International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Internet of Things-Based Personal Device for Diabetes Mellitus Treatment and Management

Anurup Salokhe, VIT University, India*
Murugan Krishnamoorthy, VIT University, India

ABSTRACT

The importance of diabetes treatment in various conditions majorly included elder individuals and home patients with diabetes having very difficult conditions. Variables influence blood glucose levels in a patient. Symptoms like sickness, physical movement, drugs, and intravenous liquids cause unusual and conceivably hazardous variances in glucose regimen glycemic list and in this way patients need to measure portions. The glucose sugar level inside a human could be estimated by inserting IR radiation. For this purpose, a personal device was created to assist in the determination of insulin therapy dose and consider further factors. The arrangement proposed relies on the internet of things from one viewpoint of a patient dependent on close to home RFID cards and the doctor to give worldwide network between the individual gadget made for the patient dependent on 6LoWPAN, program for attendants/doctors to screen individual wellbeing cards, the glycemic file data framework, and the patient web-based interface.

KEYWORDS

6LoWPAN, CGM Sensor, Diabetes Mellitus, Hyperglycemia, Hypoglycemia, RFID

1. INTRODUCTION

DIABETES MELLITUS type 1 (DM) a severe and expensive worldwide public health issue today. Research organization figures show that there are today 180 million people suffering from diabetes globally, reaching a total of approximately 300 million through 2025. Mellitus diabetes is a condition with multiple complications. Those with diabetes, for instance, are at expanded danger of creating cardiovascular, kidney or renal disappointment, lower beheading of the appendages, and even lower future than somebody without diabetes. Such confusions may bring about death.

As per the above-mentioned evidence, people with diabetes must take some steps to minimize complications.

DOI: 10.4018/IJHIoT.304441
*Corresponding Author

One crucial precaution to take is to maintain the blood sugar levels as near as possible to ordinary. Productive diabetes the executives incorporates self-observing, including glucose checking, glucose levels following, utilization of drug, and self-care practices, for example, sustenance control and day by day work out. Self-checking could give information required to directing glucose levels by adjusting the eating regimen, exercise, and medication schedule. The preservation of additional health details will also help patients track any problems that may occur. And keeping track of their overall health records is essential for individuals-a systematic strategy rather than only tracking their blood sugar measurement.

A ton of diabetes treatment frameworks are accessible today, however huge numbers of these frameworks are adjustable and center just around glucose scale or a couple of contemplations. Subsequently in this exploration, we are planning a comprehensive technique structure of the diabetes treatment framework where an individual wellbeing record would be joined with this program. The individual clinical record is a wellbeing record where people hold wellbeing records and archives identifying with all aspects of wellbeing. In addition to helping individuals control diabetes, the new program would also help track all body processes and help avoid problems that could occur from diabetes. Besides, the proposed program would use a cell phone to gather information about sugar intake, macronutrient intake, workout, and medication was taken.

2. LITERATURE SURVEY

Diabetes mellitus is projected to be one of the world's largest chronic illnesses and rising public health concerns. This condition raises the risk that a patient may suffer numerous health problems including heart and kidney failure. These suggestions can, be that as it may, be limited generously by managing blood glucose levels (Lakshmi et al., 2018). Factors, for example, tolerant illness, got drugs, physical and mental pressure, physical action, opiates, intravenous liquids, and supper plan (diet) can cause unconstrained, conceivably perilous changes in glucose levels, which brings about scenes of hypoglycemia and hyperglycemia. For instance, a scene of hyperglycemia (high glucose level) postpones the mending procedure and raises the danger of contamination (Rhee et al., 2017; Ruhani, 2017).

Ongoing work shows that utilizing self-administration systems for diabetes manages glycemia and the related fluid glucose level. For these purposes, programming solution (Anbananthen & Syaifuddin, 2013) were indicated for blood glucose checking and displaying.

Since these arrangements have a difficult that depends upon a Desktop, exclusive kinds of easy to use arranging, for example, glucometer inserted in computerizing photography(Chauhan, 2017) and mobile cell, for example cell wellbeing arranging (mHealth)(Alelyani, 2018), are being characterized. Hearty research work and program have been seen as of late tending to the structure and execution of mHealth-based diabetes the executives systems(Sargunam & Anusha, 2019). An ongoing deliberate survey checked this present methodology's suitability as far as its accomplishment in overseeing diabetes and its consequences for escalating circulatory strain management (Reddy et al., 2017).

Web of Things (IoT) is among the advancements in systems administration as of late that associate the web with present day detecting and working gadgets for an all-IP structure, incorporating neighborhood and remote articles through the usage of information obtaining and correspondence usefulness. IOT design will include basic object recognition, sensor, and communication functionality as the basis for autonomous collaborative facilities and technologies creation. Extensive testing has currently been published on the use of this term in various applications (Thati et al., 2015). But no research to date discusses this idea and proposes a framework for the pervasive control of individual diabetes.

This article introduces a specific diabetes treatment system focused on the Internet web of Things to include the young era of digital assisting servicing and understand some of the aforementioned insulin treatment causes, to minimize the amount of screen time of patient high blood sugar and hypoglycemia and thus related hazards. This personal computer supports 6LoWPAN networking

to link the specific user to the built personal gateway (Haskard et al., 2010), RFID distinguishing proof to initiate the victim's profile from the individual wellbeing card, remote RS232's & IRDA's interchanges to interface the glucometer within various providers, and the shading touchpad to speak within the customer. Moreover, this PC is recognized by a glycemic list the board framework (with more than 2,600 ordered things and. merchandise) that can give subtleties on the impact of dietary glucose, a product program for specialists/clinical experts to modify and check the victim's individual wellbeing card dependent on RFID, A cloud interface for remote patients and advisor the board and, at last, a product layer concentrated on man-made reasoning to distinguish practical insulin treatment for patients supplements this PC. The key objective of this methodology is to give individuals more noteworthy access, information, and cooperation in the customized treatment program of their insulin treatment consolidating the appropriate models that follow.

3. METHODOLOGY

Methodology contains hardware and software components as subsections explained as follows:

3.1. Hardware Component

1. *Microcontroller IC ATmega328P*: The Atmel 8-piece AVRs RISC's base upon microcontrollers incorporates 32 KBs of ISP's streak memory of read-compose capacity, 1 KB of EPROM, 2 KBs of SRAM's, 23 broad useful I/O tomahawks, 32 universal useful worked registers, 3 particular clock & counters with differentiate mode, inside & of outer interferes. USART sequential programmer. Byte-arranging 2 of wire sequential controller, SPI sequential info, 6 of channel & 10 of piece A to D connector (8 channel TQFP or QFN & MLF bundle, programmable inside oscillator guard dog time and five force sparing gadget chose modes. The system works in the spectrum from 1.8-5.5 volts.
2. *CGM Sensor:* Nonstop glucose observing (CGM) gadgets monitor glucose sugar contents through the stipulated time. CGM clients utilize a robotized utensil to include a small sensor wire simple below their skins. The CGM sensor placing is kept set upon by a glue fix, so the senor can screen glucose levels in interstitial liquid during the days as well as nights. A lightweight, reusable transmitting appends to the sensor wired and send the remote, constant perusing to a beneficiary, empowering the client to get to the data. A shrewd gadget good together the CGM frame worked App will filled in the showcase instrument for specific frameworks. The recipient or perfect shrewd framework shows the present degree of glucose, just as chronicled rate designs. At the point when such glucose levels are surpassed, the CGM beneficiary or potentially good brilliant gadget can likewise be arranged to send custom alerts to the client.

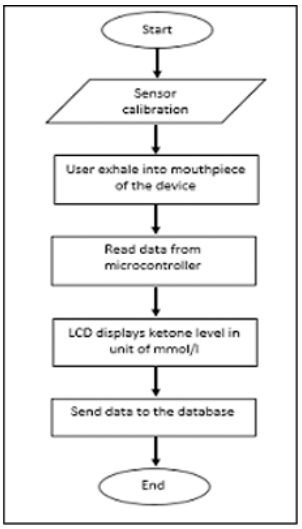
Figure 1. ATmega328P

Figure 2. CGM Sensor

3. *RFID:* RFID is abbreviated as for "radio recurrence frequencies identity distinguishing proof" and alluded to an innovative utilizing which a pre use catches advanced information encoded in RFID labels or little names through radio signals. RFID is like barcoded format, within that information is recovered from tags or imprint by a PC that put away info as data in a database. The more important is that information from the RFID labels can be perusing past the view, while standard tags must coordinate having an optical scanner.

3.2. Flow Diagram & RFID

Figure 3. RFID



3.3. Software Component

1. *Proteus Design Suite*: The Proteus Programmed Suite is an exclusive set-up of programming apparatuses for the most part utilized for computerizing electronic programming.
2. *MATLAB: MATLAB* (grid research facility) is a multi-worldview numerical registering condition and MathWorks created restrictive programming language.

3. *Things Speak*: Thing Speak is an open-source (IoT) program and an API for putting away and recovering information from objects over the Internet or through a neighborhood utilizing the HTTP and MQTT conventions.

4. ARCHITECTURE

Architecture of the project involves proposed design model structure, flow diagram and comparison tables having vital information.

4.1 Proposed Design

4.1.1. Tables

5. WORKING OF DEVICE

The idea of this gadget is principally centered around furnishing a diabetes understanding with an advanced individual convenient gadget that can record fluids glucose measurement and give direction

Figure 4. Proposed Architecture

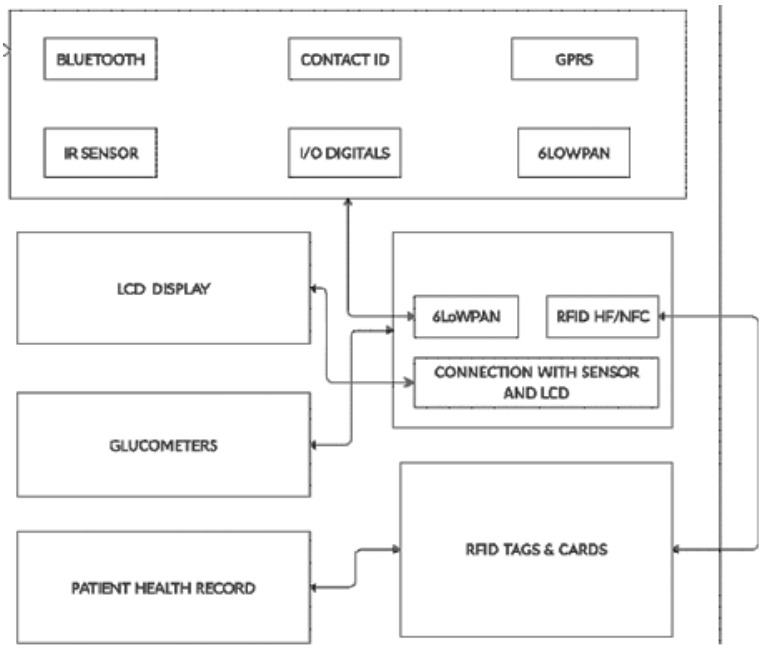


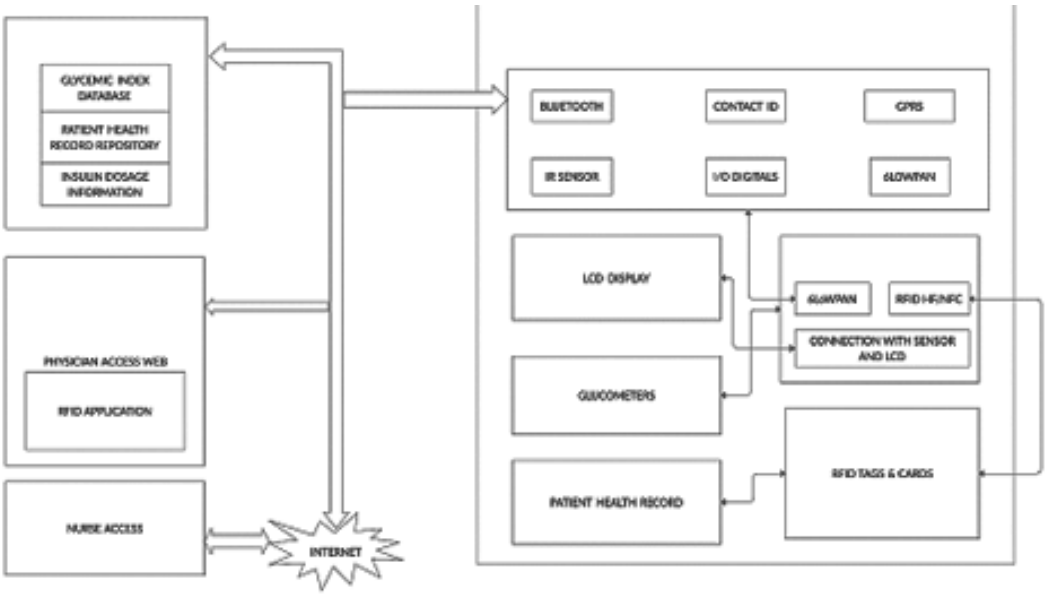
Table 1. Glucose level table

Glucose levels (mg/dl)	*Rate (mg/dl)*
Abnormal (low sugar)	Less than 65 (mg/dl)
Normal	65 to 120 (mg/dl)
Abnormal (high sugar)	Greater than120 (mg/dl)

Table 2. Test cases table

Test Cases	Scenario	Outcome
Hyperglycemia	Blood glucose level above 125 mg/dL	Display the high sugar level using CGM sensor
Hypoglycemia	Blood glucose level below 60 mg/dL	Display the low sugar level using CGM sensor
Insulin therapy	Blood sugar level maintains at 90mg/dL	A regular dose of insulin to get a normal blood sugar level display
High-Risk detection	Blood glucose level is 110 mg/dL with family history	Prediabetes levels of blood sugar

Figure 5. Architecture diagram For Personal Device



to the patients in regards to next dinner and insulin(liquid) imbuement. The set up structure is centered around the web of things that gives a worldwide system availability and overseeing framework for sensors, instruments, clients and information. This proposition along these lines acquaints a design with make worldwide correspondence to the diabetes care data framework, to accelerate the administration instrument and to upgrade its patients, sensors, and everything around it. This architecture involves many innovative Internet networking technologies such as RFID and 6LoWPAN technologies, which form the foundation of a future generation of internet- based personal services. The key justification for considering issues in our proposal on the Web was that 6LoWPAN access enables staff to be directly connected to the Internet and other information technology, including the definite diabetes control system and RFID offers simple and fast paint identifying and loading the patient's healthcare as a device. The Iot was considered for our proposal. 6LoWPAN is an IETF prototype that expands the wireless network sensor (WSN) over the Internet and then adds a layer supporting IPv6 to IEEE 802.15.4. This defines a wireless link to low latency (LoWPANs) networks. These networks have a much smaller scale, a low bandwidth rate, a low throughput and a low transmission power than other WPAN (e.g. Bluetooth and Wi-Fi). All of this in order to manufacture less power and less-priced sensors.

RFID's is the barcode evolutions that makes it easy to recognise physicians, nurses and patients. It also helps to improve barcode-based approaches by allowing certain data to be stored with RFID cards and tags while barcode enables the storing of an ID code. The additional memory capacity is valuable for preserving patient medical profile information, i.e. in the electronic medical record.

It is significant as it enables the patient health record to be reviewed locally even if the device doesn't have Access to the internet.

5.1. Glycemic Index And Webportal Database

There are two angles to the strategy for diabetes the board. At the one side, this decides the information base of the Glycemia's Indexes things database, which is the Diabetic Information Systems. The Mo vital will use the internet to view the GI readings through the glucose information system. At the other hand, this information can also be obtained from the web site created, offering registered users a convenient way to search and receive a list of food items as per their insulin treatment guidelines. The patient can search for the items that match his glycemic index by type or category, select the products they want and sustain the items checklist for the future.

5.2. Management Of Patient Information Using Rfid

The framework is used and/or reviewed by the physician and nurse for the patient profile and the prescribed dosage as per guidelines of board for insulin. Such documents are kept on Movital's individual health card for the patient.

User Data: This segment contains recognizing data for the client, similar to name, address, age, tallness, weight and national or private protection approach numbers. Coming up next is the framework structure.

Info on dosage: this is the doctor's approved insulin therapy sheet. The column data's are determined by the glucometer mgs /dls of glucose sugar in fluid blood. Such fields are then filled out in accordance with the patient's profile as per the doctor's advice. All of this is used for multiple main meals every day: dinner, breakfast.

Type of insulin: two kinds of insulin are present here: bolus (fast) and basal (slow). Slowly insulin is consumed one a day. aThe tables completed in the dosage informations area covers Bolus insulin, showing the length, peak effect time and start time for each glucose active ingredient chosen, in order to measure the effect of insulin.

Index of body mass: this aspect is recognized here as BMI.

RFID read settings: the end segment is the config connections wherein IP addresses & ports are selected. These applications was linked with an RFID card reader to the libNFC-based software. This is linked by a socket because the USB reader is C-based in interaction and Java Program is the diabetes control program. In parallel, the RFID reading includes in the networks may be used in post aspect via the IPv6 network. Presents how libNFC and USB readers bind to the program. Touchatag's RFID module is ACS 122.

6. RESULT

6.1. Matlab Sensors Simulation Sample Code

7. CONCLUSION

Thus, we have implemented the simulation of IOT based personal device for diabetic treatment management on explicit simulation software's which are MATLAB and Proteus 8 Professional. The graphs showed up in MATLAB demonstrated the fluctuating glucose levels i.e. hyperglycemia (Up-

Figure 6. Simulation using MATLAB

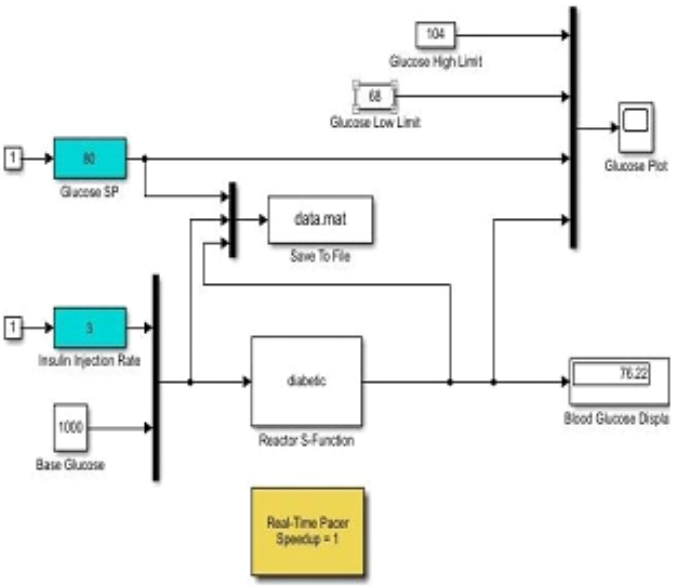


Figure 7. MATLAB simulation pseudocode

```
function xdot = blood_glucose(t,x)
global u A
% Input (1)
% Insulin infusion rate (mU/min)
U = 3;
% States (3)
% Plasma Glucose Conc. (mmol/L)
G = x(1,1);
% Plasma Insulin Conc. (mU/L) in remote compartment
X = x(2,1);
% Plasma Insulin Conc. (mU/L)
I = x(3,1);
% Disturbances (1):
% Meal glucose disturbance (mmol/L-min)
% Disturbance from the large meal
D = 3 * exp(-0.05 * t);
% Parameters
% Basal values of glucose and insulin conc.
G_basal = 4.5; % mmol/L
X_basal = 15; % mU/L
I_basal = 15; % mU/L
% For a type-I diabetic
P1 = 0.028735; % min-1
P2 = 0.028344; % min-1
P3 = 5.035e-5; % mU/L
V1 = 12; % L
n = 5/54; % min
Gdot = -P1 * (G - G_basal) - (X - X_basal) * G + D;
Xdot = -P2 * (X - X_basal) + P3 * (I - I_basal);
Idot = -n * I + U / V1;
% Vector to return
xdot = [Gdot; Xdot; Idot];
```

Figure 8. MATLAB Plot 1 Insulin Level Graph

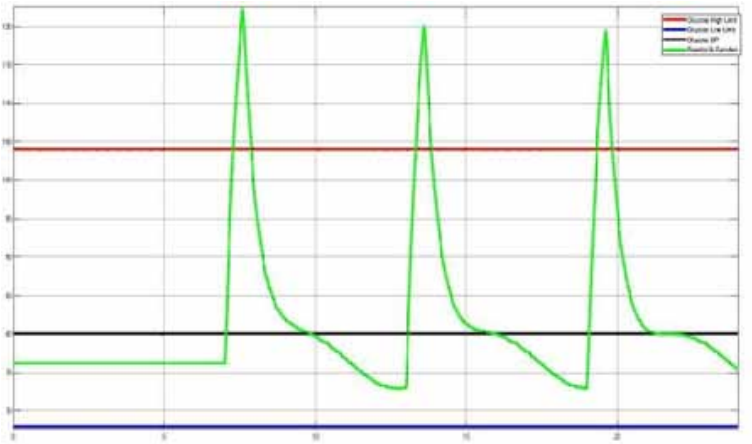


Figure 9. MATLAB Plot 2 Insulin Variation Graph

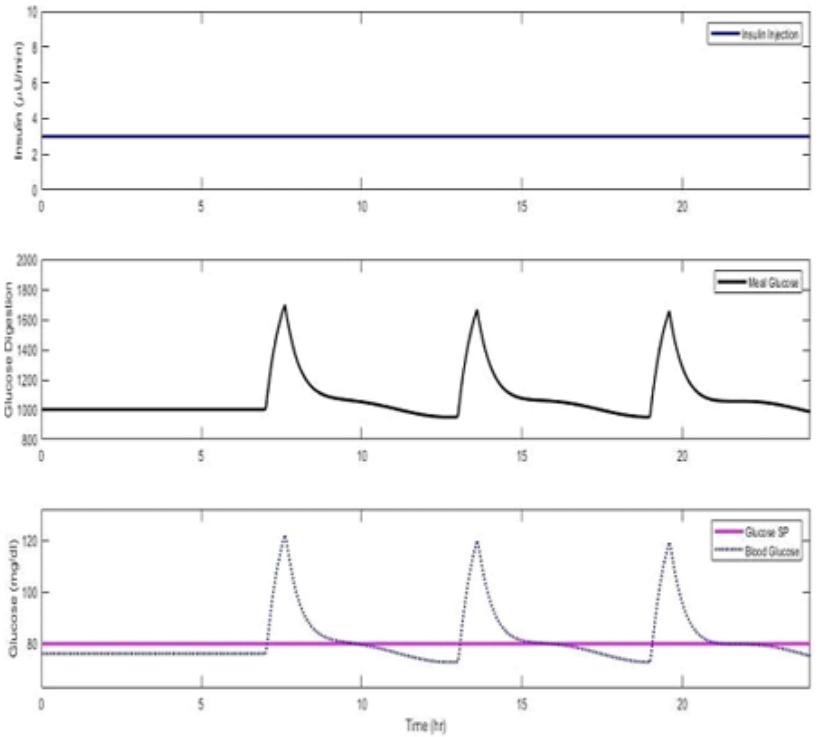


Figure 10. Proteus simulation

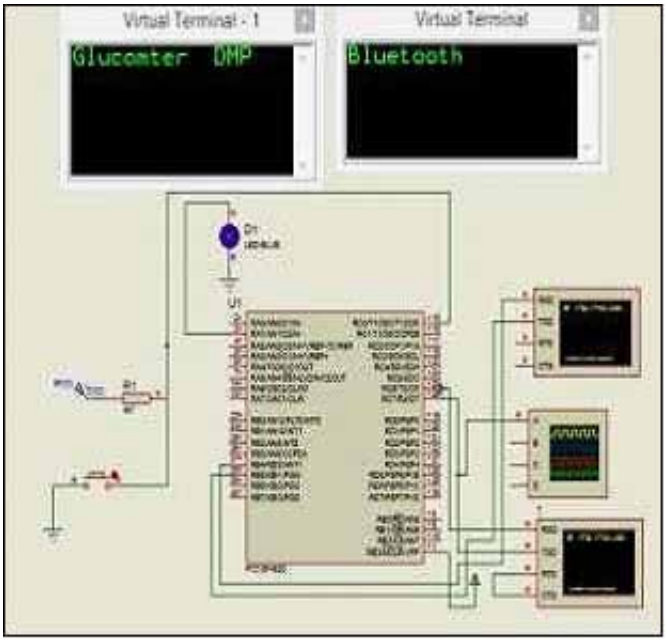
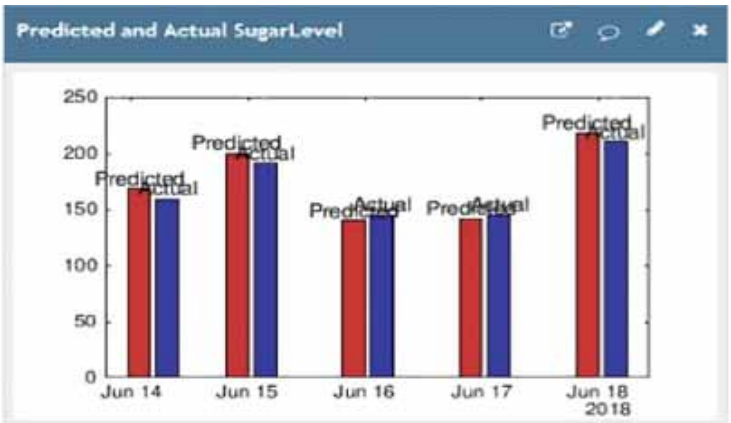
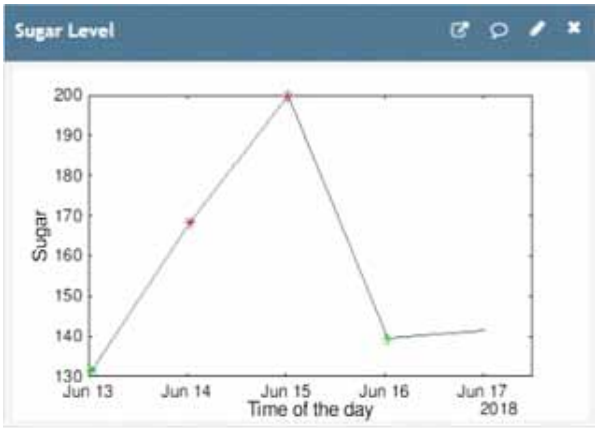


Figure 11. Predicted and Actual Sugar level in ThingSpeak



level sugar) and hypoglycemia (down- level sugar) with respect to a glycemic index containing predefined glucose levels. The Proteus included the schematic representation of the circuit implemented which acts as an interface between the virtual hardware and the mobile device. The data collected from the patient get transmitted to the doctors as well as nurses using RFID tags so that the patient gets a good treatment. The 6LoWPAN protocol has been used for retrieving the data of a particular patient through wireless communication. Thus, the history of the patient could be saved on the cloud database to further access whenever required. The Internet of Things (IoT) feature allows for the significant-time management system of diabetes. Thus, the efficiency of the web-based personal diabetes monitoring device has been shown and implemented successfully.

Figure 12. Sugar level in ThingSpeak



REFERENCES

Alelyani, S. (2018). *Internet- of-Things in Telemedicine for Diabetes Management*. IEEE.

Anbananthen & Syaifuddin. (2013). Framework: Diabetes Management System. In *IMPACT-2013*. IEEE.

Chauhan, R. (2017). *Diet Monitoring and Management of Diabetic Patient using Robot Assistant based on Internet of Things*. ICEECCOT.

Haskard, K. B., Martin, L. R., & DiMatteo, M. R. (2010). *Health Behavior Change and Treatment Adherence: Evidence-Based Guidelines for Improving Healthcare*. Oxford University Press.

Lakshmi, Subbaiahs, & Vasanthakumar. (2018). IoT for monitoring diabetic patients. *International Journals of Advanced Research, Idea and Innovative in Technologies*.

Reddy, V. R., Deshpande, P., Choudhury, A. D., Jayaraman, S., & Thokala, N. K. (2017). A non-invasive Diabetes Mellitus Classification System using Photoplethysmogram signal. *Pervasive Computing and Communications Workshops, IEEE International Conference*. doi:10.1109/PERCOMW.2017.7917526

Rhee, J., Syaekhoni, M. A., & Alfian, G. (2017). A Personalized Healthcare Monitoring System for Diabetic Patients by Utilizing BLE-Based Sensors and Real-Time Data Processing. *Sensors (Basel)*, *18*, 2183. PMID:29986473

Ruhani, A. (2017). *IoT-based Personal Health Care Monitoring Device for Diabetic Patients*. IEEE.

Sargunam & Anusha. (2019). *IoT Based Mobile Medical Application for Smart Insulin Regulation*. IEEE.

Thati, A., Sau, T. K., Chowdhury, S. R., & Biswas, A. (2015). *Breath acetone-based non-invasive detection of blood glucose levels* (Vol. 8). IEEE.

Anurup Atul Salokhe received his Bachelor of Technology in Biomedical Engineering from Mumbai University, Maharashtra. He is currently pursuing Master in Technology in Computer Science Engineering from Vellore Institute of Technology. His research interest includes IOT, Wireless Sensor Networks, Robotics, Artificial Intelligence and Machine Learning.

Murugan Krishnamoorthy received his Bachelor of Technology in Information Technology from Anna University Chennai, Tamil Nadu, India and Master of Engineering in Computer Science and Engineering from Anna University of Technology, Tiruchirapalli, Tamil Nadu and India. He received his Ph. D in the Faculty of Information and Communication Engineering from Anna University, Chennai, Tamil Nadu, and India. He is currently working as an Assistant Professor (Senior) in the School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology (VIT), Vellore, Tamil Nadu and India. His research interest includes Wireless Networks Network Security, Cryptography and Security Cyber Security, Cyber Forensics and IOT.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Smart and Secure Dyeing Industrial Water Pollution Monitoring Using IoT

Gathir Selvan B., Sri Ramakrishna Engineering College, India
Allirani S., Sri Ramakrishna Engineering College, India

ABSTRACT

Textile industries are responsible for one of the major environmental pollution because they release undesirable dye effluents. Therefore, environmental legislation commonly obligates textile factories to treat these effluents before discharge into the water bodies. The main aim of this project is to control the parameters causing pollution and to reduce the effect of these parameters without affecting the natural or industrial environment. The industrial waste is continuously sensed from a pH sensor. If any one parameter exceeds its standard level, this information will send to the pollution control board through the IoT module. Another important step is these parameters can be monitor through the internet by using a web page (cloud). These systems find the amount of pH present in the industrial waste during treatment. Thus this project will monitor and control pollution efficiently a nd the data can be transferred through cloud communication. Cayenne is a GUI to the user and IoT is used for outside world interaction for information transfer.

KEYWORDS

Cayenne, Dye Effluents, GUI, IoT module, pH Sensor, Textile Industry, Web Page (Cloud)

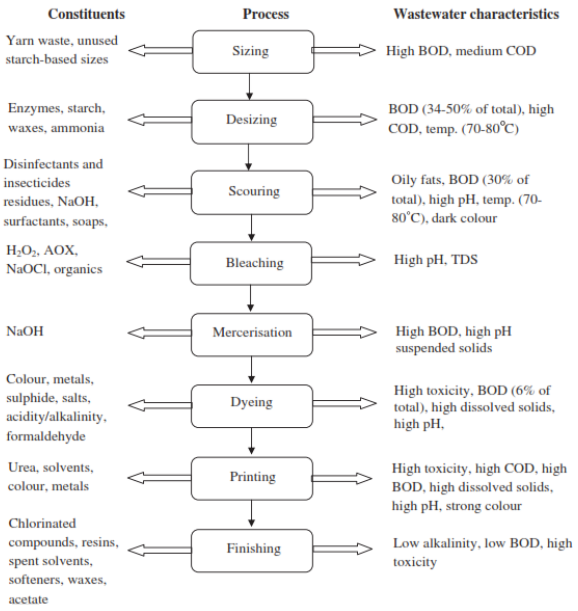
INTRODUCTION

Textile industries positively affect the economic development worldwide. China is the most important exporter of all types of textiles, followed by the European Union, India and then the USA. However, one of the problems associated with textile factories is the unacceptable effluent, especially dyes, which are difficult to degrade. The classification of textile industries depends on the type of fabrics they produce, including cellulosic materials obtained from plants (e.g. cotton, rayon and linen), protein fabrics, which come from animals (e.g. wool, silk and mohair), and synthetic fabrics produced artificially (e.g. nylon, polyester and acrylic). Fiber production in textile factories includes dry and wet processes. The wet process uses a considerable quantity of potable water and releases highly contaminated wastewater. This process consists of sizing, de-sizing, sourcing, bleaching, mercerising, dyeing, printing and finishing techniques.

- **Sizing:** The process of giving a protective coating on the warp yarn to minimize yarn breakage during the weaving.
- **De-sizing:** The process of removing sizing agent from woven fabric prior to subsequent processes, such as bleaching, dyeing, and finishing.
- **Scouring:** The process of removing impurities.

DOI: 10.4018/IJHIoT.305227

Figure 1. The wet process



- **Bleaching:** The process of removing or lightening colored materials.
- **Mercerization**: The process of improving lustre, dyeability, and strength of cellulosic material.
- **Dyeing:** The process of coloring fibers, yarns, or fabrics.
- **Printing:** The application of colorants in definite, repeated patterns to fabric, yarn, or sliver by any one of a number of methods other than dyeing.
- **Finishing:** The final process given to a textile material to give good appearance, functional properties, such as water-repellent, shrink-resistant, and wrinkle-resistant.

Washing and drying processes are also applied after different process stages, such as desizing, bleaching, and mercerizing, and especially after dyeing process to remove the dyestuff, which is not fixed on the textile.

Existing System

- In existing Pollution monitoring system the pH Value of the waste water can only be measured by the industry.
- These pH value measurements are only done by the concern industry people.
- The pH value submitted to pollution control are not the real pH value.
- Pollution control boards are unaware of the pH value of waste water which is let into major Water bodies.
- This results in Hazardous Water Pollution which leads to unbalance in ecosystem and Humans are affected by harmful diseases.

Proposed System

- The textile industry is one of the largest and most important industrial sectors in India.
- Because the textile industry consumes large quantities of water and produces highly polluted water discharge, its environmental impact is high.
- Water is expensive to use, treat and dispose.

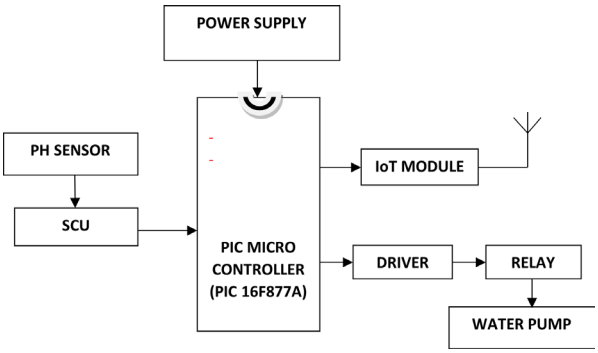
- In this Project a new Pollution monitoring system is introduced to reduce water pollution and other consequences.
- In this monitoring system pH Sensor is placed in Waste water outlet tube.
- This sensor measure the Alkaline and Acidity level of the waste water before let them into water bodies.
- The pH value of the waste water should be Neutral(pH=7).This is the standard pH value for waste water after treatment.
- Once abnormal level of water pH is found by pollution control, they can easily control the industrial outlet water pump through cayenne server-based cloud communication.
- After proper Neutralization and Purification the outlet pump will be turned on.
- Therefore, water conservation and reuse are critical necessity for the textile industry because decreasing water and wastewater treatment and recycling costs can be beneficial.

BLOCK DIAGRAM OF POLLUTION MONITORING USING IOT

Hardware Snapshot

See Figure 2.

Figure 2. Smart And Secure Dying Industrial water Pollution Monitoring uisng IOT



Hardware Output

Cayenne Webpage Output

See Figures 3-5.

Figure 3. Data Collected using pH sensor is transmitted to Cayenne Webpage through IoT device(NodeMcu). This Webpage is under the controll of Local Pollution Controll Board.

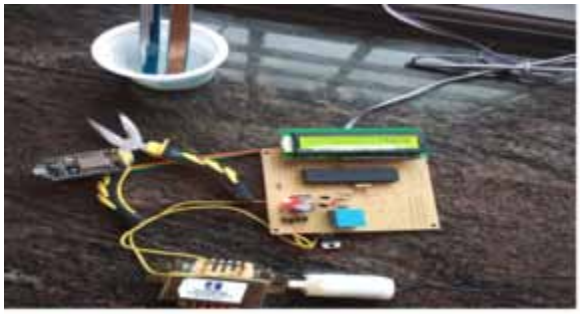


Figure 4. This LCD display is located in Industrial Waste Monitoring Room

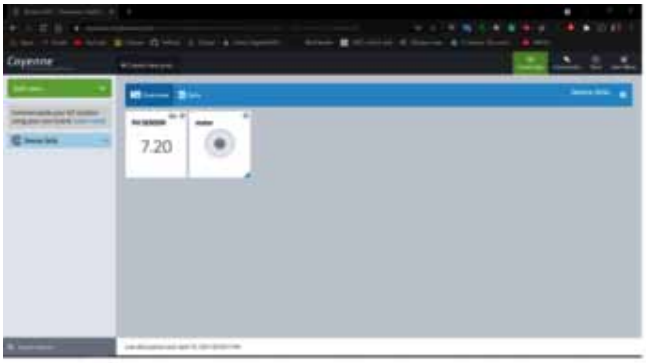


Figure 5. This LCD display is located in Industrial Waste Monitoring Room. Second LED light indicates that Pump is in ON condition.

CONCLUSION AND FUTURE SCOPE

Conclusion

This project is made with preplanning, thus it provides flexibility in operation. Thus, a cost effective and user-friendly system has been developed to monitor the pollutants in the industry effectively. Thereby limiting the pollution in the environment.

Future Scope

- This Pollution Monitoring system can be implemented in every industry all over the country for the betterment of the environment.
- This Monitoring system can be modified based on the industry like for Steel industries we can add temperature sensor, humidity sensor, gas sensor.
- In Future add on to this project if the pH value is lesser or greater/if the monitoring system is damaged either wanted or accidentally the industry can be fined a huge amount under the "Environmental Protection Act 1986".
- Industries total waste disposal in a year can be calculated and yearly graph can be generated.
- By adding their database local pollution board can automatically fine the industries which trespasses the environmental conditions.
- In future Automatic shutting down of water pump can be done. If the pH value deviates from the standard pH value of the waste water.

REFERENCES

Koli, S., Hande, P., Tatale, S., Shirsat, A., & Ahir, S. (n.d.). Pollution Monitoring and Reporting System.

Liu, X., Jia, M., Zhang, X., and Lu, W. (2018). A novel multichannel internet of things based on dynamic spectrum sharing in 5g communication. *IEEE Internet of Things Journal*, *6*(4), 5962–5970.

Mia, R., Selim, M., Shamim, A. S., Chowdhury, M., Sultana, S., Armin, M., Hossain, M., Akter, R., Dey, S., & Naznin, H. (n.d.). *Review on various types of pollution problem in textile dyeing & printing industries of Bangladesh and recommendations for mitigation*.

Nandanwar, T., Dhabarde, S., & Bhagat, S. (n.d.). Review On Industrial Environment Monitoring System Using Avr328.

Nandhakumar, S., Vengat, R., Ramkumar, R., & Rakesh, K. (n.d.). *IoT Based Pollution Monitoring System for Effective Industrial Pollution Monitoring and Control*.

Ortega, A., Frossard, P., Kovacevi J., Moura, J. M. & Vandergheynst, P.(2018). Graph signal processing: Overview, challenges, and applications. *Proceedings of the IEEE*, *106*(5), 808–828.

Sandryhaila, A., & Moura, J. M. (2013). Discrete signal processing on graphs. *IEEE Transactions on Signal Processing*, *61*(7), 1644–1656.

Samet, J. M., Speizer, F. E., Bishop, Y., Spengler, J. D., & Ferris, B. G. Jr. (1981). The relationship between air pollution and emergency room visits in an industrial community. *Journal of the Air Pollution Control Association*, *31*(3), 236–240.

Shanaz, Z., Kumar, P.S., Rahul, R., Kumar, R., & Kumar, S. (n.d.). *IoT based Industrial Pollution Monitoring System*.

Shuman, D., Narang, S., Frossard, P., Ortega, A., & Vandergheynst, P. (2013). The emerging field of signal processing on graphs: Extending high dimensional data analysis to networks and other irregular domains. *IEEE Signal Processing Magazine*, *3*(30), 83–98.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Social Cybersecurity and Human Behavior

S. Raschid Muller, Capitol Technology University, USA
https://orcid.org/0000-0002-1742-7575

Darrell Norman Burrell, Marymount University, USA & Capitol Technology University, USA*
https://orcid.org/0000-0002-4675-9544

ABSTRACT

National security in the 21st Century require investments in social cybersecurity that involves basic research into the human interaction between technology and social behavior and beliefs. National security dictates increasing capital spending into appropriate tools for identifying and neutralizing external manipulation of open and free societies. Supplementary policy changes that to reflect the technical complexity of the modern information environment while remaining true to national values are also needed. This paper uses an applied and case study research approach to explore the applications of emerging approaches.

KEYWORDS

bot, cognitive security, cybersecurity, cyberspace, disinformation, memes, misinformation, social cybersecurity, traditional cybersecurity

INTRODUCTION

National security in the 21st Century require investments in social cybersecurity that involves basic research into the human interaction between technology and social behavior and beliefs (Beskow & Carley, 2020). National security dictates increasing capital spending into appropriate tools for identifying and neutralizing external manipulation of open and free societies. Supplementary policy changes that reflect the technical complexity of the modern information environment while remaining true to national values are also needed. Finally, the appropriate research investments coupled with wise policy with a whole-of-government approach ensure that national and societal continue unchanged in their essential forms with democratic institutions (Beskow & Carley, 2020).

An integrated involvement of the whole-of-government in review can help to create and/or improve national capacity for policy coherence in social cybersecurity matters (Cázarez-Grageda, 2019). Engaging actors across policy domains to promote cross-sectoral and vertical collaboration enables complex interlinkages to be considered systematically, with a view to exploiting synergies and at worst, to avoid trade-offs, and cross-border and intergenerational impacts to be assessed (Cázarez-Grageda, 2019). Similarly, involving "sub-national and local stakeholders can help to raise awareness at the sub-national level and motivate stakeholders at this level to become engaged in implementing the 2030 Agenda" (Cázarez-Grageda, 2019, p. 8).

Cybersecurity is often treated as a national security issue with responses to attacks implemented by military and intelligence agencies that created path dependencies in which tensions between the

DOI: 10.4018/IJHIoT.305228
*Corresponding Author

private sector and government continue. In addition, over-classification of cyberthreats occurred, and the broader societal impacts of malicious use of the Internet are underestimated (Burton & Lain, 2020). Cybersecurity concerns intensified around the millennium due to the upcoming Year 2000 (Y2K bug), the advent of cyberattacks during the conflict in Kosovo War and the subsequent fears that emerged over terrorist use of the Internet and cyberterrorism in the post 9/11 environment (Burton & Lain, 2020). As a result, the need to formulate urgent solutions to cybersecurity challenges became more apparent (Burton & Lain, 2020). In many countries, including the three major superpower countries (e.g., United States, Russia, and China), military and intelligence agencies acquired a prominent role in cybersecurity (Burton & Lain, 2020). This national, military and intelligence-agency-led approach to cybersecurity was widespread and had several negative consequences for dealing with cybersecurity threats (Burton & Lain, 2020). Burton and Lain (2020) addressed these issues by proposing a move towards a societal security-based approach to cyber theory and policy.

METHOD

The method used was a content analysis of the current and relevant literature. The value of this approach is the ability to take dispersed research conversations and combine them into one coherent dialog on the topic. The value of this topic and this paper is that the subject is emerging and developing in real-time. Currently, there is minimal research on the matter. The keyword search included: cybersecurity, cyberspace, social cybersecurity, traditional cybersecurity, bot, memes, disinformation, misinformation, and cognitive security with a specific focus on the articles on Google Scholar with the highest number of citations and papers published in the last five years.

Cybersecurity

Social cybersecurity is distinct from cybersecurity (Carley, 2020). Cybersecurity focuses on machines, and how computers and databases can be negotiated. In divergence, social cybersecurity focuses on humans and how humans can be compromised, converted, and relegated to the unimportant. Where cybersecurity experts are expected to understand the technology, computer science, and engineering; social cybersecurity experts are expected to understand social communication and community building, statistics, social networks, and machine learning (Carley, 2020).

Cybersecurity is defined as protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks which range from business organizations to personal devices (Chatterjee, 2020). Cybersecurity is also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories (AO Kaspersky Lab, 2021). Within social cybersecurity, artificial intelligence is coupled with social network analysis to provide new tools and metrics to support the decision maker. Research in social cybersecurity enables new tools to support research methodology and metrics-based decision making for communicators (Carley, 2020).

The attacks are divided into five different categories such as (1) network security, (2) application security, (3) information security, (4) operational security, and (5) disaster recovery along with business continuity (Chatterjee, 2020). *Network security* and *application security* focus on securing computer networks, coupled with software and device free from threats and vulnerabilities (Chatterjee, 2020). *Information security* protects the integrity and privacy of data, both in storage and in transit. *Operational security* includes the processes and decisions for handling and protecting data assets. The users have permission to access a network and are given the procedures that determine how and where data are stored or shared. *Disaster recovery* refers to the reaction of an organization if a loss of data takes place and tries to restore its operational capabilities to continue the operation of an organization (Chatterjee, 2020). Disaster recovery and business continuity define how an organization responds to a cybersecurity incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how an organization restores its operations and information to return to the

same operating capacity as before the event. *Business continuity* is a plan the organization falls back on while trying to operate without certain resources (AO Kaspersky Lab, 2021).

Cost of Cyber Threats. According to a report by Risk Based Security (2019), cyber threats have increased rapidly, stating a data breach of more than 7.9 billion records in the year 2019. The threats are increasing every day; as per a report by Digital Information World (2019), the world will spend close to $133.7 billion alone by the year 2022 on cybersecurity solutions and services. Within the first nine months of 2019 there have been 5,183 breaches reported with 7.9 billion records shown, and on track to reach 8.5 billion (Risk Based Security, 2019). Compared to the mid-year of 2018, the total number of breaches was up 33.3% and the total number of records showing more than doubled, up 112%. Six breaches alone accounted for 3.1 billion records uncovered within three months. In total, there were over 15.1 billion records unprotected exceeding industry projections. There were 7,098 breaches reported in 2019, a 1% increase on 2018, though the gap is anticipated to grow throughout the first quarter of 2020 as more 2019 incidents are revealed (Risk Based Security, 2019).

The modern information environment has created a different new warfare domain known as *cybersecurity*. As a response to this emerging threat, social cybersecurity allows a democratic society to continue to exist while retaining its core values. The National Research Council consequently has recognized it as a key computational social science area of relevance to the intelligence community (National Academies of Sciences, Engineering, and Medicine, 2019). To accomplish this, social cybersecurity professionals need multidisciplinary science and appropriate technology to instantly identify and neutralize modern disinformation threats that are taking aim at the core tenets of society (Beskow & Carley, 2020).

Disinformation. Disinformation is not the same as false information or "fake" news. False information is shared with others without the intent to mislead and is referred to as misinformation. In fact, people share misinformation because they believe it to be true when it is not true (Public-Private Analytic Exchange Program, 2019). Disinformation's purpose is to mislead others because the information is created and disseminated with the intent to cause harm, especially during election cycles (Wardle, 2018). Misinformation. Misinformation is information that is not true or false but is shared without the intent to cause harm (Wardle, 2018).

SOCIAL CYBERSECURITY

Social cybersecurity is an emerging scientific and engineering area. Social cybersecurity is an applied field focused on the science to characterize, understand, and forecast cyber mediated changes in human behavior's activity, coupled with social, cultural, economic, and political outcomes (Carley, 2018). Research in social cybersecurity demonstrated that social media and personalized data assistants are critical technologies that affect the ways humans navigate this cyber mediated information cyber space, and the way individuals interact and engage in activities and conversations with others (Carley, 2018). The idea of social cybersecurity to those leaders and information security experts asserted that better user adoption of security is one of the best practices. For information security professionals, it is well known that individuals working in an organization are the greatest risks in cybersecurity (Mierzwa, 2020).

Social cybersecurity professionals and experts use computational social science techniques to identify, counter, and measure the impact of communication objectives (Carley, 2020). The methods and findings in this area are critical, and advance industry-accepted practices for communication, journalism, and marketing research. The field of social cybersecurity has a theory, an application, and a policy component. The methods build on work in high dimensional network analysis, data science, machine learning, natural language processing, and agent-based simulation. These methods are used to provide evidence about *who* is manipulating social media and the Internet for or against an individual or an organization, *what* methods are used, and *how* social manipulation methods can be countered. These methods also support cyber diplomacy (Goolsby, 2020). Cyber diplomacy is building strategic partnerships with other countries around the world to enhance collective action and

cooperation against shared threats, assembling like-minded coalitions on vital policy issues, sharing information and national initiatives, and confronting bad actors (Painter, 2020).

Social cybersecurity involves humans using technology to *hack* other humans. The targets are humans and the society that binds them (Beskow & Carley, 2019b). Social cybersecurity is an emerging subdomain of national security that affect all levels of future warfare, both conventional and unconventional, with strategic consequences (Storrick & Carley, 2020). In social cybersecurity, the emphasis is influencing or manipulating individuals, groups or communities and so affecting their behaviors with an emphasis on socio-political cultural consequences (Carley et al., 2018). Cataclysmic changes in how people communicate in cyberspace are dramatically altering society, allowing information to spread faster, farther, and with less assurance of its accuracy, and enabling groups to form and recruit members online to foster social divides (Carley & Carley, 2020).

Social cybersecurity is an emerging subdomain of national security that affects all levels of future warfare, both conventional and unconventional, with strategic consequences (Beskow & Carley, 2019b). Social cybersecurity is inherently multidisciplinary computational social science. "Emerging theories blend political science, sociology, communication science, organization science, marketing, linguistics, anthropology, forensics, decision science, and social psychology" (Carley et al., 2018, p. 390).

Social cybersecurity involves how better cybersecurity behaviors can be inclined positively using social influence (Mierzwa, 2020). Social cybersecurity is an emerging branch of cybersecurity that deals with the understanding of human behavior. Studies in social cybersecurity cut across different and seemingly unrelated fields such as communication, technology, machine learning, psychology, sociology, and forensics (Usiagwu, 2020). Social cybersecurity involves humans using technology to hack other humans. The targets are humans and the society that binds them (Beskow & Carley, 2019b).

Social cybersecurity is an emerging scientific area focused on the science to characterize, understand, and forecast cyber-mediated changes in human behavior, social, cultural, and political outcomes, and to build the cyber-infrastructure needed for society to persist in its essential character in a cyber-mediated information environment under changing conditions, actual or imminent social cyber-threats. (Carley et al., 2018, p. 1)

Some work in social cybersecurity is derived on most scientific fields (Carley, 2020).

Over 1,437 papers were examined through 2019. Each journal was coded by the dominant scientific fields with which it was associated. The results were a set of 43 disciplines. Nodes are disciplines and are sized by number of articles. Links are number of articles associated with both disciplines (Carley, 2020). In Figure 1, the discipline-to-discipline network where the links indicates the number of articles drawn on both disciplines. The size of the nodes indicates the number of articles associated with that discipline.

SOCIAL INFLUENCE THEORY

Cialdini's Social Influence Theory is among the most prominent theories of how people are persuaded to change their behaviors. Using techniques of interviewing and participant observation among "compliance professionals" such as door-to-door salespeople, Cialdini and Goldstein found evidence for six categories of persuasion techniques referred to as *weapons of influence* for their potency and chance of success. These are (1) *reciprocity* or desire to repay what someone else did and to share resources in a network of obligation; (2) *commitment* and *consistency* or a desire to live up to a commitment once a choice is made or to take a public stand; (3) *social proof* means a tendency to see a behavior as correct in a given situation to the degree that others are observed performing it; (4) *liking* which refers to a basic drive to cooperate and comply with those whom personal affinities are shared; (5) *authority* consists of an instinct to obey people in authority or experts; and (6) *scarcity* represents a greater desire for those resources which are perceived as limited.

Das (2018) confirmed that social influences strongly affect cybersecurity behaviors; thus, making it possible to encourage better cybersecurity behaviors by designing security systems that are

more social. Das further noted that social cybersecurity investigates how people handle attacks and threats and also influence people to make better security decisions through social proof techniques. For example, user social proof is when current users recommend a company's products and services based on their experiences with the brand.

Faklaris' (2018) social cybersecurity research group investigated how to leverage findings in social psychology to encourage safer cybersecurity behaviors. Much cybersecurity research focused on users as isolated actors. Venkatesh et al. (2003) viewed individuals' information processing and decision making about technology that is partly driven by their relationships with others and their need to accurately gauge their situation or context. These relationships are driven by and presented a consistent self-concept to themselves and others (Cialdini & Goldstein, 2004).

COGNITIVE SECURITY

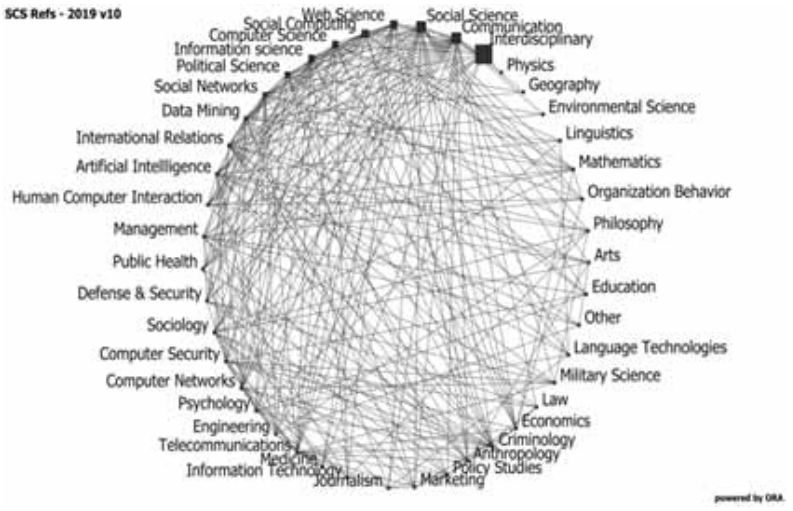
Social cybersecurity is also distinct from cognitive security (Carley, 2020). Cognitive security is focused on human cognition and how messages can be crafted to take advantage of normal cognitive limitations. In contrast, social cybersecurity is focused on humans situated in society and how the digital environment can be manipulated to alter both the community and the narrative. Where cognitive security experts are expected to understand psychology, social cybersecurity experts are expected to have a broader social science expertise.

Traditional Cybersecurity

Social cybersecurity differs from traditional cybersecurity (Beskow & Carley, 2019b).

Traditional cybersecurity involves humans using technology to "hack" technology. The target is information systems (Beskow & Carley, 2019b). Much has been written about traditional cybersecurity, which focuses on humans using information systems to hack other information systems—but much less has been made about the capabilities required for social cybersecurity, which focuses on humans who use the same information systems to hack other humans (Beskow & Carley, 2020). While information operations have existed since antiquity, the modern age has allowed them at a scale, complexity, distance, and impact unheard of even five decades ago (Beskow & Carley, 2020).

Figure 1. Network diagram of the interdisciplinary nature of the field of social cybersecurity



THE BEND MODEL

The BEND Forms of Maneuver. Carley and Beskow (2020) characterized a set of 16 socio-cybersecurity forms of maneuver in the BEND model. The desired end state for information operations varies. Traditional information operations increase support for the desired narrative and reduce support for the counternarrative. Other operations simply have a desired end state of increased agitation and reduced trust, regardless of the narrative (Beskow & Carley, 2019b). This agitation serves to drive wedges into society. Either desired end state is supported by the BEND forms of maneuver (see Figure 2). The BEND acronym is derived from 16 forms of maneuver presented in the table: four start with "B," four with "E," four with "N," and four with "D."

Figure 2. The BEND model of describing social cybersecurity forms of maneuver

	INFORMATION MANEUVER		NETWORK MANEUVER
	Knowledge Network Manipulation Things you can do by affecting what is being discussed.		**Social Network Manipulation** Things you can do by affecting who is talking/listening to whom.
Positive		Positive	
Engage	Discussion that brings up a related but relevant topic.	Back	Actions that increase the importance of the opinion leader.
Explain	Discussion that provides details on or elaborates the topic.	Build	Actions that create a group or the appearance of a group.
Excite	Discussion that brings joy/happiness/cheer/enthusiasm to group.	Bridge	Actions that build a connection between two or more groups.
Enhance	Discussion that encourages the group to continue with the topic.	Boost	Actions that grow the size of the group or make it appear that it has grown.
Negative		Negative	
Dismiss	Discussion about why the topic is not important.	Neutralize	Actions that limit the effectiveness of opinion leader to reduce the number who can or do follow or reply or attend to.
Distort	Discussion that alters the main message of the topic.	Nuke	Actions that lead to a group being dismantled.
Dismay	Discussion about a topic that brings worry/sadness/anger to the group.	Narrow	Actions that lead to the group becoming sequestered from other groups.
Distract	Discussion about a totally different topic and irrelevant.	Neglect	Actions that reduce the size of the group or make it appear that the group has grown smaller.

The BEND forms of maneuver describe how an actor manipulates the marketplace of beliefs, ideas, and information. The two forms of maneuver are information maneuver and network maneuver to build on dismiss, distort, dismay, and distract paradigms introduced by Nimmo (2015) at the Atlantic Councils Digital Forensic Research Lab. The BEND model categorizes forms of maneuver by polarity as well as whether the target is the *information* or the *network* (Beskow & Carley, 2019b).

Information Maneuver. Information maneuver is the manipulation of information and the flow or relevance of information in cyberspace. Examples of information maneuver include misdirection or introducing unrelated divisive topics into a thread in order to shift the conversation. Hashtag latching is tying content and narratives to unrelated trending topics and hashtags. Smoke screening means spreading content (both semantically and geographically) that masks other operations. Thread jacking is aggressively disrupting or co-opting a productive online conversation (Beskow & Carley, 2019b).

Cyberspace. The cyberspace domain is one of the most critical areas of national defense (Fort George G. Meade, 2020a). Cyberspace is a field that requires the most highly trained, professional, and knowledgeable individuals available. The United States Cyber Command (USCYBERCOM) is

the nation's unified combatant command for the cyberspace domain and has been in operation for a decade. Headquartered with the National Security Agency at Fort George G. Meade, Maryland, USCYBERCOM is a military command that operates globally in real time against determined and capable adversaries. The Command comprises military, intelligence, and information technology capabilities. USCYBERCOM has three main focus areas: Defending the Department of Defense Information Network (DoDIN), providing support to combatant commanders for execution of their missions around the world, and strengthening the nation's ability to withstand and respond to significant cyber-attacks (Fort George G. Meade, 2020a).

The United States and Australia have signed the first cyber-only arrangement established between the U.S. Army and an allied nation, which highlights the value of Australia's partnership in the simulated training domain (Fort George G. Meade, 2020b). This project arrangement is a milestone for the joint U.S.-Australian cooperation. The purpose of this arrangement is to develop virtual training range and to counter known and potential adversarial threats, to refocus joint efforts to invest in the new, emerging, and smart technologies that strengthen the ability to fight and win wars (Fort George G. Meade, 2020b). For the Department of Defense (DOD), defending the security of the U.S. and sustain peace abroad is the goal of DOD. Military leaders must understand this emerging discipline of social cybersecurity and how it impacts the nation's armed force and the nation's values (U.S. Department of Defense, 2018).

Cyberspace is a powerful multiplier of the destabilizing effects of manipulated information. Cyberspace allows high connectivity, low latency, low cost of entry, multiple distribution points without intermediaries, and a total disregard for physical distance or national borders (Rugge, 2018). Most importantly, anonymity and the lack of certain attribution of an attack make cyberspace the domain of ambiguity (Rugge, 2018). Artificial Intelligence (AI) technology within this information environment is enabling both state and non-state actors to manipulate the global marketplace of beliefs and ideas at unprecedented speed, with global impact (Storrick & Carley, 2020).

Artificial Intelligence Techniques. Artificial intelligence techniques, particularly machine learning and natural language processing techniques are the main tools used in social cybersecurity (Carley, 2020). AI and machine learning (ML) are often pointed to as force multipliers in dealing with the vast quantity of digital data available. These technologies have value; however, they are not the cure for what is envisioned (Carley, 2020). The problems faced by the military in social cyberwar are continually changing and often occur only once; thus, new techniques for responding are continuously needed. Further, current AI and ML techniques are often focused on easily measured data rather than the more unpredictable socio-political-cultural context (Carley, 2020).

Fact-checking tools using humans or human-AI teams are providing valuable guidance but currently take a long time to determine if a story or narrative contains inaccurate information (Carley, 2020). Assessing intent is difficult if the sender intentionally tried to deceive (disinformation) or was just mistaken (misinformation). Many disinformation campaigns were not based on inaccurate facts, but on innuendo, fights of illogic, reasoning from data taken out of context. Many times, stories labeled as disinformation are simple alternative interpretations of facts. AI only helps for some types of disinformation. When AI is less useful, the more unique the storyline, and the faster the story spreads (Carley, 2020).

Garrett and Poulsen (2019) evaluated two studies to test the effectiveness of highlighting inaccurate political posts on social media. Study 1 involved testing fact-checker flags, peer-generated flags, and a flag indicating that the publisher self-identified as a source of humor. Garrett and Poulsen predicted that each of these flags would be effective depending on prior beliefs and that the humor flag would be most effective. Their prediction was found to be effective by reducing beliefs and sharing intentions. Findings showed no evidence that fact-checker flags and peer-generated flags were advantageous or beneficial. Both studies yielding similar results.

Cognitive Security and AI. Cognitive security combines the strengths of AI and human intelligence. Cognitive AI learns with each interaction to proactively detect and analyze threats in real time and respond to threats with greater confidence and speed (Matheny et al., 2019). Cognitive security also provides insights into security analysts for making informed decisions with speed and

accuracy. Health care in the United States, historically focused on encounter-based care and treating illness as it arises rather than preventing it, is now undergoing a sweeping transformation toward a more population health–based approach. This transformation occurred via a series of changes in reimbursement (Matheny et al., 2019). Among these changes are many years of managed care and population management explorations and increases in reimbursement for value-based care and prevention. In an attempt to manage the overall health of the patient beyond treatment of illness, both value-based care and prevention are considered (Kissam et al., 2019; Mendelson et al., 2017). Considerable concern exists about AI personnel are replacing humans in the workforce when they are able to perform functions that used to be performed by humans. While as many as 47% of current jobs contain tasks that may be automated, less than 5% of jobs will be fully automated by 2030 (Liang et al., 2019). Similar to previous new technology, many AI tools will augment and not replace workers by automating subtasks of a job. This augmentation may raise demand in some industries while depressing wages in others like education professions and healthcare industry (Liang et al., 2019). However, computer scientists design AI with human users in mind, and AI usually extends the capacity, capability, and performance of humans, rather than replacing them (Liang et al., 2019; Matheny et al., 2019).

Network Maneuver. Network maneuver is the manipulation of the actual network (Beskow & Carley, 2019b). In these maneuvers, an adversary plans a social network that is the projection of social and conversational connections in the cyber component. Examples of network maneuver include opinion leader co-opting and gaining access and acknowledgment from an online opinion leader, and leveraging his or her influence to spread narrative, community building, and community bridging (Beskow & Carley, 2019b). *Community building* is building a community around a topic, idea, or hobby and then injecting a narrative into this group. The building was accomplished in Ukraine by building communities of young men around adult content-sharing accounts. Next, an injection of anti-Ukrainian and pro-Russian rhetoric is placed into those networks. *Community bridging* is injecting ideas of one group into another group, and the ideas can be accepted by both groups (Beskow & Carley, 2019b).

Social Network. One of the key tools in social cybersecurity is high dimensional dynamic social network analysis (Carley, 2020). Social network analysis is the analysis of who interacts with whom. Network techniques have long been used in intelligence for identifying groups and tracking adversarial actors and by marketers for identifying key informants and opinion leaders (Carley, 2020). With social media such techniques have been expanded to enable accessible solutions for massive data that consider multiple types of relations among actors as well as relations among resources, ideas and so forth. High dimensional dynamic network techniques underlie social media analysis (Carley, 2020).

SOCIAL MEDIA ENVIRONMENT

The social media environment contains machine learning tools that are helping to find the Bots and Memes with malicious intent, as well as who is using them (Beskow & Carley, 2020). Social media are increasingly relevant in shaping the public opinion, but they are just echo chambers. Foreign actors with malicious intent can easily exploit this intrinsic feature of social media manipulating online information to influence the public opinion (Rugge, 2018). A *bot* is any social media account that allows a computer to execute basic social media activities (such as tweet, retweet, friend, follow, like, reply). Bots can be positive, neutral, or malicious. Positive bots include personal assistants and accounts that warn people of impending natural disaster. Neutral bots generally focus on spam, proliferating content that ranges from commercial advertising to adult content. Malicious bots are involved in intimidation, propaganda, and slander. Internet *memes* are progressively used in information warfare. Virtually all are anonymous, gradually more political, and require advanced multimedia and multimodal machine learning to dissect, memes are becoming a stronghold of indoctrination and disinformation operations (Beskow & Carley, 2020).

Disinformation's Influence on Twitter Users. Zennettou et al. (2019) analyzed 27,000 tweets posted by 1,000 Twitter users identified with ties on Russia's Internet Research Agency and thus likely state-sponsored trolls. Zennettou et al. compared participants' behavior to a random set of Twitter users, finding differences in the content disseminated, the evolution of their account, and general behavior and use of Twitter. The findings indicated that Russian trolls managed to stay active for long periods of time and reached a substantial number of Twitter users. Zennettou et al. examined the ability of spreading news content and making it viral. Meanwhile, another finding was the effect of spreading news content and making it viral on social platforms was minor. The exception was news published by the Russian state-sponsored news outlet *Russia Today*. Information is used to strengthen narrative while attacking, disrupting, distorting, and dividing the society, culture, and values of other competing states and organizations (Beskow & Carley, 2019b). Information is strengthening its position within the elements of national power. Strategy is often viewed through the elements of national power: diplomatic, information, military, and economic (Storrick & Carley, 2020).

Fenstermacher and Larson (2020) concluded that these tools and techniques create a challenge for an Intelligence, Surveillance and Reconnaissance (ISR) force encompassed with platforms, sensors, networks, and personnel that are focused on overseas emergency operations for nearly two decades. A report on Hostile Social Manipulation stated that the tools and techniques being employed in targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, and distribution of rumors and conspiracy theories pose a potentially significant threat to U.S. and allied national interests (Mazarr et al., 2019).

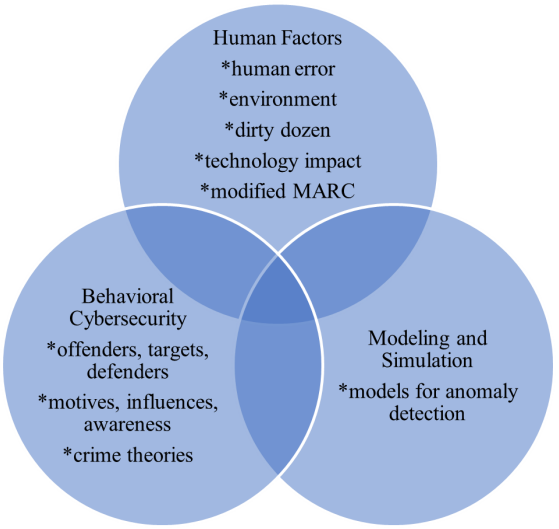
Mazarr et al.'s (2019) report on *Hostile Social Manipulation* stated that the tools and techniques being employed in targeted social media campaigns, sophisticated forgeries, cyberbullying and harassment of individuals, and distribution of rumors and conspiracy theories pose a potentially significant threat to U.S. and allied national interests. Mazarr et al. found a growing commitment to tools of social manipulation by leading U.S. competitors. The findings were sufficient to suggest that the U.S. government should take several immediate steps, including developing a more formal and concrete framework for understanding the issue and funding additional research to understand the scope of the challenge of cybersecurity threats.

CYBERSECURITY AND HUMAN BEHAVIOR

Lahcen et al. (2020) investigated how cyber criminals determined profitable business models and sophisticated attacks on networks. These researchers recommended a paradigm shift regarding the effectiveness of current techniques and practices. The purpose of their study was to provide a review of relevant theories and principles. In addition, Lahcen et al. gave insights including an interdisciplinary framework that combined behavioral cybersecurity, human factors, and modeling and simulation. This interdisciplinary framework enabled and "understanding of interconnectivity of relations and served as a background to improve research and maturity of security programs" (p. 3).

Caulkins et al. (2019) noted the difficulty in recruiting, retaining, and maintaining a validated number of cybersecurity professionals in the workspace, especially for the technical side of cybersecurity. In addition, it is difficult to recruit and retain cybersecurity professionals for the neglected aspect of non-technical, managerial-related jobs in the cyber sector. For decades, the focus within cyberspace has been on the technical needs of the underlying networks and services. Little emphasis has been on the human aspect of cybersecurity notwithstanding how to mandate the maintenance of specific commercial cyber-related certifications for cyberspace security employment. Few cyber-related organizations and teams lack a generalized understanding for the effect of human characteristics on the proficiency of cybersecurity professionals (Caulkins et al., 2019).

Figure 3. Venn diagram for the interdisciplinary framework



CONCLUSION

While social cybersecurity is an emerging scientific and engineering discipline, there is minimal research among researchers in this area; however, more research and more coordination among others within and outside of the field of social cybersecurity are needed. Initially, interdisciplinary research is transcending into transdisciplinary. Little is known about both interdisciplinary and transdisciplinary research because only a few researchers are analyzing data in these areas. The problem is research is distributed across hundreds of locations with no one conference or journal being dominant. Next, there is some research in most disciplines, but research in each of the present disciplines is negligible. More research is needed in the areas of collaborating and coordinating across groups within colleges and universities and outside researcher groups.

RECOMMENDATIONS

One of the recommendations is that organizations should invest in cybersecurity training and awareness programs to encourage employees' active engagement in complying with security policies. This training may help employees recognize and change computing security behavior. However, many organizations' cybersecurity training and awareness programs fail to achieve their goals because some employees are bored with training programs and lack enthusiasm to participate in them (He & Zhang, 2019).

There are approximately 3 million cybersecurity positions open and unfilled around the world. Without trained security staff, organizations do not have the capability to deploy the right controls or develop security processes to detect and prevent cyberattacks (Tay, 2019).

With the shortage of 3 million cyber security specialists, it is recommended that colleges and universities set up and develop courses taught by professors with master's and doctoral degrees in cyber security to recruit qualified professionals. As rates of cyber-attacks increase, the demand for cybersecurity professionals and cybersecurity budgets continue to rise. However, the imbalance of the amount of skilled cybersecurity workers along with the high demand to fill cybersecurity positions has caused a cybersecurity skills shortage (Sobers, 2021).

REFERENCES

Ablon, L. (2018). *Data thieves: The motivation of cyber threat actors and their use and monetization of stolen data*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf doi:10.7249/CT490

Albertson, M. (2020). *Cybersecurity 2021: Nation-state hacking, network vulnerability and social media manipulation*. https://siliconangle.com/2020/12/07/cy bersecurity-2021-nation-state-hacking-network-vulnerability-social-media-manipulation/

AO Kaspersky Lab. (2021). *What is cybersecurity*? https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

Beskow, D. M., & Carley, K. M. (2018). Introducing Bothunter: A tiered approach to detection and characterizing automated activity on Twitter. In H. Bisgin, A. Hyder, C. Dancy, & R. Thomson (Eds.). *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation*.

Beskow, D. M., & Carley, K. M. (2018). Bot conversations are different: Leveraging network metrics for Bot detection in Twitter. *International Conference on Advances in Social Networks Analysis and Mining*, (pp 176-183). doi:10.1109/ASONAM.2018.8508322

Beskow, D. M., & Carley, K. M. (2019). It's all in a name: Detecting and labeling bots by their name. *Computational & Mathematical Organization Theory*, *25*(1), 24–35. doi:10.1007/s10588-018-09290-1

Beskow, D. M., & Carley, K. M. (2019). *Social cybersecurity: An emerging national security requirement, military review, March-April 2019*. Carnegie Mellon University. https://www.armyupress.army.mil/Journals/Military-Review/ English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/

Beskow, D. M., & Carley, K. M. (2020). *Investing in social cybersecurity*. Naval Science and Technology—Future Force. https://futureforce.navy live.dodlive.mil/2020/03/investing-in-social-cybersecurity/

Burton, J., & Lain, C. (2020). Desecuritizing cybersecurity: Towards a societal approach. *Journal of Cyber Policy*, *5*(3), 449–470. doi:10.1080/23738871.2020.1856903

Carley, K. M. (2018). *The science of social cyber-security*. https://dl.acm.org/doi/pdf/10.1145/3241539.3241587

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational & Mathematical Organization Theory*, *26*(4), 365–381. doi:10.1007/s10588-020-09322-9 PMID:33223952

Carley, K. M., & Carley, L. R. (2020). *A meta-network approach to social influence campaigns*. Virtual Sunbelt Draft Program. http://www.pfeffer.at/sunbelt/talks/598.html

Carley, K. M., Cervone, G., Agarwal, N., & Liu, H. (2018). Social cyber-security. Halil Bisgin et al. (Ed.).In *Social, cultural, and behavioral modeling. 11th International Conference.* (pp. 389–394). Washington, DC. Springer, Cham. https://quanttext.com/wp-content/uploads/2018/09/2018_Book_SocialCulturalAndBehavioralMod.pdf

Caulkins, B. (2017). *Modeling and simulation of behavioral cybersecurity*. Cybersecurity: A Multidisciplinary Approach.

Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity skills to address today's threats. In Ahram, T., & Nicholson, D. (Eds.). Advances in human factors in cybersecurity. Advances in Intelligent Systems and Computing, 782, 187-192. Springer, Cham. doi:10.1007/978-3-319-94782-2_18

Cázarez-Grageda, K. (2019). *The whole-of-government approach: Initial lessons concerning national coordinating structures for the 2030 agenda and how review can improve their operation*. Federal Ministry for Economic Cooperation and Development. https://www.partners-for-review.de/wp-content/uploads/2019/09/Whol e-of-Government-P4R-Discussion-paper-2019.pdf

Chatterjee, R. (2020). *Difference between cybersecurity and information security*. https://analyticsindiamag.com/difference-between-cybersecurity-information-security/#:~:text=Chief%20In%2020 21-,Differences,cyber%20frauds%20and%20law%20enforcement

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*(1), 591–621. doi:10.1146/annurev.psych.55.090902.142015 PMID:14744228

Cox, T., Dombres, S., Prakash, P., & Sedano, E. (2020). *Data breaches compromised 4.5 billion records in first half of 2018*. Business Wire, Gemalto Media. https://www.businesswire.com/news/home/20181008005322/en/Data-Breaches-Compromised-4.5-Billion-Records-2018

Cybersecurity Workforce Study. (2018). *Cybersecurity professionals focus on developing new skills as workforce gap widens*. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0\h

Das, S. (2018). *Social cybersecurity: Reshaping security through an empirical understanding of human social behavior*. https://www.usenix.org/conference/enigma2018/presentation/das

Digital Information World. (2019). *Budgeting for cyberattacks: Security spending to reach 133.7 billion by 2022*. https://www.digitalinformationw orld.com/2019/05/the-future-of-cybersecurity-budgeting-infographic.html

Faklaris, C. (2018). *Social cybersecurity and the help desk: New ideas for IT professionals to foster secure workgroup behaviors*. 10.13140/RG.2.2.35580.23686

Fenstermacher, L., & Larson, K. (2020). Multi-source insights for discernment of "competition" threat. *Proceedings - Society of Photo-Optical Instrumentation Engineers*, *11423*, 1–15. doi:10.1117/12.2564517

Fort George, G. Meade. (2020). *The cutting edge of defense*. U.S. Cyber Command Public Affairs. https://www.cybercom.mil/Media/News/Article/2342894/the-cutting-edge-of-defense/

Fort George, G. Meade. (2020). *U.S. and Australia sign first-ever cyber agreement to develop virtual training range*. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/2434919/us-and- australia-sign-first-ever-cyber-agreement-to-develop-virtual-training-ra/

Garrett, R. K., & Poulsen, S. (2019). Flagging Facebook falsehoods: Self-identified humor warnings outperform fact checker and peer warnings. *Journal of Computer-Mediated Communication*, *24*(5), 240–258. doi:10.1093/jcmc/zmz012

Goolsby, R. (2020). Developing a new approach to cyber diplomacy. *Future Force*, *6*(2), 8–15.

He, W., & Zhang, Z. J. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. doi:10.1080/10919392.2019.1611528

Kaffenberger, L., & Kopp, E. (2019). *Cyber risk scenarios, the financial system, and systemic risk assessment*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/30/ cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911

Kissam, S. M., Beil, H., Cousart, C., Greenwald, L. M., & Lloyd, J. T. (2019). States encouraging value-based payment: Lessons from CMS's state innovation models initiative. *The Milbank Quarterly*, *97*(2), 506–542.

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(10), 1-18. 10.1186/s42400-020-00050-w

Liang, J., Ramanauskas, B., & Kurenkov, A. (2019). *Job loss due to AI: How bad is it going to be*? Skynet Today. https://www.skynettoday.com/editorials/ai-automation-job-loss

Lovejoy, K. (2020). *COVID-19: Five steps to defend against opportunistic cyber-attacks*. https://www.ey.com/en_us/consulting/covid-19-steps-to-defend-against-opportunistic-cyber-attackers? WT.mc_id=10807707&AA.tsrc=p aidsearch&gclid=Cj0KCQjwl9GCBhDvARIsAF unhslGD7RiZ0GsL8b2VDVcIpFhJnhySq 4Fim4pwCSTGrHJB9MZZwaVL8QaA pUYEALw_wcB

Matheny, M., Israni, S. T., Ahmed, M., & Whicher, D. (Eds.). (2019). *Artificial intelligence in health care: The hope, the hype, the promise, the peril. National Academy of Medicine Special Publication*. National Academy of Medicine.

Mazarr, M. J., Casey, A., Demus, A., Harold, S. W., Matthews, L. J., Beauchamp-Mustafaga, N., & Sladden, J. (2019). *Hostile social manipulation: Present realities and emerging trends*. RAND Corporation., https://www.rand.org/content/dam/rand/pubs/research_ reports/RR2700/RR2713/RAN D_RR2713.pdf

Mendelson, A., Kondo, K., Damberg, C., Low, A., Motuapuaka, M., Freeman, M., O'Neil, M., Relevo, R., & Kansagara, D. (2017). The effects of pay-for performance programs on health, healthcare use, and processes of care: A systematic review. *Annals of Internal Medicine*, *166*(5), 341–355.

Mierzwa, S. (2020). Improving cyber hygiene with greater social cybersecurity engagement.

Moore, M. (2020). *Top cybersecurity threats in 2020*. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

National Academies of Sciences, Engineering, and Medicine. (2019). *A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis,* (Chapter 6). Washington, DC: The National Academies Press.

Nimmo, B. (2015). Anatomy of an info-war: How Russia's propaganda machine works, and how to counter it. *Central European Policy Institute*, *15*, 1–16.

Organization of American States. (2019). *Cybersecurity considerations for the democratic process for Latin America and the Caribbean*. Cybersecurity Program of the Inter-American Committee against Terrorism of the Secretariat of Multidimensional Security. http://www.oas.org/en/sms/cicte/docs/ENG-Cybersecurity-Democratic-Process-LAC.pdf

Painter, C. (2020). Diplomacy cyberspace. *Foreign Service Journal*. American Foreign Service Association. https://www.afsa.org/diplomacy-cyberspace

Public-Private Analytic Exchange Program. (2019). *Combatting targeted information campaigns*. Department of Homeland Security. https://www.dhs.gov/sites/def ault/files/publications/ia/ia_ combatting-targeted-disinformation-campaigns.pdf

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (Eds.). (2019). *The cyber security body of knowledge*. National Cyber Security Centre. https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

Risk Based Security. (2019). *Number of records exposed up to 112% in Q3*. https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/

Rugge, F. (2018). *Mind hacking: Information warfare in the cyber age*. Analysis No. 319, Italian Institute for International Political Studies. https://www.ispionline.it /en/pubblicazione/mind-ha cking-information-warfare-cyber-age-19414

Santos, E. E., & Korah, J. (2019). Guest editorial special issue on parallel and distributed processing for computational social systems. In *IEEE Transactions on Computational Social Systems*, *6*(1), 176-177. 10.1109/TCSS.2018.2890137

Sobers, R. (2021). *134 cybersecurity statistics and trends for 2021*. https://www.varonis.com/blog/cybersecurity-statistics/

Storrick, J., & Carley, L. R. (2020). *Detecting adversarial BENDs in the information environment: Phase 2 proposal*. SBIR—STTR America's Seed Fund. https://www.sbir.gov/sbirsearch/detail/1928671

Tay, S. (2019). *A serious shortage of cybersecurity experts could cost companies hundreds of millions of dollars.* CNBC. https://www.cnbc.com /2019/03/06/cybersecurity-expert-shortage-m ay-cost-companies-hundreds-of-millions.html

U.S. Department of Defense. (2018). *Legacy homepage*. https://dod.defense.gov/

Usiagwu, M. (2020). The risk of increase in social cybersecurity in 2020. *Info Security Magazine.* https://www.infosecurity-magazine.com/ opinions/risk-increase-social-cyber/

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, *27*(3), 425–478.

Zennettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web. *Companion Proceedings of the 2019 World Wide Web Conference,* (pp. 281-226). 10.1145/3308560.3316495

Dr. S. Raschid Muller is a Cybersecurity Executive with 20 years of experience working in the government. While employed with the Department of Defense, he ran programs for the Assured Compliance Assessment Solution (ACAS), Cybersecurity Infrastructure Tools (CSI), the Joint Regional Security Stacks (JRSS), rotational engineer for the Assistant Secretary of Defense for Networks & Information Integration (ASD-NII), sole-source acquisitions lead for DISA, AFNIC, and STRATCOM for cloud solutions, and has served as the DISA Information Operations Chair and Visiting Professor at National Defense University in an academic role. He's served as the DoD CIO Representative (IPT) – Modeling and Simulation Community on Cybersecurity as well as the National Defense Industrial Association Government Representative on DoDAF 2.0 frameworks. He holds several vendor IT security certifications and is a member of the DoD Acquisition Corps. Dr. Muller is a 2020 Brookings Institute LEGIS Fellow and a 2021 UC Berkeley ELA Fellow in Goldman School of Public Policy.

Darrell Norman Burrell is post graduate student and a 2017 graduate of the National Coalition Building Institute's (NCBI) Leadership Diversity Institute. He is a Certified Diversity Professional. He is an alumnus of the prestigious Presidential Management Fellows Program www.pmf.gov. Dr Burrell has a doctorate degree with majors in Education and Executive Leadership Coaching from A.T. Still University. Dr. Burrell has an Education Specialist (EdS) graduate degree in Higher Education Administration from The George Washington University. He has two graduate degrees one in Human Resources Management/Development and another Organizational Management from National Louis University. He also has a Master of Arts degree in Sales and Marketing Management from Prescott College. He has extensive years of university teaching experience at several universities. Dr. Burrell can be reached at: dburrell2@thechicagoschool.edu

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Toward an IoT-Based Software-Defined Plumbing Network System With Fault Tolerance

Zine El Abidine Bouneb, Oum El Bouaghi University, Algeria
https://orcid.org/0000-0001-6281-3515

Djamel Eddine Saidouni, The Laboratory of Modelling and Implementation of Complex Systems, Algeria
https://orcid.org/0000-0001-8523-9800

ABSTRACT

In this paper, the authors show the application of computer science algorithms to the plumbing system. They propose a fault tolerant tap water system that is impossible without internet of things and algorithms. They show that the problem is a mutual exclusion group problem and propose an adapted algorithm version from the literature as a solution. Coupling algorithms with the configurable plumbing network will open a new field of research on IoT called software-defined plumbing network where components that have been traditionally implemented in hardware (e.g., water mixers, spring faucets, flow sensors, etc.) are instead implemented by means of software. This way we can solve other problems like instantaneous hot water, automatic cleaning of the water heater, etc. since, due to computer algorithms, the systems can be easily smart, extensible, and adaptive.

KEYWORDS

Fault Tolerant System, Group Mutual Exclusion, IoT-Based System, Software-Defined Plumbing Network System

INTRODUCTION

There are several problems with the plumbing system these days, the most important being that problems arise in system maintenance or emergencies, forcing the plumber to shut down part of the home's water supply system or of the whole network, which can disturb the inhabitants of the house. The problem can be serious in the case of a hotel practically the hotel will lose a certain percentage of customers and will have a bad reputation.

Another problem to consider is waiting and wasting water to get hot water. The cause of this problem is that the hot water pipes are filled with cold water. It is necessary to empty the cold water residing in the hot pipe to obtain the hot water requested.

Another possible scenario assumes someone is renting his house, because the water tap on the washing machine is usually only connected to the cold water pipe. If the customer's washing machine does not heat water, the home owner is forced to fix the problem for the customer to allow hot water to go to the faucet of the washing machine, if the house is well finished, capped…etc obliges the owner of the house to think twice before proceeding.

In this article, we propose a fault-tolerant and adaptive intelligent system with a piece of software, all the problems mentioned above can be solved easily and many other problems. In the case of the

DOI: 10.4018/IJHIoT.285587

washing machine without adding additional heating, we can ensure that the tap dedicated to the washing machine serves hot water at the desired temperature thanks to the IoT system.

Our system can be enhanced with machine learning easy to solve other problem like water and energy consumption monitoring. For example the system can be smart enough to make a notification for washing clothes when the water is coming to the house from the external public water network, at the moment of notification no need for pumping the water with the pump which is noisy and consume electricity this can cause a reduced bill of electricity, if the washing machine smart enough it can even start washing automatically, user just get a feedback of the success of this operation. The system can be enhanced to know which faucet is opened by the user to warn him for example if he opened the faucet of the shower he get warning via his phone with a call telling him do not take a bath right-now since the tank is not enough for your bath!

The system based on internet of the things is easily extensible for adding more features like leakage detection, automatic cleaning of the water heater. In some places in the world the water is full of limestone, heating water with gas-fired water heaters; mouth the pipes of the water heater which causes the malfunction of the water heater for example cut off the hot water totally.

Even the actual technology of smart circulating pump for getting instant hot water which work with servo mechanism cannot turn off itself automatically at night but with an IoT based system you can for example schedule the circulating pump to turn off after 10 pm automatically for eliminating the noise. Even if this pump dotted with timer it is not easy to go outside in rainy day to set the timer if the pump is in the garden for example. IoT based system offer simple user interface using cell phone for example. The system can learn when you need frequently hot water to get really a smart system. Furthermore servo mechanism for triggering pump on the demand of water from a certain tap work with a principal of detecting a decreasing in pressure. This principal cannot make a distinction between a leakage and real requesting of water at certain faucets. In contrast IoT based system can detect leakage and can't rely on servo mechanism for triggering the pump.

For example if you want to fill a container with a certain amount of water let's said 5 liter you don't even monitor the operation of filling to avoid overflow of the container since the system can learn without an extra flow sensor the time needed for filling this container.

There are a number of ways in which IoT is revolutionizing tap water systems and bring new kind of product to the market of plumbing and house appliance. For example, making a bath to baby can cause possible accident of burn due to the change of heat suddenly. This last problem is due to the fact when someone open and close cold water faucets. In case of a bath directly from the shower faucet; Mothers always fill a container with warmed water for avoiding exposing the baby directly to the heated water of the shower. A possible product for this situation a temperature sensor which send temperature information to the cloud with a PID algorithm this last can open and close cold and hot water tap with feedback algorithm to control the temperature of water to be at the desired temperature. In case of high temperature at the faucet of bathroom it is smart enough to close the faucet automatically for avoiding any accident. In this paper, we will focus on the software defined plumbing network that enable fault tolerance we start first by discussing the Hardware needed and later the necessary software.

BACKGROUND

The notion of IoT based software defined plumbing network system is new I have inspired the name from software defined radio where Radio circuit are defined by software rather than hardware in the earlier day of electronics for example filters of frequency are implemented by analog circuit which are prone to errors since the physical components with time will be old and lose their physical properties for example a resistance of $1k\ Ohm$ with time can decrease to $0.8k\ Ohm$ and the circuit will not work properly. Furthermore software defined radio system can be configured to implement any radio circuit

if the front end transceiver hardware allow. For example it can be a Gps or Talkie Walkie or anything else just by changing the firmware.

Another example is FPGA circuit where circuit can be defined and implemented based on the VHDL language. Similarly in this paper with the introduction of IoT we start thinking about plumbing network system with the same way and we believe that this work will open new research in this field, as analogy to electronics for example components lose their physical properties, which is the same in plumbing network system for example revolving knob of faucets each time break down due to operating using wet hand. Engineer has replacing this knobs with another version of plastic which is cost less, other designer use an up and down knob . IoT solution for example can be a solenoid valve operated with software. Hence it will have long life and more economical cost.

To show the importance of this field let consider another example. In some places where water is Available rarely they use spring faucets. The behavior of spring faucets is like this: when the user press the button of the faucets this last serve water for a short time and the spring of the button return back to its initial position where it close again the faucets. Using SDPNS with ordinary faucets we can mimic the same behavior of spring faucets without changing any hardware which is not the case without SDPNS. Let's consider that we have changing physically our faucets from ordinary faucets to spring faucets and after many times of use we are not satisfied about it, the time of opening the faucets is too short or not convenient for our plumbing network how we can solve this problem? Software Defined Plumbing Network System is based on IoT which has an over-the-air update option.

An over-the-air update is the wireless delivery of new software or data to intelligent devices like mobile phone or computer it start in the earlier day of java programming language with a technology called Marimba's Castanet which is a system for distributing, installing, and updating software and content over intranets and the Internet. OTA technology has increased in significance, as mobile devices evolve and applications emerge. OTA updates are a more efficient way to fix bugs and update software than to manually upgrade each individual device. it is everywhere now in windows operating system, Linux system ...etc.

This way the realization of spring faucet can be customized for each user which is not the case for the physical spring faucet. The spring faucet based on SDPNS can be cost effective using open loop system which need calibration for example the SDPNS can ask the user to fill a container of one liter and the SDPNS compute the time of filling as you may notice that we have replacing a hardware which is the flow sensor with piece of software again .What we have said before does not mean that smart plumbing device not exist we can found in some places automatic towel and soap dispensers or automatic faucets or touche-less faucets for example in hospital where contamination of virus is possible, but all of them are expensive and not connected which is not the case of IoT based SDPNS principles which separate the functional part of the system from the GUI This last in the IoT based system can be any things mobile phone, wearable device...etc . The technology of the IoT human interface is an active research area which has developed rapidly for example faucets can be endowed with gesture sensor like Google millimeter radar sensor called soli Google (2015) this last can detect any 3d gesture from free space, using this kind of sensor we can even set the temperature with virtual knob, there is other cheap infrared sensors which cost few couple of dollars which has the ability to detect many position of the hand gesture which can be used easily in our system .Among the applications are touch-less faucets in the event of a general epidemic as the proposed faucets system can be endowed easily by this touch-less sensor.

Another thing to mention is the case of absence of Internet SDPNS should offer LAN control. LAN control function is when your Wi-Fi can't access the Internet or if the server executed in the cloud is down, your devices will go offline, but you can still turn on/off the devices on dedicated app. This mode is important for IoT based system since sometimes the Internet connection lost and it is not convenient to be unable to use your plumbing system at that time.

Furthermore The component used in SDPNS does not forbid the classical use of the plumbing system if you turn for example your pump on/off using your phone application or your Amazon

Alexa in case the absence of Internet and Wi-Fi connection you can press a mechanical switch to turn your pump on or off.

Another possible solution is using the IoT-radio bridges where radio based button are used besides radio-IoT gateway devices this last devices receive commands with radio like 433 Mhz and translate them to IoT or the inverse.

Furthermore there is situation where the design of new IoT components for plumbing network can be the best solution this days and will be a must solution in the future when people will be used to, use it. When the basic components start to appear at that time we can integrate those components in CAD (computer aided design) software like Autodesk Revit Autodesk and the tool chain for the development of firmware used in those components start to emerge as well for automating the process. CAD does not mean a visual language only it can be textual language for describing the network plumbing system (Like VHDL do for digital circuit) taking in consideration the intelligence part which of course will be based on IoT technology.

Let's consider the example mentioned above in the introduction of the washing machine and the rented house. if the pipe where the washing machine is connected to, is the same pipe of the toilet and if we assume that the plumber has making a mistake and he connected this common pipe to the main hot pipe. furthermore we assume that the washing machine this time heat water and The user of the house this time need hot water in the toiled for cold winter but he need as well cold water for his washing machine. Because it is clear if he operate it with hot water it can be damaged which is a compromised situation. If we assume as well that the pipes are encapsulated inside the wall and the house has pretty finish. In this case our solution of software defined network using IoT technology is the right solution for this problem where based on IoT component and software we can serve hot and cold water in one shared pipe .This problem is Mutual exclusion problem but if the faucets are operated with more than one user here the problem will be a group mutual exclusion problem. This problem first was proposed by Joung in Joung (2000), in which an algorithm for shared memory parallel computer system is proposed. because any ME algorithm for solving ME problem can solve the group mutual exclusion problem but the processes will be executing the critical section one at time which means that these solutions does not insure concurrency which is not the case for our problem where the conflict in resource access may be necessary among only part of all processes and another part of them can access the shared resource simultaneously. Many variant has proposed in the literature to name few Madenur and Mittal (2008); Kakugawa, Kamei and Masuzawa (2008); Mittal and Mohan (2007); Joung (2000, 2002, 2003); Atreya, Mittal and Peri (2007); Thiare (2007); Swaroop and Singh (2013); Hadzilacos (2001); Raynal (2013)

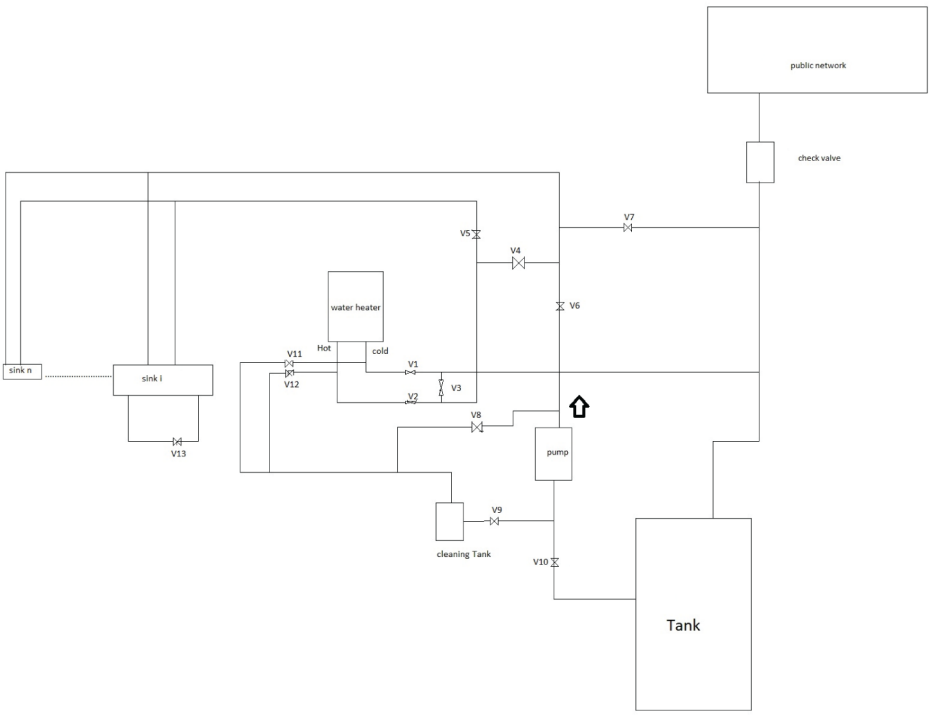
I have used the algorithm described in Kakugawa et al. (2008) which solve the group mutual exclusion problem for more advanced solution where there is many users in the system and it is easy to adapt to the context of IoT. I have adapted the algorithm to the methodology of programming of IoT which is publish subscribe and I have added the preemptive option to the algorithm without the notion of quorum where this last notion is used for decreasing the message complexity. We believe that if the number of process is small and with the broker executed on the cloud it is not important. Furthermore, the algorithm described in Kakugawa et al. (2008) use *acknowledgment* which is not the case for our algorithm we believe that this acknowledgment is used for critical system where formal methods are needed and where we are in LAN mode where internet connection is lost example autonomous vehicle at intersections in this case cars can collide, but for our case the use of the cloud in IoT system can omit this kind of acknowledgment dropping few amount of cold water when you taking shower one time a year or drinking hot water does not kill! The algorithm used here is proved formally to be safe it means those situation does not happen but since we have making other abstraction for example that no one of the valves used will break down and other abstraction for local area network like the messages will arrive in the same order they sent we are not sure. In general, when it comes to real situation manufacturer always make prototypes and operate it for millions of times to decide if it works properly even it is proved formally to be safe because human life is precious. Furthermore, in

our algorithm we have using one token and permission message not a sub-token as in Kakugawa et al. (2008) which make our algorithm slightly different. Besides we have using many queues on the token the reason for that we have considering the methodology of cloud programming which has powerful computation power regarding IoT devices which has less memory and less computation performance.

HARDWARE

We assume that the hardware used is as shown in figure 1.

Figure 1. Fault tolerant tap water system based IoT



In an ordinary tap water system and in the absence of water from the public water network there is pump for pumping water to different taps. Furthermore there is only the valves V1, V2, check valve and there is as well a servomechanism for stabilizing water pressure inside pipes this fact can trigger the pump each time a faucet is opened. The cleaning Tank does not exist in an ordinary tap water system. I have suggested it here as a small container containing the liquid of cleaning the water heater when it will be contaminated with limestone.

The valve mentioned in the proposed system, are solenoid valve or any electric valve that can be controlled by a micro-controller or by simple electric switch. For safety purpose it is possible to associate in series with each electric valve a manual valve. For automatic use of the system we just let this valves opened or we assume that the electric valves can be operated manually as well.

We assume that the symbols given to the principle cold pipe is CP and HP for Hot pipe respectively. The proposed system satisfies these properties:

1. Cold water can flow inside CP only
2. Cold water can flow inside HP only
3. Hot water can flow inside CP only
4. Hot water can flow inside HP only
5. Instantaneous hot water without wasting water
6. Automatic cleaning of the heater

As we have mentioned above each valve can be controlled independently for simplicity we can assume that each valve is controlled by an IoT based switch connected by Wi-Fi to the cloud using the famous esp8266 controller, in nowadays this kind of switches are available in the market. The first and fourth properties are straightforward. For the case of the second properties we need that the valves are in these states:

- **Closed sate:** V1,V2,V4,V6,V7,V8,V9,V11,V12,V13
- **Opened state:** V3,V5,V10

For the third case we need that the valves are in this sates respectively:

- **Closed:** V3,V5,V6,V7,V8,V9,V11,V12,V13
- **Opened:** V1,V2,V4,V10

The properties of instantaneous hot water without wasting water as I have explained in the introduction that the actual technological solution is the circulating pump in our case we don't need this circulating pump we insure this properties with the following valves are in these states:

- **Closed:** V3,V4,V6,V8,V9,V11,V12
- **Opened:** V1,V2,V5,V7,V10,V13

This Configuration permit the cold water resides in the hot pipes to be transferred to the Tank via the valve V7. This configuration remains until the Hot water reaches the faucet requesting hot water. In figure 1 I have showed only the valve V13 for an ordinary end but in reality each end has a similar valve doing the same function. In the case of circulating Pump we need only one Valve like V13 since the pump suck the water residing in hot pipes via one special valve which is special kind of valve work as follows.

The valve let water with a certain temperature to pass from hot pipe to cold pipe, when the temperature reaches the desired threshold the valve close automatically. The circulating pump can be activated with radio based remote for the other ends to insure instantaneous hot water. In our case the system is smart enough to work without circulating pump in an open loop or closed loop control if at least one end are dotted with a temperature sensor.

For the case of our system if we add a circulating pump we don't need the radio based remote control since the system is smart enough to activate the circulating pump as needed. The circulating pump for our case is simple pump which is cost-less regarding the circulating pumps in the market. In the case where more than one faucet request instantaneous hot water we control this operation by software to insure that each valve in position like V13 (i.e. between cold and hot pipe) closes when water will be hot independently. In case when we use a circulating pump we circulate water until we insure that there is only hot water in all pipes.

For the automatic cleaning of the heater can be scheduled in the right time if the valves are in these states:

- **Closed:** All valves except the opened valves below
- **Opened:** V11,V12, V8,V9

The actual state of the technology of IoT can easily implement this kind of fault tolerant system based on the notion of scenario in the cloud. A scenario is setup to auto-execute action with a certain orchestration. There are three kinds of scenario; they are different in the trigger condition. Triggered by user like press button, the second one is triggered by some data of a certain device, such as temperature, humidity, light...etc since the IoT is a subscribe-publish system. The third one is triggered by status from another device.

For example, you created a scenario to make an illusion that you are in your house for avoiding theft to steal your house; you program this on the cloud by switch on the light of the toilet for 5 minute then turned it off, then turn on the light of bathroom, after that you switch on TV, and finally the air-conditioner. In our case for example to get cold water in hot pipe you make scenario as follow:

- Close the valves V1, V2 and V4
- Open the valve V3

The missing features in this technology reside in the fact that it cannot insure the management of shared resource with group mutual exclusion which enables the feature of Fault tolerance. This will be explained in the next section.

SOFTWARE

For explaining the problem I will use a more simplified version of the hardware mentioned above this last can be reduced to cold and hot water in one shared pipe! See figure2

The system described in figure 2 work as follow: let's say that we want cold water in Tap1 to satisfy this property we need the configuration of valves in these states:

- **Opened:** V3,V4,V6
- **Closed:** V1,V2,V5,V7

C1,C2 are check valves use to insure that water does not collide and go in one direction. In the case that we want hot water in Tap1 we configure the set of valves to be in this sates respectively:

- **Opened:** V1,V2,V6,V4
- **Closed:** V3,V5,V7

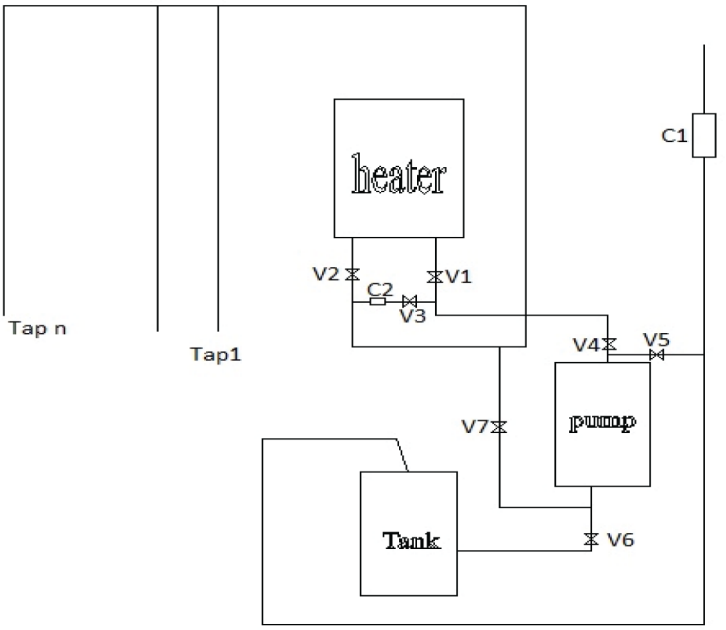
This configuration mentioned above does not insure instantaneous hot water alone we need to precede this operation by a configuration for evacuating cold water residing in pipes like this:

- **Opened:** V5,V7
- **Closed:** V1,V2,V3,V4,V6

This configuration sucks water from pipes via the Valve V7 through the pump to the tank via the valve V5.

The check valve C1 is standard that avoid pumping water outside the house, but the check valve C2 used in case we use a simple taps at the ends without water mixer. This check valve avoid cold water coming from V3 to collide with hot water coming from V2 and insure the mixing in the main

Figure 2. Hot and Cold water in shared Pipe



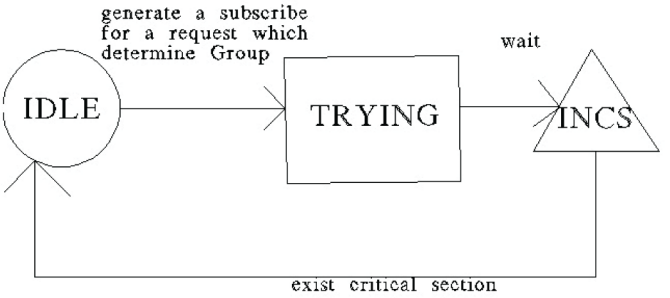
pipe with a good algorithm of PID (Proportional Integral Derivative Control) we can get water at the desired temperature. As you can see that this system is more economical than any other system just with seven electric valve, one pump and just one central heater we can insure hot, cold and warm water with only one shared pipe!.This system can be very useful especially in places where they aggregate toilet with bathroom and they look for economy in their design.

We left the attention that due to the technology of IoT we configure the faucets for a certain kind of water for example in general the faucet in the toilet has only cold water we can set this faucet to cold water only we will discuss this later in next sections.

This work fine if only one request at time but if different requests happen simultaneously the system will be in big dilemma. This is a kind of group mutual exclusion problem Joung (2000) where mutual exclusion is necessary only among the process requesting conflicting resources i.e. one process request hot water and another process request cold water, in this situation only one process can be served, but if some processes request the same kind of resources they can be served at the same time for example three process request cold water they can be served in parallel. Any resource must be accessed mutually exclusively by process from different groups, but process in the same group can access the same resource simultaneously. A process knows the existence of two groups and can determine which group it belongs to upon the request of user hot or cold water; then the execution of process flows a cycle of three phases as shown in figure 3:

We can suppose that the cold water is used for drinking it is not convenient to drink hot water. We suppose as well that we have only shared pipe for hot and cold water shared between the faucets used around the house. A user can ask for hot water as well as cold water. The concurrency among process of the same group is not considered since it is clear that no competition between process in the same group. We suppose as well that warmed water constitute another groups classified regarding the requested temperature and for simplicity here we consider only two groups cold water group and hot water group.

Figure 3. Execution states of a process



FORMALIZATION OF THE PROBLEM

It is assumed that the system contains *n* processes, denoted by {*p*1*; p*2*; …; pn*}, and the processes will not fail. Processes communicate with each other by exchanging messages. There is one communication channel between each pair of processes and it has the FIFO property, i.e. messages via the same channel are delivered in the same order as they are sent. The timestamp of any event (including sending, receiving…etc) is globally unique and comparable with others. The processes that execute the same request of resources constitute a group and they are considered as mate process. Processes in conflicting groups is rivals of each other. There can be totally two groups, one for those processes which request cold water and another group for the processes requesting hot water, denoted by $G = \{g1; g2\}$, and a process's group is dynamically determined by its current request. In an ordinary house if we consider each faucet as a process the number of process does not exceed ten.

Definition: The group mutual exclusion problem is a problem to control execution of processes to satisfy the following two conditions:

- **Group mutual exclusion (safety):** No two processes belonging to different groups, which have requested critical sections, are in their critical sections simultaneously. In our case no two processes served at the same time one request cold water and the other request hot water.
- **Starvation freedom (liveness):** A process desiring to enter critical section will succeed eventually.

Simultaneity or concurrency and waiting time are essential criteria for measuring the performance of our fault-tolerant tap water system algorithm. Simultaneity is the number of processes served simultaneously, and higher Simultaneity is better. Waiting time is the time that a process has to wait to be served after making a request. The development of an algorithm that realizes the high simultaneity and the small waiting time is not straightforward especially if there is a request from conflicting groups. Consider a situation in which certain processes are served cold water, and a process of the same group makes a request. If the request is granted immediately, the simultaneity is increased. On the other hand, requests from other processes belonging to different group must wait to be granted. The complication of designing the algorithm is the compromise simultaneity and waiting time.

Local Variables at Each P_i

Each process P_i maintains the following local variables:

- ***mode*$_i$:** Represents current status of P_i, and its value is IDLE (not interested in critical section), TRYING (making a request for critical section entry), and INCS (process is in critical section).
- ***tok*$_i$:** The token object if P_i holds it. Otherwise, its value is ⊥.
- ***publisher*$_i$:** Process name that holds the token. Its value is ⊥ if *Pi* does not know.
- ***attrib*$_i$:** A set of memory cell used for priority function queued with the process when it make a request. it can be dynamic selected or configured on the cloud for example by the user cell phone like timestamp, priority, cold, hot, enabling, disabling ..etc this attribute can be affected by the intelligence of the cloud for example via the cloud using a cell phone we can set hot water only at night or disabling water from a certain faucet in the garden to forbid children wasting water or configure certain faucets for cold water only this facts can influence $attrib_i$ directly or indirectly.

Structure of the Token

The token contains the following data:

- ***gName*:** Holds the current group. If no process is in critical section, its value is ⊥.
- ***groups[i,j]*:** A queue of request items *i* represents group and *j* is the sets of all process subscribed to the group *i*.

The attributes $attrib_i$ stored in the column [*i*] can be configured and selected based on the priority function chosen by the user, for example a timestamp or preponderance. For example, a washing machine request cold water when someone take a bath. In this case we can give more priority to the faucet of the bathroom than the faucet of the washing machine.

Operations of our Algorithm

Our algorithm is based on publish-subscribe approach used by most of IoT systems. A process can subscribe to a certain group dynamically i.e. on the time of the request. One of the processes subscribed in the group will be chosen to be the proxy of the group and take the role of the publisher when he gets the token. The token is maintained so that it is unique in the system owned by the publisher.

The uniqueness of the token used to insure a mutual exclusion between conflicting groups. Permission is given by the publisher to his group if it's their turn and the number of permission is limited only by the number of the process in the system. A process obtains the token to enter critical section if there is no process in critical section. A process enters its critical section by receiving an OK message in case other process in the same group is in its critical section. A group is selected based on certain priority function it can be manually set or by a machine learning Algorithm. Hence the Algorithm may be a preemptive Algorithm based on the priority function. For simplicity let's consider the Algorithm non preemptive right now. if the token is given to the process *p* interested to group *g*(hot water group) this last became the publisher which broadcast an acquired message to all process of the system that he is the publisher and send a broadcast message ok to all the process in the list of the group *g* to open there solenoid valve to be served. The other process interested to cold water there valve remain closed and there request of subscription will be queued on the list or the queue of cold water in the token.

If new process request *g* (hot water) and the priority remain to *g*(actual hot water group) he will be queued on the list of *g* and served automatically i.e. get a permission from the publisher.

Each time a process in the group finish he close his valve and send an unsubscribe message to the publisher, this last will withdraw the finished process from the queue of the group and the priority

function is recalculating the priority of the group since the finished process can have the heaviest priority and the priority of the group can be decreased dramatically which force the publisher to cede the token to a group with higher priority. If the priority remains to the current group the publisher continue owning the token. in case the publisher change his mind to request a different group than the current group(hot water) his request will be queued let's assume he request this time cold water . The priority of the current group (hot water is recalculated) if it is lower than the priority of the cold water group a preemptive message is send to the hot water group and in this case the publisher continue owning the token what change in this case is only the current group in the token which will be the cold water this fact will trigger an *ok* message to the cold water group to open their valves to be served. Our algorithm uses one type of tokens and permission. The publisher that holds the token knows the following two values:

- *Current group*, which is the group of processes that are currently in critical section which is not necessary his requested group; and
- *Group size*, which is the number of processes currently in critical section this last information is computed based on the number of elements in the queue of the current group.

The rough sketch of the proposed algorithm is as follows:

1. When process P_i wishes to enter critical section, it sends a **Subscribe** message to the publisher *Pj* in the system, and it waits for a token (token or permission) to arrive.
2. When process P_j receives a **Subscribe** message from P_i, it queued the process p_i in the queue of the requested group g_i, until P_j served and leave.
3. When the publisher P_k which own the token receives a subscribe request issued by *Pi*: The arrived request is, in any case, put into the queue of the token in the cloumn of the requested group. Each request in the queue is granted according to the following rules:
   a. If no process is in critical section, the token is transferred by a **token** message to a requesting process.
   b. If some processes are in critical section already and the requested group is the same as the current group,*Pk* sends a permission message to *Pi*, as long as there is no request in other group with higher priority.
   c. Otherwise, the request is kept in the queue of the token. The token may be transferred to other process to grant the request of the process, and this may happen several times. The request of P_i is eventually granted by the publisher, sayP_l , which may not be the same as *Pk*.
4. Process P_i enters critical section by receiving the token (a token message) or permission (an OK message).
5. When process *Pi* exits critical section: If *Pi* is the publisher, he continue to own the token and he yield this token based on the priority function when the procedure *handlerpendingrequest* is triggered if the chosen group is not the same group in this case a *preempt message* is published (broadcast to the all the process in the current group) and the processes in the groups remains in the queue . Otherwise, i.e., P_i has permission, it exit the group simply by sending **unsubscribe** message.

Priority Scheme of the Token Queue

The adapted Algorithm which is derived from the work of Kakugawa et al. (2008) is especially suitable for our problem in which group selection is non-uniform as we have mentioned in the related work our Algorithm is designed with an IoT approach in mind i.e. with a publish-subscribe and with preemptive

Figure 4. The symmetric Algorithm for Pi

```
OnInitialization;
begin
1 PC: true

1.1 mode_i := IDLE; valve_i=closed publisher_i = ⊥;
1.2 if (P_i = P_k) {
1.3 tok_i:= new(Token);

1.4 tok_i.gName := ⊥; tok_i groups := new(groups);
1.5 send < acquired> to each P_j
1.6 }else {

1.7 tok_i := ⊥; }
end
onSubscribeEvent(gi);
begin
2 Pc : (mode_i = IDLE)
2.1 mode_i := TRYING;

2.3 if (tok_i ≠ ⊥) Then{
2.4 enqueue(toki.groups[gi]; Pi)
2.5 call handlerpendingrequest;
2.6 else
2.7 send(subscribe; Pi; gi) to publisheri
end if
end
onUnsubscribeEvent;
begin

3 Pc : .mode_i = INCS ∨ mode_i = TRYING

3.1 if(toki ≠ ⊥) Then{
valve_i:=closed
3.2 mode_i = IDLE
3.3 dequeue(tok_i.groups[tok_i.gname]; Pi)
3.4 call handlerpendingrequest;
3.5 }else{
valve_i:=closed
3.6 mode_i = IDLE
3.7 send < unsubscribe > to publisher_i
}endif
end
handlerpendingrequest
begin

4.1 if (tok_i ≠ ⊥) ∧ tok_i.groups[tok_i.gname] = ∅ ∧ toki.groups ≠ ∅ Then{
4.2 < pj, g >= select(toki.groups)
4.3 tok_i.gName = g
4.4 send(token) to P_j

4.5 tok_i = ⊥
4.6 else

4.7 if(tok_i ≠ ⊥) ∧ tok_i.groups[tok_i.gname] ≠ ∅ Then
4.8 if priority(toki.gName) then
4.9 publish(OK, tok_i.groups[toki.gName]
4.10 else {
4.11 Publish(preempt, tok_i.groups[tok_i.gName])
4.12 < p_j; g >= select(tok_i.groups)
4.13 if p_j = publisher_i then
4.14 tok_i.gName = g
4.15 call handlerpendingrequest;
4.16 else
4.17 tok_i.gName = g
4.18 send(token) to P_j

4.19 tok_i = ⊥
}
endif
endif
endif
end
OnReceiptOf (token,tok)
begin
5.1 tok_i = tok
5.2 send < acquired > to each p_j j ≠ i
5.3 publisher_i = p_i
call handelpendingrequest
end
}
Onreceiptof(Ok) from p_k
begin
6.1 if mode_i= TRYING then
6.2 mode_i= INCS
valve_i:=opened
6.3 RequestDone
end
OnReceiptOf(acquired) from p_k
begin
7.1 publisher_i = pk
end
OnReceipt of (subscribe,pk,g)
begin

8.1 if tok_i ≠ ⊥ then
8.2 enqueue(toki.groups[g], pk)
8.3 call handlerpendingrequest
end
OnReceiptOf(unsubscribe,pk)
begin

9.1 if tok_i ≠ ⊥ then
9.2 dequeue(toki.groups[toki:gName], pk)
9.3 call handlerpendingrequest
end
OnReceiptOf(preempt ,g_i)
begin
10.1 if mode_i = INCS then
valve_i:=closed
10.2 mode_i = TRYING
10.3 call handlerpendingrequest
end
```

way. Our Algorithm can be used with cloud based approach as well as LAN mode where Internet connection is lost. If the internet connection exists the token can reside on the cloud and the mode of communication is publish-subscribe. In case the connection is lost the system can work on LAN mode this can be done by downloading the token by the publisher and the communication will be peer to peer. Because of this structure of token with encapsulated queues we can define various priority schemes. For example we can use region based priority where we can divide faucets to region like:

- kitchen {*P*0*; P*2}
- Bathroom {*P*3*; P*6*; P*1}
- toilet {*P*4*; P*5}

If we assume that we have 7 faucets in our plumbing system. We can define the precedence priority as follow:

toilet > bathroom > kitchen

Another possible approach for insuring high simultaneity or concurrency we can give priority to the group which has max request. If we assume 5 process request cold water and another 3 process request hot water The priority will be given to the cold water group because cold water group has max request. Another possible way to set priority is to give priority to individual faucets for example the faucet of the shower is more prioritize than the faucets of washing machine. We can use as well the FCFS approach.

In our design, we have associated to each process a number of attribute independently of the queue which is not the case of the work of Kakugawa et al. (2008). This attribute can be created dynamically by the selection of the user explicitly or implicitly by selecting a mode of use of the system for example FCFS necessitate to associate a timestamp attribute to the processes in the system implicitly. To better explain this idea let consider that the user can select attributes from a list and associate each attribute to another attribute predefined which can be set or computed:

```
Timestamp: time
Fulfilledrequest: Integer
Age: Integer
Priority: Real
```

Since the approach is Publish-subscribe we can subscribe the age to a session which represents a turn of new group each time the group change and the process group not selected it increase by one. The same for fulfilled request attribute we can subscribe this last attribute to the triggered procedure *Requestdone* by increasing this attribute by one. The timestamp attribute can be set at the moment where the process makes a request. Furthermore the priority attribute of the process can be computed in real time based on the attribute discussed before. We left the attention that the choice of the priority scheme can cause starvation discussed in liveness property in the next section.

Correctness Proof

Invariant 1 (invariant symmetry): All the process in the system execute the same Algorithm.
Lemma 1 (uniqueness of the token): The token is maintained so that it is unique in the system.
Proof: The creation of the token is executed once during all the life of the system in the initialization section by the process *P*0 figure 4 line 1.3 all the other operation are just sending token which conclude the proof.
Lemma 2: The handlependingrequest is executed only by the publisher the owner of the token.

Proof: The procedure *handlependingrequest* executed based on the if statement Figure4 line 4.1 or its else in line 4.7 in the two cases we have the common condition $tok_i \neq \perp$ which means that the procedure is executed only by the publisher.

Invariant 2 (invariant current group): The current group is maintained by the unique local variable of the token *gName*, i.e. at any instant:

$$t\forall g_i \in G\exists j \ such \ that \ gName = g_j \wedge \forall i \neq jgName \neq g_j$$

Lemma 3: (ok permission message):

$$\forall p_i \neq p_j \ at \ any \ instant \ t, p_i \ receiveOK \wedge p_j \ receiveOK$$
$$\Rightarrow p_i \wedge p_j \in g\left(p_i \ and \ p_j \ are \ in \ the \ same \ group\right)$$

Proof: If we assume that there is no delay in receiving messages, we can see that in Figure 4 the only statement of sending ok permission message is in line 4.9 which is a broadcasting message to one group only which conclude the proof.

Invariant 3 (Group Changing): The pre constraints for changing group are:

1. figure 4 line 4.1 the current group is empty.
2. figure 4 line 4.14 and line 4.17 after a preempt message

Lemma 4: A process p_i can exist only in one queue of group at time

Proof: A process can be queued only if he make a request and the only position where the process make request is in figure 4 line 2 mean that a request is taken in consideration only if the process is in IDLE mode and he cannot be in this state again only if *unsubscribe* event is triggered line 3.2 and line 3.7 which withdraw it from the queue this conclude the proof.

Theorem 5 (safety): For any execution, no two processes in different groups are in critical section simultaneously.

Proof: Let gr_i denote the current group of P_i and gr_j denote the current group of P_j. we assume that:

$$mode_i = mode_j = INCS \bigwedge gr_i \neq gr_j$$

Using lemma3 we conclude that an OK message was sent to gr_i at t_i and another OK message was sent to gr_j. at t_j where $t_i \neq t_j$. i.e. That the gName has been changed this means that:

- at t_i $gName = gr_i$
- at t_j $gName = gr_j$

Using the invariant 3 either the $groupesize(gr_i) = 0$ this means that $mode_i = IDLE$ or preemptive message was sent to the group gr_i this means that $mode_i = TRYING$ which is contradictory with the assumption this conclude the proof.

Theorem 6 (Liveness): A process that makes a request eventually enters critical section.

Proof: Using the notion of queue does not ensure the non starving properties. The liveness properties is based on the priority function used. Let's discuss this problem mathematically. let *r1; r2; …; rL* be a subscribe request in the queues where L is the total number of requests in All the queues we recall that the number of queues is the number of groups if we consider only cold and hot water we have two groups so we have two queues. Let's assume *r*1 is the oldest request and *rL*

is the latest one. Let's consider that *gri* is the requested group for *ri*. we assume that the priority function is defined as follow:

$$P(ri) = \alpha \times current(ri) + \beta \times timeorderG(ri) + \gamma \times MaxrequeG(ri) + \delta \times AgeG(ri)$$

where:

- α,β,γ,δ: Are positive constants used for speeding turns or slowing it based on the choice of the user, they may also be determined automatically by machine learning.
- If gri = token.gName then current(ri)= 1 else current(ri)= 0 it means if the group of ri is the current group than current(ri) equal 1 and 0 otherwise.
- If $\forall$ rj; min – timestamp(rj) $\in$ GRI then timeorderg(ri)= 1 else timeorderg(ri) = 0 in this approach we have choosing the oldest request as criteria ordering of the group.
- MaxrequeG(ri) is the max request in a group selected by ri as we have explained in the previous section.
- AgeG(ri) is the age of the group of ri which is the number of granted requests after the oldest ri is queued.

Let assume that it exist j such that the requested group of *rj* is cold water and $\forall \neq$ j ri group is hot water. Let's assume that at T1 the current group is hot water group. So we have at T1:

$$P(ri) = \alpha + \beta + \gamma \times (L-1) + \delta \times 0$$
$$P(rj) = \alpha \times 0 + \beta \times 0 + \gamma \times (1) + \delta \times 0$$

and after $t > T1$ we assume the worst case each time the hot group remains the same it means grj = cold water and $\forall \neq$ j gri = hot water. In this case at T2 we have:

$$P(ri) = \alpha + \gamma \times (L-1)$$

$$P(rj) = \beta + \gamma + \delta \times \quad (1)$$

We can see easily that:

$$t > t2\ P(ri)\ \alpha + \gamma \times (L-1)$$

and $P(rj)$ is unbounded due to the age of the group. In this case the turn returns back to j. Which conclude the proof.

Remark 1: Based on the selected attributes by the user for the priority scheme we have:

- $\alpha = 0$; $\beta >= 1$; $\gamma = \delta = 0$ this priority approach is the FCFS which is non starving scheme with low simultaneity or concurrency.
- $\alpha >= 1$; $\beta = \gamma = \delta = 0$ this schemes increase simultaneity or concurrency but this scheme is starving because if the current group has max request he will be selected all the time even if the group is the same in each initiated session.
- $\alpha, \beta > 0$:this priority approach provide both concurrency and non-starving.

PERFORMANCE ANALYSIS

In this section we analyze the performance of our distributed algorithm; we can see that our algorithm uses six kinds of message which are:

- Subscribe
- Unsubscribe
- Token
- OK
- Acquired
- Preempt

The assessment criteria used for our algorithm are:

- **Message complexity:** The worst case of number of messages exchanged per request for critical section.
- **Waiting time:** The time between a process that makes a request and its entering to the critical section measured by message hops.
- **Synchronization delay:** The time needed for the commutation between two distinct group measured by message hops.
- **Maximum concurrency:** The maximum number of processes that can enter critical section.

Theorem 7: The worst case message complexity of our algorithm is 2n where n is the number of process in the system.

Proof: The scenario of the worst case is like this: a requesting process pi send a subscribe message to the publisher this last queue pi on the requested group by pi of the token and call the procedure callPendingRequest which yield the token to pi via a transfer message then pi sends an acquired message to all the processes in the system flowed by an OK message to itself (copied) and all the other processes in the queue. Hence in total 2n messages:

- 1*subscribe message*
- 1*token message*
- $(n-1)$*acquired message*
- $(n-1)$*OK message*

Remark 2: In the case the current group is the same as the requested group by *pi* the message complexity is 1 since *pi* need to send only a subscribe message.

Theorem 8: The maximum concurrency for our algorithm is n.

Proof: When all the processes make a request for the same group, all of them will be queued on the same queue including the publisher itself and the permission will be given to all of them it means *n.*

Theorem 9: The waiting time of suggested algorithm is at most 4 message hops.

Proof: Let us monitor the sequencing of messages. a requesting process sends a *subscribe* message to the publisher then *unsubscribe* message or *preempt* message are exchanged then a *token* message for transferring the token and finally an*OK* message for entering critical section. therefor a 4 message hops are needed.

Theorem 10: The synchronization delay of the proposed algorithm is at most 2 message hops.

Proof: A process generating a request for critical section, can enter the critical section as soon as it receive the token after an unsubscribe message or a preempt message which conclude the proof.

CONCLUSION

In this paper, we have giving an example of a software defined plumbing network system. A software defined plumbing network system is a plumbing network system where components that have been traditionally implemented in hardware (e.g. water mixers, spring faucets, flow sensors, etc.) are instead implemented by means of software on a computer or embedded system. This concept of SDPNS to the best of our knowledge is new, the rapidly evolving capabilities of IoT systems render practical many concepts which was in the past impossible to be nowadays feasible. if you told some one that we can use hot and cold water using one pipe he will get an astonishment! Thanks to computer algorithms which make these things happen.

REFERENCES

Atreya, R., Mittal, N., & Peri, S. (2007). A quorum-based group mutual exclusion algorithm for a distributed system with dynamic group set. *IEEE Transactions on Parallel and Distributed Systems, 18*, 1345–1360. .10.1109/TPDS.2007.1072

Autodesk. (n.d.). *CAD for automating Plumbing Design in Revit*. https://www.autodesk.com/autodesk-university/class/

Google. (2015). *Soli a miniature radar that understands human motions at various scales: from the tap of your finger to the movements of your body*. https://atap.google.com/soli/

Hadzilacos, V. (2001). *A note on group mutual exclusion*. doi:10.1145/383962.383997

Joung, Y. J. (2000). Asynchronous group mutual exclusion. *Distributed Computing*, *13*, 189–206. doi:10.1007/PL00008918

Joung, Y. J. (2002). The congenial talking philosophers problem in computer networks. *Distributed Computing*, *15*, 155–175. doi:10.1007/ s004460100069

Joung, Y. J. (2003). Quorum-based algorithms for group mutual exclusion. *IEEE Transactions on Parallel and Distributed Systems*, *14*, 463–476. doi:10.1109/TPDS.2003.1199064

Kakugawa, H., Kamei, S., & Masuzawa, T. (2008). A token-based distributed group mutual exclusion algorithm with quorums. *IEEE Transactions on* Parallel and Distributed Systems, *19*, 1153–1166. doi:10.1109/TPDS.2008.22

Madenur, V., & Mittal, N. (2008). A delay-optimal group mutual exclusion algorithm for a tree network. *Journal of Information Science and Engineering*, *24*, 573–583.

Mittal, N., & Mohan, P. (2007). A priority-based distributed group mutual exclusion algorithm when group access is non-uniform. *Journal of Parallel and Distributed Computing*, *67*, 797–815. doi:10.1016/j.jpdc.2007.02.005

Raynal, M. (2013). *Distributed Algorithms for Message-Passing Systems*. doi:10.1007/978-3-642-38123-2

Swaroop, A., & Singh, A. (2013). The message passing group mutual exclusion: A review. *International Conference On Global Trends in IT*.

Thiare, O. (2007). *Group mutual exclusion in distributed systems*. Academic Press.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Implicit Cognitive Vulnerability Through Nudges, Boosts, and Bounces

Caroline M. Crawford, University of Houston-Clear Lake, USA
Sharon Andrews, University of Houston-Clear Lake, USA
Jennifer K. Young Wallace, Jackson State University, USA

ABSTRACT

Implicit cognitive vulnerability is a developing theoretical understanding, wherein feeling safe within an instructional environment is of significant impact upon short-term and long-term memories' cognitive acquisition of information so as to embed new information within a learner's conceptual framework of understanding. Towards successfully individualizing a learner's implicit cognitive vulnerability, the primary focus has been upon the larger community environment in which the learner is housed, yet the viability of the learner's ability and cognitive viability must also be addressed through nudges, boosts, and bounces of motivational support. Recognizing this individualized need of learners, this discussion revolves around the ability of a learner to embed implicit cognitive vulnerability within their own cognitive viability through structured and unstructured synchronous and asynchronous nudges and boosts that support self-regulatory and self-efficacy understandings.

KEYWORDS

Boost Effect, Capability, Cognition, Cognitive Processes, Competence, Heuristic, Human Cognitive Architecture, Implicit Memory, Learner, Motivation, Nudge Theory

INTRODUCTION

The instructional environment, whether traditional or non-traditional in nature, whether formal or informal, embeds the focus of the cognitive transformation of the learner. A learner's cognitive ability is impacted by the ability to obtain and retain information, especially as understood through the hyperconnective style of engagement with information that has come to be known as the Information of Things (IoT), with the cognitive impact of IoT of immense and continued study. Recognizing the importance and impact of the instructional environment in which learning occurs upon the learner, Implicit Cognitive Vulnerability as a theory has been a focus of understanding and engagement (Crawford, 2015, 2016, 2018, 2019; Crawford & Semeniuk, 2016; Crawford & Smith, 2015; Crawford, White, Young Wallace, 2019). Yet the learner's style of environment in which cognitive engagement and revising conceptual frameworks of understanding occur, there is a developing understanding around learning in landscapes of practice as well as an understanding around value creation within the bounds of more socialized elearning spaces that are inherent within the hyperconnected world of the Internet, or the Web of Things (WoT) that has been embedded within the Digital Age's immediacy of information and the socialization that occurs as inherent within the learning process (Wenger-Trayner, Fenton-O'Creevy, Hutchison, Kubiak, & Wenger-Trayner, 2014; Wenger-Trayner & Wenger-Trayner, 2015, Wenger-Trayner & Wenger-Trayner, 2020). Towards embracing the learner's

DOI: 10.4018/IJHIoT.285588

cognitive support throughout the learning process that has become a continuous spiral of engagement and re-engagement with subject matter, the learner's cognitive viability and motivational engagement must be at the forefront of consideration, potentially addressed through nudges, boosts and bounces of motivational support.

BACKGROUND

Implicit cognitive vulnerability is grounded within an understanding around the cognitive interworkings of a learner's ability to safely and openly engage within an environment, towards successfully folding new information and new ideas into one's long-term memory. Grounded in the work of learning theorists and psychologists, the understandings around Maslow's Hierarchy of Needs of physiological, safety, belongingness and love, esteem and self-actualization (Maslow, 1943, 1954, 1961, 1962a, 1962b, 1963, 1964, 1969a, 1969b, 1970, 1971, 1979, 1982, 1987, 1993a, 1993b, 1993c, 1996, 1999a, 1999b, 1999c) with next step understandings around Koltko-Rivera's (2006) work that highlights self-transcendence as a creative endeavor far beyond one's self frames the importance of an environment in which learning can occur are bound within Vygotsky's Conceptual Framework of Understanding (Vygotsky, 1933/1966, 1934/1987, 1935, 1962, 1978 1981) that highlights the ability of a person to cognitively rethink, restructure and re-frame short-term and long-term information that is the basis of initial knowledge acquisition as well as lifelong learning. Yet Wittgenstein's work (1922) work around word choices that embed nuanced meanings and potential biases as well as communicated understandings around subject matter is supportive of implicit cognition and the vulnerability of the learner's cognitive processes. Also inherent in an understanding of Implicit Cognitive Vulnerability is Bandura's work associated with a learner's motivational engagement and sense of self-efficacy, framed through motivation and self-efficacy (Bandura, 1977, 1986, 1997), including expectancy constructs (Parsons & Goff, 1978) that lead into scaffolding an understanding of Vroom's expectancy theory (1964) suggesting that an "intensity of work effort depends on the perception that an individual's effort will result in a desired outcome" (Holdford & Lovelace-Elmore, 2001, p. 8).

Yet, why focus upon Implicit Cognition and Vulnerability? Cognitive vulnerability is normally discussed in psychological circles as a level of discomfort or depression by the individual, which does impact one's cognitive abilities. Towards reflecting this understanding, Ito, Erisir and Morozov (2015) suggest that, "Purely psychological distress, without physical pain or physical discomfort, renders brain more vulnerable to a broad range of traumatic events, increasing chances of mental illness" (p. 2536; Cougle, Resnick, & Kilpatrick, 2009; Resnick, Yehuda, Pitman, & Foy, 1995). Yet, instead of a discussion around mental illness, a recognition that the discomfort and potential psychological stress associated with the learning process may reflect a cognitive vulnerability. Specifically, the learning process in itself reflects the requirement towards cognitive discomfort and the ability for the learner to open the already developed conceptual framework of understanding (Vygotsky, 1933/1966, 1935, 1981) to shift, change and reconnect old pieces of knowledge and information into new ways of thinking, also while shifting and moving knowledge from new information into the realms of established knowledge and understandings. As such, implicit cognitive understandings must be bound within a level of discomfort and vulnerability, towards understanding new information as well as engaging in creative new ways of looking at and thinking about information, resulting in the recognition of Implicit Cognitive Vulnerability that supports learners. As expressed by Crawford (2018):

Implicit Cognitive Vulnerability is a theoretical construct, a concept that engages in an understanding revolving around how a person understands information, shifts information from short-term memory into long-term memory access, and the vulnerability within the learner's cognitive processes that support or abandon the learner's ability to conceptualize the new information within prior learned information. (p. 5149)

Within instructional environments, that may be defined as traditional face to face instructional environments, distributed flipped classrooms or hybrid instructional environments, or even online instructional environments that may also encompass microlearning events, structured as well as unstructured engagement with new knowledge and progressive developmental understandings, an understanding around open and engaging instructional guidance as well as the comfortability of learner colleagues must be progressively embedded so as to highlight the possibilities around learner engagement with the new information as well as shifts in learner understandings as the new information is cognitively framed into long-term memory understandings. As suggested by Crawford, White and Young Wallace (2019):

As well, I realized that my professional journey would evolve into attempting to better understand the process of learning as an individualized endeavor. Not only towards better supporting the knowledge acquisition by learners so as to develop a base knowledge that would support enhanced engagement with the subject matter, but also towards better understanding the formation and support towards developing a viable learning environment that embraced the concepts of cognitive vulnerability (Crawford, 2015, 2016, 2018; Crawford & Semeniuk, 2016; Crawford & Smith, 2015), conceptual frameworks of understanding (Vygotsky, 1934/1987, 1962, 1978) and learning in landscapes of practice. (Wenger-Trayner, Fenton-O'Creevy, Hutchison, Kubiak, & Wenger-Trayner, 2014; Wenger-Trayner & Wenger-Trayner, 2015) (p. 7-8)

Embraced by Crawford's (2018) theoretical frame of Implicit Cognitive Vulnerability as:

The primary concerns revolving around the conception of Implicit Cognitive Vulnerability have to do with the impact of the instructional facilitator, the collegial learners, and the subject matter prior experience on the part of the learner. Each aspect within the instructional environment is integrally important to the impact upon the learner's cognitive understanding and implicit memory retention and retrieval. Simplistically stated the triad of components, or constituents, within this instructional process are imperative towards supporting and engaging the learner's successes. (p. 5150)

A further extension in engagement as regards Implicit Cognitive Vulnerability may be offered as:

An interesting discussion revolves around Implicit Cognitive Vulnerability and ways to deal with issues, controversies or problems associated with the concept of Implicit Cognitive Vulnerability. One instructional style does not meet the needs of every single learner, even if the subject matter is similar in presentation and prior knowledge attainment and understanding. Much of this may be the ways that different instructional facilitators present the subject matter to the learners; as well, much of this may be due to the community of learning that is developed and the trust that bonds the collegial learners within the instructional environment. (Crawford, 2018, p. 5152)

Through this understanding of the theoretical and modeled undergirdings associated with Implicit Cognitive Vulnerability as a theoretical understanding, it's important to frame the learner-focused understandings of the learner's motivational needs and engagement in the learning process.

MAIN FOCUS OF THE ARTICLE

The Implicit Cognitive Vulnerability theory has been developed with a primary focus upon the safe and supportively engaging learning environment, as well as the importance and impact of the instructional facilitator upon not only developing a vulnerable learning environment but also upon modeling and setting the tone of what is an environment in which learners are heard, supported, engaged

in the instructional process as well as supportive the learners towards creatively striving towards excellence in knowledge acquisition and attainment, real world understandings of subject matter, rethinking conceptual frameworks of understanding, as well as creativity of thought and reasoning around the subject matter towards transcending prior understandings. However, the triad that makes up the instructional environment, revolving around the knowledge base, is not merely the facilitative instructor and the instructional environment, but the primary focus of the instructional environment is upon the learner. The instructional environment does strive towards impactful learning opportunities, the cognitive acquisition of information is emphasizing the shift from short-term memory into long-term memory, while the creativity of the learner is enhanced through cognitive motivational support that may occur through nudging and boosting the learner's progression towards attaining or surpassing learning objectives. As such, Nudge theory supports the understanding of the learner's engagement with the subject matter within the Implicit Cognitive Vulnerability understandings, as well as Attentional Boost Effects upon the learner's motivational successes.

Instructional Environments: Impactful Learning

Impactful learning occurs within learning environments that are cognitively safe and vulnerable towards expanding the learner's knowledge acquisition and thoughts around the subject matter at hand. The engagement of learners within the instructional environment embeds the expectations that the learning climate within the instructional environment, as well as the psychological safety of the learners represent inherent needs that include an inherent acceptance of each learner, of one's ultimate belonging and assurance of being in the right place to be successful and fitting into the collegial environment. The learning environment's climate, the positivity and efficacy of undergirding expectations around learner success suggests an alignment with impactful learning and instructional engagement:

When considering the separate learning climate domains, the positive work-related well-being construct, work engagement, seemed to be specifically influenced by two domains in particular, namely 'educational atmosphere' and 'formal education'. A positive work atmosphere, constructive communication with faculty and structured, fitting, informative education are aspects likely to positively influence the enthusiastic, positive, fulfilling work-related state of mind (work engagement) of the residents. This could explain the finding that these learning climate domains ('educational atmosphere' and 'formal education') were found to be associated with work engagement. (Lases, Arah, Busch, Heineman, & Lombarts, 2017, 139-140)

Further, impactful learning occurs in an instructional environment when one considers the socialization and skill sets inherent within a Digital Age mentality that embraces IoT, suggested through Leach's (2018) work, resulting in the recognition that, "Four humanistic learning environment characteristics (i.e. relationships, community, respect, and consciousness) were found to foster five developmental postindustrial social skills (i.e. socioemotional development, communication, collaboration, sociability, character, and social responsibility) using inductive data analysis" (para. 1). This understanding leads into conceptual understandings around cognitive acquisition.

Cognitive Acquisition: Short-Term and Long-Term Memory

Relevant and irrelevant information is a consistent consideration within the Digital Age's availability of information, sometimes resulting in information overload. Within an instructional environment, the concept of designing a curriculum around framing information and the enhancement of the learner's ability to focus upon relevant information is heightened. Developing the subject matter knowledge base is the inherent undergirding upon which future knowledge acquisition, critical analysis and Bloom's lower-order thinking skills can proactively engage towards higher order thinking skills interactions.

As such, selective attention supports the ability of a subject matter novice learner to frame and focus upon relevant information, within a cognitively vulnerable and safe learning environment so as to teach and train the learner towards a progressive movement into an environment that consistently embeds irrelevant information, with the ability to focus and refocus upon relevant information while considering and ignoring irrelevant information. Herein lies the differentiation between novice learner and expert learner; not only in learning how to learn, but cognitively acquiring the critical analytic understandings to focus upon relevant information while analyzing and potentially ignoring irrelevant information towards embedding knowledge in short-term cognitive memory and then the progressive long-term cognitive memory and understanding. Yet, how does this actually work? Duncan, Ward and Shapiro (1994) suggest this is described as "attention dwell time", in which attention and dynamic understandings around relevant and irrelevant information is framed.

Creativity

Instructional environments have embedded a curiosity around creativity, wondering at the ability towards creativity within newly forming knowledge understandings as well as reframing information in new and different ways (Baruah & Paulus, 2019; Henriksen, Mishra & Fisser, 2016; Mullen, 2017; Paulus & Brown, 2007). As suggested by Henriksen, Mishra and Fisser (2016):

Creativity can be viewed as a process and/or a product, and is generally thought of as the production of useful solutions to problems, or novel and effective ideas (Amabile, 1996). An idea that has novelty, but lacks in value or effectiveness to other people, cannot be considered "creative" (Cropley, 2003). (p. 28)

Yet, within this understanding, the complexity of ideas is inherent within creative environments. Supporting the learner's creativity is vitally important as a concept, suggested by Henriksen, Mishra and Fisser (2016):

Creativity can be learned, but since it is a thinking skill it can only be "learned by doing" or as "learning in action." Creativity involves approaches to thinking rather than a set body of knowledge that can be taught. However, we can reinforce and support sustained creativity as a "habit of the mind." However, this also means that the education system and educators must recognize and support a sustained facilitation of creativity as a habit of the mind, and agree upon what that is and how to engage it. This can vary greatly across contexts and cultures. (Henriksen, Mishra & Fisser, 2016, p. 34)

The learner's abilities towards creativity within the instructional environment must be an internalized values-laden commodity, inherently supported within an instructional environment but more importantly the learner's implicit cognitive vulnerability towards trying new ideas and mixing different ideas in new and different ways, embraces a level of creativity beyond the bounds of unruly musings that mix relevant and irrelevant information. Such unruly musings may be considered brainstorming, perhaps critical analysis of nonconforming ideas in new and unusual ways, resulting in imagined cognitive frames of new thinking that could be labeled as creativity. Towards cognitive engagement:

Educational environments should encourage students in collaborative creative activities and other group tasks in order to allow for a development of group skills and collective intelligence. This kind of development is required for success in collective endeavors that are important in the workplace, research groups, and educational settings. Research on group creativity provides much valuable information for guiding the application of group creative activities in school settings. (Baruah & Paulus, 2019, p. 172-173)

Further, Paulus and Brown (2007) suggest that, "It appears that the brainstorming performance of groups is often hindered by various social and cognitive influences, but under the appropriate conditions, group idea exchange can be quite effective" (p. 248), suggesting the support of a supportively creative and curious instructional environment may support the learner's acquisition of equally supportive creativity and curiosity, reflective of a socializing and reflectively engaged group of learners have been modeled towards an environmental understanding that to "propose that sharing and building on each other's ideas in a group setting should produce cognitive stimulation" (Baruah & Paulus, 2019, p. 156), that may result in the enhancement of the learning environment and the embedded learners, resulting in an environment that offers a cognitive vulnerability and inherent creativity that supports new ways of understanding information.

Additionally, intellectual and experiential diversity of learners within a larger learning environment can positively thrive, resulting in a burgeoning sense of learning community creativity and efficacy, thereby embedding a developing model and sense of individualized learner self-efficacy as not only a learner but also associated with styles of cognitive motivation embedded within the subject matter under study. Baruah and Paulus (2019) have suggested that:

Although groups should benefit from intellectual or experiential diversity, thus far the literature has been mixed in terms of the support expressed for this expectation. Research shows that functional informational diversity in terms of heterogeneity in knowledge, expertise, or experiences in teams can enhance creative performance (Hülsheger, Anderson, & Salgado, 2009; Jackson, May, & Whitney, 1995). However, when multiple perspectives are at odds, high diversity may make it harder to resolve differences among perspectives (Olson, Walker, & Ruekert, 1995). Thus, it is not surprising that some researchers have found no effect of functional diversity on innovation. (e.g., Sethi, Smith, & Park, 2001) (p. 164-165)

The concept around Implicit Cognitive Vulnerability as a theory, when focused upon the learner, emphasizes the need of the learner's creativity while also supporting the motivational engagement and progression of interest by the learner. Yet, how does this occur? Theories embedded in learner motivation and subject matter knowledge acquisition, such as Nudge Theory (Thaler & Sunstein, 2009), Attentional Boost Effect (Hertwig & Grune-Yanoff, 2017) and even a Boost and Bounce Theory (Oliveres & Meeter, 2008).

Cognitive Motivational Support: Nudges, Boosts and Bounces

Motivation is an inherent and underlying requirement when learning is an expectation. Bandura (1977, 1986, 1997) work focus upon motivational aspects of learning, framing motivational engagement as well as a learner's self-efficacy associated with not only the learning process and ability but also associated with the subject matter. This is especially impactful when considering Implicit Cognitive Vulnerability, as a safe, supportive instructional environment is necessary towards cognitive focus and critical analytic abilities that embrace cognitive motivational support of the learner. Further, Holdford and Lovelace-Elmore (2001) frame Vroom's expectancy theory (1964) as an understanding of cognitive motivational support, that "intensity of work effort depends on the perception that an individual's effort will result in a desired outcome" (p. 8). Cognitive motivation and motivational support are further understood as actively engaged in a learner's ability to work with the subject matter, through Thaler and Sunstein's Nudge Theory (2009), Hertwig and Grune-Yanoff's understanding of Attentional Boost Effect (2017), as well as Oliveres and Meeter's (2008) work on the Boost and Bounce Theory. Through each of these cognitive motivational supports, one may recognize the synchronous and asynchronous, structured and unstructured ways through which to engage with the learner and support short-term working memory as well as long-term implicit cognitive understandings.

Nudge Theory

Nudge Theory (Thaler & Sunstein, 2009), also referred to as "nudge", focuses upon an understanding of positive reinforcement wherein understated and implicit promptings, evocations, and insinuations submit subtle yet guiding suggestions that guide someone towards a desired outcome, more specifically describing a nudge as, "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives" (p. 6). As suggested by Thaler, (2018), "By improving the environment in which people choose—what we call the "choice architecture"—they can make wiser choices without restricting any options" (para. 1). The motivational engagement of the Nudge Theory suggests a style of influence, motivation and non-forced acquiescence towards decision-making that is considered desirable and potentially obedient. The interesting aspect of Nudge Theory is the suggestion that this compliance is occurring without the focus of attention necessarily realizing what is occurring. As explained by Thaler (2018):

Sunstein and I stressed that the goal of a conscientious choice architect is to help people make better choices "as judged by themselves." But what about activities that are essentially nudging for evil? This "sludge" just mucks things up and makes wise decision-making and prosocial activity more difficult. Helpful nudges abound—good signage, text reminders of appointments, and thoughtfully chosen default options are all nudges. (para. 1-2)

Brinkmann (2017) suggested that nudges can support a teacher's motivation, as well as linking Attribution Theory that, "refers to the explanations people give to *why* they or others do what they do, *i.e.* a causal attribution" (p. 11) that may revise long-term motivational engagement throughout the instructional process; however, alignment of Nudge Theory and Attribution Theory may equally align and support learner's long-term motivational engagement in support towards cognitive motivation. The nuanced guidance, the subtle cognitive movement of a learner's thought process towards the more desirable outcome is behavioral in nature, cognitively motivating and encouraging a learner towards learning outcomes that frame, reframe and explicitly as well as implicitly shift cognitive engagement and informational understandings. As suggested by Burt (2019), "At face value, the idea of nudging (or 'liberal paternalism') may seem intrusive – but by persuading people towards better choices rather than mandating behaviours at work, it's possible to create lasting change in everything from wellbeing and safety to pension take-up, as well as empowering employees" (para. 6).

Yet Thaler also introduces the concept of "sludge", which is the opposite of nudge. Specifically suggested by Thaler (2018), "So, sludge can take two forms. It can discourage behavior that is in a person's best interest such as claiming a rebate or tax credit, and it can encourage self-defeating behavior such as investing in a deal that is too good to be true" (para. 6). As a final thought related to Nudge Theory, is that, "nudges are valuable because people behave in fundamentally irrational ways" (Burt, 2019, para. 8). Recognizing this fundamental irrational thought process, the learner's ability to align and re-align learning processes while ensuring cognitively motivational underpinnings persist, the ability of a learner towards maintaining a learning environment's Implicit Cognitive Vulnerability far beyond the bounds of an explicit learning environment is towards self-regulatory engagement as well as well-developed learner self-efficacy.

Attentional Boost Effect

As behavioral science has been interested in nudges, "Yet behavioral science also provides support for a distinct kind of nonfiscal and noncoercive intervention, namely, 'boosts.' The objective of boosts is to foster people's competence to make their own choices—that is, to exercise their own agency" (Hertwig & Grune-Yanoff, 2017, p. 973). From the nudges, wherein an external force is guiding the learner towards a stronger outcome or framing one's cognitive understandings around subject

matter, boosts offer a style of competency and capability that frames through a learner's cognitive motivation that is self-efficacy.

A counter-intuitive shift for most researchers in cognitive psychology and learning, is the Attentional Boost Effect, wherein the learner's ability to enhance the memory of images while focusing upon a specific subject matter that aligns with the imagery. Basically, as described by Mulligan, Smith, & Spataro (2016):

Stimuli co-occurring with targets in a detection task are better remembered than stimuli co-occurring with distractors--the attentional boost effect (ABE). The ABE is of interest because it is an exception to the usual finding that divided attention during encoding impairs memory. The effect has been demonstrated in tests of item memory but it is unclear if context memory is likewise affected. (p. 598)

As the imagery aligns with the subject matter, the cognitive engagement aligns well. Yet integral as a boost is the cognitive ability to engage in cognitive motivational engagement in short-term and long-term memory, associated with short-term alignment with very specific situations, wherein there is the ability of boosts that positively impact long-term boosts that are more permanent in nature and directly image implicit cognitive understandings and the potential towards behavioral engagement. The learner's level of competence meets cognitive memory through motivational boosts, while additional capability of the learner offers an appreciative enhanced engagement of subject matter towards a creative ability to work with information in new and different ways. An intriguing shift occurs within a boost understanding, suggested by Hertwig & Grune-Yanoff (2017):

We distinguish two kinds of boosts. Some are shortterm boosts. They foster a competence, but the improvement in performance is limited to a specific context. Others are long-term boosts. Ideally, these permanently change the cognitive and behavioral repertoire by adding a new competence or enhancing an existing one, creating a "capital stock" (Sunstein, 2016, p. 32) that can be engaged at will and across situations. (p. 977)

Cognitive motivational support embraces Attentional Boost Effect as a positive and proactive learner embrace of implicit memory that supports the learner's cognitive engagement and ability.

Boost and Bounce Theory

Such an intriguing experience is considered the "bounce". As described by Olivers and Meeter (2008), temporal attention reflects the prioritizing of pertinent or irrelevant information is an integral element to the learning process, as the concept of relevant events associated with an information gating system, a critical analysis of information and events that allows or denies information into the working memory of a learner, as a "blink" allow or a "bounce" deny. As described by Olivers and Meeter (2008):

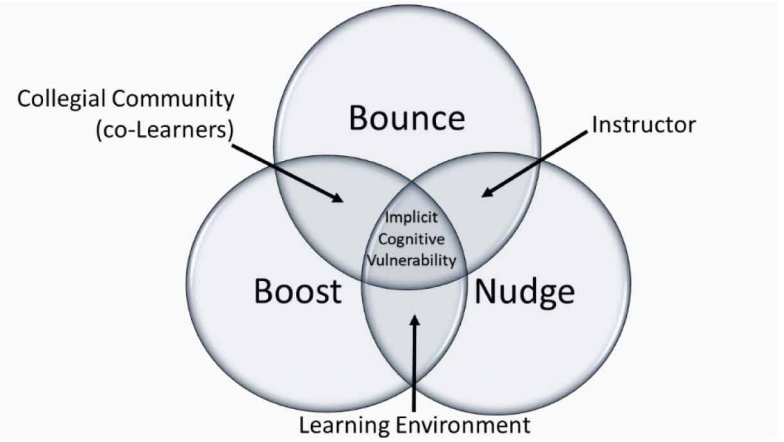
We call this theory the boost and bounce theory of temporal attention, after its two crucial but straightforward functions: Attention boosts the visual input by responding in an excitatory manner whenever relevant information (a target) is encountered. It blocks, or bounces, the visual input in an inhibitory manner whenever irrelevant information (a distractor) is encountered. The theory claims that performance is eventually determined by the interaction between these two functions and the stimulus input. It is important to note that there is no role for capacity limitations or resource depletion in explaining the attentional blink, and its apparently long time course (in the order of 500 ms) is the result of underlying microdynamics operating at a much smaller time scale. (in the order of 100 ms) (p. 840)

The concept set forth is that input is filtered by working memory, conceptually allowed through the gate or shut out by the metaphoric gating of irrelevant information for the learner's novice engagement with new subject matter. The question around to what extent a learner is able to gate keep novice subject matter is viable, s the instructional facilitator behaviorally acts as the gatekeeper within an instructional environment. As the learner's understanding of the subject matter is enhanced, the expectation that the learner's knowledge base has expanded and the conceptual framework of understanding equally expands in depth and breadth of connection. As such, the bounce aspect within the learner process shifts from an external experience controlled by an instructional facilitator, towards an internalized experience wherein the learner more thoroughly and expertly controls working memory's bounce of irrelevant information.

Implicit Cognitive Vulnerability's Framework of Impactful Nudges, Boosts and Bounces

With a developed understanding of Implicit Cognitive Vulnerability, within the instructional environment, a framework in which nudges, boosts and bounces are conceptualized is necessary and appropriate.

Figure 1. Implicit cognitive vulnerability's framework of impactful nudges, boosts and bounces



As the focus of the framework is Implicit Cognitive Vulnerability, also representing the learner, it is the central focus of the three-prong Venn Diagram. The three circles represent the Nudge Theory as represented by "Nudge", Attentional Boost Effect as represented by "Boost", as well as the Boost and Bounce Theory represented by "Bounce". The overlay of two circles is wherein designations of the Learning Environment, the Instructional Facilitator represented by "Instructor", and co-learners in the learning environment referred to as "Collegial Community (co-Learners)".

Representative of the Implicit Cognitive Vulnerability Framework, the impact of nudges, boosts and bounces are inherently on display. As a reminder, Nudge focuses upon an understanding of positive reinforcement wherein understated and implicit promptings, evocations, and insinuations submit subtle yet guiding suggestions that guide someone towards a desired outcome. Boost focuses upon an external force is guiding the learner towards a stronger outcome or framing one's cognitive understandings around subject matter, boosts offer a style of competency and capability that frames through a learner's cognitive motivation that is self-efficacy. Finally is Bounce, temporal attention reflects the prioritizing of pertinent or irrelevant information is an integral element to the learning

process, as the concept of relevant events associated with an information gating system, a critical analysis of information and events that allows or denies information into the working memory of a learner, as a "blink" allow or a "bounce" deny.

Firstly, one may represent the Learning Environment within the figure as the overlay of Nudge and Boost. The Learning Environment the external factors of the instructional facilitator and collegial community or co-learners upon the learner. This may be the positive guidance of the learning environment upon the learner, or the ability of the learning environment to self-regulate the learner as well as present appropriate subject matter knowledge and conceptual framework of understanding guidance while also offering appropriate knowledge to the learner.

Secondly, one may represent the Instructor within the figure as the overlay of Nudge and Bounce. The Instructor, also referred to as the instructional facilitator, guides and supports the learner's critical analysis of the subject matter information that is either presented within the learning environment to the learner, or framing and reframing new information for the learner that is brought into the learning environment by outside factors. The instructor supports guiding the learner's understanding of the subject matter, while guiding a critical analysis of the subject matter information as progressing the learner's subject matter understanding forward through nudging in a progressive fashion towards competency-based learning objectives while also emphasizing learner capabilities. Further, the instructor offers bounce capabilities, acting as a gatekeeper towards initially ensuring appropriate subject matter knowledge base is presented and framed for the learner, towards higher order thinking capabilities wherein the learner slowly takes upon themselves the gatekeeping process associated with critically analyzing appropriate information at higher order thinking skill expectations.

Thirdly, one may represent the Collegial Community, also referred to as co-Learners within the learning community as the overlay of Boost and Bounce. Boost within the collegial community of co-learners supports the conceptual framing of information for the learner, questioning and double-checking information as understood by the learner while also learning along with the primary learner whose implicit cognitive vulnerability is the primary focus of this discussion. Yet Bounce works in a similar manner, as the collegial community of co-learners questions, directly corrects misunderstandings, and acts as a separate gatekeeper form the facilitative instructor as the learner progressively develops a knowledge base and conceptual framework of understanding around the subject matter in focus.

CONCLUSION

Revolving around the hyperconnective style of engagement with information that has come to be known as the Information of Things (IoT), with the cognitive impact of IoT of immense and continued study, the recognition of the refining and redefining Digital Age is inherently shifting and changing the ways that people learn. Through this transformational metamorphosis in learning and informational understanding that includes the learning environments in which the learner engages, the opportunities towards reimagining and understanding learning in new and different ways can occur. The individualized needs of the learners are well represented through the Implicit Cognitive Vulnerability theory that supports the learner's needs of a safe, supportive and creative instructional environment that includes the facilitative instructor as well as the collegial community of co-learners. The motivational understandings associated with nudges, boosts and bounces represent motivational areas of emphasis including self-regulation and self-efficacy, while cognitive load concerns and short-term working memory, or explicit cognition, creates an understanding into the shift into long-term memory, also referred to as implicit cognition. The nuanced understanding of the impact upon the learner led to the Implicit Cognitive Vulnerability Framework that focuses specifically upon nudges, boosts, and bounces.

REFERENCES

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. doi:10.1037/0033-295X.84.2.191 PMID:847061

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.

Bandura, A. (1997). *Self-Efficacy: The exercise of control*. W. H. Freeman.

Brinkmann, K. (2017). How to raise teachers' motivation through "nudges" and attribution theory. *Open Journal of Social Sciences, 5*, 11-20. Retrieved from https://www.scirp.org/pdf/JSS_2017110614573975.pdf10.4236/jss.2017.511002

Burt, E. (2019, March 28). Nudge theory can help change your employees' behavior (without them even realizing). *People Management*. Retrieved from https://www.peoplemanagement.co.uk/long-reads/articles/nudge-theory-change-employees-behaviour-without-realising

Cougle, J. R., Resnick, H., & Kilpatrick, D. G. (2009). Does prior exposure to interpersonal violence increase risk of PTSD following subsequent exposure. *Behaviour Research and Therapy*, *47*(2), 1012–1017. doi:10.1016/j.brat.2009.07.014 PMID:19647229

Crawford, C. (2015). Vulnerability in learning. In J. Spector (Ed.), *The SAGE encyclopedia of educational technology* (pp. 832–835). SAGE Publications, Inc. doi:10.4135/9781483346397.n338

Crawford, C. M. (2016). Instructor immediacy and authenticity: Engaging in cognitive vulnerability within the online instructional environment. In S. D'Agustino (Ed.), *Creating teacher immediacy in online learning environments* (pp. 15–36). IGI Global. doi:10.4018/978-1-4666-9995-3.ch002

Crawford, C. M. (2018). Implicit cognitive vulnerability. In M. Khosrow-Pour (Ed.), *Encyclopedia of information science and technology* (4th ed., pp. 5149–5157). IGI Global.

Crawford, C. M. (2019). Implicit cognitive vulnerability. In M. Khosrow-Pour (Ed.), *Advanced Methodologies and Technologies in Modern Education Delivery* (pp. 729–738). IGI Global. doi:10.4018/978-1-5225-7365-4.ch057

Crawford, C. M., & Semeniuk, M. (2016). Metaphoric Representations of Cognitive Understanding via a Stairway Approach: Implicit Cognitive Vulnerability Theory through a Progressive Cognitive Taxonomical Approach. In G. Chamblee & L. Langub (Eds.), *Proceedings of Society for Information Technology & Teacher Education International Conference* (pp. 1383-1393). Savannah, GA: Association for the Advancement of Computing in Education (AACE).

Crawford, C. M., & Smith, M. S. (2015). Rethinking Bloom's Taxonomy: Implicit cognitive vulnerability as an impetus towards higher order thinking skills. In J. Zing (Ed.), *Exploring implicit cognition: Learning, memory, and social-cognitive processes* (pp. 86–103). Information Science Reference (an imprint of IGI Global). doi:10.4018/978-1-4666-6599-6.ch004

Crawford, C. M., White, S. A., & Young Wallace, J. (2019). Rethinking pedagogy, andragogy and heutagogy. *Academic Exchange Quarterly*, *23*(1), 4–10.

Hertwig, R., & Grune-Yanoff, T. (2017). Nudging and boosting: Steering or empowering good decisions. *Perspectives on Psychological Science*, *12*(6), 973–986. doi:10.1177/1745691617702496 PMID:28792862

Holdford, A. D. A., & Lovelace-Elmore, B. (2001). Applying the principles of human motivation to pharmaceutical education. *Journal of Pharmacy Teaching*, *8*(4), 1–18. doi:10.1300/J060v08n04_01

Ito, W., Erisir, A., & Morozov, A. (2015). Observation of distressed conspecific as a model of emotional trauma generates silent synapses in the prefrontal-amygdala pathway and enhances fear learning, but ketamine abolishes those effects. *Neuropsychopharmacology*, *40*(11), 2536–2545. doi:10.1038/npp.2015.100 PMID:25865929

Koltko-Rivera, M. E. (2006). Rediscovering the later version of Maslow's hierarchy of needs: Self-transcendence and opportunities for theory, research, and unification. *Review of General Psychology*, *10*(4), 302–317. doi:10.1037/1089-2680.10.4.302

Lases, S. L., Arah, O. A., Busch, O. R., Heineman, M. J., & Lombarts, M. K. (2017). Learning climate positively influences residents' work engagement and job satisfaction. *Caring for Residents*, 127-149.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370–396. doi:10.1037/h0054346

Maslow, A. H. (1954). *Motivation and Personality*. Harper.

Maslow, A. H. (1961). Are our publications and conventions suitable for the personal sciences? *The American Psychologist*, *16*(6), 318–319. doi:10.1037/h0039674

Maslow, A. H. (1962a). Lessons from the peak experiences. *Journal of Humanistic Psychology*, *2*(1), 9–18. doi:10.1177/002216786200200102

Maslow, A. H. (1962b). Notes on being-psychology. *Journal of Humanistic Psychology*, *2*(2), 47–71. doi:10.1177/002216786200200205

Maslow, A. H. (1963). Further notes on the psychology of being. *Journal of Humanistic Psychology*, *3*(1), 120–135. doi:10.1177/002216786300300112

Maslow, A. H. (1964). Further notes on the psychology of being. *Journal of Humanistic Psychology*, *4*(1), 45–58. doi:10.1177/002216786400400105

Maslow, A. H. (1969a). The farther reaches of human nature. *Journal of Transpersonal Psychology*, *1*(1), 1–9.

Maslow, A. H. (1969b). Toward a humanistic biology. *The American Psychologist*, *24*(8), 724–735. doi:10.1037/h0027859

Maslow, A. H. (1970). Religions, Values, and Peak Experiences. New York: Penguin.

Maslow, A. H. (1971). *The Farther Reaches of Human Nature*. Viking.

Maslow, A. H. (1979). *The Journals of A. H. Maslow* (R. J. Lowry, Ed., Vol. 1–2). Brooks/Cole.

Maslow, A. H. (1982). The Journals of Abraham Maslow (R. J. Lowry, Ed., & J. Freedman, Abridger). Brattleboro, VT: Lewis.

Maslow, A. H. (1987). *Motivation and Personality* (R. Frager, J. Fadiman, C. McReynolds, & R. Cox, Eds.; 3rd ed.). Addison Wesley.

Maslow, A. H. (1993a). A theory of metamotivation: The biological rooting of the value-life. In A. H. Maslow (Ed.), *The Farther Reaches of Human Nature* (pp. 289–328). Penguin/Arkana.

Maslow, A. H. (1993b). Theory Z. In A. H. Maslow (Ed.), *The Farther Reaches of Human Nature* (pp. 270–286). Penguin/Arkana.

Maslow, A. H. (1993c). Various meanings of transcendence. In A. H. Maslow (Ed.), *The Farther Reaches of Human Nature* (pp. 259–269). Penguin/Arkana.

Maslow, A. H. (1996). Critique of self-actualization theory. In E. Hoffman (Ed.), *Future visions: The Unpublished Papers of Abraham Maslow* (pp. 26–32). Sage.

Maslow, A. H. (1999a). Cognition of being in the peak-experiences. In A. H. Maslow (Ed.), *Toward a Psychology of Being* (3rd ed., pp. 81–111). Wiley.

Maslow, A. H. (1999b). Peak-experiences as acute identity experiences. In A. H. Maslow (Ed.), *Toward a Psychology of Being* (3rd ed., pp. 113–125). Wiley.

Maslow, A. H. (1999c). Some dangers of being cognition. In A. H. Maslow (Ed.), *Toward a Psychology of Being* (3rd ed., pp. 127–138). Wiley.

Mulligan, N. W., Smith, S. A., & Spataro, P. (2016, April). The attention boost effect and context memory. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 42*(4), 598-607. 10.1037/xlm0000183

Oliveres, C. N. L., & Meeter, M. (2008). A boost and bounce theory of temporal attention. *Psychological Review*, *115*(4), 836–863. doi:10.1037/a0013395 PMID:18954206

Parsons, J. E., & Goff, S. B. (1978). Achievement & motivation: Dual modalities. *Journal of Educational Psychology*, *13*(1), 93–96. doi:10.1080/00461527809529199

Resnick, H. S., Yehuda, R., Pitman, R. K., & Foy, D. W. (1995). Effect of previous trauma on acute plasma cortisol level following rape. *The American Journal of Psychiatry*, *152*(11), 1675–1677. doi:10.1176/ajp.152.11.1675 PMID:7485635

Thaler, R. H. (2018, August 3). Nudge, not sludge. *Science*, *361*(6401), 431. doi:10.1126/science.aau9241 PMID:30072515

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Vroom, V. H. (1964). *Work and motivation*. Wiley.

Vygotsky, L. S. (1933/1966). Play and its role in the mental development of the child. *Social Psychology*, *12*(6), 62–76.

Vygotsky, L. S. (1934/1987). Thinking and speech. In R.W. Rieber & A.S. Carton (Eds.), The collected works of L.S. Vygotsky, Volume 1: Problems of general psychology (pp. 39–285). New York: Plenum Press.

Vygotsky, L. S. (1935). *Mental development of children during education*. Uchpedzig.

Vygotsky, L. S. (1962). *Thought and language*. MIT Press. doi:10.1037/11193-000

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes*. Harvard University Press.

Vygotsky, L. S. (1981). The genesis of higher mental functions. In J. V. Wertsch (Ed.), *The concept of activity in Soviet psychology*. Sharpe.

Wenger-Trayner, E., Fenton-O'Creevy, M., Hutchison, S., Kubiak, C., & Wenger-Trayner, B. (2014). *Learning in Landscapes of Practice: Boundaries, Identity, and Knowledgeability in Practice-Based Learning*. Routledge. doi:10.4324/9781315777122

Wenger-Trayner, E., & Wenger-Trayner, B. (2015). *Communities of practice: A brief introduction*. Retrieved from https://wenger-trayner.com/introduction-to-communities-of-practice/

Wenger-Trayner, E., & Wenger-Trayner, B. (2020). *Learning to Make a Difference: Value Creation in Social Learning Spaces*. Cambridge University Press. doi:10.1017/9781108677431

Wittgenstein, L. (1922). *Tractus Logico-Philslophicus*. Harcourt, Brace & Company, Inc.

Caroline M. Crawford, Ed.D., is a Professor of Instructional Technology at the University of Houston-Clear Lake in Houston, Texas, United States of America. She earned her doctoral degree from the University of Houston in Houston, Texas, United States of America, in 1998, with specialization areas in Instructional Technology and Curriculum Theory, and began her tenure at the University of Houston-Clear Lake (UHCL) the same year. At this point in Dr. Crawford's professional career, her main areas of interest focus upon communities of learning and the appropriate and successful integration of technologies into the learning environment; the learning environment may be envisioned as face-to-face, blended and online (virtual or text-driven) environments, as well as microlearning deliverables.

Sharon Andrews, Ph.D., is a Professor and Chair of Software Engineering at the University of Houston-Clear Lake. Her areas of research within the domain of software engineering include software architecture, architecture description languages, architecture erosion and drift, domain and knowledge engineering, reusable architectures, innovation and creativity in engineering, and safety critical software process design. She holds a Ph.D. in Computer Science.

Jennifer K. Young Wallace, Ph.D., is an assistant professor at Jackson State University in Jackson, Mississippi. Her area of research is primarily educational leadership, with a significant background in the K-12 environment as well as expertise in teacher education as well as educational leadership. Further, she had been a successful Coordinator of CAEP/Assessments.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

A Brief Study on Smart Medicine Dispensers

Dayananda P., JSS Academy of Technical Education, Bangalore, India
Amrutha G. Upadhya, JSS Academy of Technical Education, Bangalore, India
Nayana B. G., JSS Academy of Technical Education, Bangalore, India
Priyam Poddar, JSS Academy of Technical Education, Bangalore, India
Vandana Rao Emaneni, JSS Academy of Technical Education, Bangalore, India*

ABSTRACT

The article's purpose is to throw light on the presentation of an enhanced idea of the usage of a growing technology of internet of things. The proposed system SPEC 2.0 (smart pill expert system) is used to automate the capability of dispensing the right dosage of medicine pills at the given interval. The proposed system has been designed to be used at your home, your workplace, at hospitals by a user in any age group and then possibly expanding the functionalities to the visually impaired. The system focuses on providing access control and monitoring management through a mobile app with no monthly subscriptions to the service being offered. The user has been given control of the system through the application to help set the time interval for dispensing the medication. There will also be alerts and notifications that are sent if the pills haven't been removed from the final container box. The system is tested, and the results are determined by growing the modules for dispensing the pills at certain predefined time intervals.

KEYWORDS

Expert System, Health, Healthcare IoT, IoT Motorization Service, Medication Monitoring, Medicine Dispenser Application, Smart Medication, Smart Medicine Dispenser

INTRODUCTION

Advancements made in the field of smart healthcare technologies have provided people a better life situation in the present years. This would have been even more notable if the percentage of medication errors could be identified and corrected. Due to this negligence, there has been quite a lot of deaths and quite an enormous increase in the expenditures by millions each passing year. In the present-day scenario, since medical devices are incorporated on a network, due to its security issues, interoperability breaches are increasing in number day by day, resulting in enormous business losses. To curb this very risk, automation and consumer-based technologies are being adopted for the medical devices. Health care is at the heart of IOT, with applications varying from health monitorization to disease prognosis. These applications provide the visualisation of identification, diagnostic study, treatment procedures

DOI: 10.4018/IJHIoT.294893
*Corresponding Author

and regular monitoring through the devices that are implanted in IOT. The main achievements are to reduce the cost and easy usage for its users by providing better user experience and easy operational customisation. For seamless connectivity and better performance, a systematic scheduling scheme plays a very important role due to the availability of limited resources. In the healthcare domain, smart devices like a gateway, a server and a database help in creation of data to be sent as medical services to the authorized organisations. In the upcoming years, IOT will play a huge role to address the above issues in the healthcare domain. Through IOT, various countries across the world, have adopted this new turnover in the field of medical health care, by designing and developing new frameworks and applications integrating services and security. The objective is to construct a device that is relatively small and light weight, that is developed as a software in such a way that patients receive their medication reliably and safely as prescribed by their physician. The device also provides alert messages which helps to take medicines in time as well as refilling the medications.

BACKGROUND

(Reddy & Chavan, 2020) (Casciaro et al., 2020) The system SPES provides expertise on the real-time analysis and support to every user relying on medication. Since Medicinal Nonadherence (MNA) is one of the huge factors for extended betterment, money issues, and sudden demises, SPES tries to curb these inconveniences by supporting several users, the option for controlling and monitoring their actions, simultaneously, in order to curb any misleading events. The SPES provides an easy UI and a trouble-free way of maintaining the physical dispenser system with an AI-Chat service that caters to the needs of the user's queries. (Al-haider et al., 2020) The medicine planner provides functionalities to pre-sort a prescription on a daily basis. This is especially catered to the needs of elderly and visually impaired personal to have a better management of their meds. The planner has 2 distinct functionalities of providing a self-filling mechanism and an alert notification mechanism during the time of medicine intake. (Rao et al., 2020) The kit proposed can be programmed to provide a proposition to guide users to consume their correct medicine at the exact specified time interval through the employment of an alert functionality, buzzers and LED. This is a small grant to improve life existence for a better healthy future for the world. (Mahmud et al., 2020) This IOT based intelligent medicine container houses several sensors and servers for frequent health monitoring check-ups. This allows wireless communication between the user and their caregivers with regard to their monthly health check-ups and removes the burden of a physical meeting session. Since the main goal is to focus on the correct medication schedules, aged generations will be benefited the most as they require constant taking care off. The servers are used for embedding the time schedule along with the medication details. There is also an embedded temperature sensor for examining of the user's body temperature. (Sangvanloy & Sookhanaphibarn, 2020) An automatic pet feeder has been constructed for allocation of the dry pet food for dogs and cats, with customization based on each pet owner. This provides an effective manner of taking care of the food patterns comfortably. (Moise et al., 2020) The design facilitates easy monitoring and controlling functionalities via mobile app with no cost plans. The system is controlled by the user through his phone or through the buttons present on the machine itself for choosing his required number of medications for a given time interval. There are alert messages sent to provide an indication for whether the medication was removed from the container or not. (Nijiya et al., 2018) The system has been built around prescription drugs which will assist in authenticating a patient's access of such medication based on their identity and prescribed schedule, and also simplifies the pharmacist or doctor to monitor this consumption. The system consists of intelligent reminders, care taker reminders, and dosage tracking and also notifies each time the container box is opened to provide a security feature that avoids stealing of medicines. Prescription drugs are sometimes consumed without any intent initiated by a doctor and sometimes the users may be forgetful to consume their medication, causing irregular consumption periods. To help curb these events, the system helps patients take their medication on time with value added

safety measures, facilitating for a speedy recovery. (Jadhav et al., 2020) The product improves the automation of functional modules through the usage of an existing mobile app "Blynk" to have a definite control over the feeder. Through the networks, the amount of feed will be controlled along with its duration of dispensing. This functionality is implemented by clicking the button provided on the app, that will in turn control the opening and closing of the hole in the dispenser cap. (Mugisha et al., 2020) A pill dispenser with alarm which is provided with a facility of notifying on the smart phones to help patients take right medicine at appropriate time that have been prescribed with several medicines. The existing systems have existing alarm modules present for indication of medication time. This could be a drawback for elderly patients to hear the alarm if the pill dispenser is placed at a lengthy distance from them or due to hearing loss concerned with age factor. There is not any dispenser system that provides in-built mobile alerts to remind the patients about medication thus far. Hence, the system is built using the Instapush application for the pop-up notifications and combination of infrared sensors and microcontroller to control the medication dosage and time period for consumption. (Bombarda et al., 2019) A different approach of abstract state machines have been introduced to develop this system. The development phase is very critical as even if one component fails, then it possesses great life-threatening injuries to the users who are diligently making use of the service. To prevent this situation, a precise procedure has been adopted to measure the probabilities of defeats. With this statistics, validation and verification modules are conducted in a well-documented incremental procedure. In addition, regulation (IEC62304) and guidelines are presented and by phase wise enhancement a fine model is attained which can be interpreted to code.

MAIN FOCUS OF THE ARTICLE

Comparative Analysis Study

There are currently three technology-based pill dispensers that are available in the market. Based on each of its salient features and limitations, an overall conclusion of the technology has been derived. We also look into the already existing marketed pill dispensers to get a broader view into its offered features. Table 1 summaries the various distinct features offered by the systems.

Merits and Demerits

Through the proposed systems, there is a usage of a crisp design to reduce the number of hardware components. There is an option of customizable and flexible medication routine provided through a mobile application. Assurance of security is a key distinction. The event of overdosage is well taken care of by ensuring proper disposal protocols. Alarm and sound notifications are deployed for indication of dispensing and overdosage events. The main scope is to provide an easy-to-use UI design. For the indicator events, message alerts are sent through SMS services. The systems offer a single user interface for a given environment usage. There is always a limitation to the medications supplied to the system for dispensing. Only solid medications are deployed. There is no guarantee to prevent non-adherence as it's up to the user's end to consume the medication at the end of the day. There is no power supply back-up provided for running efficiently. The article proposes a new approach to overcome problems such as non-expandability, inconvenience, low reliability and communication inefficiency.

Applications

The pill dispensers find its application in various domains, especially in the medicine and healthcare stream. Several hospitals across the world have adopted these systems to ease the work pressure on nurses for providing the correct dosage of medications to each and every patient at the right duration of time. These systems are also deployed in nursing homes to keep track of each person's medications. This also provides a sense of independence to the elderly not to worry about their health going

Table 1. Technology-based comparative analysis

Sl. No	Technology-based Comparison	Salient Features	Limitations	Overall Conclusion of Technology
1	Sensor-based Systems			
	Smart Medicine Dispenser with Alarm via Smart Phone Notification. (Othman & Ek, 2016)	• Alarm notifications to indicate the right medication. • Alerts and communications sent via a mobile application.	• No security arrangements have been considered. • Single user system interface. • No support services have been provided.	• Detection of opening and closing of medicine compartments • Portability • Antibacterial • Mobile App • Battery power • Accuracy of detection of medication is very low.
	Autonomous Pill Dispenser: Mechanizing the Delivery of Tablet Medication. (Chawla, 2016)	• Dispensing pills on schedule basis. • Control via middleware	• Security protocols haven't been considered. • Single user. • Flip mechanism for dispensing medication via the users. • No support services have been provided.	
	Smart Medication Box for Reminder and Monitoring Purposes (Minaam & Abd-ELfattah, 2018)	• Notifications and reminders sent through middleware. • Improved medicine fidelity.	• Security events haven't been taken into consideration. • No support middle wares have been deployed.	
	Electronic Smart Box for Continuous Monitoring (Hayes et al., 2006)	• Determination of whether a wrong compartment was accessed. • Prompts user if the medication has been missed.	• No 'hands-on' service. • Not cost efficient • Single user system interface. • Limited security for user authentication.	
2	Accessibility-based Systems			
	RFID-based Smart Medicine Drawer (Becker et al., 2009)	• Detection of opening and closing of medicine compartment door. • Tracking of medicines via RFID tags on "bottles".	• Based on assumption made - 'If a bottle is removed, a pill has been taken'. • Limited security with respect to the RFID tags placed on containers.	• Detection of absence or presence of medication via an antenna. • Non-invasive • Requires combination with sensors and devices for verification purpose. • Based on several assumptions with respect to self-sorted medications.
	RFID-based Medication Adherence Intelligence System (McCall et al., 2010)			
3	Vision-based Systems			
	Computer vision system for monitoring intake of medication (Batz et al., 2005)	• Detection of absence or presence of medication with the help of a camera. • Antibacterial	• Combination of sensors and devices required for security verification functionality.	• Camera resolution must be good enough to recognise the movements. • Camera placement is assumed to be monitoring the medication area. • Camera detects and observes normal and abnormal medication activities through gestures made by the hand.
	Video surveillance of medication intake (Valin et al., 2006)			
4	Existing Systems			
	Philips' Pill Dispenser (Philips & Dibner, 2004)	• Flexible dispensing • Alert notifications • Safety features • Rechargeable battery	• Not the best affordable option. • Range of home safe devices isn't quite scalable.	• Fall detection available. • Monthly payment on per-use basis. • Device design is neat, compact and an improved update from the previous designs. • Customization of the ideal service plan. • Mobile app tie-up to coordinate easy communication between a user and his caregiver. • Waterproof design. • Better and efficient battery life. • Customer Care services. • Free shipping.
	Hero's Pill Dispenser (Diaz & Vepuri, 2012)	• Pill dispenser • Mobile Application • Notification via sounds and sights • Automated Fidelity Tracking	• Applicable for pills that are solid and are not halved or quartered. • No power backup. • Initial set-up required.	• Flexible by providing scheduling for up to 10 different medications on a daily dosage basis. • 90 days predefined interval for medicine dispensing. • Independent of dosage size and shape. • Audible and visible alarm alerts for missed dosages. • Security through notification. • Quite affordable. • Never runs out. • Free shipping. • Pay per plan.

haywire. The most common environment with maximum usage is found in one's home where people belonging to a certain different age group can set up the device to cater to the group's requirements for accurate dispensing of the right prescribed dosage at the specified time interval. Nowadays, through collaborations with Cloud services and integrated end services, the whole process has been automated to provide hassle free and tension free working. They can be further deployed to expand its horizon of benefits and usage to huge organisation with integration of people's information for a seamless network connectivity usage. In the future, there would be the concept of "contactless" appointments and meetings where in a doctor would prescribe the medications on the fly through an application which would then automatically fill up the required medication for dispensing for a given a patient. Through these dispensers, life is made easy and convenient.

CONCLUSION

Non-Adherence to medication is a grave issue with increasing growth in numbers of affected people with chronic diseases. To enhance this adherence, we have proposed the SPEC 2.0 to enhance the already existing problems like non-expand-ability, inconvenience, low reliability and lack of communication. The system comprises of sensors and micro-controllers with the help of which data is analysed by the machine and it eventually dispenses medication based on the user's customization. The proposed system provides several advantages like scalability, remote manageability, reduced cost management and effort, facilitating the update of the medication schedule configured in the smart dispenser. The smart pill expert system can be used to as a solution to improve medication adherence by prevention of under and over dosing. However, it fully cannot prevent non-adherence events occurring voluntarily like pretending to consume the medication or discarding them after dispensing. It can find its usage in every household or hospital that has a medical supervision and can be marketed as an efficient solution. The main achievement is to facilitate a healthy, tension free life to those who are taking pills regularly and to provide this solution at an affordable cost.

REFERENCES

Al-haider, A. J., Al-sharshani, S. M., Al-sheraim, H. S., Subramanian, N., Al-maadeed, S., & Chaari, M. Z. (2020). Smart medicine planner for visually impaired people. In *Proceedings of International Conference on Informatics, IoT, and Enabling Technologies (ICIoT '20).* IEEE.

Batz, D., Batz, M., Da Vitoria Lobo, N., & Shah, M. (2005). A computer vision system for monitoring medication intake. In *Proceedings of the Second Canadian Conference on Computer and Robot Vision* (pp. 362–369). IEEE.

Becker, E., Metsis, V., Arora, R., Vinjumur, J., Xu, Y., & Makedon, F. (2009). SmartDrawer: RFID-based Smart Medicine Drawer for Assistive Environments. In *Proceedings of the Second International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '09)*. Association for Computing Machinery.

Bombarda, A., Bonfanti, S., & Gargantini, A. (2019). Developing medical devices from abstract state machines to embedded systems: a smart pill box case study. In *Proceedings of International Conference on Objects, Components, Models and Patterns*. Springer.

Casciaro, S., Massa, L., Sergi, I., & Patrono, L. (2020). A smart pill dispenser to support elderly people in medication adherence. In *Proceedings of the Fifth International Conference on Smart and Sustainable Technologies (SpliTech '20)*. IEEE.

Chawla, S. (2016). The autonomous pill dispenser: Mechanizing the delivery of tablet medication. In *Proceedings of the Seventh Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON '16)*. IEEE.

Diaz, A., & Vepuri, K. (2012). *Hero automatic pill dispenser*. https://herohealth.com/our-product

Hayes, T. L., Hunt, J. M., Adami, A., & Kaye, J. A. (2006). An Electronic Pillbox for Continuous Monitoring of Medication Adherence. In *Proceedings of the International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE.

Jadhav, K., Vaidya, G., Mali, A., Bankar, V., Mhetre, M., & Gaikwad, J. (2020). IOT based automated fish feeder. In *Proceedings of the International Conference on Industry 4.0 Technology (I4Tech '20)*. IEEE.

Mahmud, O. A., Khan, M. K., Roy, R., & Alamgir, F. M. (2020). Internet of things (IOT) based smart healthcare medical box for elderly people. In *Proceedings of the International Conference for Emerging Technology (INCET '20)*. IEEE.

McCall, C., Maynes, B., Zou, C. C., & Zhang, N. J. (2010). RMAIS: RFID-based medication Adherence Intelligence System. In *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology*. IEEE.

Minaam, D. S. A., & Abd-ELfattah, M. (2018). Smart drugs: Improving healthcare using Smart Pill Box for Medicine Reminder and Monitoring System. *Journal of Future Computing and Informatics*, *2*, 443–456.

Moise, M. V., Svasta, P. M., & Mazăre, A. G. (2020). Programmable IoT pills dispenser. In *Proceedings of the Forty Third International Spring Seminar on Electronics Technology (ISSE '20)*. IEEE.

Mugisha, G. A., Muhumuza, C., Uzoka, F. M., Nwafor-Okoli, C., Nabunje, J., Arindagye, M., & Bukenya, J. N. (2020). Usability evaluation of low-cost smart pill dispenser by health care practitioners. In *Proceedings of the Future Technologies Conference (FTC '20)*. Springer.

Nijiya, P. K., Najeeb, J., Rimna, A., Safa, K. P., Silvana, M., & Adarsh, T. K. (2018). Pill care - the smart pill box with remind, authenticate and confirmation function. In *Proceedings of the International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR '18)*. IEEE.

Othman, N. B., & Ek, O. P. (2016). Pill dispenser with alarm via smart phone notification. In *Proceedings of the Fifth Global Conference on Consumer Electronics*. IEEE.

Philips, R., & Dibner, A. (2004). *Automated medication dispensing device*. https://www.lifeline.philips.com/business/medicationdispensing

Rao, A., & B. S., , PShivani, , AMohan, , R. (2020). IoT-based smart medicine kit. In *Proceedings of International Conference on Electronics, Computing and Communication Technologies (CONECCT '20)*. IEEE.

Reddy, J. E. P., & Chavan, A. (2020). AI-IOT based smart pill expert system. In *Proceedings of the fourth International Conference on Trends in Electronics and Informatics (ICOEI '20)*. IEEE.

Sangvanloy, T., & Sookhanaphibarn, K. (2020). Automatic pet food dispenser by using internet of things (IoT). In *Proceedings of the Second Global Conference on Life Sciences and Technologies (Life Tech '20)*. IEEE.

Valin, M., Meunier, J., St-Arnaud, A., & Rousseau, J. (2006). Video surveillance of medication intake. In *Proceedings of the Twenty Eighth Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS'06)*. IEEE.

Dayananda Pruthviraja is currently working as Professor & HOD in the Department of ISE at JSSATE. He has Obtained Ph.D. degree from VTU and M.Tech degree from RVCE. His focus area is Image processing & Information Retrieval. He was with MSRIT, Bengaluru, India in Department of ISE as an Assistant Professor. He has published international journals and conference papers in the field of Image processing & Information retrieval.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Adaptive IoT Technology for Measuring Salinity, Dissolved Oxygen, and pH in Aquatic Environments

Jarrod Trevathan, Griffith University, Australia*
https://orcid.org/0000-0002-7328-8741

Dzung Nguyen, Griffith University, Australia

ABSTRACT

This paper presents an extension to an IoT platform for remote near real-time aquatic environmental monitoring that incorporates electrical conductivity (i.e., salinity), dissolved oxygen, and potential of hydrogen (pH) sensors. The predecessor to this system could be remotely deployed for extended periods of time but was limited to measuring temperature, lux (light), and turbidity only. This paper outlines how the platform was expanded upon to include the additional environmental parameters (i.e., salinity, dissolved oxygen, and pH) by selecting the appropriate compatible sensor technologies, redesigning the electronic componentry/physical buoy, and undertaking thorough system integration testing. The authors present the hardware and software challenges faced to adapt the platform to the new sensor parameters, illustrate the latest buoy design, describe the calibration process, and demonstrate in-house and commercial field-testing. The system can be deployed for 12 months between maintenance cycles and has been used in environmental research and commercial prawn farm water quality monitoring.

KEYWORDS

Calibration, Dissolved Oxygen, Electrical Conductivity (Salinity), Internet of Things (IoT), pH, Remote Monitoring, Sensors

1. INTRODUCTION

Delicately balancing the needs of natural aquatic ecosystems is difficult with pressures from encroaching urbanisation and population growth (McGrane (2016)). Aquatic environmental monitoring programs are an essential strategy in providing timely and accurate information to decision makers to aid in planning and management (Danielsen et al. (2010), Laut et al. (2013)). There are two main approaches to aquatic environmental monitoring: 1) Manual human-based field sampling; or 2) Remote monitoring using *Internet of Things* (IoT) technologies.

Traditionally, water quality parameters are physically measured via field instruments and water samples gathered for laboratory analysis (Abowei (2010)). However, this process is costly,

DOI: 10.4018/IJHIoT.294894
*Corresponding Author

time consuming, hazardous and can present multiple sources of error. Water samples typically require prompt analysis to guarantee accurate results as quality deteriorates over time (i.e., changes occur in the sample container's mini ecosystem, which no longer reflect the system the sample was extracted from). Field-testing equipment is often expensive to maintain/handle due the harsh conditions they are exposed to in various environments. Retrieving samples at night can be difficult without adequate lighting (and disturbing the natural peace). Areas with rough terrain and concealed shrubbery may restrict movement and could be inhabited by dangerous/venomous animals. Field technicians must be highly skilled and aware of the health risks involved with undertaking regular field work.

An alternative approach is to use IoT technologies to undertake remote monitoring (Gholizadeh, Melesse and Reddi (2016), Glasgow et al. (2004), Lee et al. (2018)). Networked sensors (or *wireless sensor networks* (Madakam et al. (2015))) are deployed in the environment and provide remote telemetry at periodic intervals on water quality/condition. This approach acts as an early warning/indicator of common issues affecting water quality, rather than just a measurement tool. Water management agencies can proactively prepare for and react to potential disasters, thereby mitigating environmental damage and/or loss of life and property. There exist numerous commercial systems for undertaking remote aquatic environmental monitoring (Fondriest (2021), Hach (2021), Analytical Solutions (2021)), but these tend to be expensive and technologically restrictive (i.e., proprietary). Some proposals from the scientific literature include (Hongpin et al. (2015), Simbeye and Yang (2014), Li et al. (2013), Sung, Chen and Wang (2014), Ragai et al. (2017)), but these systems are now either defunct, do not capture sufficient quality data across a broad range of environmental parameters, do not scale commercially (i.e., are for experimental research purposes only), or are also cost-prohibitive.

Trevathan et al. (2021) presented a remote aquatic near real-time monitoring IoT platform that can be deployed for up to 12 months between maintenance cycles. However, the platform was restricted to measuring underwater temperature, lux (light) and turbidity (Trevathan, Read and Schmidtke (2020), Trevathan et al. (2020)). While this platform is robust, the limited types of sensor parameters (i.e., temperature, lux and turbidity) are insufficient for undertaking holistic environmental assessments. Factors such as salt content, oxygenation and water acidity are often critical factors that influence fish and plant species survivability (Bartram and Ballance (1996)).

This paper outlines how this existing IoT platform was upgraded to incorporate additional sensors for measuring electrical conductivity (salinity), dissolved oxygen and potential of hydrogen (pH). This required selecting the appropriate compatible sensor technologies, redesigning the electronic componentry and physical buoy body, and undertaking thorough system integration testing. We discuss the hardware and software challenges faced to select and adapt the system to the new sensor parameters. The enhanced design is presented along with how the sensors were scientifically calibrated and tuned with lessons learned from in-house and commercial field-testing of the system. The platform is robust and can be deployed for 12 months between maintenance cycles (i.e., sensor servicing and recalibration) provided that a periodic cleaning schedule is adhered to. The result is a commercial research-grade remote IoT aquatic environmental monitoring platform that is as accurate and comparable to similar systems on the market (i.e., within 1% error margin of other commercial equipment), but substantially more affordable given its approach to development and manufacture (Trevathan and Sharp (2020)).

This paper is organised as follows: Section 2 presents the problem motivation and related work. Section 3 outlines the design methodology, shows how the system hardware and software was adapted to include additional sensor parameters (i.e., electrical conductivity, dissolved oxygen and pH) and describes the calibration process. Section 4 provides a performance evaluation of the system in terms of its ability to collect data on the additional sensor parameters using in-house and commercial field trials; and Section 5 provides concluding remarks and avenues for future work.

2. PROBLEM MOTIVATION AND RELATED WORK

2.1 Problem Motivation

Trevathan et al. (2012) and Trevathan and Johnstone (2018) presented a vision for an affordable aquatic environmental monitoring platform that operates in near real-time (i.e., 15-minute intervals). The data sampled is compiled into a http post and sent over a 3G mobile network to a cloud-based server where the data is processed and presented (via a ThingsBoard[1] IoT dashboard). Multiple iterative prototypes of the system are illustrated that support various aquatic environmental studies (Hanington and Johnstone (2016)) and education initiatives[2] (Trevathan and Johnstone (2018)).

Trevathan et al. (2021) outline an advanced version of this platform (referred to as the *General-Purpose Sensor Board* (GPSB)) that measures:

1. Above and underwater lux/illuminance (lx);
2. Underwater temperature (°C); and
3. Turbidity (NTU).

The platform also measures internal system status parameters for diagnostic purposes: 1) Internal humidity and temperature; 2) Battery voltage (volts); 3) Solar charge (volts); 4) Operational status – uptime (seconds); 4) Transmit status – post attempts (count); and 5) Signal strength (-dB).

The system is a successful proof-of-concept and has been deployed in multiple aquatic environmental settings to gather preliminary data on its operating potential. Units have functioned for up to 12 months in the field (via solar charging) and can sustain operations for 2 months in the absence of sufficient solar charging. The buoy contains recycled 18650 Li-ion battery cells and other e-waste componentry (see Trevathan and Sharp (2020)). However, the platform does not fully capture all of the required water quality parameters desirable for a holistic assessment (i.e., it is missing the highly sought-after parameters of electrical conductivity, dissolved oxygen and pH).

Table 1 illustrates how water quality is categorised into parameters under three attributes: 1) Physical; 2) Chemical; and 3) Biological. Water temperature has a significant influence on many other chemical parameters measured and consequently the habitability of aquatic life. Plant and fish species have a desirable temperature, salinity (electrical conductivity), dissolved oxygen concentration and acidity (pH) level they thrive in.

Electrical Conductivity is a measure of the water's ability to pass an electrical flow through the medium and is related to the concentration of ions in the water from dissolved salts and other chemical compounds (Jones (2002)). Electrical conductivity is typically measured in micro siemens per centimetre (μS/cm) for freshwater bodies. An increase in temperature, results in an increase in electrical conductivity. Salinity is a measure of total dissolved salts in the water. Different aquatic species can tolerate different levels of salinity. Changes in electrical conductivity generally occur from introducing other volumes of water with differing concentrations (e.g., rainwater or floodwater) or a reduction in water volume through evaporation.

Dissolved Oxygen indicates the concentration of free O2 molecules in water (measured in milligrams per litre (mg/L) or saturation (1-100%)) (Rose and Long (1988)). Some species can survive

Table 1. Common factors that influence water quality

Physical	Chemical	Biological
Temperature (°C)	Electrical Conductivity (μS/cm)	E. Coli
Turbidity (NTU)	Dissolved Oxygen (mg/L)	Bacteria/Viral Concentration
Total Dissolved Solids (ppm)	Potential of Hydrogen (pH)	Algae Growth

in low dissolved oxygen concentrations (1-6 mg/L), whereas others require high concentrations (up to 15 mg/L). Dissolved oxygen concentration is typically higher at the water surface due to air diffusion and/or photosynthesis through plants. 100% saturation does not equate to the same quantity in mg/L as the concentration can vary by water temperature, air pressure and conductivity. Oxygen solubility decreases with increases in temperature (concentration decreases with temperature increase), is lower at higher air pressures above sea level (above 1 atm), and exponentially decreases as salt concentrations increase (increased conductivity reduces dissolved oxygen concentration). Dissolved oxygen varies over day/night cycles and throughout the year due consumption/generation of oxygen from plants and other organisms. Photosynthesis from plants can over-saturate the water (> 100% saturation). Low dissolved oxygen concentrations or oxygen depletion can stress fish species and eventually cause a 'fish kill' event in water bodies where oxygen is consumed more quickly than it can generate (via photosynthesis or diffused air).

Potential/Power of Hydrogen (pH) measures how acidic/basic the water body is (i.e., the concentration of hydrogen ions (H+) in the water) (Dickson 1993). pH scales from 0 to 14 on a base-10 logarithmic scale, where 7 is completely neutral and is a standard for pure water. Below 7 equates to more H+ ions and higher than 7 equates to more hydroxyl ions (OH-) in the water body. pH can be used to determine alkalinity (measured as mg/L) when the solution is 100% air saturated. Different aquatic organisms require specific regions of pH to sustain life. pH fluctuates over the day/night cycle due to carbon dioxide (CO2) absorption in water, by reacting with water creating carbonic acid (H2CO3). The degree of change is dependent on the water's alkalinity and is more noticeable in bodies with larger rates of organic respiration and decomposition (introducing CO2 into water other than surface diffusion).

With these definitions in mind, this paper's purpose is to highlight how the remote IoT aquatic environmental monitoring platform outlined in Trevathan et al. (2021) was expanded to include the additional water quality sensor parameters of electrical conductivity, dissolved oxygen and pH (in addition to the existing temperature, lux and turbidity sensors).

2.2 Related Work

There is limited work pertaining to remote platforms capable of measuring multiple water quality parameters. In this section we briefly outline the supporting related work in the area.

Gholizadeh, Melesse and Reddi (2016) investigates commonly used approaches and sensors employed in evaluating and quantifying water quality. The parameters include: chlorophyll-a, colored dissolved organic matters, Secchi disk depth, turbidity, total suspended sediments, water temperature, total phosphorus, sea surface salinity, dissolved oxygen, biochemical oxygen demand and chemical oxygen demand.

In a similar vein, Glasgow et al. (2004) present developments in real-time remote monitoring for hydrologic properties. Specifically, they investigate methods for the rapid detection of, and responses to, environmental threats imposed by increased nutrient loadings, development of hypoxic and anoxic areas, toxicants, and harmful algal bloom outbreaks leading to fish kill events and potential human health impacts.

Stupar et al. (2012) describe a remote water salinity measurement system based on a low-cost intensity-based side-polished fibre-optic U-shaped sensor. The salinity sensor is made of a multimode plastic optical fibre, and the sensor determines the salinity by measuring the refractive index. Measurement resolution and uncertainty of proposed salinity sensor are 0.001 and 0.002, respectively. The system uses ZigBee for remote telemetry and LabVIEW software for visualisation and analysis of the data. This system is limited to measuring salinity only.

Li et al. (2013) discuss an aquaculture remote monitoring system based on the Android platform. The system observes temperature, water level, dissolved oxygen and pH. Measurements are stored in an SQLite database. However, this system does not address electrical conductivity.

Simbeye and Yang (2014) present a real-time wireless sensor network monitoring and control system for aquaculture. The system measures temperature, dissolved oxygen content, pH and water level. Water quality parameters and transmitted to a base station host computer using Zigbee. The host computer provides data analysis, processing and presentation using LabVIEW. They present an experimental evaluation of network quality metrics, battery performance and data aggregation.

Sung, Chen and Wang (2014) describe an automated real-time aquaculture monitoring system that measures dissolved oxygen and temperature only. The data is captured and displayed via ZigBee wireless transmission signal transmitter to remote computer terminals. Visual Basic 2010 software is used to design the interface functions and control-sensing module. The authors claim that the system is low-cost, low-power, and easy-to-operate with wireless transmission capability. The system uses a combination of mains electricity and solar power.

Hongpin et al. (2015) propose a solar powered real-time aquaculture water quality platform. The system uses a Pt1000 temperature sensor, a YCS-2000 dissolved oxygen sensor, pH electrode and ammonia nitrogen sensor. A STM32F103 chip handles data processing. Zigbee and GPRS modules are used for data transmission. The system was connected with aerator to influence dissolved oxygen concentration. This system does not address electrical conductivity.

Lee et al. (2015) investigate how information from disparate sensor networks can be brought together for integration, analysis and visualisation. The system is based on Sensor Web Enablement standards and uses remote water quality monitoring case studies involving various sensor parameters including temperature, salinity, photosynthetic active radiation and water pressure.

Ragai et al. (2017) present a proof-of-concept for remote monitoring and control of fish farms using a wireless sensor network. The system allows continuous monitoring of temperature, dissolved oxygen and pH. The system sends alerts to fish farm administrators allowing them to take appropriate measures based on the water condition in the fish tanks. The system aims to reduce accidental fish mortality.

Quintero-Polanco, Betancourt and Molina-Mosquera (2018) presents a prototype for monitoring, recording and control of temperature, dissolved oxygen and pH in a tilapia fish farming. The system has a DS18B20 temperature sensor, an Atlas Scientific™ dissolved oxygen probe and a SEN0161 pH sensor. A Raspberry Pi manages the system, and a web-based graphical interface was developed.

Scarpa (2020) proposed pH monitoring for sweat levels in wearable computing applications has been proposed. Wang et al. (2020) have undertaken similar work for embedding pH sensors in clothing fibres to monitor electrochemical changes in the wearer's skin.

Thorsland and van Vliet (2020) have collected 40 years of global salinity measurements from surface water and groundwater. The dataset has been gathered through a combination of traditional and electronic means – which highlights the need for ongoing remote data collection approaches.

The IoT approach for measuring water quality has been the impetus for numerous recent work. Huan et al. (2020) have developed a water quality monitoring system for aquaculture ponds. Manimegalai (2020) explores cloud-based approaches for assessing remote water quality data. Pasika and Gandla (2020) propose a low-cost IoT system for smart water quality monitoring. Kanagaraj et al (2020) depict a method for measuring temperature and turbidity via IoT. Ighalo, Adeniyi and Marques (2021) provide a review of some of the latest proposes for IoT water quality monitoring.

3. METHODOLOGY

Trevathan et al. (2021) outlines the technical specifications for three iterations of buoy design for remote aquatic environmental monitoring (and associated field deployments) culminating in the GPSB. In this section we show how the GPSB was enhanced to incorporate electrical conductivity, dissolved oxygen and pH measurements. This required the consideration of new hardware (sensors), updated software, modification to the physical buoy design, and sensor calibration.

3.1 Hardware Overview

Figure 1 provides an overview of the hardware architecture for the remote aquatic environmental monitoring system. At the core of the system are the following components:

- Arduino Mega 2560[3] (microcontroller);
- TinySine™ 3G/GPRS/GSM Shield[4] (for remote telemetry);
- Internal temperature and humidity sensor (DHT22);
- Temperature (Adafruit™ MCP9808[5]), light (Adafruit™ TSL2561/91[6]) and turbidity sensors;
- 2W-6V solar panels;
- RGB status LED (on enclosure lid);
- Power management and solar charging circuitry; and
- Duty cycling/timing circuitry.

Figure 2 presents the technical schematic for an Arduino Mega 2560. (Note that all schematics and board layouts were designed using Autodesk Eagle version 8.6.) The Arduino Mega 2560 operates at 5 volts and interfaces with numerous generic sensors. The Arduino has 8K of SRAM and 4K of EEPROM. The Mega 2560 has 54 digital pins, 16 analog pins, 4 UARTs and a 16 MHz crystal oscillator. Arduino was chosen for its simplicity, versatility, low-power consumption and compatibility with other systems.

Figure 3 illustrates a TinySine 3G GPRS/GSM shield. The TinySine is based on the popular Adafruit™ Fona GSM shield[7] and supports a SIM5320 module. There are two versions of the TinySine – European (900/2100MHz) and US (850/1900MHz). The TinySine operates with a Mini GSM/Cellular Quad-Band Antenna (2dBi) and has an integrated GPS. The TinySine basically uses the Fona software library, but some additional work was required to transmit data via a HTTP post (see Trevathan and Johnstone (2018)). Sensor data is organised as a JSON string prior to transmission and is parsed on receipt by the server before being stored in a database.

Figure 1. Hardware functional block diagram for the remote aquatic monitoring system

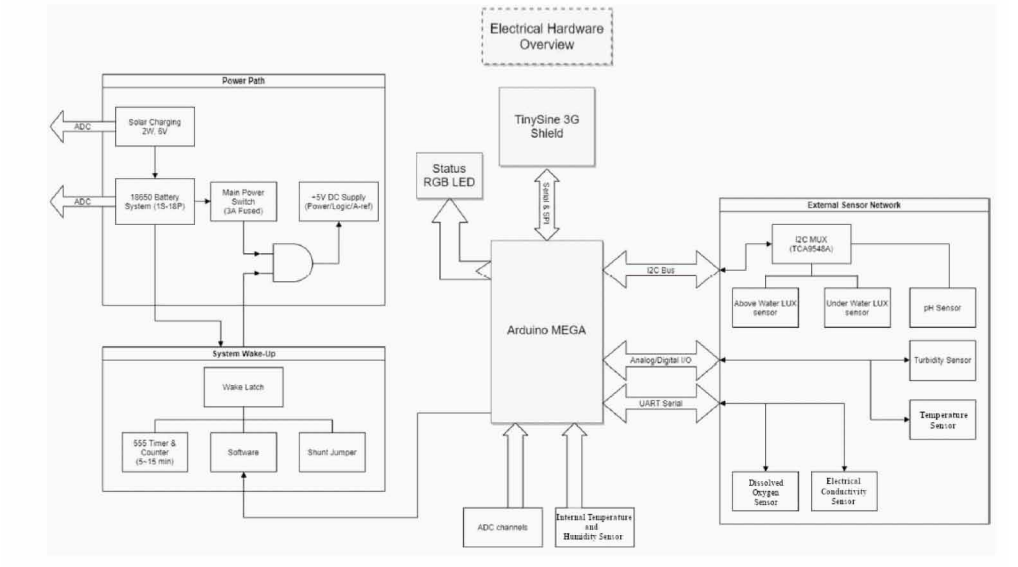


Figure 2. Arduino Mega 2560 microcontroller schematic (left) and microcontroller unit (right)

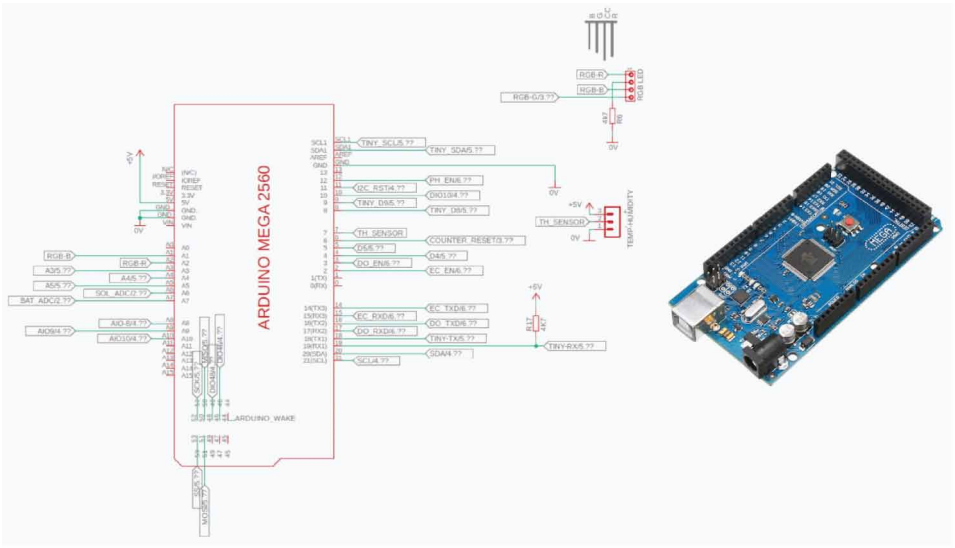


Figure 3. TinySine 3G/GPRS/GSM shield schematic (left) and shield (right)

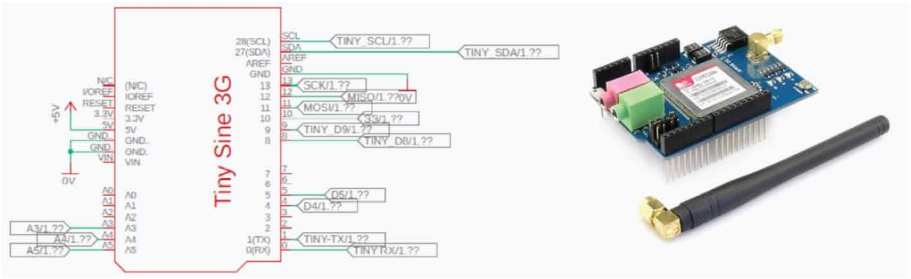


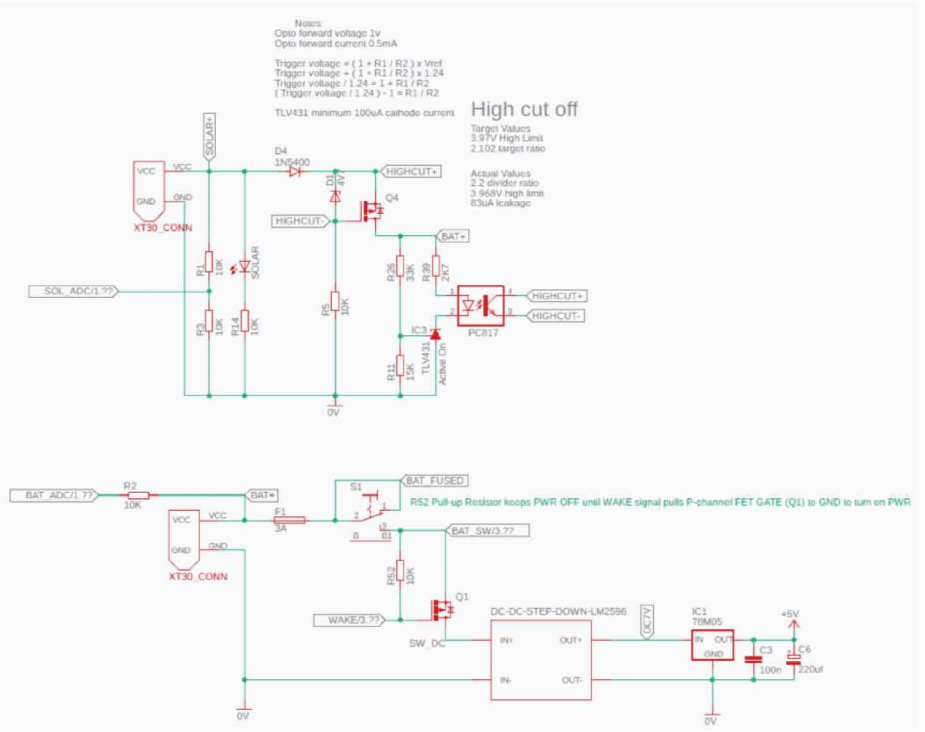
Figure 4 highlights the power management and solar charging circuitry for the system. Two 6 volt (1 watt) solar panels supply power to a CN3083 SOP8 high efficiency solar energy charging circuit chip. A high voltage cut-off prevents the batteries from charging beyond 4.2 volts. 18650 Li-ion laptop batteries are used (re-purposed from e-waste). A DC 3-32 volt step up to 5-35 volt boost convertor voltage regulator is used to step the battery voltage down to the required 5 volts for the Arduino to operate. The 78M05 voltage regulator protects the circuit from overvoltage conditions.

Figure 5 depicts the duty cycling and timing circuitry for the system. The core timing revolves around a 555 timer. The most significant bit triggers the wake-up signal, which powers up the buoy. When the buoy finishes executing its code, it sends a sleep command to re-initiate the timer. If this signal is missed, a software watchdog timer will attempt to send the signal again. If the signal is again missed, the buoy will stay awake for at most 15 minutes before a secondary hardware timer kicks in and forces the buoy into sleep.

3.2 Integrating Sensors for Measuring Electrical Conductivity, Dissolved Oxygen and pH

In order to select appropriate sensors for measuring electrical conductivity, dissolved oxygen and pH, several factors had to be considered. The first was ease of integration with our existing platform.

Figure 4. Power management and solar charging schematic



Ideally, the sensors should operate at 5 volts and/or be Arduino compatible. The sensors must be accurate for a scientific application with a known acceptable error rate (i.e., < 5%). The sensors must also be relatively inexpensive and provide as broad range of readings as possible for the price point. For example, a dissolved oxygen sensor that reads up to 100 mg/L would be more favoured compared to one that only reads up to 20 mg/L for relatively the same price and accuracy.

Towards this end, Atlas Scientific™ provides the most suitable sensors for our application. The sensors are Arduino compatible (i.e., operate at 5 volts), can be calibrated with an acceptable and known error margin, are relatively inexpensive ($175 - $300 USD) and take readings over a wider range than similar or less expensive sensors. Sensors can be submerged indefinitely in fresh and saltwater environments (provided appropriate water proofing of the connector).

Probes come in two versions: 1) Laboratory grade; and 2) Industrial grade. The laboratory grade probes are of a less durable construction than the industrial grade probes. However, the laboratory grade probes are approximately $100 less than the industrial. For the initial trials described in this paper, we employed the laboratory grade probes (further discussed in Section 4.2.1).

Figure 6 illustrates the Atlas Scientific™ laboratory grade probes for A) electrical conductivity, B) dissolved oxygen and C) pH respectively. Each sensor requires a specific embedded EZO systems module in order to operate (also shown in Figure 6). These circuits communicate with the sensors to take measurements and provide control of sensor configuration parameters. The circuits embed logic for calibration offsets to be applied to readings and compensations for influencing factors such as temperature, salinity and pressure (depending on the probe). Table 2 shows the specifications of the electrical conductivity, dissolved oxygen and pH probes/EZO modules respectively.

The electrical conductivity probe (Figure 6 A) has two electrodes positioned opposite from each other. An AC voltage is applied to the electrodes causing cations to move to the negatively charged

Figure 5. Duty cycling and timing schematic

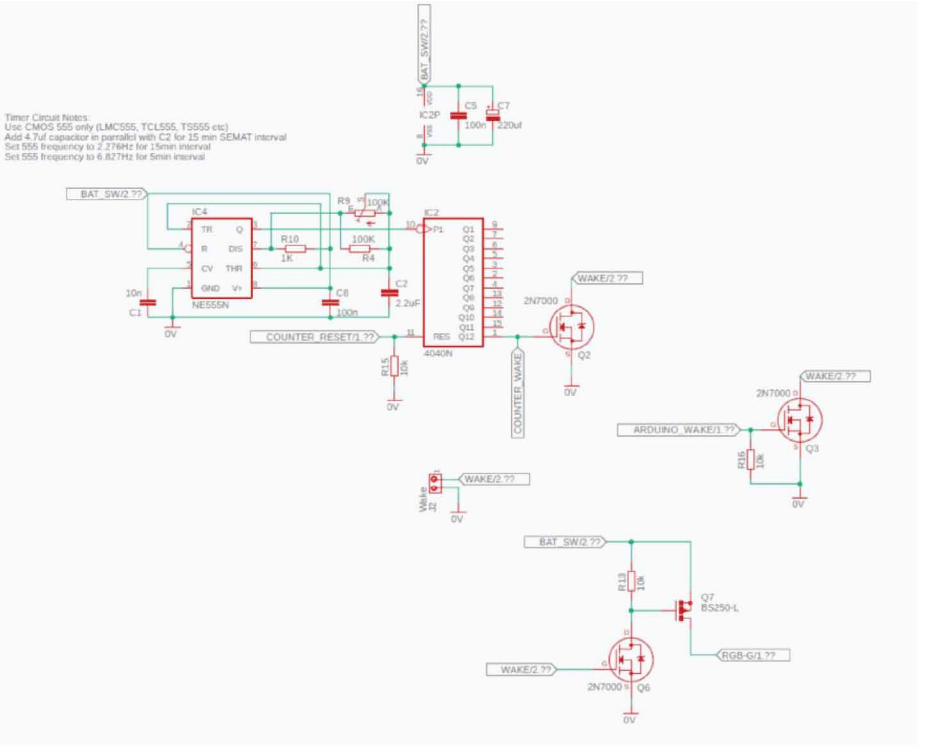
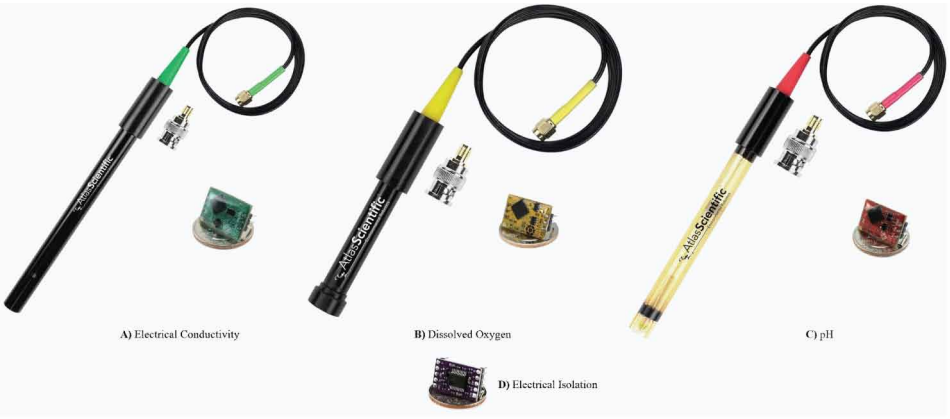


Figure 6. Atlas Scientific™ laboratory grade probes and EZO modules



electrode, while the anions move to the positively electrode. The more free electrolyte the liquid contains, the higher the electrical conductivity. We chose a K 10 probe as it provided the widest range of readings (i.e., 10 µS/cm to 1 S) making it more versatile for environmental applications.

The dissolved oxygen probe (Figure 6 B) is a galvanic design that consists of a PTFE membrane, an anode bathed in an electrolyte and a cathode. Oxygen molecules defuse through the probe's membrane at a constant rate (without the membrane the reaction happens to quickly). Once the

Table 2. Atlas Scientific™ Electrical Conductivity, Dissolved Oxygen and pH probe/EZO specifications

	Electrical Conductivity	Dissolved Oxygen	pH
Measures	Conductivity (µS/cm) Total dissolved solids (ppm) Salinity (PSU (ppt) 0.00 – 42.00) Specific gravity (sea water) (1.00 – 1.300)	Dissolved oxygen	pH
Range	0.07 – 500,000+ µS/cm	0.01 – 100+ mg/L 0.1 – 400+ % saturation	.001 – 14.000
Accuracy	+/– 2%	+/– 0.05 mg/L	+/- 0.002
Supported Probes	K 0.1 – K 10	Any galvanic probe	Any type/brand
Calibration	1 or 2 point	1 or 2 point	1, 2, 3 point
Data Protocol	UART & I^2C	UART & I^2C	UART & I^2C
Compensation	Temperature	Temperature, salinity and pressure	Temperature
Default I^2C Address	100 (0x64)	97 (0x61)	99 (0x63)
Operating Voltage	3.3V – 5V	3.3V – 5V	3.3V – 5V
Data Format	ASCII	ASCII	ASCII

oxygen molecules have crossed the membrane they are reduced at the cathode and a small voltage is produced. If no oxygen molecules are present, the probe will output 0 mV. As the oxygen increases so does the mV output from the probe. Each probe will output a different voltage in the presence of oxygen. Note that this probe requires constant water flow to maintain stable readings. A refill of the electrolyte every 18 months (or sooner) is also required.

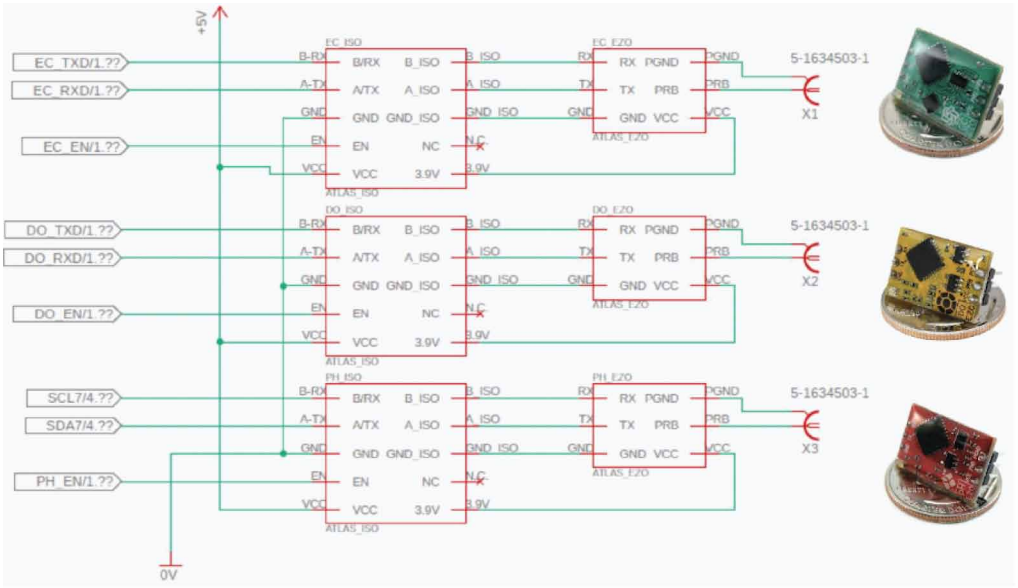
The pH probe (Figure 6 C) measures the hydrogen ion activity in a liquid. At the tip of a pH probe is a glass membrane. This glass membrane permits hydrogen ions from the liquid being measured to defuse into the outer layer of the glass, while larger ions remain in the solution. The difference in the concentration of hydrogen ions (outside the probe vs. inside the probe) creates a very small current. This current is proportional to the concentration of hydrogen ions in the liquid being measured. The pH probe must be stored in a buffer solution when not in use to ensure that glass membrane does not dry out.

The Atlas Scientific™ EZO sensor modules have two different communications protocols that have to be manually set between UART and I^2C. By default, they are set to UART (baud rate: 9600). Only two UART channels are available on the GPSB. This is unfortunate as experience has taught us that on occasion I^2C can be unstable and fail which results in no readings being taken (refer to Trevathan et al. (2021)). Electrical conductivity and dissolved oxygen were chosen to use UART (as these sensors were deemed to be more critical to our applications). pH was set to I^2C mode.

Each Atlas Scientific™ probe operates using simple Arduino code and libraries. An EZO module accepts an ASCII string argument in CSV format. Until calibrated, the EZO module parses sensor values under default environmental conditions. For example, the temperature compensation is set to 25°C, and the pressure compensation (for dissolved oxygen) is set to 1 bar/atm. Each device returns a different reading based on extra input argument/s in the ASCII CSV string. Each probe can withstand slow to fast water flow rates. However, dissolved oxygen readings decrease after over 10-15 seconds of being exposed to stagnant water (flow rate approximately 60 mL/min or less).

Atlas Scientific™ sensor probes and module circuitry can be susceptible to noise from extremely low currents (µA) and low voltages (mV). As such, the circuits require electrical isolation (see Figure

Figure 7. Atlas Scientific™ EZO sensor schematic



6 D). Other potential sources of noise for the circuit board could come from the *Switch Mode Power Supply* (SMPS) and the 3G GSM. To minimise exposure, the EZO modules were placed the furthest away from the power supply circuitry.

3.3 Integrating a New Lux Sensor – Adafruit™ TSL2591

The Adafruit™ TSL2561 that have historically been used by the GPSB for above and underwater light readings became discontinued during the development of this iteration of the remote IoT aquatic environmental monitoring platform. The decision was made to use the Adafruit™ TSL2591 lux sensor as a replacement. However, the TSL2591 does not provide three addressable I^2C address in the same manner as the TSL2561. This means only one device can be used for the fixed I^2C address on the TSL2591, which is problematic as the platform requires two lux sensors (i.e., for above and below water readings).

To resolve this issue, an I^2C multiplexer was added to this revision. This effectively allows the same I^2C address for both lux sensors to be used, but they are assigned to different addresses of the multiplexor. We chose an Adafruit™ TCA9548A 1-to-8 I^2C Multiplexor Breakout[8]. Figure 8 illustrates the schematic for the new I^2C multiplexor and how the TSL2591 sensors were incorporated into the design.

3.4 Mechanical Integration of the Sensor Probes and Circuitry

To accommodate the new sensor probes, significant re-engineering of the buoy body was required (Figure 9 A). Four irrigation risers extend below the buoy canister to house the electrical conductivity, dissolved oxygen and pH sensors, and the sensor head (which contains the temperature, lux and turbidity sensors). The buoy canister was enlarged to 150 ml diameter to accommodate the larger PCB that interfaced the new sensor circuitry.

A new 3D printed lid was designed with a resin backfilled channel to limit water ingress possibilities (Figure 9 B). Sturdier and higher performing glass solar panels replaced the plastic solar panels from the previous buoy design.

Figure 8. I/O and I²C multiplexor schematic

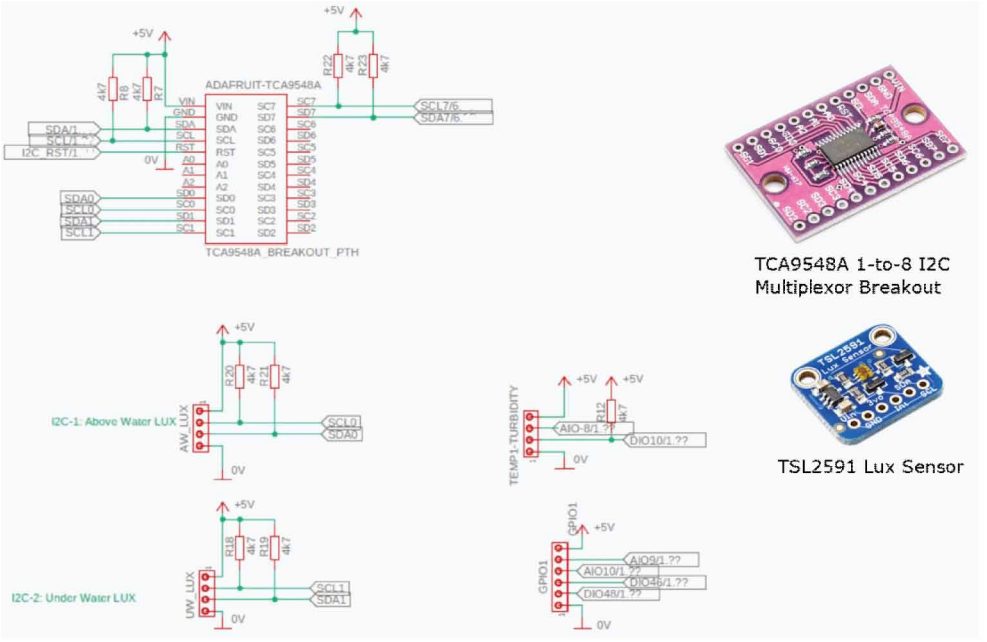
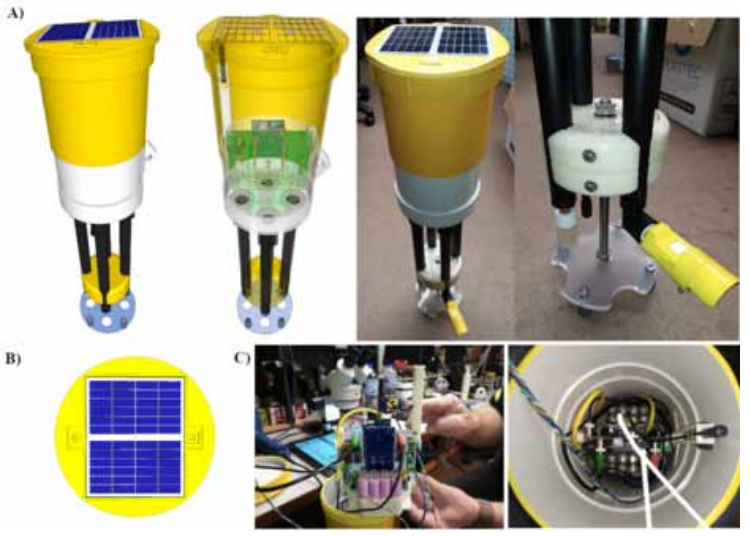


Figure 9. (A) Assembled buoy and sensor probes; (B) Re-engineered boy lid; and (C) Internal frame mounting and wiring



To keep the weight towards the bottom of the buoy, it was decided to place the power circuitry at the bottom of the PCB near the battery pack. The EZO modules, their isolator units and probe BNC connectors are at the top of the PCB. This allows easy access to connect and disconnect the probe cables when the board needs to be removed from the enclosure. Each EZO module has its PCB area beneath the isolator and BNC connector segregated from the main ground plane to act as an isolated ground plane in their respective isolation zone (Figure 9 C).

The circuit board is held in place on a 3D printed base, which also houses the 16x18650 Li-ion cells. Once completely wired, this frame slides into guiding posts that are bolted/screwed down. The enclosure had undergone number changes that affected the buoyancy and height above water such that the antenna for wireless telemetry has been extended/wired to sit at the bottom of lid to allow optimal signal strength during transmission.

3.5 Calibration

Calibration is the process of aligning the sensors readings with a known accurate source to reduce reading errors and make the sensor measurements as accurate as possible (Bychkovskiy et al (2003), Fang and Bate (2020)). This is typically achieved by measuring a sensor against another accurate calibrated device or using a calibration solution that conforms to a scientific standard.

There are several approaches to calibration that impact upon measurement quality:

1. **One-point calibration:** A single reference point is used. All sensor readings are then inferred relative to that point.
2. **Two-point calibration:** Two references are used to create a linear relationship. Sensor readings then fall on that curve.
3. **Multi-point calibration:** Multiple references are used, typically for complex non-linear relationships.

After the initial calibration procedure, two additional steps are required:

1. **Verification:** Sensors are tested in controlled environments and measured against other equipment. This is to ensure that the sensors are reading as they should with a known error.
2. **Validation:** Sensors are validated in field conditions against other equipment. This step ensures that the sensors are actually reading correctly in field conditions so that any lab-based constraints or errors in the calibration process are identified.

Atlas Scientific™ devices come with calibration solutions and instructions. The main difficulties involve creating a temperature-controlled environment for the sensors and calibration solutions (typically 25°C) in an attempt to reduce error sources. Meticulous care must be taken during the calibration process to provide the greatest degree of sensor accuracy as possible.

The electrical conductivity probe involves a two-point calibration process. Atlas Scientific™ provides two calibration solutions at 12,880 µS (low point) and 150,000 µS (high point). Once the EZO is set to calibration mode, a series of readings are taken in each respective solution until the calibration off-set is locked in. Calibration for this probe is suggested as a one-off procedure that should not have to be repeated. However, we have not yet been able to verify this claim for extended field trials.

Dissolved oxygen calibration can be either one or two-point. One-point is sufficient if accuracy below 1 mg/L is not required. One-point calibration essentially involves taking a reading in the open air. Two-point calibration requires the probe to be placed in a zero dissolved oxygen calibration solution. Temperature, pressure and salinity compensations are necessary for dissolved oxygen.

pH calibration is a three-point process involving pH 4 (alkaline), pH 7 (neutral) and pH 10 (acidic) solutions. The probe is placed in each respective calibration solution and a reading taken.

4. RESULTS AND DISCUSSION

4.1 In-House Environment Testing

A test tank was constructed in front of a vertical garden (Figure 10) to simulate an aquatic environment with small fish and plants to stimulate oxygenation and consumption in the water. The water is

Figure 10. Aquatic test environment

periodically pumped out to irrigate the vertical garden, where runoff water returns to the tank. This water cycling introduces changes in electrical conductivity and dissolved oxygen concentration. The test tank is a predominantly open system, which introduces variables for testing sensor behaviour.

The platforms solar charging and power management systems were tested in these settings. minor tweaks were made to the duty cycling timing and circuit to optimise battery life. The new sensors' behaviour was monitored over several months. Temperature clearly has an impact on all of the parameters. Dissolved oxygen and pH oscillated with the day/night cycle as expected. During the trial period, dissolved oxygen levels dropped to critical. However, a fish kill disaster was averted when the sensor readings were trusted, and intervention occurred to resolve the water quality issue.

4.2 Field Test Environment

4.2.1 Calibration Results

For the verification, two approaches where taken. One was to create a saltwater environment. The other was to create a slightly acidic environment. We attempted to maintain a uniform temperature (25°C) for the sensor probes and the solutions used. The results for two buoys (labelled SB17 and SB18) are explained below. The buoys were verified against a Hach field meter that contained electrical conductivity, dissolved oxygen and pH probes. The Hach was factory calibrated.

Table 3 gives the electrical conductivity verification results. 6 litres of water was mixed with 430 grams of iodised table salt. Note there is some degree of discrepancy between the DO results for the Hach and the two buoys.

Table 4 gives the pH verification results. 5 litres of water was mixed with 1 litre of white vinegar. The discrepancy between the dissolved oxygen results for the Hach and the two buoys does not occur during this test.

Table 3. Electrical conductivity verification results

	Temperature	EC	DO	pH
Hach	25.4°C	117.4 mS/cm	8.12 mg/L	7.11
SB17	25.06°C	105.7 mS/cm	4.09 mg/L	6.961
Hach	25.2°C	117.2 mS/cm	8.14 mg/L	7.14
SB18	24.81°C	108.8 mS/cm	4.52 mg/L	6.97

Table 4. pH verification results

	Temperature	EC	DO	pH
Hach	26.8°C	793 µS/cm	6.47 mg/L	3.09
SB17	26.12°C	807.6 µS/cm	6.09 mg/L	3.03
Hach	25.7°C	780 µS/cm	6.63 mg/L	3.11
SB18	25.24°C	833 µS/cm	6.61 mg/L	3.02

Table 5 presents the validation results for the two buoys. The buoys were placed in the in-house testing environment (described in Section 4.1) and compared against the Hach.

4.2.2 Field Test Applications

The buoys have undertaken two significant field test trials. The first is for supporting commercial environmental research in North Queensland rivers and creeks. Two buoys (SB17 and SB18) have been deployed at various locations for extended periods to complement existing measurement mechanisms. Readings from the buoys were within the calibrated range of error from readings taken from other scientific devices. Samples were taken at 15-minute intervals giving a total of 96 readings (per sensor parameter) over each 24-hour period.

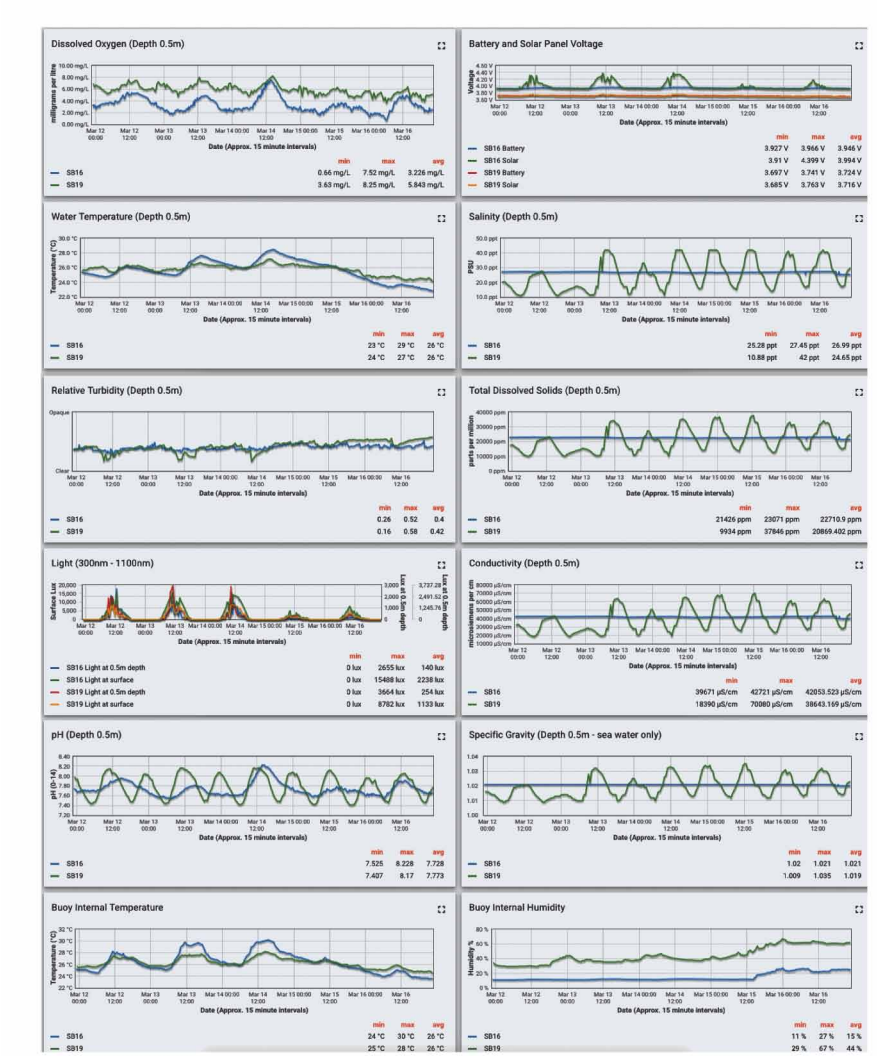
At this point it should be noted that there were some issues with the robustness of the Atlas Scientific™ laboratory grade sensor probes when deployed in adverse environmental conditions out in the field. The probes are prone to damage/breakage from mishandling or collision with submerged objects. As such, the decision was made to replace the laboratory probes with industrial probes to observe the difference. Additional physical barriers were also incorporated into the buoy design to help protect the sensors from damage.

The second field test trial is at a commercial prawn farm in South East Queensland. Two calibrated buoys were deployed (SB16 and SB19) – one in a prawn farm pond and the other in the nearby river. Figure 11 presents the data for these buoys over a 5-day period. Regular interventions are required in prawn farm ponds to keep the water quality parameters within a tolerable range for prawn production (e.g., aeration and water changes). The buoys' measurements are in-line with the

Table 5. Validation results

	Temperature	EC	DO	pH
Hach	26.0°C	860 µS/cm	7.21 mg/L	7.73
SB17	25.38°C	1048 µS/cm	6.33 mg/L	7.64
SB18	25.25°C	1087 µS/cm	6.75 mg/L	7.71

Figure 11. Commercial prawn farm data for SB16 and SB19 (ThingsBoard IoT dashboard)



prawn farm's existing monitoring practices when water quality parameters were changing and the need for and extent of interventions required.

Of particular interest to the prawn farmers was the previously unknown impact of salinity in the river due to intense rainfall events. During such events there is an influx of freshwater from upstream sources that eventually meets the saltwater interface as the river approaches the open ocean. Our system was able to show the influx of freshwater in near real-time. Furthermore, the prawn farm became aware of the extent of which the elevated water levels due to tidal movements were actually holding the fresh water in the system. This was a lot longer than previously thought. As such, the capability provided by the system described in this paper can clearly help decision makers take informed actions around interventions that can lead to productive/positive outcomes.

A further notable issue is the fouling rate of the sensors (i.e., build-up of detritus, algae and/or barnacles). Different water bodies foul at different rates. However, the fouling eventually results in the sensors becoming less sensitive over time. We observed that in the prawn farm deployment that

cleaning was required approximately every two weeks. Cleaning was undertaken by means of a mild 5% hydrochloric acid wash to remove hard and soft debris. Note that sensors cannot be scrubbed as this may damage delicate electrodes and membranes.

5. CONCLUSION

This paper presented an IoT platform for remote aquatic environmental monitoring. The system is capable of measuring water temperature, above and below surface lux, turbidity, electrical conductivity (salinity), dissolved oxygen and pH. Measurements are sent via 3G GSM and displayed on a ThingsBoard IoT dashboard.

This proposal expanded upon an existing system and showed how Atlas Scientific™ sensors for electrical conductivity, dissolved oxygen and pH were incorporated into the platform. This involved redesigning the PCB to interface with these sensors, connectors and EZO chips. Furthermore, upgrading to a TSL2591 lux sensor required an I^2C multiplexor to be incorporated into the design to allow multiple lux sensors to be addressed. The physical buoy was re-engineered to fit the larger profile PCB and accommodate the additional sensors. Sensor calibration was undertaken using calibration standard solutions and the process was verified and validated against Hach scientific instruments.

The platform was tested in-house initially in a constructed aquatic environment. During this trial, the duty cycling and power budget were tweaked. The sensor behaviour was also observed, temperature compensations applied, and preliminary data collected on the system's performance. The sensors were shown to be responsive to the environmental conditions.

The system is now at a commercial stage and has been field tested by two commercial clients. One application is in scientific environmental research, the other is in prawn farm water quality monitoring. Sensor readings have proven to be accurate (compared to other measurements taken by additional equipment). However, sensor fouling over time is a problem. As such, periodic cleaning is required – and must form a core part of system maintenance when deployed in the field. Also, the fragility of laboratory grade sensors is an issue. We are currently looking into upgrading these sensors to industrial grade probes in order to improve the platform's robustness. The platform can be remotely deployed for 12 to 18 between major maintenance cycles (i.e., sensor servicing and recalibration).

Future work involves providing additional telemetry mechanisms/options for retrieving the data. Firstly, we intend on integrating a LoRa telemetry option where the GSM signal is weak or non-existent so that the buoy can relay its data via a nearby base station. Secondly, a Bluetooth option will be investigated to force a buoy to wake up in the field and allow for the data to be extracted. Finally, we will investigate the use of an ESP32 to expand the system capabilities even further.

ACKNOWLEDGMENT

The authors would like to thank Simon Schmidtke, James Taylor, Tony Sharp and Ian Trevathan.

Funding: This work was supported in part by the Australian Research Council Linkage (LP190101083), Logan City Council EnviroGrants scheme and Griffith University Institute for Integrated and Intelligent Systems.

REFERENCES

Abowei, J. F. N. (2010). Salinity, dissolved oxygen, pH and surface water temperature conditions in Nkoro River, Niger Delta, Nigeria. Advance Journal of Food Science and Technology, 2(1), 36-40.

Analytical Solutions. (2021). *Analytical Solutions Australia*. www.analyticalsolns.com.au

Bartram, J., & Ballance, R. (Eds.). (1996). *Water quality monitoring: a practical guide to the design and implementation of freshwater quality studies and monitoring programmes*. CRC Press. doi:10.4324/9780203476796

Bychkovskiy, V., Megerian, S., Estrin, D., & Potkonjak, M. (2003). A collaborative approach to in-place sensor calibration. In *Information processing in sensor networks* (pp. 301–316). Springer. doi:10.1007/3-540-36978-3_20

Danielsen, F., Burgess, N. D., Jensen, P. M., & Pirhofer-Walzl, K. (2010). Environmental monitoring: The scale and speed of implementation varies according to the degree of people's involvement. *Journal of Applied Ecology*, *47*(6), 1166–1168. doi:10.1111/j.1365-2664.2010.01874.x

Dickson, A. G. (1993). The measurement of sea water pH. *Marine Chemistry*, *44*(2-4), 131–142. doi:10.1016/0304-4203(93)90198-W

Fang, X., & Bate, I. (2020). An improved sensor calibration with anomaly detection and removal. *Sensors and Actuators. B, Chemical*, *307*, 127428. doi:10.1016/j.snb.2019.127428

Fondriest. (2021). *Fondriest Environmental Products*. www.fondriest.com

Gholizadeh, M. H., Melesse, A. M., & Reddi, L. (2016). A comprehensive review on water quality parameters estimation using remote sensing techniques. *Sensors (Basel)*, *16*(8), 1298. doi:10.3390/s16081298 PMID:27537896

Glasgow, H. B., Burkholder, J. M., Reed, R. E., Lewitus, A. J., & Kleinman, J. E. (2004). Real-time remote monitoring of water quality: A review of current applications, and advancements in sensor, telemetry, and computing technologies. *Journal of Experimental Marine Biology and Ecology*, *300*(1-2), 409–448. doi:10.1016/j.jembe.2004.02.022

Hach. (2021). *Hach Water Analysis Solutions*. www.hach.com

Hanington, P., Rose, A., & Johnstone, R. (2016). The potential of benthic iron and phosphorus fluxes to support the growth of a bloom forming toxic cyanobacterium Lyngbya majuscula, Moreton Bay, Australia. *Marine and Freshwater Research*, *67*(12), 1918–1927. doi:10.1071/MF15219

Hongpin, L., Guanglin, L., Weifeng, P., Jie, S., & Qiuwei, B. (2015). Real-time remote monitoring system for aquaculture water quality. *International Journal of Agricultural and Biological Engineering*, *8*(6), 136–143.

Huan, J., Li, H., Wu, F., & Cao, W. (2020). Design of water quality monitoring system for aquaculture ponds based on NB-IoT. *Aquacultural Engineering*, *90*, 102088. doi:10.1016/j.aquaeng.2020.102088

Ighalo, J. O., Adeniyi, A. G., & Marques, G. (2021). Internet of things for water quality monitoring and assessment: a comprehensive review. *Artificial intelligence for sustainable development: Theory, practice and future applications*, 245-259.

Jones, R. G. (2002). Measurements of the electrical conductivity of water. *IEE Proceedings. Science Measurement and Technology*, *149*(6), 320–322. doi:10.1049/ip-smt:20020767

Kanagaraj, G., Primya, T., Rekha, K. S., Vinothini, C., & Anitha, P. (2020). IoT-Enabled Water Quality Monitoring System. In *Inventive Communication and Computational Technologies* (pp. 275–291). Springer. doi:10.1007/978-981-15-0146-3_26

Laut, J., Henry, E., Nov, O., & Porfiri, M. (2013). Development of a mechatronics-based citizen science platform for aquatic environmental monitoring. *IEEE/ASME Transactions on Mechatronics*, *19*(5), 1541–1551. doi:10.1109/TMECH.2013.2287705

Lee, Y. J., Trevathan, J., Atkinson, I., & Read, W. (2015). The integration, analysis and visualization of sensor data from dispersed wireless sensor network systems using the SWE framework. *Journal of Telecommunications and Information Technology*, *2015*, 86–97.

Lee, Y. J., Trevathan, J., Atkinson, I., & Read, W. (2018). An intelligent agent system for managing heterogeneous sensors in dispersed and disparate wireless sensor network. *International Journal of Sensor Networks*, *27*(3), 149–162. doi:10.1504/IJSNET.2018.093134

Li, H., Liu, X., Li, J., Lu, X., & Huan, J. (2013). Aquiculture remote monitoring system based on IOT Android platform. *Nongye Gongcheng Xuebao (Beijing)*, *29*(13), 175–181.

Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(05), 164–173. doi:10.4236/jcc.2015.35021

Manimegalai, R. (2020). An IoT based smart water quality monitoring system using cloud. In *2020 International conference on emerging trends in information technology and engineering* (pp. 1-7). IEEE.

McGrane, S. J. (2016). Impacts of urbanisation on hydrological and water quality dynamics, and urban water management: A review. *Hydrological Sciences Journal*, *61*(13), 2295–2311. doi:10.1080/02626667.2015.1128084

Pasika, S., & Gandla, S. T. (2020). Smart water quality monitoring system with cost-effective using IoT. *Heliyon*, *6*(7), e04096. doi:10.1016/j.heliyon.2020.e04096 PMID:32642574

Quintero-Polanco, J., Betancourt, F. R., & Molina-Mosquera, J. (2018). Control of dissolved oxygen in water for intensive tilapia culture using IoT. *Journal of Engineering and Applied Sciences (Asian Research Publishing Network)*, *13*, 9509–9516.

Ragai, H. F., Adly, I., Sayour, H. E., & Wilson, S. (2017). Remote control and monitoring of fish farms using wireless sensor networks. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)* (pp. 107-111). IEEE. doi:10.1109/ICCES.2017.8275287

Rose, S., & Long, A. (1988). Monitoring dissolved oxygen in ground water: Some basic considerations. *Ground Water Monitoring and Remediation*, *8*(1), 93–97. doi:10.1111/j.1745-6592.1988.tb00981.x

Scarpa, E., Mastronardi, V. M., Guido, F., Algieri, L., Qualtieri, A., Fiammengo, R., Rizzi, F., & De Vittorio, M. (2020). Wearable piezoelectric mass sensor based on pH sensitive hydrogels for sweat pH monitoring. *Scientific Reports*, *10*(1), 1–10. doi:10.1038/s41598-020-67706-y PMID:32616743

Simbeye, D. S., & Yang, S. F. (2014). Water quality monitoring and control for aquaculture based on wireless sensor networks. *Journal of Networks, 9*(4), 840.

Stupar, D. Z., Bajić, J. S., Joža, A. V., Dakić, B. M., Slankamenac, M. P., Živanov, M. B., & Cibula, E. (2012). Remote monitoring of water salinity by using side-polished fiber-optic U-shaped sensor. In *2012 15th International Power Electronics and Motion Control Conference (EPE/PEMC)* (pp. LS4c-4). IEEE.

Sung, W. T., Chen, J. H., & Wang, H. C. (2014). Remote fish aquaculture monitoring system based on wireless transmission technology. In *2014 International Conference on Information Science, Electronics and Electrical Engineering* (Vol. 1, pp. 540-544). IEEE. doi:10.1109/InfoSEEE.2014.6948171

Thorslund, J., & van Vliet, M. T. (2020). a global dataset of surface water and groundwater salinity measurements from 1980–2019. *Scientific Data*, *7*(1), 1–11. doi:10.1038/s41597-020-0562-z PMID:32661286

Trevathan, J., & Johnstone, R. (2018). Smart Environmental Monitoring and Assessment Technologies (SEMAT)—A New Paradigm for Low-Cost, Remote Aquatic Environmental Monitoring. *Sensors (Basel)*, *18*(7), 2248. doi:10.3390/s18072248 PMID:30002319

Trevathan, J., Johnstone, R., Chiffings, T., Atkinson, I., Bergmann, N., Read, W., Theiss, S., & Stevens, T. (2012). SEMAT—The next generation of inexpensive marine environmental monitoring and measurement systems. *Sensors (Basel)*, *12*(7), 9711–9748. doi:10.3390/s120709711 PMID:23012567

Trevathan, J., Read, W., Sattar, A., Schmidtke, S., & Sharp, T. (2020). *The Virtual Sensor Concept: Separating Sensor Software from the Hardware. In 2020 IEEE Sensors*. IEEE.

Trevathan, J., Schmidtke, S., Read, W., Sharp, T., & Sattar, A. (2021). An IoT General-Purpose Sensor Board for Enabling Remote Aquatic Environmental Monitoring. *Internet of Things*, *16*, 100429. doi:10.1016/j.iot.2021.100429

Trevathan, J., & Sharp, T. (2020). Up-Cycling E-Waste into Innovative Products Through Social Enterprise. *9th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, 185-193. doi:10.5220/0009350301850193

Wang, R., Zhai, Q., Zhao, Y., An, T., Gong, S., Guo, Z., Shi, Q. Q., Yong, Z., & Cheng, W. (2020). Stretchable gold fiber-based wearable electrochemical sensor toward pH monitoring. *Journal of Materials Chemistry. B, Materials for Biology and Medicine*, *8*(16), 3655–3660. doi:10.1039/C9TB02477H PMID:31998927

ENDNOTES

1 thingsboard.io
2 https://news.griffith.edu.au/2018/05/01/ griffith-celebrates- innovative- young- entrepreneurs- at -2018-glologan-challenge/
3 https://www.arduino.cc/en/Main/arduinoBoardMega2560/
4 https://www.tinyosshop.com/3g-gprs-gsm-shield-for-arduino-sim5320e
5 https://www.adafruit.com/product/1782
6 https://www.adafruit.com/product/439
7 https://learn.adafruit.com/adafruit-fona-3g-cellular-gps-breakout
8 https://learn.adafruit.com/adafruit-tca9548a-1-to-8-i2c-multiplexer-breakout

Jarrod Trevathan is an expert in affordable environmental monitoring technologies and ecommerce security and fraud algorithms. His current particular area is cost-effective technologies for water quality assessment and flood monitoring. Dr Trevathan is leading industry and community collaborative projects that seek to integrate technology, social enterprise and community engagement to improve environmental outcomes. This is particularly the case with water resource monitoring and disaster management (for which he has won significant community awards and prestigious Australian Research Council [ARC] funding).

Dzung Nguyen holds a BEng (Hons) from the University of Queensland. He works on electronics design, fabrication, and testing. Dzung has worked with several major electronics firms on commercial applications.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

Scalability of Pervasive Communication Networks in IoT

Manal Khayyat, Umm Al-Qura University, Saudi Arabia*
https://orcid.org/0000-0003-0830-4757

Nadine Akkari, Faculty of Computing and Information Technology, Jeddah International College, Saudi Arabia

ABSTRACT

The vision of the future IoT is to facilitate interoperability between the massive heterogeneous end-users' terminals and at the same time expedite smooth access to their vast and pervasive smart applications in the cloud. This huge number of things spread all over the cloud generates a significant burden on the current architecture of the IoT. Therefore, this paper aims to achieve scalability for future IoT. To reach the solution, the authors first investigated the encountered challenges when trying to attain scalability. Afterward, they define the main requirements along with their key enabling technologies to achieve scalability in the distributed IoT environment. Finally, a reference model with central management and control is designed, satisfying the defined scalability requirements to reach the desired future IoT architecture.

KEYWORDS

Communication Systems, Fog Computing, Internet of Things (IoT), Scalability Requirements, Software-Defined Networking (SDN)

1. INTRODUCTION

IoT has a high impact on society's daily life because it is becoming the primary technology for obtaining information. With today's advances in technology, every day, a new machine, device, or application is added to the Internet. According to the statistical data by CompTIA (2015), the number of things connected to the Internet reached 50.1 billion in 2020. The current tendency is to move everything into the cloud, to be able to share resources and utilize them effectively. Hence, there is an obvious problem with the IoT scalability that should be taken into consideration. The IoT consists of massive heterogeneous things built by different developers, using different programming languages, tools, protocols, and running on different platforms. This massive heterogeneity causes an obvious problem with the interoperability between those terminals, sensors, and applications that require increasing the resources and also making them work together. Therefore, the contributions of this paper are summarized as follows:

DOI: 10.4018/IJHIoT.294895
*Corresponding Author

- Investigate the challenges that might occur while achieving the scalability requirements.
- Define eight main requirements and their enabling technologies toward a scalable IoT architecture.
- Design reference model architecture that is satisfying the scalable IoT environment.

The rest of the paper is organized as follows. Section 2 discusses the related work on the field. Section 3 highlights the challenges encountered with the scalability requirements. Section 4 identifies eight requirements for a scalable IoT architecture and their corresponding key enabling technologies. Section 5 proposes a reference model architecture for scalable IoT. Finally, section 6 concludes the paper.

2. RELATED WORK

As of today, the Internet network has witnessed a huge increase in its scalability. That is attributed to the increasing number of smart devices and machines connected to the Internet, forming a vast, pervasive network of things. Hence, many efforts are focusing on increasing the scalability of the IoT. Many efforts discussed the main elements that should be included in the future IoT architecture towards facilitating the scalability. For instance, the researcher in (Helel, 2016) mentioned the strategic agent that adds intelligence to the infrastructure of the IoT. He recommends including the OSGi framework to host distributed services on the cloud. Moreover, he highlights the importance of utilizing the Atlas middleware to increase the scalability by providing replication of services and managing the dynamic distributed cloud environment. However, even though the proposed solution in (Helel, 2016) implements combinations of optimization algorithms, it has some weakness because the recent release of the Atlas middleware considers only one single computer for processing the middleware manager, while the IoT environment has an enormous number of computers and not only one (King et al., 2006). Furthermore, the researchers in (Shen et al., 2017) propose a scalable architecture for the IoT called the "MicroThings". They firstly reviewed the traditional architecture for the IoT and then added a centralized controller in the middle between the information and the application layers. The centralized controller consists of two main parts, which are the storage and the computing components. The problem in this solution is that it lacks accomplishing the interoperability between the different systems in the IoT environment. Another scalable solution for the IoT that preserves the centralized control and management feature was introduced by (Guo et al., 2017), who employ the transparent computing technology in the design. The primary purpose of the transparent computing technology is to make the services transparent to users by decoupling the software from the hardware machines (Ren et al., 2017). However, this solution is practical only with the wired networks, while it encounters significant challenges when moving to wireless networks. Thus, it couldn't be used in real-world IoT situations. The authors in (Ren et al., 2017) have also recommended employing the transparent computing technology and transferring the services from the cloud to the edge, to speed-up the processing and increase the scalability requirement in the IoT. Although their proposed solution that employs transparent computing is considered paramount, it lacks the use of one central platform for coordinating and managing the heterogeneous resources in the IoT environment. The authors in (Sarkar et al., 2014) propose a distributed layered architecture for the IoT, called Distributed Internet-like Architecture for Things (DIAT). They encourage using an IoT daemon for managing the different heterogeneous devices and also enable the interoperability between them. However, they didn't theorize the functionalities of the cloud applications, and they didn't explain the strategy to deal with the data in the cloud.

Moreover, the authors in (Shimojo et al., 2001) integrated two of the most powerful technologies to enable scalability in the IoT, which are the SDN and the Fog computing. SDN proved to increase the capacity and centrally manage the resources as it takes control away from the network. On the other hand, Fog computing can deliver real-time data with minimized latency. The authors in (Zarko et al., 2017) designed a solution for a scalable IoT that utilizes a backend platform for facilitating

central management and control of heterogeneous devices included in the IoT environment. It also enables mobility between the devices and ensures their interoperability.

From the presented literature, we notice that even though there are many efforts to accomplish the scalability in the IoT architecture, there is still a need to reach an optimal solution that covers all the scalability requirements and solve their associated open problems, which is the goal of this study.

3. CHALLENGES WITH THE SCALABILITY REQUIREMENT

This study provides a holistic view of the main elements needed to achieve the scalability required in the IoT environment. However, as a consequence of reaching optimized scalability, we might encounter the cost of other posing challenges. This section of the study highlights the open problems in the scalability of the IoT and illustrates the possible solutions to mitigate them.

Achieving interoperability between multiple heterogeneous systems distributed over the cloud is a huge encountered challenge, specifically in the IoT environment. The networks themselves could be heterogeneous and vague from each other. Consequently, the devices installed on the different types of networks will also be using different kinds of network protocols. This scenario clarifies the problem of interconnecting the multiple different devices in the cloud (Lee et al., 2017). The interoperability problem can be mitigated utilizing a unified resources platform that can centrally manage and control the heterogeneity between the various resources and seamlessly identify them to each other's and connect them (Zarko et al., 2017). The authors in (Moens et al., 2020) recommended adding a middle platform tier using machine learning algorithms within their recommended scalable IoT architecture.

Another robust solution besides the platform is to include a gateway capable of translating protocols between the devices (Lee et al., 2017). However, it worth mentioning that forwarding all the connections to pass through the translation gateway might cause a traffic congestion problem.

Thus, using the software-defined networking (SDN) will overcome the traffic generated in the network as it takes the control away from the data plane and, subsequently, reduce the traffic overhead flowing over the network (Shimojo et al., 2001).

Considering that the SDN central controller itself can have a single point of failure problem. This problem is dangerous as it might cause the whole system to become idle and not responding. A practical solution will be to build SDN as a distributed networking solution instead of being centralized. Distributing a replicated SDN central networking controller enables it to reroute the task given to a malfunctioning server to another good condition server, which means that SDN is eligible to re-configure and optimize the network depending on its recent condition (Lee et al., 2017).

Moreover, security and privacy are risky challenges that are always encountered whenever there is work on increasing the number of resources and opening them for the public. Malicious nodes might disturb the connection and leak sensitive information from private networks. A solution to secure and protect the IoT network from external attacks is to add a secure middleware bus that implements all the security requirements on the IoT system (Rehman et al., 2016).

Regarding users' privacy in an open environment like the IoT, a couple of privacy technologies could be employed, such as encryption, onion routing, and using the virtual private network (Rehman et al., 2016). The degradation in the IoT performance, like latency in the processing operation, is a challenging aspect that should be taken into consideration. Replication of multiple operating servers and databases in a pipeline model will increase the performance. The virtualization technology could also increase the number of serving machines to raise-up the performance. Both physical replication and virtualizations can speed-up the processing latency. An advanced virtualization technology that is able to predict latency and avoid it is Fog computing (Shimojo et al., 2001). Fog computing provides a virtualized platform that can process data at the edge of the network. Noting that moving the processing from the cloud into the edge could dramatically speed-up the computation process. It can improve the quality of service and also decrease the consumed bandwidth (Shimojo et al., 2001).

After reviewing the previous designed IoT architectures in the field (Guo et al., 2017), (Moens et al., 2020), (Ren et al., 2017), (Sarkar et al., 2014), (Shen et al., 2017), and (Zarko et al., 2017); we found that there are open problems with the existing architectures since they either defined for a particular type of application such as for health monitoring, smart transportation, safe city, or were designed for generic application but lack some significant features. Hence, there is a significant need to explore all the current rigid technological advances that support the scalability requirement and introduce them into one unified scalable IoT architectural solution.

4. EIGHT SCALABILITY REQUIREMENTS AND THEIR KEY ENABLING TECHNOLOGIES

With the major shift in the IoT paradigm that has an increasing number of users and also increasing amounts of data, the traditional IoT technologies are not sufficient for the future IoT quality expectation. Thus, the optimized technologies to satisfy the future scalable IoT requirements are discussed in this section of the paper. Several rigid technologies can be employed to satisfy the scalability attribute in the IoT. Thus, we selected the most robust and suitable technological solutions and categorized them under eight main scalability requirements, as illustrated in table 1.

Following is a description of the scalability requirements.

4.1 Central Management and Control

The IoT consists of mini-nets spatially distributed over different far away geographical locations and each mini-network includes devices and resources. Thus, there is a need to centrally manage and

Table 1. The roadmap elements for a scalable IoT and their key enabling technologies

Scalability Element	Key Enabling Technologies
a. Central management and control	
Networks level	- Software Defined Networking (SDN) - Network Function Virtualization (NFV)
Services level	- Open Services Gateway initiative (OSGi) - Packet Scheduler - Traffic Shaper
Servers level	- Hypervisor - Load Balancer
b. Transparency	- Transparent Computing (TC) - Middleware
c. Virtualizations	- Sun xVm (VirtualBox) - Citrix Xen
d. Reliable communication systems	- Internet Engineering Task Force (IETF) - Internet Protocol version 6 (IPv6) - Constrained Application Protocol (CoAP)
e. Cross-platforms and on-demand services	- Fog Computing - Open Application Platform - Sensing and Gateway Platform
f. Cognitive understanding of involved resources	- Recognition programming languages like the Device Description Language (DDL) - Strategic agent
g. Optimized extensibility	- Reconsideration algorithm for enhanced Real-Time Transport Protocol (RTP) scalability - Parallel scalability optimization algorithms
h. Intelligent sensing and tracking	- Wireless sensors networks (WSN) - Radio Frequency Identification (RFID)

control the distributed mini-nets (Guo et al., 2017). The management and control are taking part in three levels, which are networks, services, and servers.

On the level of the entire networks, we should employ efficient technologies to monitor and supervise the beneath distributed multi-networks centrally. The recommended solution for the best network connectivity is using SDN integrated with NFV, as suggested in (Akyildiz et al., 2016) and (Hakiri et al., 2015).

SDN is a unified controller that separates the control plane from the data plane. This abstraction improves the underlying network performance. Moreover, it provides a common infrastructure for multiple heterogeneous networks. The researchers in (Hakiri et al., 2015) and (Qin et al., 2014) are recommending the use of the SDN controller for the future IoT.

The main idea behind NFV is to virtualize network functions. This abstraction decouples the functions from the physical hardware, allowing the network functions to be centrally managed and controlled through the cloud servers. It also enables sharing and reusing the virtualized functions all over the networks (Akyildiz et al., 2016).

In regard to the services level, there is a need to employ technologies that give the IoT users the advantage of entertaining the cloud services without worrying about the comprehended operating systems and hardware. OSGi is a framework used in the software development process to allow the reusability of components via services in the cloud while hiding the implementation of the components from each other (Helel, 2016). There is also the packet scheduler, which categorizes received packets to enable the system to provide the expected quality of service by either assigning the packets as guaranteed services or as controlled-load services (Nader, 2015). Similarly, the traffic shaper manages the disorderly packets received in the system by regulating them to prevent generating unnecessary traffic congestion in the network. In addition, it disables the unexpected higher usage of the system bandwidth (Nader, 2015).

On the servers level, the hypervisor is responsible for creating and managing virtual machines lying under it. In case of specific server failure, the hypervisor acts as an interface between the failed server and others to enable other servers in the network to take on the responsibility of performing the required task. Therefore, it enables the fault-tolerance feature. Furthermore, the load balancer forwards the requested tasks to appropriate servers based on the server holding the least load (Nader, 2015).

4.2 Transparency

Dividing the functionalities into multiple separate layers satisfies transparency because the division strategy decouples the orthogonal features and encourages their independent development without any interference between the tasks. The transparency simplifies detecting errors and resolving them quickly. The researchers in (Guo et al., 2017) and (Ren et al., 2017) recommend using the TC to increase the scalability of the IoT. The main idea behind the TC is to decouple the software from the hardware machine, as well as to decouple the computing component from the storage component. Moreover, multiple types of middle-wares, such as the Atlas and the Aneka, could achieve the desired transparency since they decouple the functionalities on multiple layers. Using “Atlas” middleware and running separate prongs of it on each IoT layer debated for achieving scalability by the author in (Helel, 2016), who proposed centric architecture for a scalable smart city called “CEB”.

4.3 Virtualizations

The virtualized object can hold the digital representation of the real object to simplify the process of locating the real physical object and communicating it with other virtual objects in the IoT (Sarkar et al., 2014). Various virtualizations software can create virtual objects, such as the “VirtualBox”, which is free and well suited for small multiple distributed networks. Furthermore, it has an elastic memory that can hold up various virtual machines and supports the remote devices connectivity (Hess & Newman, 2009). There is also the “Citrix Xen”, which is fast and high-performance virtualization technique

that provides ubiquitous connectivity to its users (Hess & Newman, 2009). Citrix incorporates the hybrid complex devices, platforms, and technologies into one flexible virtualized solution.

4.4 Reliable Communication Systems

Wireless communication is always posing challenges over wired communication, such as high interference, unstable connections, and limited bandwidth (Guo et al., 2017). Thus, a suitable protocol package, such as the "IETF" should be employed to overcome these challenges. IETF developed a suite of standards and protocols that support the connections between multiple different services and applications in an IoT environment (Sheng et al., 2013). IPv6 is a standard protocol developed by IETF for identifying and locating connected devices to the Internet through their IP addresses. It can address huge distributed locations because it is global, stable, and extensible protocol. However, it has some challenges related to limited bandwidth and low power (Sheng et al., 2013). Thus, IETF developed a better protocol called CoAP. CoAP is developed by the IETF to satisfy the IoT requirements, because dealing with IoT requires real-time responses from cloud applications and exchanging of big data through numerous tiny and cheap sensors. CoAP runs over UDP, which allows multicast communication (Kovatsch et al., 2014). It shores alternative transports and preserves interoperability among different applications (Cirani et al., 2014).

4.5 Cross-Platforms and On-Demand Services

Unified resources management platforms can provide the cross-platforms and supply services or applications only when needed. A rigid platform is the "Fog computing", which extends cloud computing to the edge of the network. This technique enables transferring the management of services and applications from the cloud into the edge, which offers many advantages over cloud management, such as fast service delivery, enhancement in the IoT scalability, controlling network traffic, and decreasing energy consumptions (Yi et al., 2015). It is claimed that Fog computing is the most suitable platform for the IoT due to its numerous characteristics that dominate the heterogeneity in IoT devices (Bonomi et al., 2012). Moreover, there is the open application platform, which provides reusable functions and open Application Programming interface (API) in an IoT environment (Chen et al., 2014). It is recommended to manage the sensing devices and actuators using the sensing and gateway platform. Because it provides one standard interface module connecting the physical interfaces of all sensors, gateways, actuators, and readers involved in an IoT. The platform has many features that make it a strong enabling technology, such as hosting a central interface, self-adaptive, and self-configuration (Chen et al., 2014).

4.6 Cognitive Understanding of Involved Resources

Cognitive understanding assists in minimizing the amount of data retrieved from the vast cloud, which is a helpful technique to use both applications and data wisely.

Programing languages, such as the Device Description Language (DDL), which is developed to eliminate the need to write new software for every newly added device to the network, is a vital scalability requirement. This language adds a description of each device type along with its services, configuration, and the way it works (Riedl & Naumann, 2017). Thus, it can be utilized within the sensors' platform to add written specifications for each sensor plugged into the cloud. This recognition of sensors achieves the required common cognitive understanding between them (Helel, 2016).

The scalable cloud-sensor architecture for the IoT has been designed, and it was recommended to add a strategic agent on the edge layer of it (Helel, 2016). The purpose of adding the agent is to look up and down the layer to understand the application and the data. It is a strategically important entity because the applications are pushed into the cloud instead of being on the beneath the layers. Thus, there should be coordination and outsourcing going from the edge layer to enhance the scalability and add smartness to the IoT infrastructure.

4.7 Optimized Extensibility

In the IoT environment, we need to connect the diverse devices used in our daily life with the cyber digital world. This physical-virtual connection is not easy and needs optimization algorithms to ensure its scalability and efficiency.

The Real-Time Transport Protocol (RTP), which is used on the Internet for streaming real-time applications such as audio and video, is facing significant challenges when a massive number of users join a multicast session at nearly the same time. The generated flood of packets in the Real-Time Control Protocol (RTCL) that is mainly responsible for transmitting control information is producing a congestion problem. To solve this problem, a timer algorithm called reconsideration is proposed. This algorithm can reduce the initial flood of packets, and it can scale-up the number of joined sessions from anywhere (Rosenberg & Schulzrinne, 1998).

Moreover, the parallel optimization algorithms enhance the scalability because they consider the number of involved processors in processing a specific problem. As well as, they consider the size of the problem being solved. Parallel algorithms provide a metric that is very helpful in measuring the linearly increasing performance in a scalable environment.

4.8 Intelligent Sensing and Tracking

There are a massive number of small, lightweight, and cheap sensors and actuators blended all over our daily lives representing a network of wireless sensors known as WSN. The WSN enables ubiquitous sensing throughout the pervasive IoT networks (Gubbi et al., 2013). The autonomous sensors in the WSN are spatially spread over multiple physical locations to sense and collect specific information regarding the surrounding environment. However, the network centrally controls all the small sensors.

RFID are tiny sized memory chips that can save, update, and delete data. The RFID tag can handle various useful information besides only recognizing identity. The tag can store geographic locations, as well as nearby physical information. It can also access memory's history to act based upon historical information. Adding flash-memory-aware storage and buffer enable the scalability in the IoT (Le-Tuan et al., 2020). Thus, combing a security framework with RFID enables an excellent secure and scalable operation of sensing and tracking technologies for the IoT (Ray et al., 2014).

5. PROPOSED REFERENCE MODEL ARCHITECTURE

After investigating the challenges associated with the scalability requirement, and after studying the advanced technological solutions to achieve efficient scalability in the IoT environment, we propose a fundamental change in the current IoT architecture. The proposed architecture for the future scalable IoT is illustrated in figure 1.

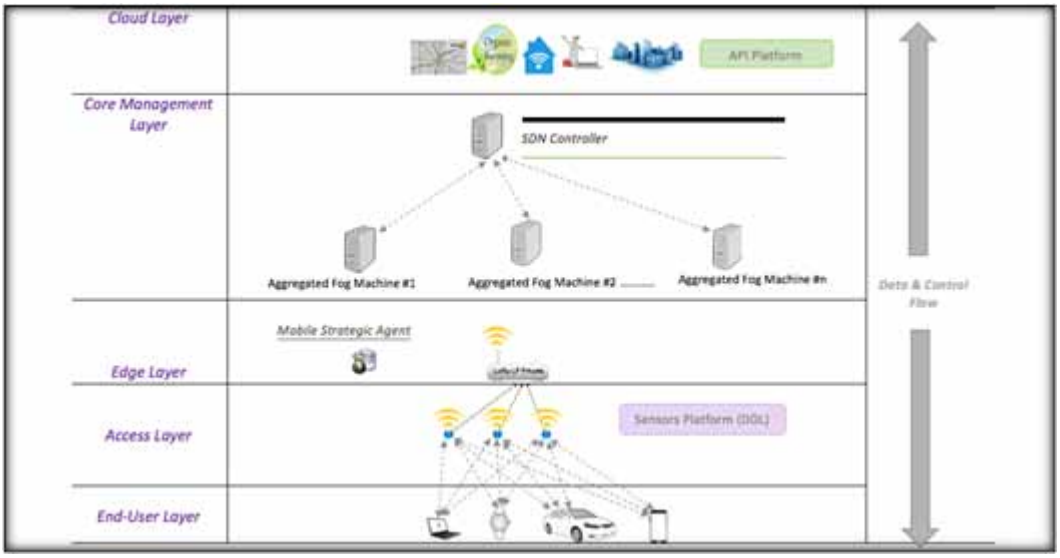
From figure 1, we notice that the proposed reference model is integrating robust solutions to compose one large-scale system. It is a generic layered architecture consisting of five layers, which are end-user, access, edge, core management, and cloud. Note that, the data and the control are flowing all over the architecture. Following is a detailed explanation of each one of the introduced five layers and the main scalability requirements that it satisfies:

1. **End-user layer:** It is the layer including all the users' terminals, devices, equipment, machines, etc. that needs to be connected to the cloud.

This layer should use the (CoAP) protocol to satisfy the reliable communication systems scalability requirement that enables strong connection to the upper layers:

Satisfied scalability requirement: d

Figure 1. Proposed reference model for scalable IoT



2. **Access Layer:** It includes the sensors that collect data from end-user layer and forward them into the edge layer. The functioning of these various sensors should be controlled and managed centrally. Thus, a sensors platform is added to the access layer to do the controlling task. It adds description of each connected device using the Device Description Language (DDL) to be able to understand all devices, their job, and the way they function. This cognitive understanding scalability requirement achieves interoperability between all connected terminals. In addition, the use of the sensors' platform achieves the intelligent sensing and tracking of the involved resources scalability requirement:

Satisfied scalability requirements: f and h

3. **Edge layer:** Includes OSGi gateway that takes collected data from the access layer and forward them to the rest of the internet. This gateway supervises the sensors under it to turn-off all idle sensors and inactivate their links. This act helps significantly in decreasing the power and energy being consumed. In addition, the gateway that is controlling all underneath sensors satisfies the central management and control on the services level. As well as, it accomplishes the cross-platforms and on-demand services salability requirements.

The edge layer includes strategic mobile agent. Its role is to add smartness to the architecture even if the involved devices are not smart. That is achieved by enabling to create instances from the agent and move them to the desired applications whenever there is data/task needed; and then return back to the edge layer to allow the gateway to forward only required data to the internet. The agent should follow both wired and wireless transmission control protocols during its migration to support all types of connections. This approach helps in using both application and data wisely, as well as, it satisfies the cognitive understanding scalability requirement:

Satisfied scalability requirements: a, e, and f

4. **Core management layer:** This layer represents a variety of networks communication methods to successfully communicate data from beneath layers up to the cloud applications. It includes all fog machines that collect data from beneath devices and then, forward them to aggregated fog machines. Note that, fog computing satisfies the cross-platforms and on-demand services scalability requirement.

All the work is performed under the control of the SDN, which decouples the data from the control and satisfies the transparency scalability requirement. The physical servers are connected to the cloud through this layer. They are organized into multiple virtual machines by aggregating every small set of neighboring servers into one virtual machine, and then connects all the virtual machines to the parent hypervisor physical server using routers. This virtualization scalability requirement assists in aggregating and sharing resources among multiple users who are geographically isolated from each other. In addition, it has the advantage of resources management. The parent centralized hypervisor physical server is added on the top of all underlying virtual fog machines to control them and ensure their connectively. This approach of controlling the work ensures fault-tolerance. The hypervisor does also the job of load balancing, which control the traffic flow between servers since it checks every server load and distribute the incoming traffic load over servers based on the least-connect algorithm. Hence, the central management and control on the entire network scalability requirement is satisfied using the SDN, while on the servers' level, it is satisfied using the hypervisor.

Satisfied scalability requirements: a, b, c, and e

5. **Cloud layer:** Has all the smart applications that are accessed from beneath layers through the internet. It should include scalability optimization algorithms to achieve the optimized extensibility scalability requirement.

Moreover, the cloud layer includes API platform to centrally manage and control the processing of all applications in the cloud, which satisfies the cross-platforms and on-demand services scalability requirement.

Satisfied scalability requirements: e and g

6. CONCLUSION

This study investigates previously performed efforts in the field of scalable IoT architecture. It begins by investigating the challenging open problems that arise when trying to achieve the scalability, and the solutions to overcome them. Then, it highlights eight primary requirements that satisfy the scalability in the IoT, followed by their corresponding key enabling technologies. Moreover, the study came-up with a new scalable architecture for the future IoT.

Implementing the proposed scalability requirements and applying their recommended solutions result in lots of benefits, such as increasing the number of users being served and providing ubiquitous connectivity to them. In addition, the proposed architectural solution allows the connection of large-scale heterogeneous IoT devices in a fully integrated architecture that controls heavy traffic and facilitates the fault-tolerance features in the network.

REFERENCES

Akyildiz, I. F., Nie, S., Lin, S., & Chandrasekaran, M. (2016). *5G roadmap: 10 key enabling technologies*. .10.1016/j.comnet.2016.06.010

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). *Fog Computing and Its Role in the Internet of Things Characterization of Fog Computing*. Academic Press.

Chen, S., Member, S., Xu, H., Liu, D., Member, S., Hu, B., & Wang, H. (2014). A Vision of IoT. *Applications, Challenges, and Opportunities With China Perspective*, *1*(4), 349–359.

Cirani, S., Davoli, L., Ferrari, G., Medagliani, P., Picone, M., & Veltri, L. (2014). *A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things*. .10.1109/JIOT.2014.2358296

CompTIA. (2015). *Sizing up the Internet of things*. Retrieved from https://www.comptia.org/resources/sizing-up-the-internet-of-things

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Guo, H., Ren, J., Zhang, D., Zhang, Y., & Hu, J. (2017). A scalable and manageable IoT architecture based on transparent computing. *Journal of Parallel and Distributed Computing*. Advance online publication. doi:10.1016/j.jpdc.2017.07.003

Hakiri, A., Berthou, P., Gokhale, A., & Abdellatif, S. (2015). *Publish/Subscribe - Enabled Software Defined Networking for Efficient and Scalable IoT Communications*. Academic Press.

Helel, S. (2016). *A Scalable Cloud-Sensor Architecture for the Internet of Things*. Retrieved from https://www.youtube.com/watch?v=qqMuCOQyfxI

Hess, K., & Newman, A. (2009). *Virtualization technologies compared. online article from the book, Practical Virtualization Solutions: Virtualization from the Trenches*. Pearson Education, Inc. https://www.computerworld.com/article/2528781/virtualization/virtualization-technologies-compared.html

King, J., Bose, R., Yang, H., Pickles, S., & Helal, A. (2006). *Atlas : A Service-Oriented Sensor Platform*. Academic Press.

Kovatsch, M., Lanter, M., & Shelby, Z. (2014). *Californium : Scalable Cloud Services for the Internet of Things with CoAP*. Academic Press.

Le-Tuan, A., Hayes, C., Hauswirth, M., & Le-Phuoc, D. (2020). Pushing the Scalability of RDF Engines on IoT Edge Devices †. *MDPI*, *20*(2788), 1–32. doi:10.3390/s20102788 PMID:32422961

Lee, S., Bae, M., & Kim, H. (2017). Future of IoT Networks: A Survey. *Applied Sciences (Basel, Switzerland)*, *7*(10), 1072. doi:10.3390/app7101072

Moens, P., Bracke, V., Soete, C., Vanden Hautte, S., Avendano, D. N., Ooijevaar, T., & Van Hoecke, S. et al. (2020). Scalable Fleet Monitoring and Visualization for Smart Machine Maintenance and Industrial IoT Applications. *MDPI*, *20*(4308), 1–15. doi:10.3390/s20154308 PMID:32748809

Nader, F. M. (2015). *Computer and Communication Networks* (2nd ed.). Prentice Hall.

Qin, Z., Denker, G., Giannelli, C., Bellavista, P., & Venkatasubramanian, N. (2014). *A Software Defined Networking Architecture for the Internet-of-Things*. Academic Press.

Ray, B. R., Abawajy, J., & Chowdhury, M. (2014). Scalable RFID Security Framework and Protocol Supporting Internet of Things. *Computer Networks*, *67*(March), 89–103. Advance online publication. doi:10.1016/j.comnet.2014.03.023

Rehman, A., Rehman, S. U., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and Privacy Issues in IoT. *International Journal of Communication Networks and Information Security*, *8*(3), 147–158. doi:10.4018/978-1-60960-848-4.ch013

Ren, J., Guo, H., Xu, C., & Zhang, Y. (2017). Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing. *IEEE Network*, *31*(5), 96–105. doi:10.1109/MNET.2017.1700030

Riedl, M., & Naumann, F. (2017). EDDL - Electronic Device Description Language. Academic Press.

Rosenberg, J., & Schulzrinne, H. (1998). *Timer Reconsideration for Enhanced RTP Scalability*. Academic Press.

Sarkar, C., Prasad, R. V., & Rahim, A. (2014). *A Scalable Distributed Architecture Towards Unifying IoT Applications*. Academic Press.

Shen, Y., Zhang, T., Wang, Y., Wang, H., & Jiang, X. (2017). MicroThings: A Generic IoT Architecture for Flexible Data Aggregation and Scalable Service Cooperation. *IEEE Communications Magazine*, *55*(9), 86–93. doi:10.1109/MCOM.2017.1700104

Sheng, Z., Yang, S., Yu, Y., Vasilkos, A., & Leung, J. (2013). A Survey on the IETF Protocol Suite for the Internet of Things. *Standards, Chalenges, and Opportunities*, (December), 91–98.

Shimojo, F., Kalia, R. K., Nakano, A., & Vashishta, P. (2001). *Linear-scaling density-functional-theory calculations of electronic structure based on real-space grids : design, analysis, and scalability test of parallel algorithms*. Academic Press.

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). *Fog Computing : Platform and Applications*. .10.1109/HotWeb.2015.22

Zarko, I. P., Soursos, S., Gojmerac, I., Ostermann, E. G., Insolvibile, G., Plociennik, M., . . . Bianchi, G. (2017). Towards an IoT Framework for Semantic and Organizational Interoperability. GIoTS 2017 - Global Internet of Things Summit Proceedings. doi:10.1109/GIOTS.2017.8016253

Manal M. Khayyat received the B.Sc. degree (Hons.) in Computer Science from King Abdulaziz University, Saudi Arabia, in 2007 and received the M.Sc. degree of Applied Science in Quality Systems Engineering from Concordia University, Canada, in 2015. She also received a Ph.D. degree in Computer Science from King Abdulaziz University, Saudi Arabia, in 2020. She worked at the IT department of Effat University, Saudi Arabia, from 2007 to 2010. Then, she worked as a lecturer at King Abdulaziz University, from 2012 to 2019 and she is currently working as an assistant professor at Umm Al-Qura University, Saudi Arabia. Her research interests include computer vision, image processing, natural language recognition, deep learning, and the Internet of Things.

Nadine Akkari received her PhD degree in Telecommunications Networks from National Superior School of Telecommunications (ENST), Paris, France, in 2006. Dr. Akkari is specialized in Next Generation Networks: mobility and QoS provisioning, 5G, SDN, wireless sensor networks and IoT. Her research led to international collaborations and research grants. She has number of publications in international journals and conferences. She is a senior member of IEEE, Editorial board member of Adhoc Elsevier journal, and member of Lebanese Order of Engineers.

International Journal of Hyperconnectivity and the Internet of Things
Volume 6 • Issue 1

The Effect of the Use of Social Media on Organizational Commitment

Pavithra Salanke, New Horizon College of Engineering, India*
Osibanjo A. Omotayo, Covenant University, Nigeria
https://orcid.org/0000-0003-1793-2763
Deepak K. V., Bangalore Institute of Technology, India

ABSTRACT

Social media offers an opportunity for firms to generate value through the facilitation of employee experiences. Using social media, business creates an environment of collaboration. This article suggests that organizational commitment of employees is prejudiced by social media usage. The study attempts to answer how social media helps in improving the organizational commitment in terms of affective, normative, and continuance commitment. The study was empirically tested by using the employee survey data collected from IT employees working in Bangalore. The paper concludes with a brief of the usage of social media in IT companies and its consequences.

KEYWORDS

Organization Commitment, Social Media

1. INTRODUCTION

The concept of employee commitment was emphasized several decades ago when Katz (1964) opine that "workers behaviour, essential for effectiveness includes" joining and continuing with the firm, carrying out explicit role obligation, and engaging in innovative and spontaneous activity that goes beyond defined roles. Katz (1964) further assert that engaging good employees is imperative for an organisation but a critical and even greater responsibility is the organization's ability to create a committed workforce thus; the need for managers to understand the concept of commitment and how it can be influenced within the work environment must be studied by managers. As a result of today's competitive and vigorous world every firm is facing new challenges regarding competitive organizational performance and creating committed workforce (Anthony, 2017). In this global and dynamic setting, no organization can compete at the maximum level, unless its employees are committed to the objectives of the organizations. Hence, it is important to understand the concept of commitment and how it can be influenced in the work environment for optimal performance. Conceptually, an employee commitment is a psychological state that binds the employee to the organization. (Bipeledei & Rachel, 2018). This implies that employee commitment is a connection between an employee and the firm such that he/ she want to continue serving the organisation

DOI: 10.4018/IJHIoT.294896
*Corresponding Author

and to help it achieve its objectives. Nevertheless, Meyer, Stanley & Parfyonova (2012) used a multidimensional approach to describe commitment and consider it to have affective, continuance and normative perspectives which will be further explored in this study.

The challenge of new employees leaving the organization as a result of low commitment after they have been trained remains critical. Streams of research acknowledged that a good number of organisations are contending with issues like employee retention, job performance, productivity and various employee engagement outcomes including employee commitment (Gonzalez, Leidner, Reimenschneider & Koch, 2013 & Xiongfei, Xitong & Douglas, 2016). More so, it is indisputable that encouraging employees to discharge their duties meritoriously and be committed to firm towards achieving organizational goals and objectives is one of the weighty challenges for many firms as opine by (Akinbode, Opayemi & Sokefun, 2013).

Several studies have been done on finding the new methods to how to increase the commitment of the employees in the organization in other to achieve success (Mkhyzer& Rehman, 2012; Bipeledei& Rachel, 2018). Madu, Asawo and Gabriel (2017) assert that the quest for organizational success in this 21st century depends on the firm's ability to promptly respond to the unpredictable work environment, having a multi-skilled workforce as well as engaging workers who will feel connected physically, cognitively and emotionally to work roles. One of the key elements of the employee engagement framework is the deep affective involvement of workers who are active in their jobs. Undoubtedly, twenty first century firms are fast embracing the use of social media in recent times as its importance cannot be overemphasized. Essentially, social media have transformed communication in people's lives with their wide spread growth and its application (Xiongfei, *et al*, 2016). The usability and application of social media has even penetrated the workplace, facilitating organizational communication and knowledge work which was impossible in the past (Akinbode, *et al,* 2013). Recently, social media tools have provided a new tool for organizational to communicate and internal social media systems are being used by firms to help new employees learn about their jobs, their colleagues and the organization (Gonzalez, *et al*, 2013).

Furthermore, several researchers not only assert social media has been facilitating organizational communication and knowledge work but further opine that there is a strong interest to use social media tools to improve the communication, establish social relationships among workers and thus improving the level of trust between themselves, getting new acquaintances, exchanging information, and collaborating toward a common objective (Atzori, Lera, & Morabito, 2014&Chang & Hsiao, 2014). For several decades, scholars in human resource have been emphasizing the importance of organizational commitment of employees as a key variable to employee turnover and success (Van Maanen, 1975; Mowday, Porter & Steers, 1979; Balfour & Wechsler 1996; Larson &Fukami, 1984). But scant studies have emerged on how employee commitment can be facilitated through the use of social media by firms. (Deans 2011) also opine that the ability of internal social media networks has not been exploited by many companies and that many firms remain skeptical about social media advantages. Very little is known about the benefit derived by the use of corporate social media in general and the use of internal social networking networks in particular (Andriole, 2010).

The impact of social media uses and its impact on organizational commitment will be discussed in this paper. We empirically examined whether social media has an effect on organization commitment. This paper provides the literature review, then the model and hypothesis framed. This is followed by research methodology, analysis and discussion.

2. LITERATURE REVIEW

2.1. Social Media

Social media is a platform through which employees connect or act as a team with one another inside and outside the organizations (Daowd, 2016,). Social media not only provides a complete knowledge

management but also provides very simple and flexible tools to the management (Cao & Ali, 2018,). Currently, the available social media applications (e.g. Facebook, whatsapp, twitter and LinkedIn) are playing an important role in human interaction within organizations and employees use online applications at workplace because these applications bring efficiency in operations. Researchers however assert that organizations may face opportunities, threats, weaknesses and strengths (SWOT) owing to use of social media (Kane, 2017; Tajudeen, Jaafar, &Ainin, 2018). As a matter of fact, social media can be a weakness for the firms when it negatively affects its productivity and may become the strength for the organization when it is used to develop a relationship and used to build the capacity of the employees (Tajudeen, *et al*, 2018). Even though social media plays an important role on an employees' job performance, inadequate importance was given to the use of social media at workplace as regards employee commitment.

Basically, there are number of factors that influence job performance or the commitment of an employee in an organization. Individual ability, knowledge and skill are examples of internal factors while the working environment, characteristics of apportioned tasks, incentive, tools, organizational structure and Human Resource Management practices are examples of external factors (Lu, Guo, Luo, & Chen, 2015; Mericoz, 2015.; Sani & Maharani, 2015.). Moreso, organizational support at workplace increases organizational commitment, which tends to increase the individual and collective performance of employees (Haque & Yamoah, 2014;) Therefore, notionally, we can assume that instances like the use of social media in workplace can drive employee commitment.

In addition, social media allows its users to build of social activity and also allows its users to develop and distribute user-generated content without any time as well as space constraints (Carr & Hayes, 2015; Kaplan & Haenlein, 2012). Social media is a 3-part network: information-producing devices, information devices, and people who use that information for their official and personal purposes (Carr& Hayes, 2015). Social networks provide their users with search and privacy functionality. They also connect with a no. of users who share and communicate with each other. (Gerald, 2012).

Many social network apps like face book, YouTube, twitter, blogs, Skype, WhatsApp and photo sharing sites a are available that organizations can use for their official purposes. Macnamara & Zerfass, (2012) opine that private and special social networks are used for communication in the organizations like Yammer, smaller organizations use podcasts.

Social media usage is classified in 3 ways. (Ali-Hassan, Nevo, & Wade, 2015):

- Social media is generally used for socializing with people and strengthening their relationships among friends, relatives and colleagues.
- It is used for the affective need of pleasure and emotional experiences.
- For the cognitive use, to fulfill their needs by freely searching for information and gain more knowledge.

Prior studies have provided tentative insights into the capability of social media. However, their implementation in the work environment remains contentious. On the deleterious side, social media have been attributed to reducing productivity and increasing disturbance (Xiongfei, *et al*, 2016).

2.2. Organization Commitment

Organizational commitment is typically characterized as the strong desire to remain a part of the organization. Field & Buitendach, (2011) in their study, discovered that happiness and work engagement have predictive importance for affective organizational commitment.

Ashraf, Jaffri, & Sharif (2012) study also reveals that mission of the organization has a greater impact and strong positive association with organizational commitment. Schaufeli & Bakker, (2003) study revealed that firm's success is inevitable without a greater level of organizational commitment. Albdour & Altarawneh, (2014) further opine that employees who are in a satisfying work environment

usually show high level of job engagement and organizational engagement and this in turn will lead to organizational commitment.

There are several definitions of organizational commitment but the most comprehensive and popular of those definitions is that of Meyer, Stanley & Parfyonova (2012) who describe commitment using a multidimensional approach and cogitate it to have affective, continuance and normative angles. The affective dimension of commitment refers to an emotional connection to and engrossment with an organisation; continuance commitment indicates the apparent costs of exiting an organisation; and normative commitment refers to the felt obligation to support and remain an employee of the organisation. Notionally, it can be determined from the aforementioned definition that employee commitment is a bond between the employee and the organisation such that the employee wants to continue serving the organisation and to help it achieve its objectives.

2.3. Social Media and Affective Commitment

The affective commitment refers to an emotional connection and inclination to an organisation.

Firm's cannot but encourage their employees to be committed because, (Mugizi, Bakkabulondi, &Bisaso, 2015) for instance suggest that organizational commitment heightens knowledge sharing between employees. This implies that knowledge sharing as a development whereby an employee exchanges the knowledge he/ she possesses with other members for them to understand, apply and develop that knowledge. Accordingly, with knowledge sharing, information, skill or expertise are reciprocally exchanged among coworkers in the organisation (Mugizi, et al; 2015). Due to the nature of social media as an effective social networking platform where organizational members meet, connect, and share information, it will only be imperative for an organisation to use it as a tool for knowledge sharing. This is because social media consist of communication tools, providing multiple communication channels in both social and work environments (Centrukaya& Rashid, 2018). Madu, *et al* (2017) assert that engaging workers with tools and conducive work environment will make employees connected physically, cognitively and emotionally to work roles.

Thus, social media has become the need of every organization in competitive and rapidly changing environment.

2.4. Social Media and Continuance Commitment

Scholars in this context generally believe that employee commitment is important because it enhances employee job performance and lessens the frequency of employees exhibitingundesirable behaviour (Bipeledei, E & Rachel, D, 2018; Centrukaya& Rashid, 2018). Centrukayo& Rashid (2018) further assert that employees are ready to accept organisational change and enhances knowledge sharing among the employees in order to be dedicated.

Continuance commitment refers to an awareness of the cost associated with leaving the organization (Meyer, *et al*, 2012). The potential cost of leaving an organization includes the threat of wasting the time and effort spent acquiring nontransferable skills, losing attractive benefits, living seniority and having to uproot family and disrupt personnel relationships (Meyer, *et al*, 2012) Apart from the cost involved in leaving the organization, continuance commitment will also develop as a function of a lack of alternative employment opportunities. When employees are encouraged to use social media tool to work, their relationship with other members of the organization can be enhanced as social helps to build relationships.

2.5. Social Media and Normative Commitment

Normative commitment refers to the employee's feeling of obligation to remain with the organization. Employees with high level of nomination commitment feel that they ought to remain with the organization because they are indebted to it. Meyer, *et al,* (2012) suggest that the feeling of commitment to remain with an organization may result from the internalization of nominative influences exerted on an employee.

Social media provides a better forum tounderstand how individuals build their networks, exchange and share information with eachother. Ali-Hassan,Nevo,&Wade,(2015) opine that social media is generally used for socializing with people andstrengthening their relationshipsamongfriends,relat ivesandcolleagues, fulfil touching need of pleasure and emotional experiences. Alli-Hassan, *et al* (2015) further posit that employees use social media for cognitive use to fulfill their needs by freely searchingforinformationandgain more knowledge. When employees have access to these benefits from their colleagues and superiors, they feel obligated to remand with the firm.

2.6. Theoretical Nexus Between Social Media and Employee Commitment- Social Exchange Theory

Social exchange perspective proposes that employee's behaviour is the result of an exchange relationship. Social exchange theory according to (Redmond, 2015) involves individual voluntary behaviour that originates from a sequence of social interactions. Social exchange also refers to the common interactions between two or more parties that are centered on voluntary actions of reciprocity (Wylie & Toni, 2016). Redmond (2015) described the process of social exchange as a reciprocity activity that begins with an individual giving an input into a relationship and receives an output from the same relationship.

According to social exchange theory, Cheruyak-Hai and Rabenu (2018) further posited that reciprocity-based relationships have implications for behaviour and enhance positive work attitudes and performance. Cheruyak-Hai and Rabenu (2018) also referred to social exchange as voluntary actions of individuals that are motivated by the principle that when one person does another a favour, there is an expectation of some future return that is not stipulated in advance.

This implies that when an employee sees or observe that organisational, supervisor, and coworker support to his work experienced by him through shared knowledge, through the use of social media, this will foster the employee disposition positively and have an added effect on work outcomes like motivation and employee commitment. This implies that when workers feel supported and valued by employers, they will return the favour by exhibiting positive work outcomes.

In addition, Tianan, Yu-Ming. Mingjing, Yuanling, Jianwei, Qian and Lai-Chu (2015) asserted that strong support from colleagues and superiors improves work environments by relieving employee stress, which enhances job satisfaction and performance. Tianan, *et al,* (2015) also opined that superiors are expected to give their subordinates professional support and resources for development. Employees with this kind of experience and feelings will be obliged to pay the firm back positively by being committed. Furthermore, Dunn, Daastor& Sim (2012) in their studies in the US identified that transformational leadership practice of inspiring the vision of the firm and encouraging the input of other employees in an organization is associated with employee commitment. This however was not the same result in another study in other climes from their study. Thus, this necessitate calls for further research on the constructs in other contexts such as the developing countries like India.

3. RESEARCH HYPOTHESIS

H_1: Usage of Social Media has no effect on affective commitment.
H_2: Usage of Social Media Usage has no effect on continuance commitment.
H_3: Usage of Social Media has no effect on normative commitment.

4. RESEARCH METHODOLOGY AND DATA COLLECTION

The Study explores the effect of social media usage on organization commitment in Bangalore IT Sector. For the Survey a 5-pointLikert scale was used for the data collection. The data was gathered online through Google forms. Part A of the questionnaire dealt with the demographic details of the

employees and Part B had the questions on Organization commitment. The sample size of the survey was IT employees working in Bangalore. For the analysis Simple Random sampling method was used. 224 responses were recorded and used for the analysis.

Figure 1 illustrates our model of the research. The model shows the effect of use of social media in the organization commitment in three ways- Normative, Continuance and affective.

5. RESULT ANALYSIS

Table 1 depicts the statistical analysis of the respondent's demographic characteristics ranging from gender, age, work experience, educational qualification, and the current positions of the respondents as at the time of filing this report. The gender distribution of the respondents shows that out of 224 respondents, 67.0% were male, while 33.0% were female. This suggests that most of the respondents were male. This could be attributed to the nature of ICT related jobs which are male-dominated. It was also discovered that most of the respondents were found to be within the age ranging from 21-40 years. This also implies that most of the people in ICT related businesses were young people. The work experience of the respondents spread across less than 6 months to 10 years. This suggests that a good number of respondents have reasonable work experience, particularly in their present job. Regarding the educational qualification of the respondents, it was discovered that most of the respondents have Master degrees. This suggests that all the information provided by the respondents can be said to be reliable. Besides, most of the respondents are associate cadre in their place of work which represents 56.3%, 28.1% of the respondents were managers, while 15.6% of them were supervisors.

Table 2 shows the outer loading, while Table 3 depicts the R-square values, T-statistics and total effects of all the observed variables. This suggests that social media usage has a major impact on organizational (affective, continuance and normative) commitment. Also, all items are reflective, and the minimum acceptable value for a factor loading is 0.70. It was discovered that most of the constructs have values greater than 0.70, and none is less than 0.40. This implies that they all have composite reliability. Cronbach α reliability coefficient was used to evaluate thedegree of internal consistency. The outcomes showed that Cronbach Alpha values are higher than the minimum standard of > 0.70. This implies that the reliability analysis of all the constructs has high internal consistency. The factor a loading of these items was used to calculate the average variance extracted (AVE). Since all the constructs average variance extracted values are above 0.5, therefore, it gives room for the establishment of convergent validity.

This study investigated the impact of use of social media on organization commitment with relation to IT sector in Bangalore. The results from the study were interpreted using key statistics such as structural path coefficient, the R-square value, t-statistics as well as the p-values, which determines the level of significance of the study. The pictorial Depiction of the results is shown in Figure 1. The Partial Least Square (PLS) model, as shown in Figure 1, shows the path coefficient

Figure 1. Research model

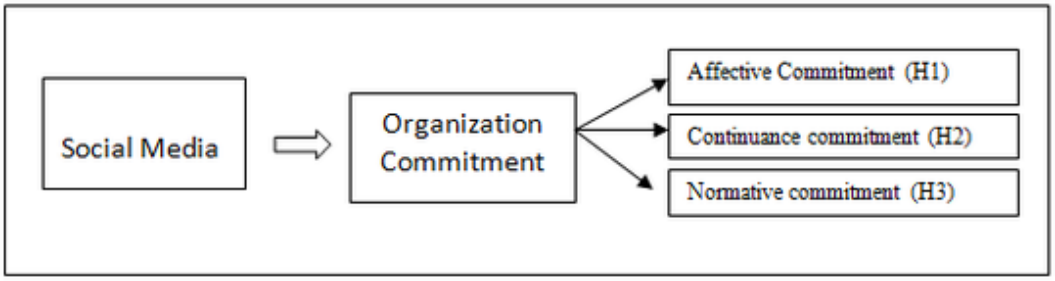


Table 1. Respondents demographic characteristic

	Frequency (N)	Percentage (%)
Gender		
Male(M)	150	67.0
Female(F)	174	33.0
Total	**224**	**100.0**
Age		
21-30 years	124	55.4
31-40 years	81	36.2
41-50 years	17	7.6
51-60 years	2	.9
Total	**224**	**100.0**
Work Experience		
(1 - 2)years	48	21.4
(3-5)years	43	19.2
(6-10)years	45	20.1
More than 10 years	17	7.6
6months-1 year	38	17.0
Less than 6 months	33	14.7
Total	**224**	**100.0**
Educational Qualification		
Bachelors	93	41.5
Master's Degree	131	58.5
Total	**224**	**100.0**
Position		
Manager	63	28.1
Supervisor	35	15.6
Associate	126	56.3
Total	**224**	**100.0**

and determines the level of relationship between social media usage and organizational (affective, continuance and normative) commitments.

The entire three formulated hypothesis presented in Table 3 showed significant relationships at 0.05. Specifically, the path coefficient for hypothesis one showed that social media usage significantly influenced affective commitment at (β=0.468, R^2=0.219, T-value=4.798>1.96, P-value =0.000 <0.01). The path coefficient value of 0.468 suggests a moderate relationship between social media usage and affective commitment, while the R^2 value of 0.219 implies that 21.9% variation in affective commitment can be explained by social media usage.

In a related development, the path co-efficient for hypothesis two also revealed that usage of social media has a very good impact influence on continuance commitment at (β=0.386, R^2=0.149, T-value=4.253>1.96, P-value =0.000 <0.01). The path coefficient value of 0.386 indicates a fair

Table 2. Construct reliability and validity

		Loading	AVE	Compose Reliability	Cronbach's Alpha	RhO.A
Constructs		**≥ 0.7**	**≥0.5**	**≥ 0.8**	**> 0.7**	
Social Media Usage (SMU)			0.660	0.886	0.827	0.833
	SMU1	0.764				
	SMU2	0.754				
	SMU3	0.827				
	SMU4	0.898				
Affective Commitment (AC)			0.631	0.894	0.850	0.861
	AC1	0.774				
	AC2	0.870				
	AC3	0.856				
	AC4	0.613				
	AC5	0.832				
Continuance Commitment (CC)			0.653	0.904	0.868	0.888
	CC1	0.813				
	CC2	0.827				
	CC3	0.752				
	CC4	0.837				
	CC5	0.808				
Normative Commitment (NC)			0.573	0.816	0.744	0.752
NC1		0.755				
NC2		0.672				
NC3		0.575				
NC4		0.759				
NC5		0.663				

relationship between social media usage and continuance commitment, while the R^2 value of 0.149 implies that 14.9% variation in continuance commitment can be explained by social media usage.

For hypothesis three, the study also discovered that usage of social media usage has an impact and is significantly influencing on normative commitment at (β=0.502, R^2=0.252, T-value=7.118>1.96, P-value =0.000 <0.01). The path coefficient value of 0.502 indicates a considerable and significant meaningful relationship between the usage of social media and normative commitment while the R^2 value of 0.252 indicates that 25.2% variation in normative commitment can be explained by social media usage.

6. DISCUSSION AND CONCLUSION

The purpose of this study was to check the effect of social media on organization commitment. To examine this, we surveyed the IT employees in Bangalore. The theoretical model was supported

Figure 2. PLS Model of Use of social media usage on organization commitment

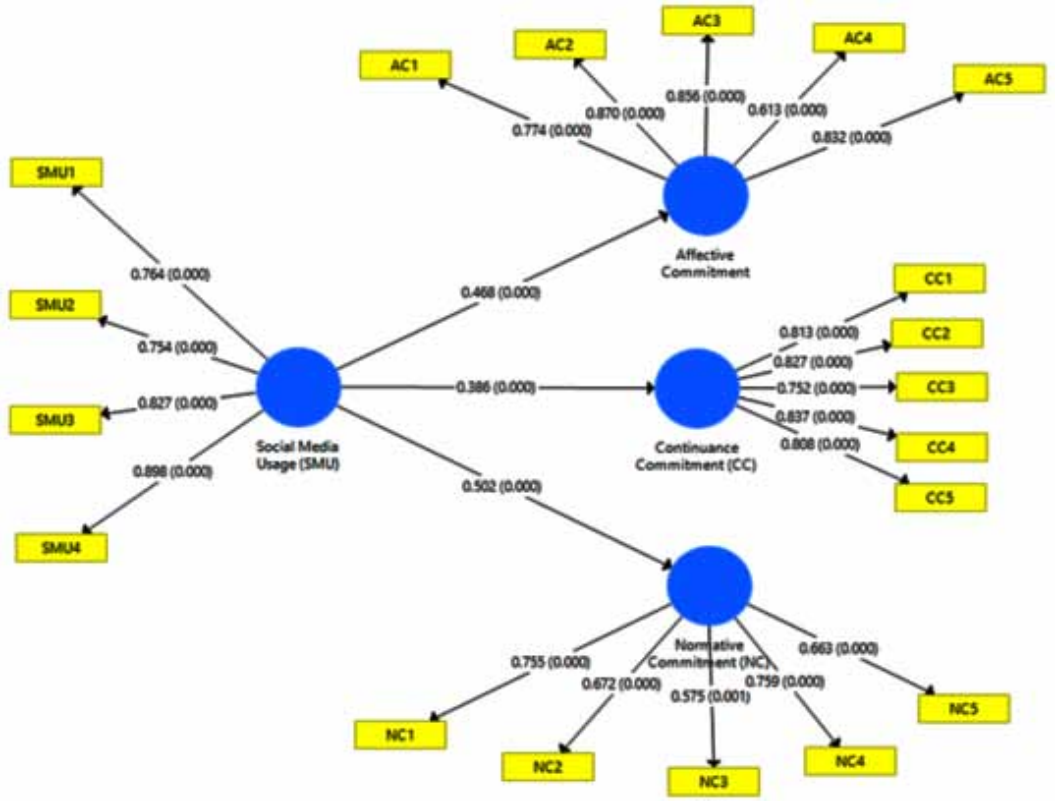


Table 3. Test of hypotheses

Hypotheses	Coefficients	R-Squared	t-value	p-value	Empirical Evidence
Usage of Social Media has no effect on affective commitment	0.468	0.219	4.798	0.000	Null hypothesis Rejected
Usageof Social Media Usage has no effect on continuance commitment.	0.386	0.149	4.253	0.000	Null hypothesis Rejected
Usage of Social Media has no effect on normative commitment.	0.502	0.252	7.118	0.000	Null hypothesis Rejected

by our three hypothesized relationships and is confirmed by our findings. The findings suggest that social media can help to improve organization commitment. Social Media can be used by the employees for work related purposes, and analysis proves that usage of social media helps in achieving organization commitment. Figure 2 illustrates the effect of usage social media on affective, continuance & normative commitment.

Researchers should consider the results of this study in view of its limitations, which relates to our data collection. The study limits to IT industry only. There are no measures of social media use and we have used our own Social Media measures from few of the Social Media literature. We have not measured in the aspects of social media use like time used and

spent by the employee; tasks& duties completed using social media. Our research sample size was limited to 224.

Despite of these limitations the study advances on social media research. This research helps organizations to transform and understand that social media initiatives can positively influence organization commitment. We hope this research helps the organizations and the managers to use social media to transform organizations for better commitment from their employees.

REFERENCES

Akinbode, J., Opayemi, R., &Sokefun, E. (2013). Impact of online social networking on employees' commitment to duties in selected organizations in Lagos State, Nigeria. *Journal of Business and Economic Development, 1*(1), 94-100.

Albdour, A. A., & Altarawneh, I. I. (2014). Employee engagement and organizational commitment: Evidence from Jordan. *International Journal of Business, 19*(2), 192–212.

Ali-Hassan, H., Nevo, D., & Wade, M. (2015). Linking dimensions of social media use to job performance: The role of social capital. *Journal of Strategic Information Systems, 24*, 65–89.

Andriole, S.J. (2010). Business impact of Web 2.0 Technologies. *Communications of the ACM*, *53*(12), 67-79.

Anthony, A. (2017). Employee commitment and its impact on performance, Asian journal of Economics. *Business and Accounting*, *5*(2), 1–13.

Ashraf, Z., Jaffri, A., & Sharif, M. (2012). Increasing Employee Organizational Commitment by Correlating Goal Setting, Employee Engagement and Optimism at Workplace. *European Journal of Business, 4*(2), 71–77.

Atzori, L., Iera, A., & Morabito, G. (2014). From 'smart objects' to 'social objects': The next evolutionary step of the internet of things. *Communications Magazine, IEEE*, *52*(1), 97–105. doi:10.1109/MCOM.2014.6710070

Balfour, D. L., & Wechsler, B. (1996). Organizational commitment: Antecedents and outcomes n public organizations. *Public Productivity & Management Review, 19*, 256-277.

Balfour, D. L., & Wechsler, B. (1996). Organizational commitment: Antecedents and outcomes n public organizations. *Public Productivity & Management Review, 19*, 256-277.

Bipeledei, E., & Rachel, D. (2018). Employee commitment to work as an ingredient for service delivery of selected firms in Bayelsa State. *International Journal of Economics and Business Management*, *4*(1), 80–92.

Cao, X., & Ali, A. (2018). Enhancing team creative performance through social media and transactive memory system. *International Journal of Information Management*, *39*, 69–79. doi:10.1016/j.ijinfomgt.2017.11.009

Cao, X., Guo, X., Vogel, D., & Zhang, X. (2016). Exploring the influence of social media on employee work performance. *Internet Research*, *26*(2), 529–545. doi:10.1108/IntR-11-2014-0299

Carr, C. T., & Hayes, R. A. (2015). Social Media: Defining, Developing, and Divining. *Journal of Communication, 23*, 46–65.

Centrukaya, A., & Rashid, M. (2018). *Internet application and management*. International Congress on Cultural Heritage and Tourism.

Chang, T. S., & Hsiao, W. H. (2014). Time spent on social networking sites: Understanding user behavior and social capital. *Systems Research and Behavioral Science*, *31*(1), 102–114. doi:10.1002/sres.2169

Cheruyak-Hai, L., & Rabenu, E. (2018). The new era workplace relationships: Is social exchange theory still relevant? *Industrial and Organisational Psychology*, *11*(3), 456–481. doi:10.1017/iop.2018.5

Daowd, A. (2016). *The Impact of Social Media on the Performance of Microfinance Institutions in Developing Countries: A Quantitative Approach*. Academic Press.

Deans, P.C. (2011). The impact of Social Media on C-Level Roles. *MIS Quarterly Executive*, *10*(4), 187-200.

Dunn, M. W., Dastoor, B., & Sim, R. L. (2012). Transformational leadership and organisational commitment: A cross-cultural perspective. *Journal of Multidisciplinary Research*, *4*(1), 45–59.

Field, L. K., &Buitendach, J. H. (2011). Happiness, work engagement and organisational commitment of support staff at a tertiary education institution in South Africa. *SA Journal of Industrial Psychology, 37*, 1–10. <ALIGNMENT.qj></ALIGNMENT>10.4102/sajip.v37i1.946'

Gonzalez, E. S., Leidner, D. E., Cindy Riemenschneider, C., & Koch, H. (2013). The impact of internal social media usage on organizational socialization and commitment. *Thirty Fourth International Conference on Information Systems*, Milan.

Haque, A. U., &Yamoah, F. (2014). Gender Employment Longevity: I.T staff response to Organisational Support Programme in Pakistan. *International Journal of Academic Research in Business and Social Science, 4*(12), 324-347.

Kane, G. C. (2017). The evolutionary implications of social media for organizational knowledge management. *Information and Organization*, *27*(1), 37–46. doi:10.1016/j.infoandorg.2017.01.001

Kane & Alavi. (2012). *What's Different About Social Media Networks? A Framework and Research Agenda*. Academic Press.

Kaplan, A. M., &Haenlein, M. (2012). Social media: back to the roots and back to the future. *Journal of Systems and Information Technology, 14*(2), 101-104.

Katz, D. (1964). The Motivational basis of organization. *Behaviour Science, 9*, 131-133.

Larson, E. W., & Fukami, C. V. (1984). Relationships between worker behavior and commitment to the organization and union. *Proceedings of the Academy of Management Journal*, 222-226. doi:10.5465/ambpp.1984.4979013

Lu, B., Guo, X., Luo, N., & Chen, G. (2015). Corporate Blogging and Job Performance: Effects of Workrelated and Nonwork-related Participation. *Journal of Management Information Systems*, *32*(4), 285–314. doi:10.108 0/07421222.2015.1138573

Macnamara, J., & Zerfass, A. (2012). Social Media Communication in Organizations: The Challenges of Balancing Openness, Strategy, and Management. *Journal of Strategic Communication, 6*, 287–308.

Madu, G., Asawo, S., & Gabriel, J. (2017). Physical workplace environment and employees' engagement: A theoretical exploration. *International Journal of Arts and Humanities*, *1*(10), 865–884.

Meriçöz, S. (2015). *Çalişanlarin Örgütsel Adalet Algilarinin İş Tatm İn İne Ve İş Performansina Olan Etk İsİ: Ampİrİk BİrÇalişma* (YüksekLisans). Bahçeşehİr Ünİversİtesİ.

Meyer, J. P., Stanley, L. J., & Parfyonova, N. M. (2012). Employee commitment in context: The nature and implication of commitment profiles. *Journal of Vocational Behavior*, *80*(1), 1–16. doi:10.1016/j.jvb.2011.07.002

Mkhyzar, Z. R &Samia, T. (2012). Employee commitment and their performance are inter-related: A behavioural study from Pakistan. *Kuwait Chapter of Arabian Journal of Business and Management Review, 1*(7).

Mugizi, W., Bakkabulondi, F., & Bisaso, R. (2015). Framework for the study of employee engagement. *The Journal of Higher Education*, *7*(2), 15–17.

Redmond, V. (2015). "Social exchange theory". *English technical report and white papers, 5*. http://libidriastate.edulengl_reports/5

Salanova, M., & Schaufeli, W. B. (2008). A cross-national study of work engagement as a mediator between job resources and proactive behaviour. *The International Journal of Human Resource Management, 19*(1), 116–131. 10.1080/09585190701763982

Sani, A., & Maharani, V. (2015). Relationship between Human Resource Management (HRM) Practices and Organizational Performance Moderated by Organizational Commitment. *Australian Journal of Basic and Applied Sciences*, *9*(7), 185–188.

Schaufeli, W. B., & Bakker, A. B. (2003). UWES Utrecht Work Engagement Scale Preliminarty Manual. *Journal of Occupational Health Psychology*, (November), 58. 10.1037/t01350-000

Schaufeli, W. B., Bakker, A. B., & Salanova, M. (2006). The measurement of workengagement with a short questionnaire: a cross-national study. *Educational and Psychological Measurement, 66*(4), 701–716. 10.1177/13164405282471

Tajudeen, F. P., Jaafar, N. I., & Ainin, S. (2018). Understanding the impact of social media usage among organizations. *Information & Management*, *55*(3), 308–321. doi:10.1016/j.im.2017.08.004

Tianan, Y., Mingjing, Y., & Jianwei, Q. (2015). Effects of co-worker and supervisor support on job stress and presenteeism in an aging workforce: A structural equation modelling approach. *International Journal of Environmental Research and Public Health*, *13*(1), 72. doi:10.3390/ijerph13010072 PMID:26703705

Pavithra S. is a faculty member of Department of Management Studies, New Horizon College of Engineering. She holds an MBA (HR) Degree from Visvesvaraya Technological University and pursuing her PhD in the area of Employee Engagement in Visvesvaraya Technological University, PGDMM from KSOU, B.Sc., Degree in "Maths, Electronics and Mathematics" from Bangalore University. Prof. Pavithra. S has a rich experience in academics and research. Her areas of interest include Emotional Intelligence, Employee Training, Employee Engagement and Strategic Management. She has taught various subjects in Post Graduate programme level viz, management and organizational behaviour, personal growth and interpersonal skills, human resource management, recruitment, and selection, etc. She has authored multiple research papers which are published in reputed international and national journals.

Osibanjo A. Omotayo has PhD (Management) from Babes Bolyai University, Cluj-Napoca, Romania. He has taught management and computer application courses in the industry. He is presently an Associate Professor of Industrial Relations/Human Resource Management, Department of Business Management, College of Management & Social Studies, Covenant University, Nigeria. He teaches courses in Human Resource Management, Industrial Relations, Collective Bargaining, Current Issues in Human Resource Management, etc. He is a scholar per excellence and has several publications to his credit in reputable local and international journals such as International Journal of Applied Behavioral Economics (IJABE); Cogent Business and Management; SAGE Open; Journal of Human Resources in Hospitality and Tourism; The Journal Contemporary Management Research; Bulletin Economic Sciences Series; Serbian Journal of Management; Journal of Competitiveness; Virgil Madgearu Review of Economic Studies and Research; Heliyon; Sage Open; Allied Business Academies.

K. V. Deepak is presently working as Associate Professor at Bangalore Institute of Technology, affiliated to Visvesvaraya Technological University. He possesses both MBA & and PhD from Bahadur Institute of Management Sciences, University of Mysore. He has also qualified the Karnataka State Eligibility Test (KSET) for lectureship/ Assistant Professor conducted by UOM on behalf of University Grants Commission. He has a vast teaching experience of more than 15 years for postgraduate students. His areas of specialization include Marketing Management, Supply Chain Management, and Logistics Management & E-Marketing. He has published more than 15 research papers in various international Journals (with impact factor). He has been awarded the best paper presenter in the International Conference in Dubai during 2011, organized by Asia Management Science Association & Putra Intelek International College, Malaysia. He has the credit of publishing three books for on E-Marketing, International Human Resource Management and Business Law and Policy respectively.