system Toolbox is an ideal application to simulate, analyze, and test the physical layer of LTE networks. It is also suitable to accelerate LTE algorithm and verify designs, prototypes, implementations compliance with the LTE standard [24].

Table 2. Simulation parameters

Parameters	Value
Bandwidths	$20MH_z$
Operating Frequency	$2GH_z$
Numbers of RB	25
Scheduling Time(TTI)	1ms
Number of Slot Carrier	300
Slot Duration	1ms

The first analysis evaluated the throughput performance of QAPF, EX-PF and LOG Rule. The simulation results are displayed in Figure 3. It is observed that the throughputs for the three algorithms are quite close. However the QAPF performed better than the EX-PF and the LOG rule.

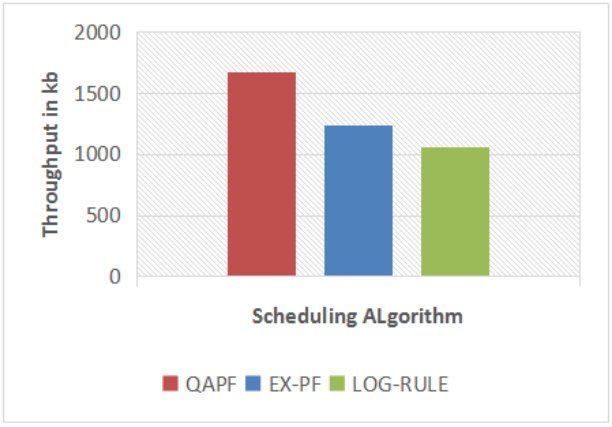

Figure 3. Throughput

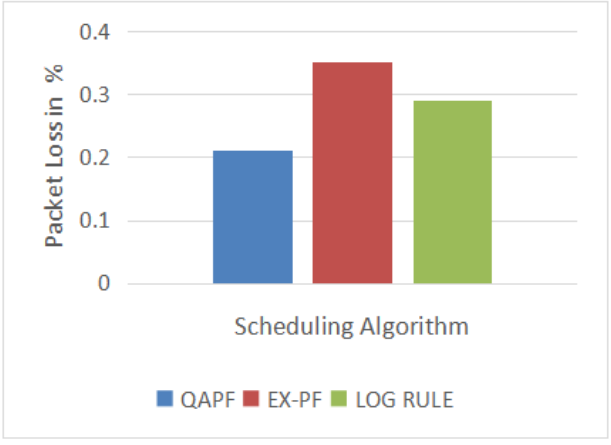

Figure 4. Packet Loss ratio

The second analysis evaluated the Packet Loss Ratio of QAPF, EX-PF and LOG rule shown in Figure 4. The lower the PLR value, the better the scheduler, EX-PF has a highest Packet loss ratio followed by LOG rule and QAPF. Therefore, QAPF performed better than EX-PF and LOG rule.

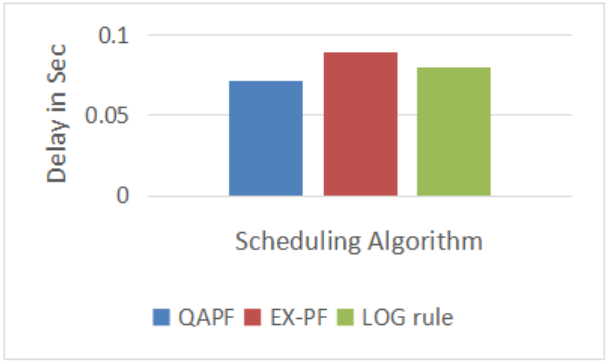

Figure 5. Delay Algorithm

Third analysis evaluated the packet average delay and it was observed that EX-PF has the highest Delay followed by LOG rule and QAPF. QAPF performs better than EX-PF and LOG Rule as shown in Figure 5.

7. Conclusions

The performances of the algorithms were evaluated and compared using packets loss, average delay and throughput. The following discoveries were made: QAPF has the highest throughput, lowest average delay and PLR when compared to EX-PF and LOG Rule. EX-PF has the highest PLR and delay while LOG Rule has the least performances in all the three metrics. In a reliable communication such as data and voice, throughput and packet delivery are very important in which QAPF is more appropriate according to the results of the research.

References

[1] Lawal M.A, Saidu I. Mohammed A., and Sade Y.A.(2017). Downlink Scheduling Algorithms in LTE Networks: A Survey IOSR Journal of Mobile Computing & Application (IOSR-JMCA) e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 4, Issue 3 PP 01-12 www.iosrjournals.org.

[2] Sulthana S. F. and Nakkeeran R. (2014). Study of Downlink Scheduling Algorithms in LTE Networks, Journal Of Networks, Vol. 9, No. 12.

[3] Mousavi H., Iraj S. Amiri, M.A. Mostafavi , C.Y. Choon (2019). LTE physical layer: Performance analysis and evaluation Applied Computing and Informatics 15 pp 34-44.

[4] Chadchan S. M. and Akki C. B. (2013). A Fair

DOI: https://doi.org/10.30564/jcsr.v3i4.3555

Downlink Scheduling Algorithm for 3GPP LTE Networks, I.J. Computer Network and Information Security, 2013, 6, 34-41. Published Online May 2013 in MECS (http://www.mecs-press.org/).
DOI: 10.5815/ijcnis.2013.06.05.

[5] Kuboye, B. M. (2019). Long Term Evolution (LTE) Network Evaluation in the South-West Region of Nigeria, European Journal of Engineering Research and Science, 4(3), 86-92.
DOI: https://doi.org/10.24018/ejers.2019.4.3.1160.

[6] Bechira N., Nasreddinea M., Mahmouda A., Walida H. and Sofiena M. (2014) Novel Scheduling Algorithm for 3GPP Downlink LTE Cellular Network Procedia Computer Science 40 (2014) 116-122.

[7] Kuboye, B.M. (2018) Performance Evaluation of Scheduling Algorithms for 4G (LTE). Communications and Network, 10, 152-163. https://doi.org/10.4236/cn.2018.104013.

[8] Zyren J. (2007). "Overview of the 3GPP Long Term Evolution Physical Layer" White Paper, fre csale semiconductor.

[9] Matin M. A. (2014). Chapter 1 Evolution of Wireless and Mobile Communications", IGI Global.

[10] Mousavi H., Amiri I. S., Mostafavi M.A., Choon C.Y. "2019". LTE physical layer: Performance analysis and evaluation, Applied Computing and Informatics.

[11] Zhou (2012). From LTE to LTE-A, LTE-Advanced Air Interface Technology.

[12] Aggarwal C. and Srivastava K.(2016). Securing IOT devices using SDN and edge computing, International onference on Next Generation Computing Technologies (NGCT).

[13] Wang H. Z., Sun Z. H., Wang J., and Liu, F. (2014). Study on the Resource Scheduling Algorithm for LTE-Advanced Downlink Systems. Applied Mechanics and Materials, 577, 1017-1021. https://doi.org/10.4028/www.scientific.net/amm.577.1017.

[14] Myo I. M. and Mon M. T (2015). Qos-Aware Proportional Fair (QAPF) Downlink Scheduling Algorithm For Lte Network Proceedings Of Seventh The IIER International Conference, Singapore, 3rd January 2015, ISBN: 978-93-84209-80-3.

[15] Sadiq B., Madan R., and Sampath A.., (2009). Downlink Scheduling for Multiclass Traffic in LTE, Eurasip Journal of Wireless Communication Networks, vol. 2, pp. 9-13, Oct. 2009.

[16] Elhadad M. I., El-Rabaie E.M., Abd-Elnaby M. (2014). Enhanced PF Scheduling Algorithm for LTE Downlink System, Mobile Computing Vol. 3.1, www.mc-journal.org.

[17] Sudheep S. and Rebekka B., (2014) "Proportional equal throughput scheduler — A very fair scheduling approach in LTE downlink," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-6.
DOI: 10.1109/ICICES.2014.7034111.

[18] de Oliveira R. P., de Góis L. A. and Foronda A. (2018). Enhanced PF Scheduling Algorithm for LTE Networks, International Journal of Communication Networks and Information Security (IJCNIS) Vol. 10, No. 1.

[19] Uyan O.G., Gungor V.C. QoS-aware LTE-A downlink scheduling algorithm: A case study on edge users. Int J Commun Syst. 2019. https://doi.org/10.1002/dac.4066.

[20] Yaqoob J. I. A.Y., Pang W. L., Wong S. K. and K. Y. Chan (2020) Enhanced exponential rule scheduling algorithm for real-time traffic in LTE network, International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 2, pp. 1993~2002 ISSN: 2088-8708.
DOI: 10.11591/ijece.v10i2.pp1993-2002.

[21] Kuboye, B.M., A. J. Gabriel, A. F. Thompson, and V. O. Joseph (2018). Analysis of Algorithms in Long Term Evolution (LTE), Journal of Computer Science and Its Application, 25(2), 59-71, ISSN: 2006-5523. https://www.ajol.info/index.php/jcsia/article/view/179867.

[22] Mohd A, Mohd H O, Muhammed I. A, Rahmat B., (2014). Performance comparison of Downlink Packet Scheduling Algorithms in LTE Network, Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia.

[23] Nwawelu U. N., Ani C. I. and Ahaneku M. A., (2017). Comparative Analysis of the Performance of Resource Allocation Algorithms in Long Term Evolution, Nigerian Journal of Technology (NIJOTECH), Vol. 36, No. 1, pp. 163-171. http://dx.doi.org/10.4314/njt.v36i1.21.

[24] MathWorks. Simulink Documentation. Available at https://www.mathworks.com/help/lte/ accessed on 9/9/2021.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

REVIEW

Natural Language Processing and Its Challenges on Omotic Language Group of Ethiopia

Girma Yohannis Bade*

Department of Computer science, School of Informatics, Wolaita Sodo Uninveristy, Wolaita, Ethiopia

ARTICLE INFO

Article history
Received: 23 August 2021
Accepted: 26 September 2021
Published Online: 13 October 2021

Keywords:
Omotic group
NLP
Challenges
Application

ABSTRACT

This article reviews Natural Language Processing (NLP) and its challenge on Omotic language groups. All technological achievements are partially fuelled by the recent developments in NLP. NPL is one of component of an artificial intelligence (AI) and offers the facility to the companies that need to analyze their reliable business data. However, there are many challenges that tackle the effectiveness of NLP applications on Omotic language groups (Ometo) of Ethiopia. These challenges are irregularity of the words, stop word identification problem, compounding and languages 'digital data resource limitation. Thus, this study opens the room to the upcoming researchers to further investigate the NLP application on these language groups.

1. Introduction

1.1 Natural Language Processing (NLP) and its Application

You probably saw the news on the latest digital assistants that can book your next any appointment over the phone. And heard about the Artificial Intelligence (AI) algorithm that can answer eighth grade elementary science questions better than humans. You may have even interacted with a chatbot that can answer your simple banking questions. You are possibly carrying a mobile phone that can translate your sentences to 100 different languages in real time. All these technological achievements are partially fueled by the recent developments in NLP [1]. NPL is an application of artificial intelligence and offers the facility to companies that need to analyze their reliable business data. According to [2], the NLP's market is expected to grow 14 times in 2025 than it was in 2017. Some of the application of NLP are as follows according to [2]:

Market Intelligence

Marketers can use natural language processing to understand their customers in a better way and use those insights in creating effective strategies.

Sentiment Analysis

Humans have the gift of being sarcastic and ironic during conversations. With sentiment analysis, NPL helps to manage the mentions on social media and tackle them before they disseminate.

Hiring and Recruitment

We all will agree that the HR department performs one

**Corresponding Author:*
Girma Yohannis Bade,
Department of Computer science, School of Informatics, Wolaita Sodo Uninveristy, Wolaita, Ethiopia;
Email: girme2005@gmail.com

DOI: https://doi.org/10.30564/jcsr.v3i4.3614

of the most crucial tasks for the company: With the help of Natural Language Processing, this task can be done more easily.

Text Summarization

This is one of the NLP application and used to summarize the most important information from the vast content to reduce the process of going through the whole data in news, legal documentation and scientific papers.

Survey Analysis

The problem arises when a lot of customers take these surveys leading to exceptionally large data size. All of it cannot be comprehended by the human brain. That's where natural language processing enters the canvas. These methods help the companies to get accurate information about the customer's opinion and improve their performance.

Machine Translation

Machine Translation is one of the applications of NLP and uses a neural network to translate low impact content and speed up communication with its partners.

Email Filters

NLP makes use of a technique called text classification to filter emails. It refers to the process of classification of a piece of text into predefined categories.

Grammar Check

Yes, this natural processing technique is here to stay. Tools like Grammar provide tons of features in helping a person write better content. It is one of the most widely used applications of NLP that helps professionals in all job domains create better content.

Stemming algorithms

Stemming algorithms are commonly known in a domain of Natural Language Processing (NLP) and which has a positive impact on Information Retrieval (IR) system and Morphological Analysis. Now a day, information technology has contributed a great availability of recorded information to exist. The mass production of electronic information, digitalized library collections and the awareness of society, increased the demand for storing, maintaining and retrieving information in a systematic way [3]. Information retrieval (IR) one of such a systematic ways is designed to facilitate the access to stored information [4]. To enhance the effectiveness of IR performance, the suffix stripping process (stemmer) helps by reducing the different variants of terms into common forms as conflating the variants of words [9].

1.2 Capabilities NLP

Sentences segmentation: identifies where one sentence ends and another begins. Punctuation often marks sentence boundaries.

Tokenization: identifying individual words, numbers, and other single coherent constructs. Hashtags in Twitter feeds are example of constructs consisting of special and alphanumeric characters that should be treated as one coherent token. Languages such as Chinese and Japanese do not specifically delimit individual words in a sentence, complicating the task of tokenization.

Part-of-speech tagging: assigns each word in a sentence its respective part of speech such as a verb, noun, or adjective.

Parsing: derives the syntactic structure of a sentence. Parsing is often a prerequisite for other NLP tasks such as named entity recognition.

Name entity recognition: identifies entities such as persons, locations, and times within documents. After the introduction of an entity in a text, language commonly makes use of references such as 'he, she, it, them' instead of using the fully qualified entity. Reference resolution attempts to identify multiple mentions of an entity in a sentence or document and marks them as the same instance.These methods can tell us what people are saying, feeling, and doing or determine where documents are relevant to transactions. Companies need a new approach to combine the structured and unstructured components—the old ways don't really work—they just aren't effective.

1.3 Omotic Languages

Ethiopians are ethnically diverse [5], with the most important differences on the basis of linguistic categorization. Ethiopia has 86 different languages that can be classified into four major groups. The vast majority of languages belong to the Semitic, Cushitic, Omotic Group and Nilo-Sahara, these all are part of the Afro-Asiatic family [7].

The Omotic languages are predominantly spoken between the Lakes of southern Rift Valley and Southwest of Ethiopia around River Omo (hence their name). These language groups have 28 languages. However, they are little studied and the Afro-Asiatic membership of Omotic is controversial being regarded by some as an independent family. Omotic have affinities with Cushitic, another branch of Afro-Asiatic. The following table shows the

 DOI: https://doi.org/10.30564/jcsr.v3i4.3614

lists of Omotic languages.

Table 1. Lists of Omotic languages

Anfillo	Dime	Kachama-Ganjule	Nayi
Ari	Dizzi	Kara	Oyda
Bambassi	Dorze	Kefa	Shakacho
Basketto	Gamo-Gofa	Kore	Sheko
Bench	Ganza	Male	Welaita
Boro	Hammer-Banna	Melo	Yemsa
Chara	Hozo	Mocha	Zayse-Zergulla

1.4 Morphology in Omotic Language Groups

There is no grammatical gender. The main identification is between animate and inanimate. In animate nouns, gender is determined by sex. Inanimate nouns are inflected like masculine nouns. Only definite nouns are marked for plural, and the singular is unmarked. Omotic distinguishes subject and object by case suffixes as well as by tonal inflection. In some languages the subject case is marked (nominative) while the object remains unmarked (i. e., identical to the quotation form of the noun). In other languages the object is marked (accusative) while the subject is unmarked. The Ometo group shows a predominance of marked-nominative languages, whereas other North Omotic languages and the South Omotic ones have, mostly, accusative systems [8].

Morphology is the study of word structure [9]. All languages have word and morphemes. Morphemes are the minimal units of words that have a morphological meaning and cannot be subdivided further. There are two main types of morphemes: free and bound. Free morphemes can occur alone and bound morphemes must occur with another morpheme [9]. For the word "badly", an example of a free morpheme is "bad", and an example of a bound morpheme is "ly". The morpheme "ly" is bound because although it cannot stand alone. It must be attached to another morpheme to produce a word.

The Omotic Language has 29 consonant phonemes, including voiced glotalized consonant, which have been analyzed as consonant clusters. It also has five vowel phonemes, which can be combined to long vowels and diphthongs. In Ometo, there are two ways of forming words, affixation and compounding. Among three types of affixes (prefix, infix, suffix); suffixation, adding suffix (morpheme) to the word at the end is common. This process, in Ometo makes word lengthy [5].

Basically three types of affixes are there, prefixes, infixes, and suffixes.

Prefix:-is a morpheme that can be attached at the beginning of the word.

Infix:-this morpheme can be found at between of a word.

Suffix:-this can be added at the last of the word.

However, among these three morphemes, prefix and infix morphemes do not exist in Omotic group, the only morpheme that exists in Omotic group is suffix.

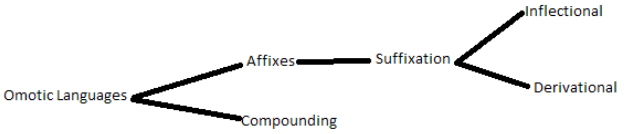

Figure 1. Omotic group morphology

2. Challenges of NLP

General challenges

NLP is a powerful tool with huge benefits, but there are still a number of Natural Language Processing limitations and problems:

- Contextual words and phrases
- Synonyms
- Irony and sarcasm
- Ambiguity
- Errors in text or speech
- Colloquialism and slang
- Domain specific languages
- Low resource languages
- Lack of research and development

Ambiguity

Ambiguity in NLP refers to sentences and phrases that potentially have two or more possible interpretations.

Lexical ambiguity

A word that could be used as a verb, noun, or adjective.

Semantic ambiguity

The interpretation of a sentence in context. For example, I saw the boy on the beach with my binoculars. This could mean that I saw a boy through my binoculars or the boy had my binoculars with him.

Syntactic ambiguity: In the sentence above, this is what creates the confusion of meaning. The phrase with my binoculars could modify the verb, "saw," or the noun, "boy."

Even for humans this sentence alone is difficult to interpret without the context of surrounding text. POS (part of speech) tagging is one NLP solution that can help solve the problem, somewhat.

DOI: https://doi.org/10.30564/jcsr.v3i4.3614

NLP Specific challenges on Omotic languages

a)Irregularity

Some of words in Omotic group are irregular. For instance, addussa 'long', adduqqees 'is getting long', and addussatetta 'length'are basically one word 'Long' classes but the stemmer results it in two forms'adduss-' and 'adduqq-'in Wolaita language which is one the popular Omotic language group. Even if it is possible in view of linguistic, it has a different sense in Information Retrieval point of view.

b)Stop words Concept

Stop words are functional (non-content bearing) words. They give sense for other words. The most suggested function words or stop words are propositions, conjunctions, articles and such likes. For example, the man jumped down. Here bolded terms are stop words. The issue of stop words is also worth mentioning in relation to retrieval effectiveness. The removal of stop words from indexing and query, results in effectiveness of retrieval by reducing storage requirement and increasing the matching of a query with index terms of a document [6]. Stop words in English, known and identifiable but in Omotic group they very confusing to identify them from others, for instance in Wolaita "I ba bala qottis" means He hide his mistakes. Form this statement "ba " has two literal meaning. One is "to go" and other indicate as stop word 'his'. SO identifying stop words in Omotic language group is very challenging task.

c)Compound word concept

Compounding is the second main word formation process in Omotic language group. Even if compound morphemes are rare in Omotic language, their formation process is irregular. As a result, it is difficult to determine the stem of compounds from which the words are made. The example below shows compounding in Wolaita which accounts majority of Ometo.

wora-kanna 'jackal', literally 'the dog of the forest'
demba hariya 'zebra, literally 'field donkey'
keetta-'asa 'family', literally 'the people of a house'
mache-'isha 'brother-in-law', literally 'wife's brother'
aaye-michchiyo 'aunt', literally 'mother's sister'

One of the application of NLP is stemming but somebody may face confusion which one to stem to get root word.

d)Limitation of digital datasets

As Omotic language is one of the least resourced language in Ethiopia, it suffers from the limitation of digital datasets. If somebody wants to make research on one of Omotic languages, he or she has to collect the real time data. There is no collected online accessible Omotic digital data.

Other challenges for NLP researches [10]:

Improvement of the performance of individual analyzers, especially at the semantic/pragmatic level,i. e having single actor but in different place, coreference system would consider them two different entities.

Domain adaptation methods to tune generic NLP processors to deal with process descriptions in a specific organization or sector. This may require the creation/ acquisition of tailored ontologies that help specifying with the right terms important parts of the process and relations among these relevant domain concepts.

Definition of new tasks, such as the detection of exclusivity, parallelism/concurrency, decision points, or iteration of tasks described in the text.

Use of world knowledge to improve the results

Each natural language has its own characteristics and features. So, it's quite difficult to follow the rules of ones for other languages. This is because of different prefixes and suffixes, and exceptions needs a special handling and a careful formation of frame with specific norms. These issues common for all languages not only for Omotic language groups.

3. Conclusions

Omotic language groups are morphologically rich language. This effect is due to its inflectional and derivational morphologies. Suffixes in Omotic language plays a great role in forming many variants of words. As a result, more than one combination of the suffixes can be appended to the root and; thus the length of the words in Omotic language is very long. Stemmer one of the NLP applications in information retrieval (search engines) is increasing recall without decreasing precision, because both document indexes and queries use stems.

Even though there are many capabilities in NLP like sentences segmentation, part-of-speech tagging, tokenization etc, there is a challenges in NLP researches like ambiguity, synonyms, contextual words, improvement in individual analyzer, and definition of new task. Event the above challenges are common to all languages, the most affecting challenges for NLP application on Omotic language groups are irregularity, stop words identification, compounding and limitation of digital datasets.

References

[1] https://www.software.slb.com/blog/natural-lan-

 DOI: https://doi.org/10.30564/jcsr.v3i4.3614

guage-processing---the-new-frontier?gclid=EAIaIQobChMI3NKS3ISu8gIVBertCh2AVA1yEAAYASAAEgL96vD_BwE.

[2] https://www.mygreatlearning.com/blog/trending-natural-language-processing-applications/.

[3] Lemma Lessa. "Development of stemming algorithm for wolaytta text."M.Sc. Thesis, Addis Ababa University, Department of Information Science, Addis Ababa,(2003).

[4] Salton,G. & McGill, N."Introduction to Modern Information Retrieval". New York: McGraw-Hill, (1983).

[5] O'Grady, W., (1997). Contemporary Linguistics: An Introduction. London: Longman.

[6] Savoy, Jacques. (1993). "Stemming of French Words Based on Grammatical Categories." In Journal of American Society for Information Science, 44(1):PP. 1-9.

[7] https://www.britannica.com/topic/Omotic-languages.

[8] http://www.languagesgulper.com/eng/Omotic.html.

[9] O'Grady, W., (1997). Contemporary Linguistics: An Introduction. London: Longman.

[10] Challenges and Opportunities of Applying Natural Language Processing in Business Process Management.

[11] https://tanzu.vmware.com/content/blog/3-key-capabilities-necessary-for-text-analytics-natural-language-processing-in-the-era-of-big-data.

DOI: https://doi.org/10.30564/jcsr.v3i4.3614

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Enhanced Information Systems Success Model for Patient Information Assurance

Lilian Adhiambo Agunga* **Joshua Agola** **Paul Abuonji**

School of informatics & innovative systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya

ARTICLE INFO

Article history
Received: 18 September 2021
Accepted: 9 October 2021
Published Online: 13 October 2021

Keywords:
Information assurance
ISS
Modeling
Privacy
Security
TAM
User satisfaction

ABSTRACT

The current health information systems have many challenges such as lack of standard user interfaces, data security and privacy issues, inability to uniquely identify patients across multiple hospital information systems, probable misuse of patient data, high technological costs, resistance to technology deployments in hospital management, lack of data gathering, processing and analysis standardization. All these challenges, among others hamper either the acceptance of the health information systems, operational efficiency or expose patient information to cyber attacks. In this paper, an enhanced information systems success model for patient information assurance is developed using an amalgamation of Technology Acceptance Model (TAM) and Information Systems Success Model (ISS). This involved the usage of Linear Structured Relationship (LISREL) software to model a combination of ISS and Intention to Use (ITU), TAM and ITU, ISS and user satisfaction (US), and finally TAM and US. The sample size of 110 respondents was obtained based on the total population of 221 using the Conhrans formula. Thereafter, simple random sampling was employed to select members within each category of employees to take part in the study. The questionnaire as a research tool was checked for reliability via Cronbach's Alpha. The results obtained showed that for ISS and ITU modeling, only perceived ease of use, system features, response time, flexibility, timeliness, accuracy, responsiveness and user training positively influenced the intention to use. However, for the TAM and ITU modeling, only TAM's measures such as timely information, efficiency, increased transparency, and proper patient identification had a positive effect on intension to use. The ISS and US modeling revealed that perceived ease of use had the greatest impact on user satisfaction while response time had the least effect on user satisfaction. On its part, the TAM and US modeling showed that timely information, effectiveness, consistency, enhanced communication, and proper patients identification had a positive influence on user satisfaction.

**Corresponding Author:*
Lilian Adhiambo Agunga,
School of informatics & innovative systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya;
Email: merabadhi@gmail.com

 DOI: https://doi.org/10.30564/jcsr.v3i4.3734

1. Introduction

Information assurance refers to the process of protecting data in electronic healthcare records system. Information assurances are the measures that are tailored for the protection of patient information in the healthcare organization process. According to [1], however, information assurance may involve responsibilities, coverage, and accountability of security professionals. It may also incorporate proactive as well as defensive procedures geared towards protecting information. Device interconnectivity and ubiquitous computing have continued to penetrate the healthcare sector. This has seen the rise in the development of technologies such as Medical Internet of Things (MIoT), which is also referred to as or Internet of Healthcare Things (IoHT), or Internet of Medical Things (IoMT). As discussed in [2], these technologies play a major role in the healthcare sector and hence the well-being of billions of people across the globe. It is explained in [3] that owing to the ubiquity of internetworking technologies such as MIoT, wireless implanted medical devices have gained increase in usage, application and complexity. One of the key drivers of the MIoT devices is their ability to monitor patients remotely. Unfortunately, this requires remote connectivity which with rapid growth in usage and complexity lead to increased threat of cyber security attacks [4]. Apart from these technologies, a number of repositories of information concerning the health status of the patients do exist. These repositories are collectively referred to as health information systems (HISs) and according to [5], they are created and managed in digital formats. The patients' records in this regards contains medical history including operations, hospitalizations, medications, laboratory results and relevant health care information.

Hospital Information System (HIS) is a class of health information systems widely utilized in clinical settings and according to [6], establishing the success rate of HISs is an ongoing research area. This is because its implications are of interest for researchers, physicians and managers. Healthcare information technology serves to bring forth reduction of healthcare costs as well as enhancements of its quality. As explained in [7], the deployment of information technology coupled with E-health is one of the underpinning developments geared towards open governance. For instance, blockchain technology (BC) has been deployed to facilitate safe delivery and secure management of healthcare data. The BC technology can also boost secure data sharing which can potentially reform the conventional healthcare practices. Ultimately, this can render healthcare more reliable and effective. As discussed in [8], proposals are being made for the block chain technology to be deployed for personalized healthcare administration.

BC primarily exhibits six key elements that make it attractive in HIS. These features include immutability, transparency, decentralization, autonomy, anonymity and being open source. As such, authors in [9] point out that there has been growing interest in employing the BC technology for safe and secure administration of healthcare. In addition, authors in [10] have proposed the deployment of this technology in biomedical while authors in [11] have suggested the deployment of BC to simulate the brain including thinking, and sharing of e-health data. Regarding medical data sharing, the BC technology can assure privacy and security as this data is transferred between clinical specialists and healthcare entities. In most health setups, healthcare data documentation has not been computerized, which renders this process ineffective and tiresome [12]. Efficient, accurate and cross validation checks as well as data retrieval are all possible from electronic health records system through automation of these procedures [13]. Authors in [14] point out that electronic data sharing among healthcare providers has led to the improvement of the healthcare services as well as reductions in clinical errors. To boost this electronic data sharing, information system standards play a key role [15,16].

This paper proposes information system success model with the attributes that can potentially curb the identified pitfalls of the current HIS. The main contributions of this paper include the following:

i. We investigate information system success (ISS) model dimensions that can enhance patient information assurance.
ii. Based on the identified information system success model dimensions, we model relationships among various Technology Acceptance Model (TAM) and ISS constructs.
iii. Depending on the correlation coefficients of the various paths, irrelevant constructs are eliminated to yield an enhanced ISS model for patient information assurance.

The rest of this paper is organized as follows: section II presents related work while section III gives an outline of the adopted methodology. On the other hand, section IV presents and discusses the modeling results. Finally, section V concludes the paper and gives future directions.

2. Related Work

A number of HIS technologies have been deployed in the healthcare sector, such as Electronic health (e-health), Medical Internet of Things (MIoT), Internet of Medical Things (IoMT, Internet of Healthcare Things (IoHT), and more recently, the blockchain (BC) enabled HISs. As poined out in [17], electronic medical records (EMR) system

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

usability is a major healthcare informatics issue owing to lack of standard user interfaces. In addition, patient harm as a result of usability errors and user-unfriendly functionalities. Another challenge of HIS revolves around ethical and privacy issues. As explained in [18], data security remains a challenge in most HISs as most software applications have bugs that can be compromised. On their part, authors in [19] consider data standardization as a major obstacle, owing to its inadequacy.

Considering MIoTs, it is pointed out in [20] that their implementations are dogged with insecure networks, limitations of power, storage and memory capacity. This renders MIoT infrastructure vulnerable to cyber attacks. Authors in [21] elaborate that to offer healthcare that is tailored to particular patients, unique identifiers should be developed to facilitate easy identification of patients and their healthcare data among various healthcare providers. However, majority of healthcare facilities lack this unique patient identifier that operates across multiple hospitals information systems such as HIS. On the other hand, authors in [22] discuss that soaring technological costs for healthcare technologies, resistance to embrace technology among shareholders, lack of standardization during data gathering and processing, privacy and security of patients' information are some of the factors that impede HIS implementation. The electronic healthcare records information has several implications in the decision making process in patient care and health policies. According to [16], the privacy and security of patients' digitized records is very key for the adoption of HIS. On the other hand, authors in [23] have identified resistance to technology adoption by physicians as being a hindrance towards automated healthcare provision. In addition, fear of potential misuse of patients' records by medical officers has been cited in [24] as being critical setback towards HER implementation.

To address some of the information assurance issues, authors in [25] have developed an Ethereum protocol based private BC for safe and secure use of remotely accessed patient data. Similarly, author in [26] has proposed a public BC for encryption, whose goal is to secure health data storage. On the other hand, an integrated BC approach for patient data sharing and management has been presented in [27]. Using this scheme, safe and secure storage and exchange of personal patient medical data is possible. On the other hand, authors in [28] have proposed a framework that facilitates automated evaluation of patients' healthcare status. On their part, authors in [29] have implemented a platform for healthcare information exchange. This scheme achieves both authenticity and privacy during patient electronic data exchange among various HIS platforms. In addition, a systematic and innovative architecture capable of not only protecting classified patient records but also address major privacy and security issues in patients' data has been developed in [30]. Similarly, a remote healthcare framework for monitoring, diagnosis and treatment of cancer tumors has been introduced in [31]. To achieve this goal, smart contracts were utilized.

3. Methodology

Based on the identified challenges of healthcare patient information assurance and the dimensions of information system success model, this research purposively adopted both ISS and TAM. In this regard, TAM was selected owing to its ability to offer theoretical underpinnings for technology adoption. On the other hand, ISS was chosen due to its ability to effectively technological features such as information quality, system quality and service quality to the adoption of various systems. As pointed out in [32], ISS serves to theoretically explain and estimate system usage as well as the underlying success factors.

3.1 Target Population and Sampling

This research targeted 5 healthcare facilities with 221 staff within Homabay County, Kenya. Included in the study are 60 data clerks, 40 healthcare records officers, 30 nursing officers, 71 clinical officers and 20 medical officers. This gives an approximate target population of 221 respondents as shown in Table 1.

Table 1. Target Population

Group	Target Population
Data Clerks	60
Health Records officers (HRIOS)	40
Nursing Officers	30
Clinical Officer	71
Medical Officers (Doctor)	20
Total	**221**

The sample size was obtained based on the Conhrans formula which allows the researcher to derive an appropriate sample size based on some required precision, confidence level and the probable proportion of the features that are inherent in the population.

$$n = \frac{n_0}{1 + \frac{(n_0 - 1)}{N}}$$

Where:

n_0 = Is Cochran's sample size recommendation

N = Is the population size

n = Is the new, adjusted sample size

Where n_0 is obtained from:

$$\frac{Z^2 pq}{e^2}$$

Here, e represents the desired level of precision, p is the proportion of the population which has the attribute in question, and q is (1 – p). On the other hand, z was obtained from the z-table. For a confidence level of 95%, the value of e=5%, giving a value of 1.96 for z. Then substituting these values in in the above formular gives the values in Table 2 below.

Table 2. Sample Size

Group	Target Population	Applied Sample size
Data Clerks	60	30
Health Records officers (HRIOS)	40	20
Nursing Officers	30	15
Clinical Officer	71	35
Medical Officers (Doctor)	20	10
Total	221	110

Based on the cumulative values for different target population proportion, the target population for this study was 221 respondents. As such, the next task was sampling during which the selection of members within each employees category to take part in the study was undertaken. After applying Cochran's formula, applied sample size was obtained for each category of employees, whose total was 110 as shown in Table 2. As such, this research utilized a sample size of 110 respondents who were then provided with the questionnaires. Within each employee applied sample size stratum, a simple random sampling was employed to select study respondents.

3.2 Reliability of Research Instrument

In this paper, Cronbach's Alpha was employed to evaluate the reliability of the questionnaire that was utilized for data collection. To achieve this, reliability coefficient was computed for all the variables under study. It was noted that Cronbach's Alpha lay between 0 and unity (1), where a coefficient of zero pointed to the questionnaire's lack internal consistency. On the other hand, a coefficient of unity (1) implied complete internal consistency of the employed questionnaire. Theoretically, a reliability coefficient of 0.7 or more is regarded as being sufficient.

3.3 Proposed Enhanced ISS Model for Patient Information Assurance

Although many models have been proposed to explain and predict the use of a system, the Information System Success model was designed to determine the factors most important in successful adoption of a new system in line with information assurance. Based on the responses obtained, Figure 1 shows the proposed enhanced ISS model for patient information assurance. As shown in Figure 1, system quality, information quality and service quality were all constructs from the ISS while perceived usefulness and perceived ease of use were constructs from the TAM. Both ISS and TAM constructs were hypothesized to influence both the intention to use (ITU) and user satisfaction (US). On its part, user satisfaction was hypothesized to have an influence on the intention to use.

In this research, system quality was measured using perceived ease of use (PEOU), system features (SF), response time (RT) and flexibility (FL). On the other hand, information quality was measured using timeliness (TM), accuracy (AC), and trustworthiness (TW). Service quality was gauged using assurance (AS), responsiveness (RP) and user training (UT).

Regarding TAM, timely information (TI), accurate information (AI), effectiveness (ESS), efficiency (EFF), consistency (CSS), relevance (RL), enhanced communication (EC), increased accountability (IA), increased transparency (IT), proper patients identification (PPI), cost reduction (CR) and data security (DS)all measured perceived usefulness while perceived ease of use was measured using user friendliness (UF), standard user interfaces (SUI), workflow compatibility (WC) and interoperability (INT). Figure 2 shows the relationships among the intention to use (ITU) constructs.

As shown in Figure 2, the ISS model constructs were ten (10) which included PEOU, SF,RT, FL, TM, AC, TW, AS, RP, and UT. In this case, these ten constructs were measurable variables while ITU was latent variable.

The straight lines emanating from measurable variables and moving towards the latent variable represented the correlation coefficients. Further, Figure 2 shows that TAM had sixteen measurable variables which included TI, AI, ESS, EFF, CS, RL, EC, IA, IT, PPI, CR, DS, UF, SUI, WC, and INT. From Figure 1, the same constructs that measured ITU also measured user satisfaction (US) as shown in Figure 3. As shown here, the ISS model constructs were ten (10) which included PEOU, SF,RT, FL, TM, AC, TW, AS, RP, and UT. In this case, these ten constructs were measurable variables while ITU was latent variable. As was the case for ITU, the straight lines emanating from measurable variables and moving towards the latent variable represented the correlation coefficients. Further, Figure 3 shows that TAM had sixteen measurable variables which included TI, AI, ESS, EFF, CS, RL, EC, IA, IT, PPI, CR, DS, UF, SUI, WC, and INT.

Based on the values of the correlation coefficients,

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

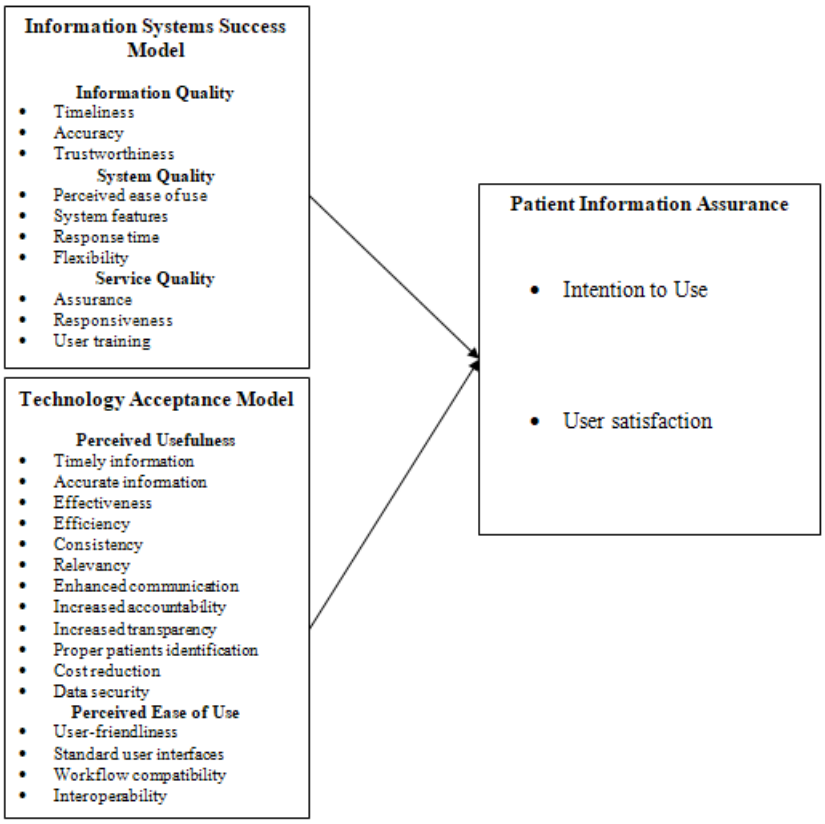

Figure 1. Proposed Enhanced ISS Model for Patient Information Assurance

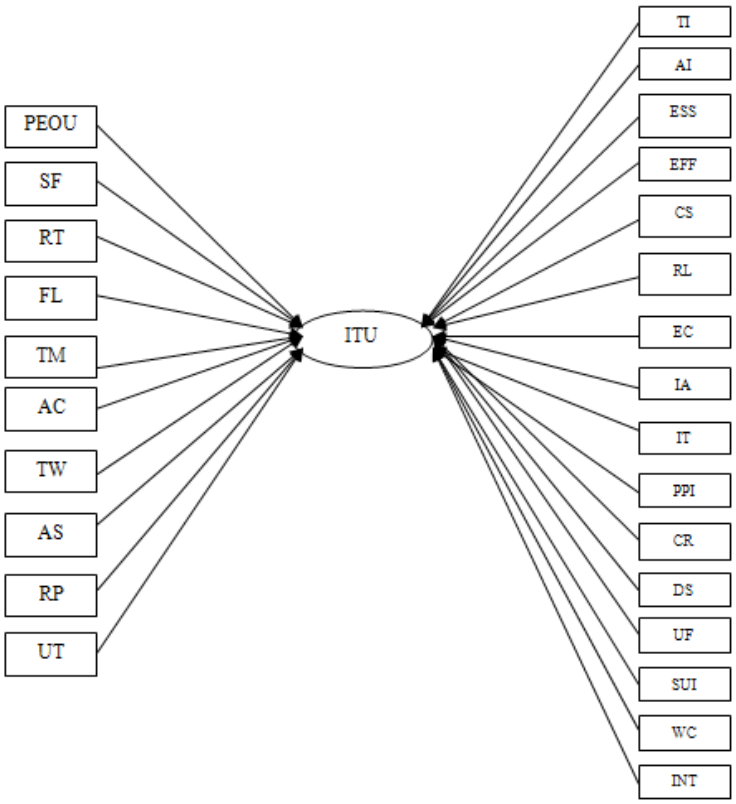

Figure 2. Intention to Use Constructs

 DOI: https://doi.org/10.30564/jcsr.v3i4.3734

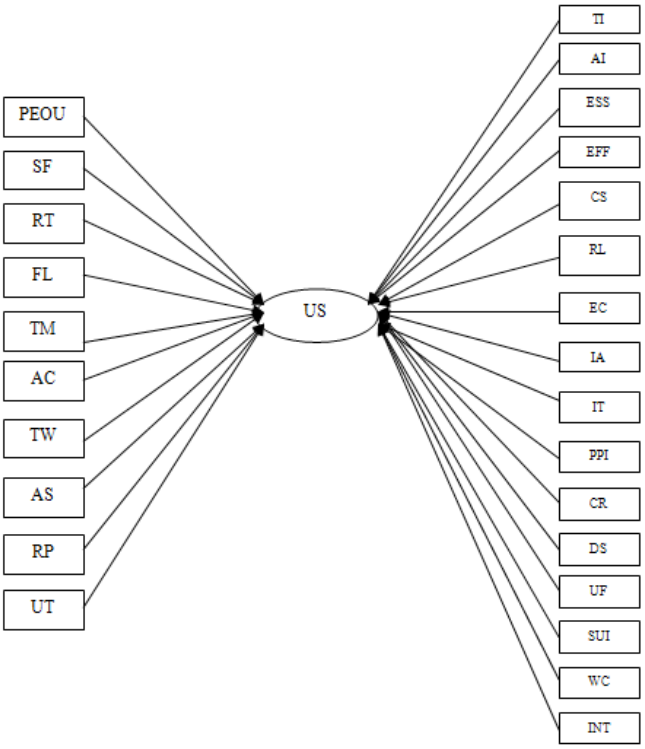

Figure 3. User Satisfaction Constructs

some of these variables were dropped while others were adopted. The criteria for variable rejection or adoption were based on the cut-off correlation coefficient of 0.5, below which the construct was a candidate for elimination while above which the construct was a candidate for adoption. Here, the final model then consisted of the adopted constructs for both ITU and US as elaborated in section IV.

4. Results and Discussion

The researcher distributed a total of 110 questionnaires out of which, 87 were returned. This represented 79.1% questionnaire return rate, which was well beyond the recommended 30%. The proposed enhanced information system success model for patient information assurance was modeled stepwise, including the Information Systems Success Model (ISS) and Intention to Use (ITU) modeling, TAM and ITU, ISS and user satisfaction (US), and finally TAM and US as discussed below.

4.1 Modeling ISS and ITU

In this modeling, the ITU was the latent variable while ISS constructs such as system quality measures (perceived ease of use -PEOU, system features -SF, response time-RT and flexibility -FL), information quality measures (timeliness -TM, accuracy -AC, and trustworthiness – TW, and service quality measures (assurance -AS, responsiveness –RP, and user training-UT) were the observed variables. Figure 4 shows the correlation coefficients between the ITU and the ISS observed variables. It is clear from Figure 4 that whereas some correlation coefficients were positive, and others were negative. For instance, ITU_PEOU, ITU_SF, ITU_RT, ITU_FL, ITU_TM, ITU_AC and ITU_RP and ITU_UT each had a positive correlation coefficient while ITU_TW and ITU_AS had negative correlation coefficients.

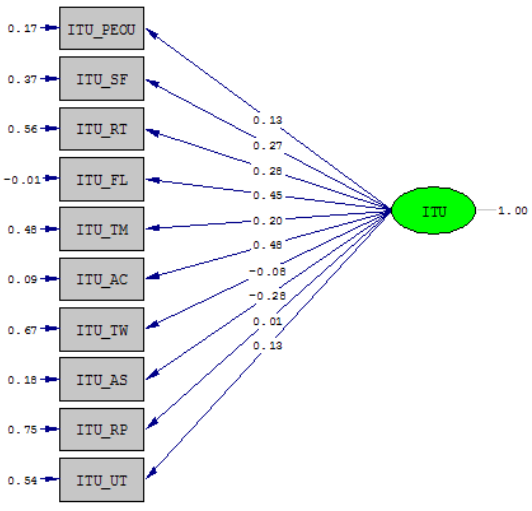

Figure 4. Modeling ISS and ITU

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

Consequently, ITU_TW and ITU_AS were candidates for elimination. As such, only perceived ease of use, system features, response time, flexibility, timeliness, accuracy, responsiveness and user training positively influenced the intention to use. Whereas flexibility with a correlation coefficient of 0.48 had the highest influence, responsiveness with a correlation coefficient of 0.01 had the least influence.

4.2 Modeling TAM and ITU

In this modeling ITU was the latent variable while TAM's constructs such as timely information (TI), accurate information (AI), effectiveness (ESS), efficiency (EFF), consistency (CSS), relevance (RL), enhanced communication (EC), increased accountability (IA), increased transparency (IT), proper patients identification (PPI), cost reduction (CR) and data security (DS) all measured perceived usefulness while perceived ease of use was measured using user friendliness (UF), standard user interfaces (SUI), workflow compatibility (WC) and interoperability (INT) were observed variables. Figure 5 shows the correlation coefficients obtained.

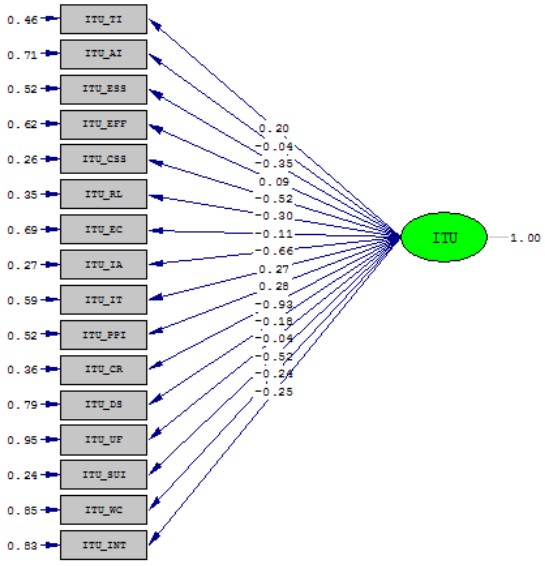

Figure 5. Modeling ITU and TAM

As shown in Figure 5, among the TAM's measures, some had positive while others had negative correlation coefficients. The PU measures that had negative correlation coefficients included ITU_INT, ITU_WC, ITU_SUI, ITU_UF, ITU_DS, ITU_CR, ITU_IA, ITU_EC, ITU_ITU_RL, ITU_CSS, ITU_ESS and ITU_AI. All these measures were therefore candidates for elimination. On the other hand, ITU_TI, ITU_EFF, ITU_IT, and ITU_PPI had a positive correlation coefficient. Whereas proper patients identification with correlation coefficient of 0.28 had the highest influence on intention to use, efficiency with a correlation coefficient of 0.09 had the least effect on intention to use. Consequently, only TAM's measures such as timely information, efficiency, increased transparency, and proper patient identification had a positive effect on intension to use.

4.3 Modeling ISS and US

To carry out this modeling, ISS measures such as such as system quality measures (perceived ease of use -PEOU, system features-SF, response time-RT and flexibility -FL), information quality measures (timeliness -TM, accuracy -AC, and trustworthiness –TW, and service quality measures (assurance -AS, responsiveness –RP, and user training-UT) were the observed variables while US was the latent variable. Figure 6 shows the correlation coefficients between the US and the ISS observed variables.

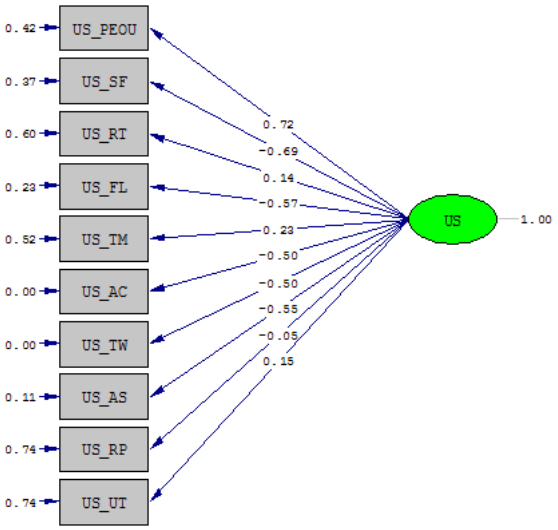

Figure 6. Modeling ISS and US

It is clear from Figure 6 that US_SF, US_FL, US_AC, US_TW, US_AS, and US_RP had negative correlation coefficients and hence were eliminated. On the other hand, US_PEOU, US_RT, US_TM, and US_UT had positive correlation coefficients and were retained. Whereas perceived ease of use with a correlation coefficient of 0.72 had the greatest impact on user satisfaction, response time with a correlation coefficient of 0.14 had the least effect on user satisfaction.

4.4 Modeling TAM's and US

In this modeling, US acted as the latent variable while TAM's measures such as such as timely information (TI), accurate information (AI), effectiveness (ESS), efficiency (EFF), consistency (CSS), relevance (RL), enhanced

 DOI: https://doi.org/10.30564/jcsr.v3i4.3734

communication (EC), increased accountability (IA), increased transparency (IT), proper patients identification (PPI), cost reduction (CR) and data security (DS) all measured perceived usefulness while perceived ease of use was measured using user friendliness (UF), standard user interfaces (SUI), workflow compatibility (WC) and interoperability (INT) were observed variables. Figure 7 shows the correlation coefficients between the US and the TAM's PU observed variables.

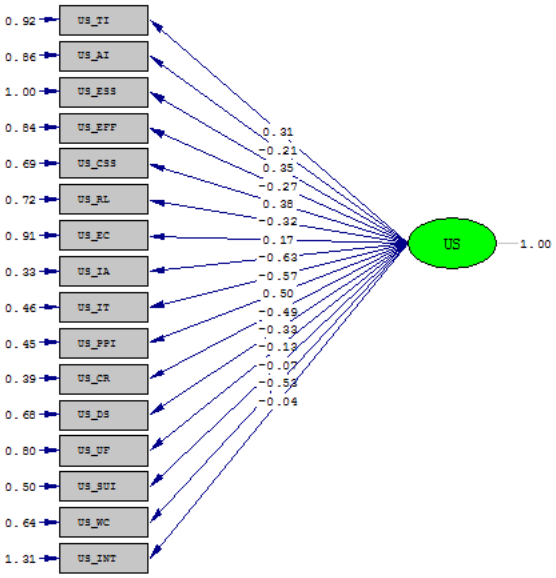

Figure 7. Modeling TAM and US

As shown in Figure 7, US_AI, US_EFF, US_RL, US_IA, US_IT, US_CR, US_DS, US_UF, US_SUI, US_WC, and US_INT had negative correlation coefficients and hence were candidates for elimination. On the other hand, US_TI, US_ESS, US_CSS, US_EC, and US_PPI had positive correlation coefficients. As such, timely information, effectiveness, consistency, enhanced communication, and proper patients' identification had a positive influence on user satisfaction. Among these positive effectors, proper patients' identification with a correlation coefficient of 0.38 had the largest impact on user satisfaction while enhanced communication with a correlation coefficient of 0.17 had the least influence on user satisfaction. Table 3 presents the adopted constructs for each of the modeling that was carried out.

It is clear from Table 3 that US_PEOU had the largest correlation coefficient while ITU_RP had the least correlation coefficient. In addition, ITU_PEOU had the same correlation coefficient as that of ITU_UT. Similarly, ITU_TM had the same correlation coefficient as that of ITU_TI. A similar observation can be made for ITU_IT and ITU_SF, and also for ITU_RT and ITU_PPI. To arrive at the final model, the adopted constructs in Table 3 were again re-modeled. Figure 8 shows the combined modeling of ITU against ISS and TAM.

Table 3. Adopted Constructs and their Correlation Coefficients

Modeling	Adopted Constructs	Correlation Coefficients
ISS and ITU	ITU_PEOU	0.13
	ITU_SF	0.27
	ITU_RT	0.28
	ITU_FL	0.45
	ITU_TM	0.20
	ITU_AC	0.48
	ITU_RP	0.01
	ITU_UT	0.13
TAM and ITU	ITU_TI	0.20
	ITU_EFF	0.09
	ITU_IT	0.27
	ITU_PPI	0.28
ISS and US	US_PEOU	0.72
	US_RT	0.14
	US_TM	0.23
	US_UT	0.15
TAM and US	US_TI	0.31
	US_ESS	0.35
	US_CSS	0.38
	US_EC	0.17
	US_PPI	0.50

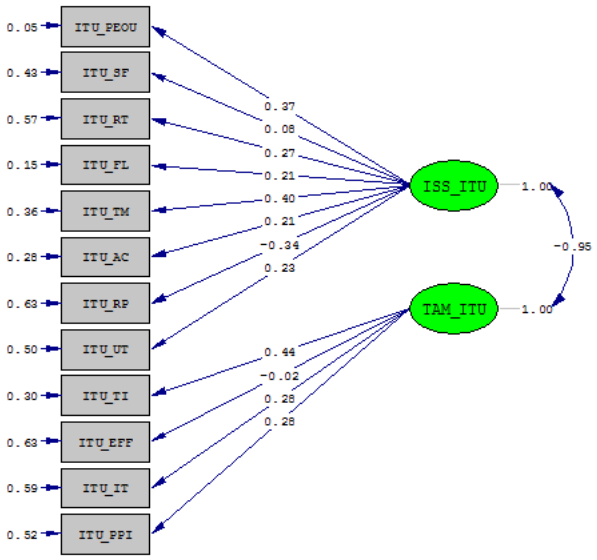

Figure 8. Semi-Attuned TAM-ISS

As shown in Figure 8, all the ISS measures were positively correlated except ITU_RP. For the case of TAM, all the measures were positively correlated except ITU_EFF. As such, these two measures were eliminated

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

and the modeling executed again to yield the model shown in Figure 9. It is clear from Figure 9 that all the correlations coefficients are now positive.

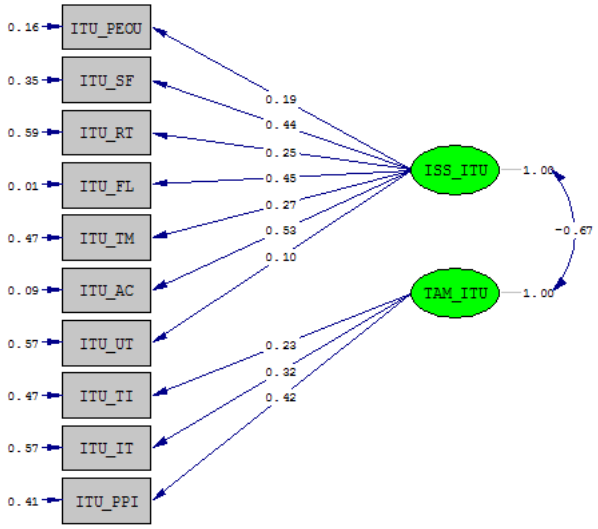

Figure 9. Attuned TAM-ISS

A similar procedure was repeated for TAM-US by running the combined modeling of US against TAM and ISS. As shown in Figure 10, all the correlation coefficients were positive, hence there was no need to attune this model further.

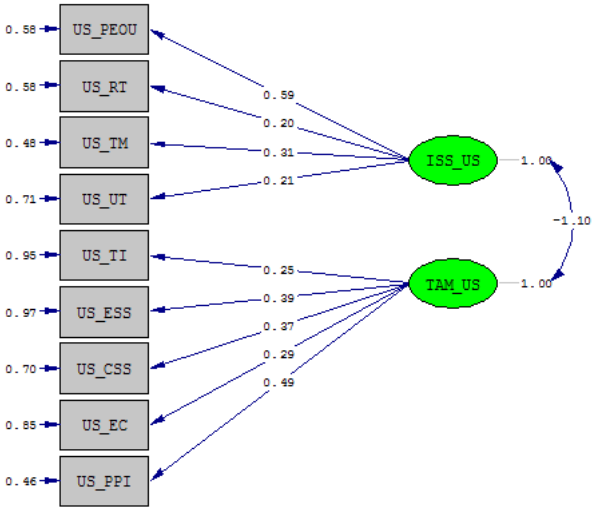

Figure 10. Attuned TAM-US

Based on the attuned models of Figure 9 and Figure 10, the final model developed in this research is shown in Figure 11. It is evident from Figure 11 that the ISS' system quality, information quality and service quality all affected intension to use as well as user satisfaction. For instance, perceived ease of use influenced both intention to use and user satisfaction. However, based on the correlation coefficient values, then its influence on user satisfaction with a coefficient of 0.59 was greater than its influence on intention to use which had a coefficient of 0.19. Regarding the effect of response time on both intentions to use and user satisfaction, the correlation coefficient of 0.25 for intention to use was greater than that of 0.20 for user satisfaction. As such, response time had more effect on intention to use than user satisfaction.

Similarly, timeliness had more influence (correlation coefficient of 0.31) on user satisfaction that on intention to use (correlation coefficient of 0.27); user training had more influence (correlation coefficient of 0.21) on user satisfaction that on intention to use (correlation coefficient of 0.10); timely information had more influence (correlation coefficient of 0.25) on user satisfaction that on intention to use (correlation coefficient of 0.22); and proper patient identification had more influence (correlation coefficient of 0.49) on user satisfaction that on intention to use (correlation coefficient of 0.42).

Regarding the reliability of the research tool, its assessment was carried out using Cronbach' alpha as shown in Appendix I. It is clear from Appendix I that, out of the 52 observed variables, only one variable (ITU Cost reduction) loaded lower than the threshold Cronbach's alpha of 0.7. Among the variables with Cronbach's alpha above 0.7, the least value was 0.723 while the highest value was 0.799. Consequently, the questionnaire used measured what it was actually supposed to measure and hence the results obtained are reliable.

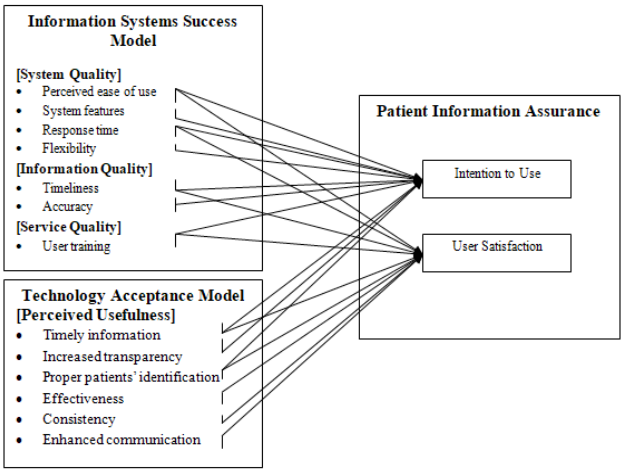

Figure 11. Proposed Enhanced ISS Model

5. Conclusions

The aim of this paper is to develop an enhanced information system success model for patient information assurance was modeled stepwise. This involved modelling a combination of Information Systems Success Model (ISS) and Intention to Use (ITU), TAM and ITU, ISS and

 DOI: https://doi.org/10.30564/jcsr.v3i4.3734

user satisfaction (US), and finally TAM and US. For the ISS and ITU modeling, only perceived ease of use, system features, response time, flexibility, timeliness, accuracy, responsiveness and user training positively influenced the intention to use. However, for the TAM and ITU modeling, only TAM's measures such as timely information, efficiency, increased transparency, and proper patient identification had a positive effect on intension to use. The ISS and US modeling revealed that perceived ease of use had the greatest impact on user satisfaction while response time had the least effect on user satisfaction. On its part, the TM and US modeling showed that timely information, effectiveness, consistency, enhanced communication, and proper patients identification had a positive influence on user satisfaction. The study findings are recommended to the decision makers of the healthcare system. This is due to potentiality of helping them understand the factors that may facilitate the development of enhanced information systems success model in their health facilities that will ultimately boost information assurance.

References

[1] M. Evans, L.A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks*, *9*(17), 4667-4679, 2016.

[2] W.J. George, and S.M. Shawon, "Exploring Challenges And Opportunities In Cybersecurity Risk And Threat Communications Related To The Medical Internet Of Things (MIOT)," *International Journal of Network Security & Its Applications (IJNSA)*, 11(4), pp. 75-86, 2019.

[3] S. Murphy, "Is cyber security possible in healthcare?," *National Cyber-security Institute Journal*, 1(3) 49-63, 2015.

[4] Loukaka, Alain and Rahman, Shawon, "Discovering New Cyber Protection Approaches From a Security Professional Prospective," *International Journal of Computer Networks & Communications (IJCNC)*, 9(4), 2017.

[5] D.A. Handel DA, "Implementing electronic health records in the emergency department," *J Emerg Med*, 38: 257-263, 2010.

[6] E. Zahra, T. Hamed, D. Kolsoum, M. Sayyed, and T. Mahmood, "Determining the Hospital Information System (HIS) Success Rate: Development of a New Instrument and Case Study," *Macedonian Journal of Medical Sciences,* 7(9):1407-1414, 2019.

[7] Y.H. Al-Mamary, A. Shamsuddin, and N. Aziati, "The relationship between system quality, information quality, and organizational performance," *International Journal of Knowledge and Research in Management & E-Commerce*, *4*(3), 7-10, 2014.

[8] A. Asad, Z. Aisha, Z. Muhammad, A. Kainat, K. Aiman, and S. Georgia, "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," *MDPI*, 3, pp. 1-16, 2019.

[9] J. Zhang, N. Xue, and X. Huang, "A Secure System for Pervasive Social Network Based Healthcare," *IEEE Access*, 4, 9239–9250, 2016.

[10] T.T. Kuo, H. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Am. Med. Inform. Assoc*. 24, 1211–1220, 2017.

[11] S. Angraal, H.M. Krumholz, and W.L. Schulz, "Blockchain technology: applications in health care," *Circulation: Cardiovascular quality and outcomes*, *10*(9), e003800, 2017.

[12] S. Acharya, B. Coats, A. Saluja, and D. Fuller, "Secure electronic health record exchange: achieving the meaningful use objectives," in *2013 46th Hawaii International Conference on System Sciences*, *IEEE*, pp. 2555-2564, 2013.

[13] G. Comandé, L. Nocco, and V. Peigné, "An empirical study of healthcare providers and patients′ perceptions of electronic health records," *Computers in Biology and Medicine*, *59*, 194-201, 2015.

[14] D.I. Rosenthal, "Instant replay," in *Healthcare*, *Elsevier*, vol. 1, No. 1-2, pp. 52-54, 2013.

[15] C.A. Caligtan, and P.C. Dykes, "Electronic health records and personal health records," in *Seminars in oncology nursing,* WB Saunders, 27(3), pp. 218-228, 2011.

[16] B.S. Buckley, A.W. Murphy, and A.E. MacFarlane, "Public attitudes to the use in research of personal health information from general practitioners' records: a survey of the Irish general public," *Journal of Medical Ethics*, *37*(1), 50-55, 2011.

[17] A. Otokiti, "Using informatics to improve healthcare quality," *International journal of health care quality assurance,* 32(2), pp. 425-430, 2019.

[18] N. Perlroth, and D.E. Sanger, "Hackers hit dozens of countries exploiting stolen NSA tool," *New York Times*, *12*, 2017.

[19] J.C. Hsieh, A.H. Li, and C.C. Yang, "Mobile, cloud, and big data computing: contributions, challenges, and new directions in tele-cardiology," *International journal of environmental research and public health*, *10*(11), 6131-6153, 2013.

[20] C. Camara, P. Peris-Lopez, and J.E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of Biomedical*

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

Informatics, 55, 272–289, 2015.

[21] E.C. Cheng, Y. Le, J. Zhou, and Y. Lu, "Healthcare services across China–on implementing an extensible universally unique patient identifier system," *International Journal of Healthcare Management*, *11*(3), 210-216, 2018.

[22] N.A. Mohamadali, and N.F. Ab Aziz, "The technology factors as barriers for sustainable health information systems (his)–a review," *Procedia Computer Science*, *124*, 370-378, 2017.

[23] K. Garrety, I. McLoughlin, R. Wilson, G. Zelle, and M. Martin, "National electronic health records and the digital disruption of moral orders," *Social Science & Medicine*, *101*, 70-77, 2014.

[24] M. Smith, "Electronic health records and healthcare identifiers: legislation discussion paper," *Population Health and Research Network,* 2015.

[25] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, *42*(7), 1-7, 2018.

[26] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST,* pp. 1-11, 2016.

[27] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journal of medical systems*, *43*(1), 1-9, 2019.

[28] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, and F.Y. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Transactions on Computational Social Systems*, *5*(4), 942-950, 2018.

[29] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a blockchain-based platform for healthcare information exchange," in *2018 IEEE international conference on smart computing (smartcomp),* IEEE, 49-56, 2018.

[30] M.A. Cyran, "Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today*, pp.1-6, 2018.

[31] S. Shubbar, "Ultrasound Medical Imaging Systems Using Telemedicine and Blockchain for Remote Monitoring of Responses to Neoadjuvant Chemotherapy in Women's Breast Cancer: Concept and Implementation," *Master's Thesis*, Kent State University, Kent, OH, USA, 2017.

[32] T. Guimaraes, C.P. Armstrong, and B.M. Jones, "A new approach to measuring information systems quality," *Quality Management Journal*, *16*(1), 42-51, 2009.

Appendix I: Cronbach's Alpha for Observed Variables

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ITU Perceived Ease of use	94.93	43.065	.630	.741
ITU System Features	94.44	43.388	.572	.743
ITU Response Time	94.93	43.065	.630	.741
ITU Flexibility	93.44	43.388	.572	.743
ITU Timeliness	94.93	43.065	.630	.741
ITU Accuracy	93.44	43.388	.572	.743
ITU Trustworthiness	94.44	51.063	-.701	.785
ITU Assurance	92.68	53.965	-.994	.799
ITU Responsiveness	94.44	51.063	-.701	.785
ITU User Training	94.93	43.065	.630	.741
ITU Timely Information	94.44	51.063	-.701	.785
ITU Accurate Information	94.93	50.739	-.652	.783
ITU Effectiveness	94.93	43.065	.630	.741
ITU Efficiency	94.93	50.739	-.652	.783

 DOI: https://doi.org/10.30564/jcsr.v3i4.3734

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ITU Consistency	93.69	40.286	.992	.723
ITU Relevance	94.69	40.286	.992	.723
ITU Enhanced Communication	94.93	43.065	.630	.741
ITU Increased Accountability	92.69	40.286	.992	.723
ITU Increased Transparency	93.44	51.063	-.701	.785
ITU Proper Patients Identification	94.68	53.965	-.994	.799
ITU Cost Reduction	93.20	34.206	.991	.693
ITU Data Security	94.69	40.286	.992	.723
ITU User Friendliness	94.69	40.286	.992	.723
ITU Standard User Interfaces	93.69	40.286	.992	.723
ITU Workflow Compatibility	94.69	40.286	.992	.723
ITU Interoperability	94.69	40.286	.992	.723
US Perceived Ease of use	94.69	40.286	.992	.723
US System Features	94.68	53.965	-.994	.799
US Response Time	94.69	40.286	.992	.723
US Flexibility	93.68	53.965	-.994	.799
US Timeliness	94.69	40.286	.992	.723
US Accuracy	93.68	53.965	-.994	.799
US Trustworthiness	94.68	53.965	-.994	.799
US Assurance	92.68	53.965	-.994	.799
US Responsiveness	94.68	53.965	-.994	.799
US User Training	94.69	40.286	.992	.723
US Timely Information	94.68	53.965	-.994	.799
US Accurate Information	94.69	40.286	.992	.723
US Effectiveness	95.18	46.873	.000	.760
US Efficiency	94.69	40.286	.992	.723
US Consistency	94.68	53.965	-.994	.799
US Relevance	94.69	40.286	.992	.723
US Enhanced Communication	95.18	46.873	.000	.760
US Increased Accountability	92.69	40.286	.992	.723
US Increased Transparency	92.69	40.286	.992	.723
US Proper Patients Identification	94.68	53.965	-.994	.799
US Cost Reduction	93.69	40.286	.992	.723
US Data Security	94.69	40.286	.992	.723
US User Friendliness	94.69	40.286	.992	.723
US Standard User Interfaces	94.18	46.873	.000	.760
US Workflow Compatibility	94.69	40.286	.992	.723
US Interoperability	95.18	46.873	.000	.760

DOI: https://doi.org/10.30564/jcsr.v3i4.3734

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks

Peter Sungu Nyakomitta[1*] Vincent Omollo Nyangaresi[1] Solomon Odhiambo Ogara[2]

1. Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya
2. School of Informatics and Innovation Systems, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya

ARTICLE INFO

Article history
Received: 31 August 2021
Accepted: 11 October 2021
Published Online: 14 October 2021

Keywords:
Attacks
Authentication
ECC
Key agreement
Privacy
Security
WSN

ABSTRACT

Wireless sensor networks convey mission critical data that calls for adequate privacy and security protection. To accomplish this objective, numerous intrusion detection schemes based on machine learning approaches have been developed. In addition, authentication and key agreements techniques have been developed using techniques such as elliptic curve cryptography, bilinear pairing operations, biometrics, fuzzy verifier and Rabin cryptosystems. However, these schemes have either high false positive rates, high communication, computation, storage or energy requirements, all of which are not ideal for battery powered sensor nodes. Moreover, majority of these algorithms still have some security and privacy challenges that render them susceptible to various threats. In this paper, a WSN authentication algorithm is presented that is shown to be robust against legacy WSN privacy and security attacks such as side-channel, traceability, offline guessing, replay and impersonations. From a performance perspective, the proposed algorithm requires the least computation overheads and average computation costs among its peers.

1. Introduction

A wireless sensor network (WSN) typically consists of dynamic battery powered cooperative nodes that perceive their environment in real-time and transmit the collected data to the nearest gateway node (GWN) through wireless channels [1]. As such, the sensors, remote users and GWN are the participants in any WSN communication process [2]. Since the GWN has relatively high computational power and energy compared with the sensor nodes (SNs), they can forward the received data to remote external users located further way. Consequently, WSN offer infrastructure-free packet exchanges devoid of centralized access points. These WSNs have self-configuring ability [3], and this has endeared them to applications such as industrial automation, military surveillance and process monitoring.

According to [1], the ability of sensing and comprehending unattended environments has led to their increased adoption in various domains. However, their deployments in unattended scenarios expose WSNs to numerous attacks, including physical capture that are then utilized as vectors to mount further attacks such as side-channeling [4]. As such, it is critical that these security issues be addressed prior to their deployments [5]. The open wireless channel that is utilized to relay packets from the SNs to GWNs, and also from the GWNs to remote users exposes the broadcasted intelli-

**Corresponding Author:*
Peter Sungu Nyakomitta,
Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya;
Email: pnyakomitta@yahoo.com

 DOI: https://doi.org/10.30564/jcsr.v3i4.3661

gence to many privacy and security risks [6]. This may include malicious packets injections, eavesdropping, packet re-direction, modifications among others.

As explained in [7], the heterogeneity of communication protocols deployed in WSN result in network clustering whose cooperation is limited to low caliber message exchanges. This renders the design and application of global security solutions in these deployments a bit cumbersome. Although 5G may facilitate WSN automation as well as programmability through the incorporation of Software-Defined Networks (SDN), the protection of packets exchanged over the control and data planes is still crucial [8].

Considering lower layer security at the link and network layers, techniques such as internet protocol security (IPsec) and internet key exchange (IKE) are normally deployed. However, the SNs have limited energy and computational power to handle both IPsec and IKE [9]. There is therefore a need to design lightweight mutual authentication algorithms for both lower layer and upper layer communication protection. The main contributions of this paper include the following:

- An algorithm that effectively authenticates a remote user to the sensor nodes is developed to protect against WSN adversarial attacks. It is only after successful mutual authentication that remote users can access sensor data.
- A session key is derived for protecting exchanged packets over the insecure gateway node-sensor node and gateway node-remote user wireless channels.
- Real device and user identities are enciphered using secret and public keys to thwart any spoofing attacks.
- Security analysis shows that the proposed algorithm offers perfect forward key secrecy is robust against side-channel, traceability, offline guessing, replay and impersonation attacks.

The rest of this article is organized as follows: section 2 presents some past research in this research domain, while section 3 provides an outline of the system model. On the other hand, section 4 presents and discusses the obtained results, while section 5 concludes the paper and offers some future work in this area.

2. Related Work

The rich application domains for WSN have led to numerous schemes aimed at the protection of the exchanged packets. For instance, authors in [10] have proposed an IP based scheme while a location based protocol has been presented in [11]. However, the techniques in [10] and [11] result in increased network latency. On the other hand, the elliptic curve cryptography (ECC) based scheme presented in [12] is vulnerable to side-channel, traceability and offline-guessing attacks. Similarly, an ECC based three factor authentication algorithm has been presented in [13], but fails to offer protection against privileged insider attacks. A lightweight two-factor authentication scheme has been introduced in [14], but which is vulnerable to forgery, identity and password guessing attacks. Although the protocol in [15] offers three factor authentication and key agreement, it cannot provide backward key secrecy, and is susceptible to both known session ephemeral and offline password attacks. On the other hand, the algorithm in [16] is susceptible to side-channel and offline guessing attacks.

Fuzzy logic and biometric based protocol has been developed in [17] to offer three factor authentication in WSN. However, this scheme cannot offer forward key secrecy and is susceptible to side-channel, offline password guessing, stolen smart card and stolen verifier attacks. The symmetric key based protocol is presented in [18] while a three factor authentication algorithm is introduced in [19]. However, the techniques in [18] and [19] are susceptible to offline password guessing and impersonation attacks, and cannot uphold forward key security [20]. On the other hand, the fuzzy verifier based technique presented in [21] is not robust against replay attacks. Authors in [22] have presented a two factor authentication scheme while the techniques in [23] and [24] both deploy user biometric for authentication. Although, the schemes in [22-24] have reduced authentication latencies, they have increased complexities.

Authors in [25-27] have introduced bilinear pairing based mutual authentication schemes, but which results in excessive computational overheads [28]. On the other hand, the smart card based biometric authentication algorithm in [29] cannot provide anonymity and is vulnerable to impersonation attacks [15]. An authenticated key agreement technique is developed in [30], but which is susceptible to known session ephemeral, offline password and impersonation attacks [31]. The WSN intrusion scheme presented in [32] has high false alarm rate while the protocol introduced in [31] is susceptible to traceability and smart card loss attacks [33].

Machine learning based techniques for intrusion detection in WSN have been developed in [34-37] based on neural networks, support vector machine, multi-layer perceptron, and neural networks with watermarking. While these algorithms improve the accuracy of network anomaly detection models, they also introduce high computational cost which is inadequate for WSNs. Although these techniques boost detection accuracy, they result in high computation complexities. On the other hand, the algorithm introduced in [33] for three factor authentication is vulnerable to privileged insider attacks.

3. System Model

The network architecture in the proposed algorithm

DOI: https://doi.org/10.30564/jcsr.v3i4.3661

comprised of registration authority (RA), sensor nodes (SNs), gateway node (GWN) and the mobile device (MD) through which the remote user accesses the SN data. Figure 1 shows the network architecture for the proposed authentication algorithm.

As shown in Figure 1, the SNs can freely exchange packets with each other, which are then forwarded to the gateway node for transmission to remote users. Since the communication is over the public internet, the exchanged messages need to be sufficiently protected from any feasible security and privacy violations over these networks. At the onset of the proposed algorithm, registration of the users' mobile devices through which they interact with SNs need registration at the RA. Similarly, the GWN is registered at the RA before being deployed to forward packets between remote users and SNs. Table 1 presents some of the symbols used in this paper and their particulars.

Table 1. Notations

Symbol	Description
h(.)	Hashing operation
RA	Registration authority
RA_{SK}	RA's secret key
MD_{ID}	Mobile device identity
υ_S, υ_P	MD's secret and public keys respectively
N_i	Random numbers
$Ŧ_i$	Timestamps
ω	RA and GWN shared secret key
Ċ	MD and GWN shared secret key
$Ł_1 \ldots Ł_9$	Message verification codes
$Ā_S$	Session key
ϱ	User's secret key
E_{SK}, $E_ω$, $E_ϕ$, $E_Ċ$	Encryption with keys SK, ω, ϕ & Ċ respectively
D_{SK}, $D_ω$, $D_ϕ$, $D_Ċ$	Decryption with keys SK, ω, ϕ & Ċ respectively
||	Concatenation operation
⊕	XOR operation

The proposed algorithm executes through four main phases which include parameter setting, registration, authentication and key agreement.

3.1 Parameter Setting and Registration

During the parameter setting phase, the registration authority (RA) chooses SN_{ID} and GN_{ID} as unique sensor node (SN) and gateway node (GWN) identities respectively (step 1) before computing security parameter ϕ (step 2) as shown in Algorithm 1. Afterwards, RA stores parameters {ϕ, SN_{ID}} into SN's memory. During user mobile device (MD) registration, it selects MD_{ID} as its unique identity and ϐ as the MD's unique secret value (step 3).

Algorithm 1: Parameter setting & registration

BEGIN:

1) Choose SN_{ID} & GN_{ID}
2) Derive $\phi=h(SN_{ID}||RA_{SK})$
3) Select MD_{ID} & ϐ, accept ϱ
4) Compute $U(\varrho)=(\upsilon_S, \upsilon_P)$, $ÿ=h(ϐ||\upsilon_S)$
   $MD \rightarrow RA:\{MD_{ID}, ÿ\}$
5) Calculate $p=h(MD_{ID}||RA_{SK})$, $q= p \oplus h(ÿ||MD_{ID})$, $r= p \oplus h(q||RA_{SK})$, $s=h(p||ÿ||MD_{ID})$
   $RA \rightarrow MD:\{q, r, s, h(.)\}$

END

Then, it accepts user's secret key ϱ before computing parameter U(ϱ) and MD's pseudo-identity ÿ (step 4). Next, some of the computed parameters {MD_{ID}, ÿ} are sent to RA. Upon receipt of these parameters, the RA computes intermediary security parameters p, q, r and s for later authentication (step 5). Finally, RA sends {q, r, s , h(.)} to the MD.

3.2 Authentication and Key Agreement

Whenever the user seeks some sensor services or information, proper authentication is executed before this access is granted. After successful authentication, the sensor and user's MD must agree on some session key to protect the exchanged data, as shown in Algorithm 2. The process begins by having the user set some expiration time ΔŦ for the exchanged messages. This is followed by user's entry of secret key ϱ into the MD which then derives parameters in step 1 before validating parameter s in step 2. Next, random number N_1 is generated followed by security values in step 3. Afterwards, computed parameters {q, ĝ, $Ł_1$, $Ł_2$} are sent to the RA.

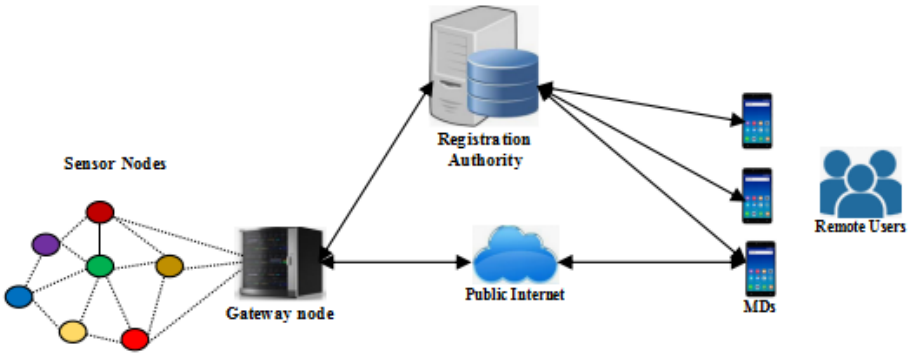

Figure 1. Network Architecture

 DOI: https://doi.org/10.30564/jcsr.v3i4.3661

Algorithm 2: Authentication and Key agreement

BEGIN:

1) Set $\Delta\mathcal{T}$ & derive $RF(g, \upsilon_P)= \upsilon_S^*$, $\ddot{y}^*=h(6||\upsilon_S^*)$, $p^*=q\oplus h(\ddot{y}^*||MD_{ID})$, $s^*=h(p^*||\ \ddot{y}^*||MD_{ID})$, $h(q||RA_{SK})=r\oplus p^*$
2) **IF** $s^*\neq s$ **THEN**: abort session
3) **ELSE**: Generate N_1 & derive $\hat{g}= MD_{ID}\oplus h(q||\upsilon_S)$, $\mathcal{L}_1=E_{SK}(N_1||SN_{ID}||GN_{ID}||\mathcal{T}_1)$, $\mathcal{L}_2=h(N_1||MD_{ID}||\mathcal{T}_1||h(q||RA_{SK}))$
   MD→RA: {q, $\hat{g}$, $\mathcal{L}_1$, $\mathcal{L}_2$}
4) Derive $MD_{ID}^*= \hat{g}\oplus h(q||RA_{SK})$, $(N_1||\mathcal{T}_1||SN_{ID}||GN_{ID})= D_{SK}(\mathcal{L}_1)$
5) Determine $\mathcal{T}_2$ & compute $\mathcal{T} = \mathcal{T}_2- \mathcal{T}_1$
6) **IF** $\mathcal{T} >\Delta\mathcal{T}$ **THEN**: abort session
7) **ELSE:** Derive $\mathcal{L}_2^*=h(N_1||MD_{ID}||\mathcal{T}_1||h(q||RA_{SK}))$
8) **IF** $\mathcal{L}_2^*\neq \mathcal{L}_2$ **THEN**: abort session
9) **ELSE:** trust MD
10) Generate N_2 & derive $\mathcal{L}_3=E_\omega(MD_{ID}||\phi||SN_{ID}||N_1||N_2||\mathcal{T}_3)$, $\mathcal{L}_4=h(\mathcal{L}_2||MD_{ID}||\mathcal{T}_3||N_2||N_1)$
    RA→GWN: {$\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_4$}
11) Compute $(MD_{ID}||\phi||SN_{ID}||N_1||N_2||\mathcal{T}_3)=D_\omega(\mathcal{L}_3)$, $\mathcal{L}_4^*= h(\mathcal{L}_2||MD_{ID}||\mathcal{T}_3||N_2||N_1)$
12) Determine $\mathcal{T}_4$ & compute $\mathcal{T} = \mathcal{T}_4- \mathcal{T}_3$
13) **IF** $\mathcal{T} >\Delta\mathcal{T}$ & $\mathcal{L}_4^*\neq \mathcal{L}_4$ **THEN**: abort session
14) **ELSE:** generate N_2 & calculate $\mathcal{L}_5=E_\Phi(N_2||\mathcal{T}_5||N_1||N_3||MD_{ID})$, $\mathcal{L}_6=h(\mathcal{L}_2||\phi||N_3||MD_{ID}||N_1)$
    GWN→SN: {$\mathcal{L}_2$, $\mathcal{L}_5$, $\mathcal{L}_6$}
15) Derive $(N_2||\mathcal{T}_5||N_1||N_3||MD_{ID})= D_\Phi(\mathcal{L}_5)$, $\mathcal{L}_6^*=h(\mathcal{L}_2||\phi||N_3||MD_{ID}||N_1)$
16) Determine $\mathcal{T}_6$ & compute $\mathcal{T} = \mathcal{T}_6- \mathcal{T}_5$
17) **IF** $\mathcal{T} >\Delta\mathcal{T}$ & $\mathcal{L}_6^*\neq \mathcal{L}_6$ **THEN**: abort session
18) **ELSE:** generate N_4 & derive $\mathcal{L}_7= N_4\oplus h(\phi||N_3)$, $\bar{A}_S=h(N_3||N_1||N_4||\phi||\mathcal{L}_2)$, $\mathcal{L}_8=h(\bar{A}_S||MD_{ID})$
    SN→ GWN: {$\mathcal{L}_7$, $\mathcal{L}_8$, $\mathcal{T}_7$}
19) Determine $\mathcal{T}_8$ & compute $\mathcal{T} = \mathcal{T}_8- \mathcal{T}_7$
20) **IF** $\mathcal{T} >\Delta\mathcal{T}$ **THEN**: abort session
21) **ELSE**: Re-compute $N_4^*= \mathcal{L}_8\oplus h(\phi||N_3)$, $\bar{A}_S^*=h(N_3||N_1||N_4^*||\phi||\mathcal{L}_2)$, $\mathcal{L}_8^*=h(\bar{A}_S^*||MD_{ID})$
22) **IF** $\mathcal{L}_8^*\neq \mathcal{L}_8$ **THEN**: abort session
23) **ELSE:** derive $\mathcal{L}_9=E_{\hat{C}}(\phi||\mathcal{T}_9||N_3||N_4||\mathcal{L}_2)$
        GWN→ MD: {$\mathcal{L}_8$, $\mathcal{L}_9$}
24) Calculate $(\phi||\mathcal{T}_9||N_3||N_4||\mathcal{L}_2)= D_{\hat{C}}(\mathcal{L}_9)$
25) Determine $\mathcal{T}_{10}$ & compute $\mathcal{T} = \mathcal{T}_{10}- \mathcal{T}_9$
26) **IF** $\mathcal{T} >\Delta\mathcal{T}$ **THEN**: abort session
27) **ELSE**: Re-compute $\bar{A}_S^*= h(N_3||N_1||N_4||\phi||\mathcal{L}_2)$, $\mathcal{L}_9^*=E_{\hat{C}}(\phi||\mathcal{T}_9||N_3||N_4||\mathcal{L}_2)$
28) **IF** $\mathcal{L}_9^*\neq \mathcal{L}_9$ **THEN**: abort session
29) **ELSE:** trust GWN
30) **ENDIF; ENDIF; ENDIF; ENDIF; ENDIF; ENDIF; ENDIF; ENDIF; ENDIF**

END

Upon receiving these values, RA re-computes MD_{ID}^* before calculating the security parameter in step 4. However, in step 5, the current timestamp $\mathcal{T}_2$ is determined upon which elapsed time $\mathcal{T}$ is computed and validated in step 6. If the validation is successful, RA derives and validates message verification code $\mathcal{L}_2$ in step 7 and 8 respectively. Provided this authentication is successful, RA and MD trust each other (step 9).

The next step is the commencement of RA and GWN authentication which begins by having RA derives random number N_2 followed by derivation of parameters in step 10. Next, message {$\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_4$} is sent to the GWN, upon which it calculates security parameters in step 11. Next, elapsed time $\mathcal{T}$ is computed (step 12) before being validated together with verification message $\mathcal{L}_4$ in step 13. Afterwards, GWN generates random number N_2 followed by computation of message verification codes $\mathcal{L}_5$ and $\mathcal{L}_6$ in step 14. Thereafter, parameters {$\mathcal{L}_2$, $\mathcal{L}_5$, $\mathcal{L}_6$} are sent to the SN. Upon receipt of these values, the SN computes parameters in step 15 before computing elapsed time and validating the same together with $\mathcal{L}_6$ in step 17. If this authentication is successful, SN generates random number N_4 before deriving parameters in step 18, a subset of which {$\mathcal{L}_7$, $\mathcal{L}_8$, $\mathcal{T}_7$} is sent to the GWN. Here, the elapsed time is calculated (step 19) before being validated in step 20. If the received timestamp passes the freshness test, GWN re-computes random number N_4^* before computing parameters in step 21. Next, message verification code $\mathcal{L}_8$ is validated in step 22 such that if it is legitimate, GWN derives message verification code $\mathcal{L}_9$ before sending {$\mathcal{L}_8$, $\mathcal{L}_9$} to the MD.

Upon receipt of this message, the MD derives parameters in step 24, before determining and validating the freshness of the received message in step 25 and 26 respectively. Provided the message passes the freshness test, the MD computes session key $\bar{A}_S$ together with message verification code $\mathcal{L}_9^*$(step 27). In step 28, this verification code is authenticated such that if it is valid, then the GWN and SN can trust each other.

4. Results and Discussion

This section presents security analysis of the proposed protocol, together with its performance evaluation.

4.1 Security Analysis

In this part, it is shown that the proposed algorithm is robust against legacy WSN privacy and security attack models. In addition, it is shown that the proposed algorithm offers forward key secrecy

Forward key secrecy: in the proposed protocol, all the communicating entities share session key $\bar{A}_S=h(N_3||N_1||N_4||\phi||\mathcal{L}_2)$ for the protection of the exchanged traffic. It is clear that the computation of $\bar{A}_S$

DOI: https://doi.org/10.30564/jcsr.v3i4.3661

incorporates random numbers N_1, N_3 and N_4, which makes it dynamic in nature. In addition, it requires knowledge of RA_{SK} and MD_{ID} to computes its components, $L_2=h(N_1||MD_{ID}||T_1||h(q||RA_{SK}))$. Since these parameters are inaccessible to the adversary, this attack cannot materialize.

Impersonation attacks: suppose that an adversary wants to masquerade as a legitimate MD, GWN or RA. For MD impersonation, message {q, ĝ, L_1, L_2} must be derived by an attacker. Although the attacker may derive fake random numbers N_1^A and timestamp T_1^A and attempt to compute L_1 and L_2, other parameters such as p, RA_{SK}, ÿ and MD_{ID} are unavailable to the attacker and hence this process fails. On the other hand, any successful GWN impersonation requires the computation of message {L_2, L_5, L_6} sent from the GWN towards the SN. However, since this requires knowledge of MD_{ID}, ϕ and RA's secret key RA_{SK} all of which are unavailable to the adversary, this attack flops. Similarly, any impersonation of the SN requires proper construction of message {L_7, L_8, T_7} sent from the SN to the GWN. However, this requires that attackers have an access to both MD_{ID} and RA_{SK} and as such, this attack will not succeed.

Side-channel attacks: the aim of this attack is to employ power analysis techniques to extract MD's and GWN's stored security parameters. Suppose that an attacker has captured {q, r, s} belonging to a particular MD, where $q=p\oplus h(ÿ||MD_{ID})$, $r=p\oplus h(q||RA_{SK})$, $s=h(p||ÿ||MD_{ID})$. However, since an attacker has no access to $p=h(MD_{ID}||RA_{SK})$, it is cumbersome to re-compute these parameters for any possible replay.

Traceability attacks: the intention of this attack is to eavesdrop the exchanged messages on different authentication sessions, after which an attempt is made to associate them to a particular MD or SN. Suppose that an attacker has captured {q, ĝ, L_1, L_2} for more than two sessions. Any attempt to associate them to a particular MD will fail since their computation involves random numbers and timestamps. This essentially makes this message random, which is the same case for messages {L_2, L_3, L_4} and {L_2, L_5, L_6}.

Offline guessing attacks: the goal of this attack is to extract MD's identity MD_{ID} through side-channeling or eavesdropping the communication channels. However, this identity is either hashed or masked in other parameters in memory and before being passed across the communication channels. Even if an adversary has an access to message {q, ĝ, L_1, L_2}, it is not possible to derive MD_{ID} from either ĝ or q without knowledge of RA's secret key RA_{SK}. The masking of MD_{ID} in other parameters, followed by hashing operations render it computationally irreversible.

Replay attacks: to curb this attack, the proposed algorithm deploys timestamps to T_i to check the freshness of all received messages. Suppose that an adversary has captured the current {q, ĝ, L_1, L_2} sent from the MD towards the RA. The aim will then be to resend this message during subsequent authentication session. However, the RA has to decrypt L_1 (step 4) to obtain its timestamp that is then verified in step 6. As such, any replayed message will fail the freshness checks and the authentication process will be aborted. Similar freshness checks are executed on L_3 and L_5 and hence the proposed algorithm is robust against these attacks. Table 2 gives the security comparisons of the proposed algorithm with its peers.

Table 2. Security features comparisons

Security feature	[17]	[12]	[16]	Proposed
Forward key secrecy	χ	√	√	√
Key agreement	√	√	√	√
Impersonation	√	√	√	√
Side-channel	χ	χ	χ	√
Traceability	√	χ	√	√
Offline guessing	χ	χ	χ	√
Mutual authentication	√	√	√	√
Replay	√	√	√	√

It is clear from Table 2 that the proposed algorithm offers many admirable WSN security features as compared with other related schemes. This was followed by the algorithm in [16], while the schemes in [12] and [17] had the worst security performance because of missing three crucial security features in each.

4.2 Performance Evaluation

In this sub-section, the computation and the communication overheads of the proposed algorithm are derived. This is then followed by the comparison of the obtained values with those of other related schemes.

Computation overheads: the proposed algorithm executed hashing T_h, symmetric key encryption and symmetric key decryption T_{sm} operations. Based on Algorithm 2, the MD executes $6T_h$ and $2T_{sm}$ operations while the RA executes $5T_h$ and $2T_{sm}$ operations. On the other hand, the GWN carries out $8T_h$ and $3T_{sm}$ operations while the SN computes $5T_h$ and T_{sm} operations. Consequently, the total computational overhead in the proposed algorithm is $24T_h$ and $8T_{sm}$ operations. Using the values in [17], a single T_h operation takes 0.0005 ms while a single T_{sm} operation takes 0.1303 ms. As such, the total computation overhead is 1.05ms as shown in Table 3.

 DOI: https://doi.org/10.30564/jcsr.v3i4.3661

Table 3. Computation Overheads

Algorithm	Computation overheads (ms)
[12]	2.57
[16]	1.28
[17]	1.28
Proposed	1.04

On the other hand, the schemes in [17], [12] and [16] take 1.28 ms, 2.57 ms and 1.28 ms respectively. Based on Figure 2, the scheme in [12] had the highest computation costs followed by the algorithms in both [16] and [17].

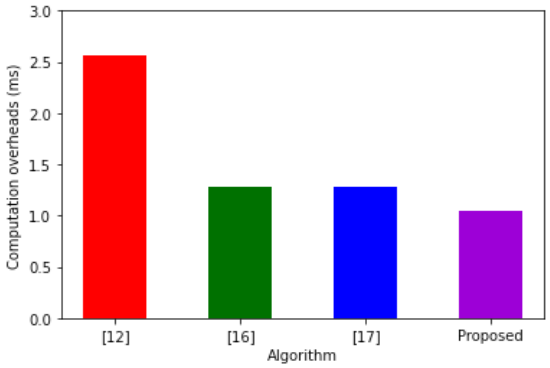

Figure 2. Computations Overheads

As such, the proposed algorithm had the lowest computation overheads among its peers. This means that the proposed algorithm is applicable in battery powered sensor nodes.

Communication overheads: for this evaluation, the values in [17] are used in which timestamps, one-way hashing ouput, random numbers secret keys, identities and random numbers are all 128 bits wide. On the other hand, each ECC point multiplication is 160 bits wide. Based on Algorithm 2, messages $\{q, \hat{g}, L_1, L_2\}$, $\{L_2, L_3, L_4\}$,$\{L_2, L_5, L_6\}$,$\{L_7, L_8, T_7\}$ and $\{L_8, L_9\}$ are exchanged during the authentication and key agreement phase. Table 4 presents the communication overheads computations in the proposed algorithm.

Table 4. Communication Overheads Derivation

Message	size (bits)
MD→RA: $\{q, \hat{g}, L_1, L_2\}$	512
RA→GWN: $\{L_2, L_3, L_4\}$	384
GWN→SN: $\{L_2, L_5, L_6\}$	384
SN→ GWN: $\{L_7, L_8, T_7\}$	384
GWN→ MD: $\{L_8, L_9\}$	256
Total	1920

On the other hand, Table 5 shows that the algorithms in [17], [12] and [16] require 1856 bits, 3072 bits and 1856 bits respectively.

Table 5. Communication Overheads Comparisons

Algorithm	Communication overheads (bits)
[12]	3072
[16]	1856
[17]	1856
Proposed	1920

As shown in Figure 3, the schemes in [17] and [16] had slightly lower communication overheads compared with the proposed algorithm.

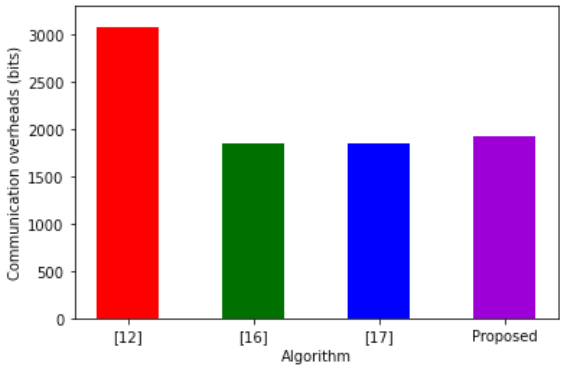

Figure 3. Communication Overheads

Although the schemes in [17] and [16] had a better performance in terms of communication overheads compared with the proposed algorithm, their designs do not consider forward key secrecy, offline guessing and side-channel attacks. As such, in overall, the proposed algorithm offered strong security and relatively lower computation and communication overheads.

5. Conclusions

Wireless sensor networks have been heavily deployed in applications such as healthcare, military surveillance and environmental monitoring. Clearly, the information exchanged in these networks is sensitive and hence should not be accessed by authorized entities. However, since the transmission of this data is over the public internet, numerous security and privacy violations can be launched against the exchanged messages. Many schemes have been presented in literature to curb these attacks. However, it has been shown that these algorithms cannot offer all salient security features needed in this environment. To fill the gaps in most of these schemes, a wireless sensor network authentication algorithm has been developed in this paper. Its security evaluation has shown its superiority to other related algorithms in terms of resilience against side-channel, traceability, offline password guessing, replay and impersonations attacks. It also displayed average best performance with regard to computation overheads, and average performance in terms of communication

DOI: https://doi.org/10.30564/jcsr.v3i4.3661

overheads. Future work lies in the evaluation of this algorithm using security and performance metrics that were not within the subject scope of this work.

References

[1] J. Mo, and H. Chen, "A lightweight secure user authentication and key agreement protocol for wireless sensor networks," Security and Communication Networks, 1-18, 2019.

[2] F. Wu, X. Li, L. Xu, L., P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with IoT notion," IEEE Systems Journal, 15(1), 1120-1129, 2020.

[3] B. Rashid and M.H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," J. Netw. Comput. Appl., vol. 60, pp. 192-219, 2016.

[4] V.O. Nyangaresi, A.J. Rodrigues, and N.K. Taha, "Mutual Authentication Protocol for Secure VANET Data Exchanges," in International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Springer, Cham, pp. 58-76, 2021.

[5] C. Miranda, G. Kaddoum, E. Bou-Harb, S. Garg, and K. Kaur, "A collaborative security framework for software-defined wireless sensor networks," IEEE Transactions on Information Forensics and Security, 15, 2602-2615, 2020.

[6] V.O. Nyangaresi, and Z. Mohammad, "Privacy Preservation Protocol for Smart Grid Networks," in 2021 International Telecommunications Conference (ITC-Egypt), IEEE, pp. 1-4, 2021.

[7] H.I. Kobo, A.M. Abu-Mahfouz, and G.P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," IEEE Access, vol. 5, pp. 1872-1899, 2017.

[8] A. De Gante, M. Aslan, and A. Matrawy, "Smart wireless sensor network management based on software-defined networking," in Proc. IEEE Commun. Biennial Symp., 71-75, 2014.

[9] V.O. Nyangaresi, and N. Petrovic, " Efficient PUF Based Authentication Protocol for Internet of Drones," in 2021 International Telecommunications Conference (ITC-Egypt), IEEE, pp. 1-4, 2021.

[10] R. Murugesan, M. Saravanan, and M. Vijyaraj, "A node authentication clustering based security for adhoc network," in Proc. IEEE Int. Conf. Commun. Signal Process, pp. 1168-1172, 2014.

[11] C. Zhu, V.C. Leung, L. T. Yang, and L. Shu, "Collaborative location based sleep scheduling for wireless sensor networks integrated with mobile cloud computing," IEEE Trans. Comput., 64(7), 1844-1856, 2015.

[12] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," Sensors, 14, 10081-10106, 2014.

[13] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," Sensors, 17(12)12, 2946, 2017.

[14] M. Turkanovi´c, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Netw., 20, pp. 96-112, 2014.

[15] Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," Wireless Networks, 25(4), 1461-1475, 2019.

[16] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," Journal of Network and Computer Applications, 76, 37-48, 2016.

[17] X. Li, J. Niu, S. Kumari, F. Wu, A.K. Sangaiah, and K.K. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications, 103, 194-204, 2018.

[18] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Networking and Applications, 8(6), 1070-1081, 2015.

[19] A.K. Das, "A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks," Wireless Personal Communications, 82(3), 1377-1404, 2015.

[20] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, 11(1), 1-20, 2018.

[21] X. Li, J. Peng, M.S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," IEEE Systems Journal, 14(1), 39-50, 2019.

[22] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," IEEE Trans. Depend. Sec. Comput., 12(4), 428-442, 2015.

[23] G. Jaswal, A. Kaul, and R. Nath, "Multimodal bio-

 DOI: https://doi.org/10.30564/jcsr.v3i4.3661

metric authentication system using hand shape, palm print, and hand geometry," in Computational Intelligence: Theories, Applications and Future Directions, Springer, Singapore, 557-570, 2019.

[24] D. Jagadiswary and D. Saraswady, "Biometric authentication using fused multimodal biometric," Procedia Comput. Sci., 85, pp. 109-116, 2016.

[25] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," IEEE Sensors Journal, 13(10), 3677-3684, 2013.

[26] C.L. Chen, T.F. Shih, Y.T. Tsai, and D.K. Li, "A bilinear pairing-based dynamic key management and authentication for wireless sensor networks," Journal of Sensors, 1-15, 2015.

[27] S. Ramachandran and V. Shanmugam, "A two way authentication using bilinear mapping function for wireless sensor networks," Computers & Electrical Engineering, 59, pp. 242-249, 2017.

[28] V.O. Nyangaresi, A.J. Rodrigues, and S.O. Abeka, "Neuro-Fuzzy Based Handover Authentication Protocol for Ultra Dense 5G Networks," in 2020 2nd Global Power, Energy and Communication Conference (GPECOM), IEEE, 339-344, 2020.

[29] A.K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," International Journal of Communication Systems, 30(1), e2933, 2015.

[30] M.S. Farash, M. Turkanovi´c, S. Kumari, and M. Holbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of things environment," Ad Hoc Networks, 36, 152-176, 2016.

[31] R. Amin, S.H. Islam, G.P. Biswas, M.K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," Computer Networks, 101, 42-62, 2016.

[32] M. Amjad, H.K. Qureshi, M. Lestas, S. Mumtaz, and J.J. Rodrigues, "Energy prediction based MAC layer optimization for harvesting enabled WSNs in smart cities," in Proc. IEEE 87th Veh.Technol. Conf. (VTC Spring), pp. 1-6, 2018.

[33] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three factor authentication and key agreement protocol for internet- integrated wireless sensor networks," IEEE Access, 5, pp. 3376-3392, 2017.

[34] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, 5, 21954-21961, 2017.

[35] M.A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," IEEE Trans. Comput., 65(10), 2986-2998, 2016.

[36] T. Ma, Y. Yu, F. Wang, Q. Zhang, and X. Chen, "A hybrid methodologies for intrusion detection based deep neural network with support vector machine and clustering technique," Sensors, 6(10), 1701, 2016.

[37] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in Proc. Int. Conf. Platform Technol. Service (PlatCon), IEEE, pp. 1-5, 2016.

DOI: https://doi.org/10.30564/jcsr.v3i4.3661

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Tel:+65 65881289
E-mail: contact@bilpublishing.com
Website:ojs.bilpublishing.com

ISSN 2630-5151 04