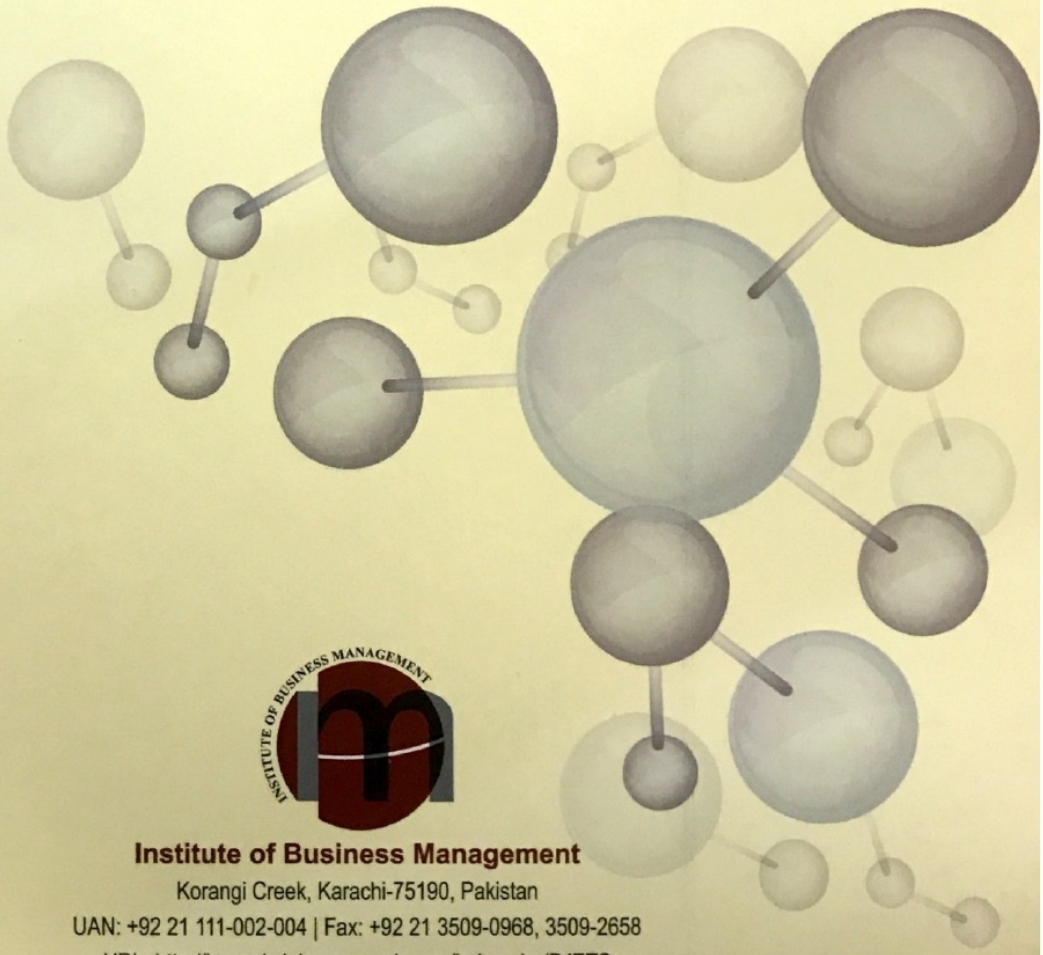
ISSN 2224-2333 (Online)
ISSN 2222-9930 (Print)

PAKISTAN JOURNAL OF ENGINEERING TECHNOLOGY AND SCIENCE

VOLUME 7 NUMBER 1



Institute of Business Management
Korangi Creek, Karachi-75190, Pakistan
UAN: +92 21 111-002-004 | Fax: +92 21 3509-0968, 3509-2658
URL: http://journals.iobmresearch.com/index.php/PJETS
URL: http://www.iobm.edu.pk | e-mail: pjets@iobm.edu.pk

Editors' Note

I am very much pleased to introduce new editorial team who took the charge from Vol. 7, Issue No. 1, June 2017 and onwards. This change marks the beginning of new era. PJETS has changes its review process, by introducing single non-blind internal review and double-blind external reviews. This means that initially after successful internal review, papers sent for double-blind external reviews having both the reviewers and author(s) identities kept confidential. We have completed six years of successful publications. The scope of PJETS is publishing and promoting innovative ideas and original research in the field of Science, Technology, Engineering and Statistical Science since 2011, twice a year. This journal aims at publishing authentic research papers with less than 19% of plagiarism to create a culture of innovation and scientific development. The focus of the journal is limited to "Computer Sciences", "Engineering", relevant "Emerging Technologies", along with "Mathematics" and "Statistics".

The mission of PJETS is to provide a platform to the researchers, faculty and students to spread their findings. The main goal is to link authors from different professions, for example academia and non-academia in particular and encourage them to share their research. We fortunately succeeded in developing a new editorial review board comprising of reputed scholars and researchers at national and international level, from academia and non-academia.

I hope the new editorial team will be great boon to give new energy to the journal and will impart their knowledge and experience to improve the quality of publications.

Note: Conference papers included in the issue are not subject to the standard of PJETS.

Prof. S.M. Aqil Burney
Editor

Member Editorial Review Board (International – Academia)

Member Editorial Review Board (International – Non Academia)

Member Editorial Review Board (National – Academia)

Member Editorial Review Board (National – Non Academia)

Contents

Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 7, No 1, June 2017

Fault Tree Analysis for a Modern Communication System

[1]K. Hamid and N. Chahine, Department of Electronics and Communications Engineering, Faculty of Mechanical and Electrical Engineering, Damascus University

***Abstract*- Wireless communications became one of the most widespread means for transferring information. Speed and reliability in transferring the piece of information are considered one of the most important requirements in communication systems in general. Moreover, Quality and reliability in any system are considered the most important criterion of the efficiency of this system in doing the task it is designed to do and its ability for satisfactory performance for a certain period of time, Therefore, we need fault tree analysis in these systems in order to determine how to detect an error or defect when happening in communication system and what are the possibilities that make this error happens. This research deals with studying TETRA system components, studying the physical layer in theory and practice, as well as studying fault tree analysis in this system, and later benefit from this study in proposing improvements to the structure of the system, which led to improve gain in Link Budget. A simulation and test have been done using MATLAB, where simulation results have shown that the built fault tree is able to detect the system's work by 82.4%.**

Keywords: Fault Tree Analysis, TETRA, MATLAB.

I. INTRODUCTION

TETRA is an abbreviation of Terrestrial Trunked Radio, which means a trunked terrestrial communications system. It is an open standards digital radio communications system. It was adopted by the European Telecommunication Standard Institute (ETSI) to meet most of the requirements of wireless radio communications system.

TETRA serves Private Mobile Radio networks (PMR) and Public Access Mobile Radio networks (PAMR). Thus, it serves many different fields such as police, ambulance, firefighters, traffic, security men, armed forces, public services, transport services, private individual's networks, factories, mines, etc.

TETRA is characterize by speed calls, providing necessary needs for a group of users, ability of direct communication between devices. It provides optimal use of frequencies and operates with a high degree of safety. It is distinguish from other networks by its ability to cancel noise effect, which makes the voice clearly audible even in places known for high degree of noise such as airports and construction sites [1].

[1] Kamal.hamid@hotmail.com

II. System Components

Figure (1) shows TETRA components, which consists of:

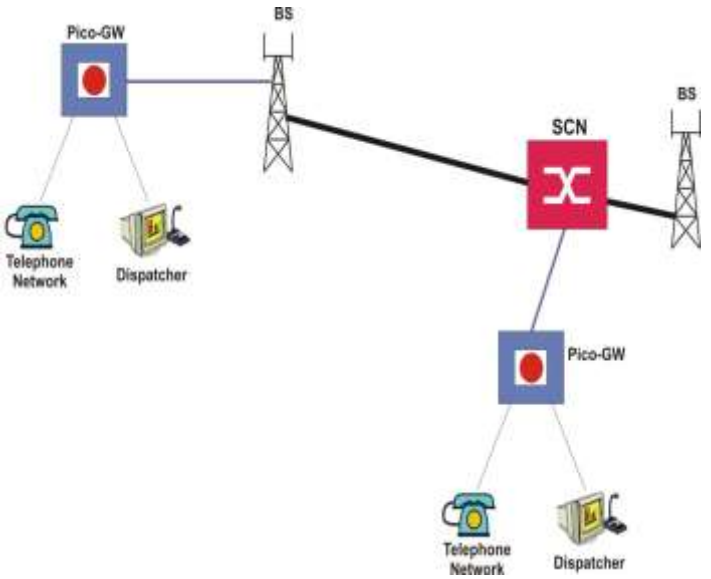


Figure 1. TETRA Components

A. Switching and Control Node (SCN)

This element is consider as the core network element for managing the network database and system communication interface. The communication interface is a tool to link the base station, command and control unit (dispatcher), and other switchboards in the network and the digital voice recorder in the network managing system (NMS).

The switchboard is also consider as the central nucleus of the network. It also has gateways port. There is a number of SCNs that form peer-to-peer network or form a network or star geographical physical structure and others [2].

B. Base Station (BS)

Base Station is responsible for geographical coverage with radio waves for an area, which is called the cell. It also provides a radio communication interface in the air for command and control unit (Dispatcher) and devices that are handled by persons and in mobile vehicles.

The Base Station is directly controlled by SCN, where (ISDN, PSN, PABX, Dispatcher) are connected to the Base Station by a local communication interface in the station. Each Base Station

supports 8 frequency carriers. Each carrier contains four time channels. As for antennas, connections are suitable according to the demand of the network investor.

This special case could work individually and without connecting the switchboard. This special case is known as Fallback status and it occurs when the station loses its connection with the switchboard (This may be due to a malfunction in the switchboard or in the connection line between them). When the station has fallback status, it can provide a partial set of fallback status; it can provide a partial set of services provided by switchboard in normal situations [2].

C. Pico-GW

Gateway secures the interfacing between the network and other networks like external phone networks and analogue radio systems that exist in the present time and will exist in the future. Gateways depend on (HW/SW) standards with high flexibility in the possibility of update and connecting different protocols [2].

D. Command and Control Unit (Dispatcher)

Command and Control Unit is a fixed station connected to the SCN by EI adapter that is used by the Dispatcher operator which is identified as a TETRA user, where it can reach TETRA services by Graphic User Interface (GUI) such as basic telephone services (voice calls, SDS, messages, call priority, etc.) and advanced telephone services, which are unsuitable for radio users (ambience listening call, allowed call by the Dispatcher), as well as managing and controlling the subscribers [2].

E. Command and Control Room

Command and Control Room (C&CR) is a system of integral digital converting and assembling, which is employed in multi-*tasking distribution for voice calls and advanced integral* data.

All calls are coded and distributed within the control room with VoIP format, which gives the C&CR operator the following advantages:

- Using one or more voice channels among known channels
- To intersect (assemble) two or more identical channels with each other
- Establishing calls between the operator and PABX/PSTN terminals

- *Allows two or more operators to communicate with each other*
- *Records all current calls (with digital format) on radio channels and telephone lines.*

F. TETRA Voice Recorder

Recording Unit in TETRA (RU) is the element in the network that secures functions of recording voice calls within the network, and allowing recording calls for individuals and groups are arranged (granting or blocking them) in their files within Home Location Register (HLR).

Calls are directly recorded in the TETRA-coded format, and are stored into a database of the RU, where a set of playback stations allows operators to browse the stored calls and to listen to them.

Recording Unit (RU) consists of two racks: the link unit (WAS-P), which allows linking up to 6 SCNs, where each SCN sends its local calls to the Recording Unit (RU) in order to record them, as well as a single management server SRUS, which manages three different recording units (RUs).

III. PHYSICAL LAYER

TETRA allocated a set of standard adapters to secure and achieve an open-vendors market as shown in figure (2).

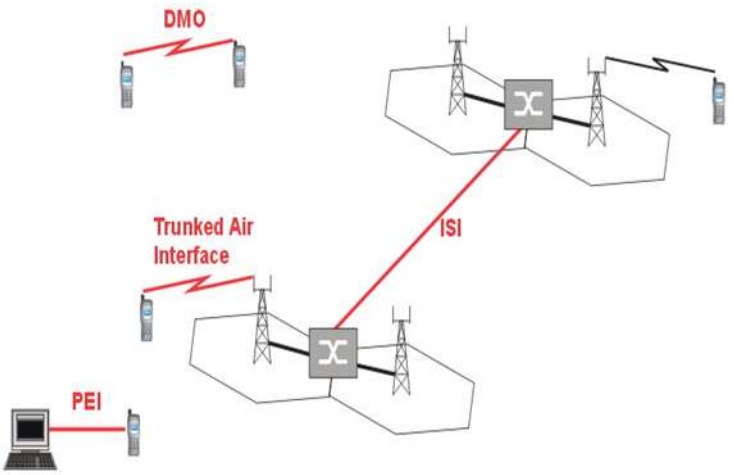


Figure 2. TETRA Standard Adapters

A. Trunked Air Interface (TAI)

It is the air interface defined by the European Telecommunications Standards Institute (ETSI) between terminals and Switching and Management Infrastructure (SwMI). It allows the air interface of two operation modes, where switching between them is done manually, they are:

- Direct Mode Operation (DMO): Direct Mode Operation does not use infrastructure of TETRA. Communication is done directly between two users. This operation is not usually done when there is not enough coverage from the system. To achieve this communication, both terminals should be within the coverage of the other terminal. Communication in this mode is a simplex communication. The terminal uses the same carrier in both sending and receiving operations. In some necessary cases, in order to establish direct communication between two terminals and each of them is not within the coverage of the other, benefit from signal repeater may be done. Repeater basically increases the coverage scope for each terminal. However, both terminals should be within the coverage scope of signal repeater. It is noteworthy that the repeater is a terminal that was programmed to operate as a repeater [3].
- Trunked Mode Operation (TMO): The terminal in the Trunked Mode Operation uses the TETRA Infrastructure, and the management of the terminal operation is fully done by the switchboard which is considered the heart of the network and responsible for its management. For the terminal to get use of the network infrastructure, it should do the recording at every operation for it. Recording is requested from the switchboard when the terminal changes its specified location area (LA). The specified location for each terminal is defined as a set of one or more network cells. The advantage of these cells is that the cell can move within them without the need to inform the network management of these movements [3].

B. Frequency Distribution

TETRA uses TDMA technique, where it provides 4 channels for users by using one frequency carrier as shown in figure (3). The width of frequency domain for each carrier is 25 KHz, which means an efficiency in using frequency domain, where the used frequency domain is 380-400 MHz. Hence, the frequency domain 380-390 MHz is used for the uplink and 390-400 MHz is used for the downlink. The frequency space for the duplexer is 10 MHz. Therefore, the frequency difference between sending and receiving frequency is 10 MHz (ETSI standard Recommendation).

The frequency plan analysis is based on the hexagonal reuse pattern. Since the system must support both TMO and DMO operation the derived allocated band for each mode is 4.5MHz for each uplink and downlink band and an additional 0.5 MHz to support 20 DMO channels (minimum

requirement) for both links. Operating frequencies for DMO mode could be chosen from both frequency domains 380-385 MHz and 390-395 MHz.

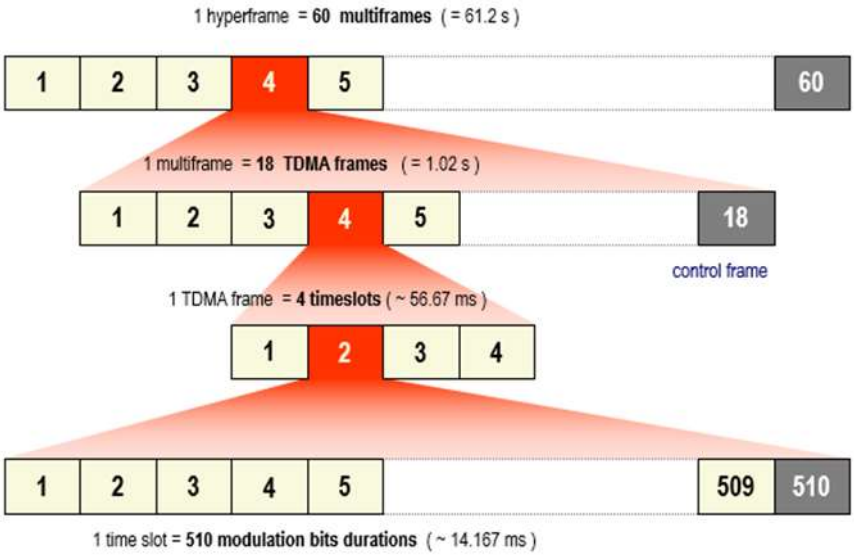
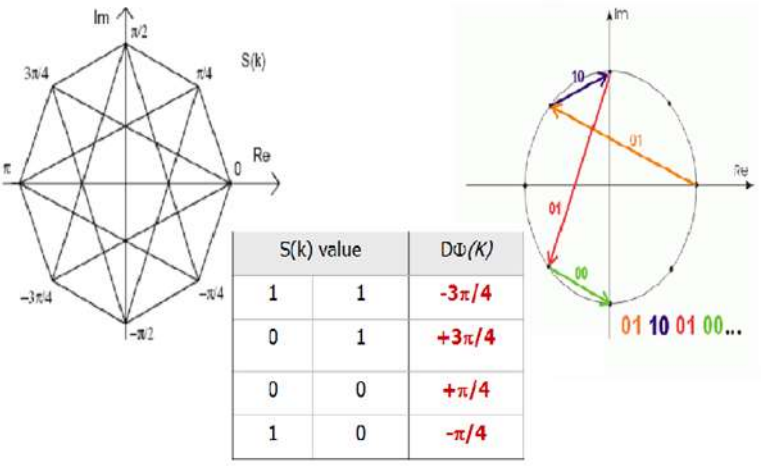


Figure 3. TDMA Frame Structure

C. Modulation

The modulation scheme used by the TETRA system is called π/4-Differential QPSK:

- the bit sequence is mapped onto a sequence of modulation symbols S(k)
- a modulation symbol is associated to a pair of modulating bits
- because of the differential encoding scheme, the generic symbol S(k) is obtained by applying a phase transition DΦ(k) to the previous symbol S(k-1)
- the phase transition DΦ(k) is a multiple of π/4



S(k) value		DΦ(K)
1	1	-3π/4
0	1	+3π/4
0	0	+π/4
1	0	-π/4

Figure 4. Modulation Technique π/4-DQPSK

IV. The Error In The System Under Study

A field study has been done under the supervision of the General authority of Syrian Wireless Communications System, which operates the system under study. The study included visits in different times to the distributing channels in Damascus city and it was located in Ibn al-Nafees Station. Problems that the system suffers from were also seen by engineers supervising its operating. They have been summarized as follows (Without referring to human errors resulted from the lack of practice):

- Number Unreachable: Sometimes there is a terminal registered in the network, but when you try to dial a call, a message appears on it that it is out of coverage areas.
- Dropped call: This problem occurs when the call is dropped before ending the conversation without dropping the call by any of the call parties.
- No Voice: In this case, the calling party is not able to hear the called party, whereas the latter can hear the calling party or both call parties could not hear each other.
- Called Busy: One of the terminals requests to establish a connection with another one, but this request is not done, and TETRA says that the second terminal is busy, while it is unoccupied.

These errors were checked practically in coordination with the General Authority, where a terminal was used and put under the circumstances under which the above-mentioned errors occur.

During making the previous tests, request was done to record all information related to the connection and it the state of connection is successful or unsuccessful. Table (1) gives the information recorded in the switchboard.

TABLE I
STRUCTURE OF INFORMATION RECORDED DURING TESTS

Characteristic Name	Values
Connection Duration	Decimal number estimated by seconds
Used Protocol	Protocol Name (text value)
Required Services	Service Name (text value)
Number of sent from mobile device bytes	Decimal Number
Number of sent from station bytes	Decimal Number
Connection Importance	Value (0) is important, otherwise the value is (1)
The number of times of failure sign into network	Decimal Number
Was signing in done	Value (0) means singing in was done, otherwise the value is (1)
Error Rate	Positive real number

First, a simulation for the physical connection channel of the system under study was done using Matlab to evaluate the system's performance. Then, information recorded during tests were used to analyze errors.

V. PRACTICAL APPLICATION

A. Simulation of physical channel of TETRA

Figure (5) gives a TETRA simulation model that has been carried out via Matlab.

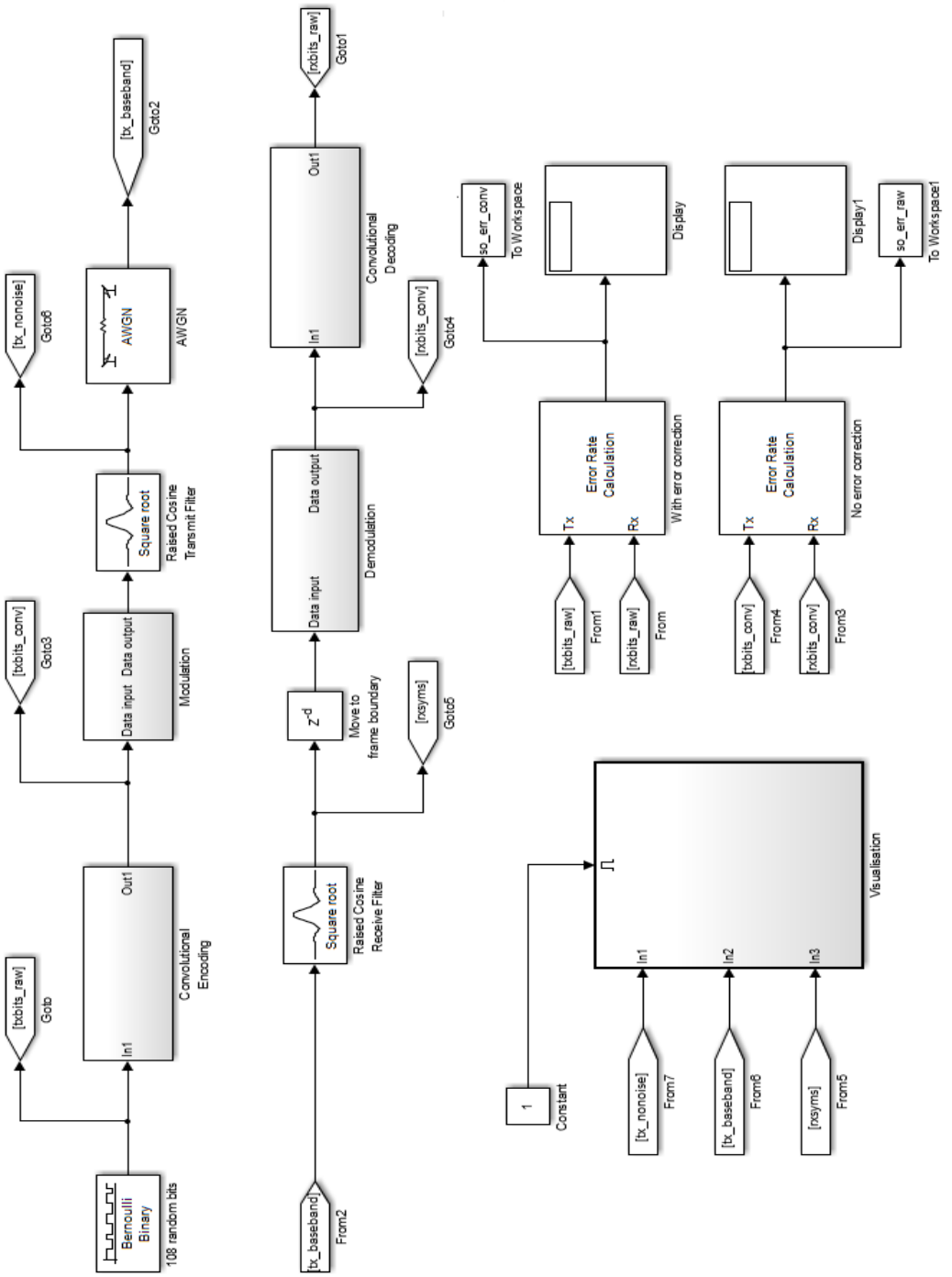


Figure 5. Simulation Model of Physical Layer

B. Explaining the simulation components

1. The Transmitter: constitutes of the following blocks respectively as shown in figure (5).
    - Error detecting and correcting Encoding and spreading: TETRA depends on convolutional encoder to detect and correct errors. Figure (6) gives the structure of the used encoder according to TETRA.

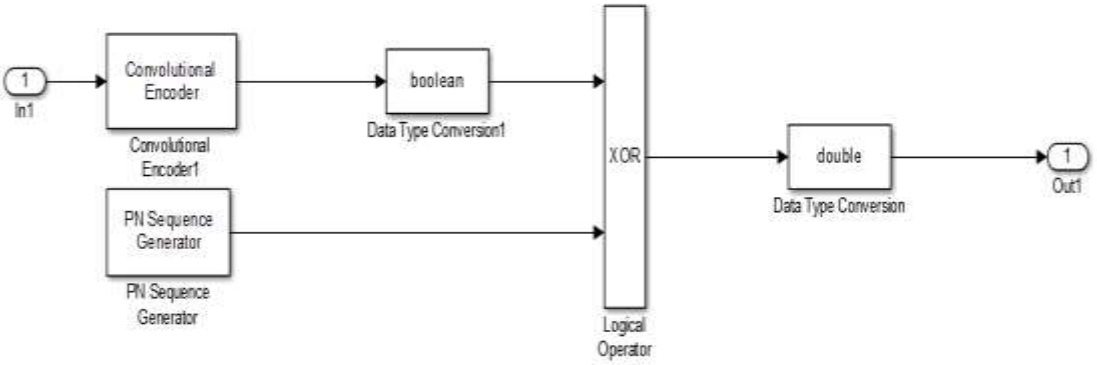


Figure 6. Error Detecting and Correcting Encoder

It also depend in spectrum disperse on dispersing using direct chains. The Convolutional Encoder 1 block carries out the encoding process, while the PN Sequence Generator block generates pseudo-random chain. Then the encoder output is multiplied by the chain output to carry out the dispersing process.

- Modulation: This block carries out the process of shaping the frame, and then it carries out the modulation. The process of the frame shaping includes the following:
    - First training sequence: It is a fixed sequence used to secure the synchronization between generators of pseudo-random sequences in transmitter and receiver. This sequence is 4 bits, which are: 0,0,1,1.
    - Adding 216 sequences of zeros.
    - Second training sequence.
    - Information bits: Which is 216-bit length.
    - End sequence is similar to finish sequence.

After that, DQPSK modulation is done, and then Guard Intervals are added with a length of 24 codes. Figure (7) gives components of modulation block.

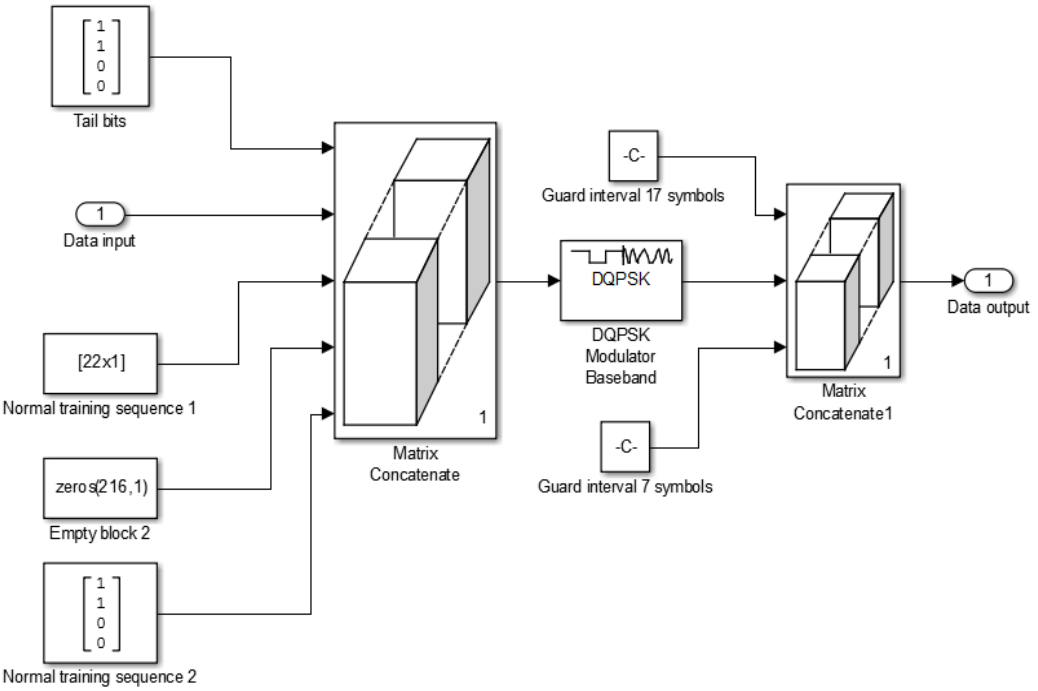


Figure 7. Shaping and Modulating Frame

- Pulse shaping: TETRA depends on pulse shaping to overcome the problems of the channel with memory, which results in Inter Symbol Interference (ISI). It depends on pulse shaper of raised cosine.

2. The Receiver: Receiving process is done oppositely to sending process as follows:
   - Pulse Shaping Decoding: Which is done using pulse shaper of raised cosine.
   - Modulation Decoding: In this block, the Guard Intervals that were added in the transmitter are deleted. Then the modulation is decoded using DQPSK modulation decoder. Finally, information are extracted from the frame resulted after modulation decoding. Figure (8) gives modulation decoding block diagram.

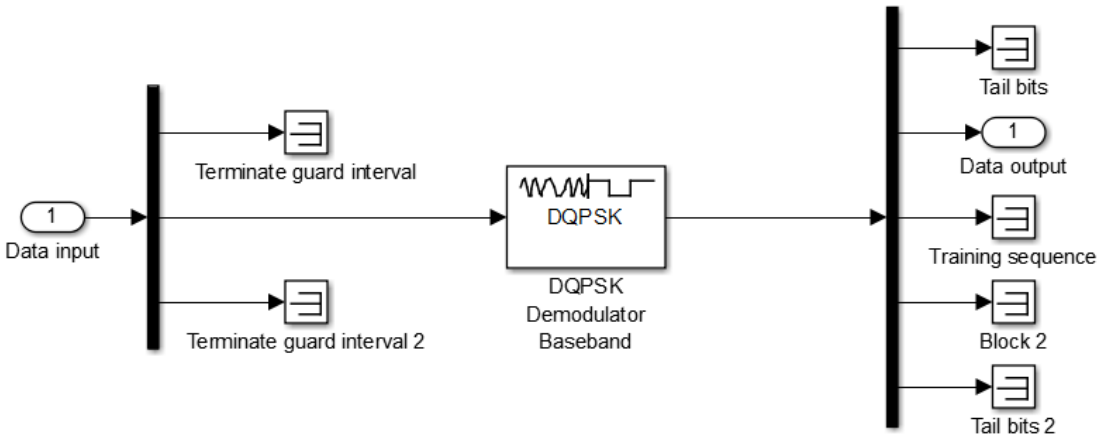


Figure 8. Modulation Decoder and Frame Decoding

- Decoding: In this block, dispersing process are being decoded by generating random sequence identical to that generated in the transmitter, and then multiply the extracted information frame to this sequence. Finally, decoding is done using Viterbi decoder. Figure (9) gives decoder diagram.

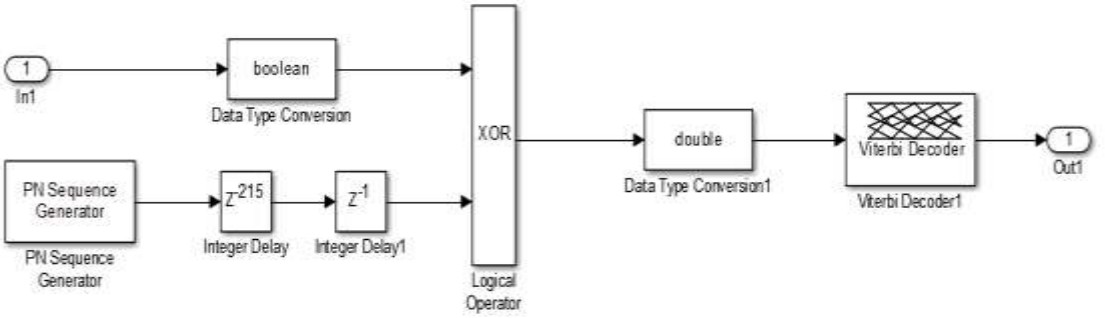


Figure 9. Error Detecting Decoder

VI. Results Of Simulation Of Physical Channel of Tetra

Simulation was done in the case of Additive Gaussian White Noise channel (AWGN) at signal to noise ratio (SNR) equal to 10 dB. Figure (10) gives Scatter Plot for the received signal, while figure (11) gives error rate.

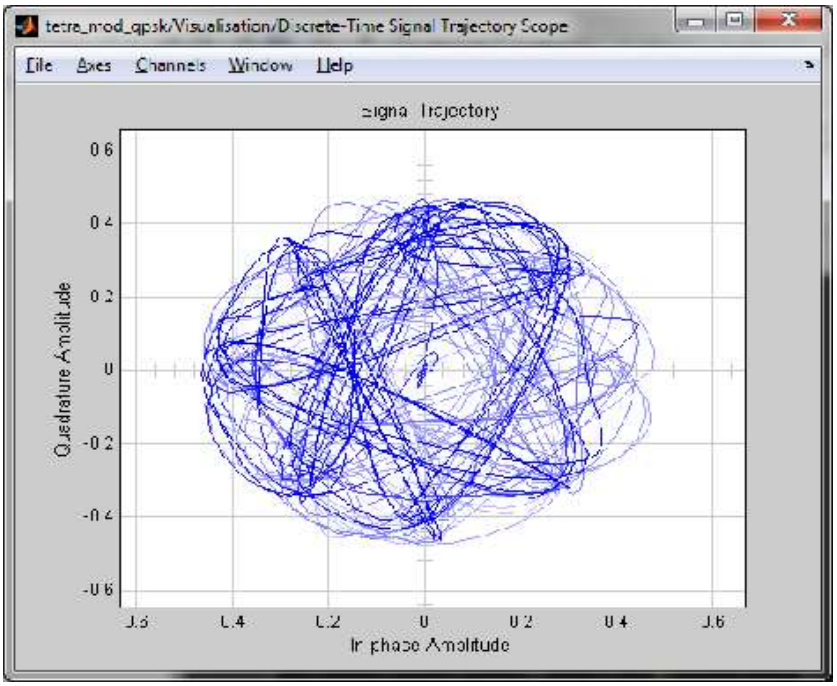


Figure 10. Scatter Plot

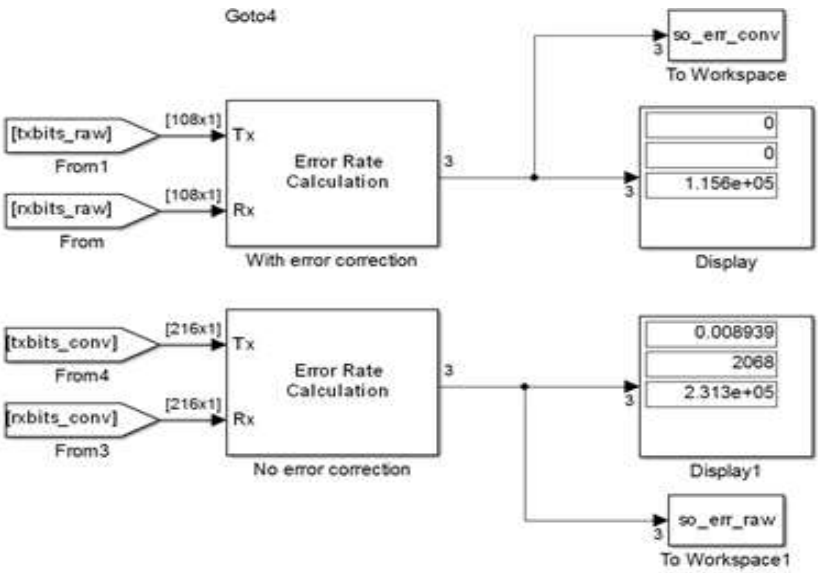


Figure 11. Error Rate

From figure (11), it is shown that the expected performance in case of signal to noise ratio (SNR) with using error detecting and correcting encoding that equals zero, while figure (10) shows that the distribution of received codes resulted from using DQPSK modulation, where this modulation is lesser resistant to noise. Yet, it secures an acceptable transfer rate to secure the system's services.

Figure (12) gives the curve of TETRA performance in case of additive Gaussian white noise channel, where it is shown that to achieve voice transfer that is achieved at an error rate that is lesser than or equal to 10-3, the system needs SNR that is more than or equal to dB 13. However, in reality, the channel is not an additive Gaussian white noise channel; therefore, the SNR should be much more than this value.

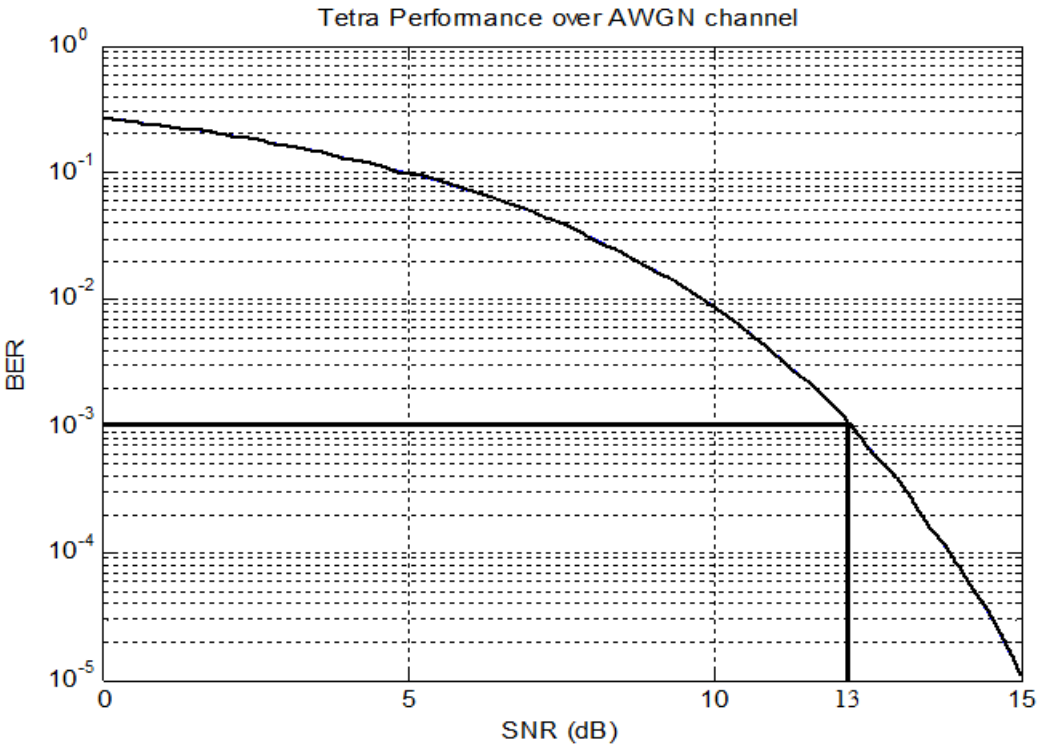


Figure 12. Curve of TETRA Performance in Case of Additive Gaussian White Noise Channel

A. Analyzing recorded data file

Data file will be used during the field tests to analyze the behavior of the system under study and to conclude when an error occurs.

From table (1), it is shown that the frame structure is variable between text values, decimal values and digital ones. Therefore, first a modulation for recorded values type should be done, where all of

them are of one type. Then, choosing real numbers values is done in field [0,1]. We call this phase the Preprocessing phase. After that, analyzing is done using neural networks to extract Fault Tree Analysis (FTA), which demonstrates how errors occur in the system under study [4] [5] [6] [7]. At the end, this tree will be tested.

1. Preprocessing: The preprocessing aims at transforming all information into digital ones as follows:
   - Digitalizing text values: First, each text value is replaced by an increasing decimal number. Assuming that the file contains different text value n, then the values that it takes are {0, 1, 2… n-1}. After that, an estimation for the possibility that this value appears during the tests period is done after repeating it many times during the test and dividing it along the file.
   - Decimal values: Which are different information such as the call duration estimated by seconds and number of sent bites from the mobile device or from the station. Processing each of these information is done separately. For the call duration, which is usually small numbers (one-hour call corresponds 3600 seconds), a bigger value is found for the call duration during the test and division is done on it. For the sent bites number, it is a number constitutes of 32 bits. Consequently, it is either too small or too big to be transformed into a real value that uses the logarithmic function. The logarithmic function is a non-text function. Therefore, for small values, it does not change their values a lot. Yet, for big values, there is a big change. There has not been a division on the bigger value during the test period, as there could be cases in which the number of sent bites does not exceed some kilobytes, and cases in which they are close to gigabyte. When being divided, the small values become very close to zero.

2. Training: The recorded file contains about 20,000 frames vary between frames that express a successful connection without problems and other that express a failed connection for some reason (one of the errors explained previously). One thousand cases were taken that express a successful connection and other one thousand express a failed connection. We notify that in current time we are not concerned about determining the error type that led to failure. These values were included to the neural networks. In order to make the training process, then drawing the detected errors tree was done and it is given in figure (13), where:

X1: Bit Error Rate, X2: Frame Error Rate, X3: Packet Error Rate, X4: Duration, X5: Number of Transmitted Bytes, X8: Number of Received Bytes, X9: Received Power, X12: Number of Retries, X32: Number of Retransmit Requests (for services other than call).

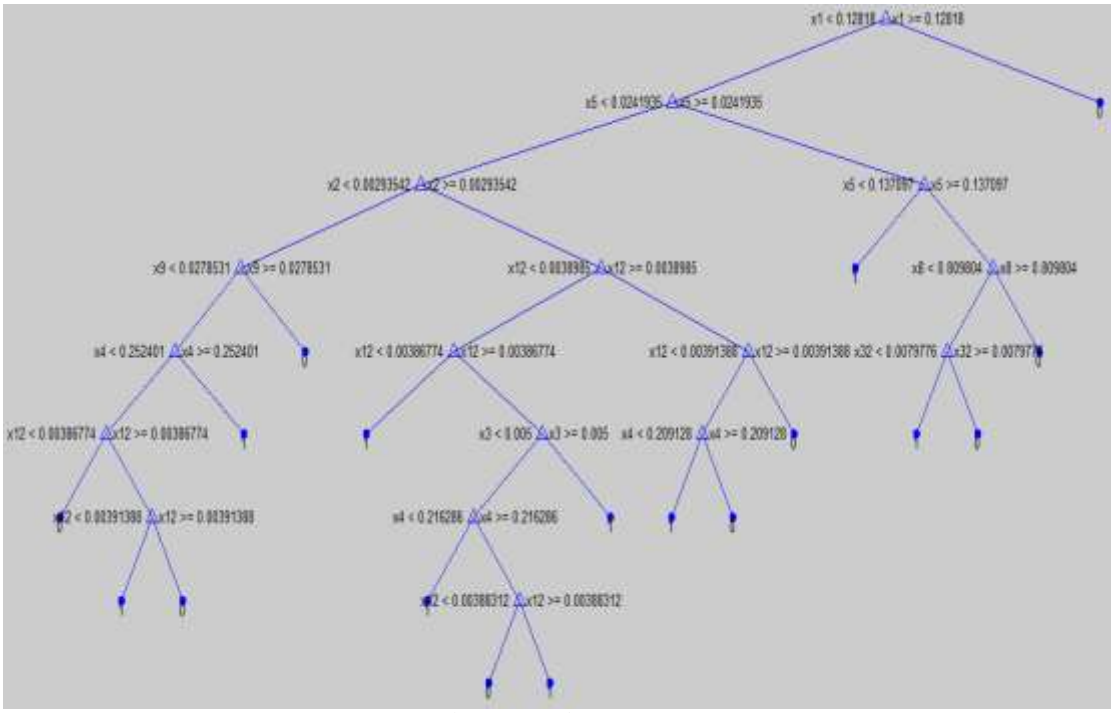


Figure 13. Fault Tree

B. Training Evaluation

The detected tree was tested during training process on the whole recorded data file (during tests, which is given in table (1)). The test result was the success of tree in detecting error occurrence at rate of 82.4% as shown in figure (14).

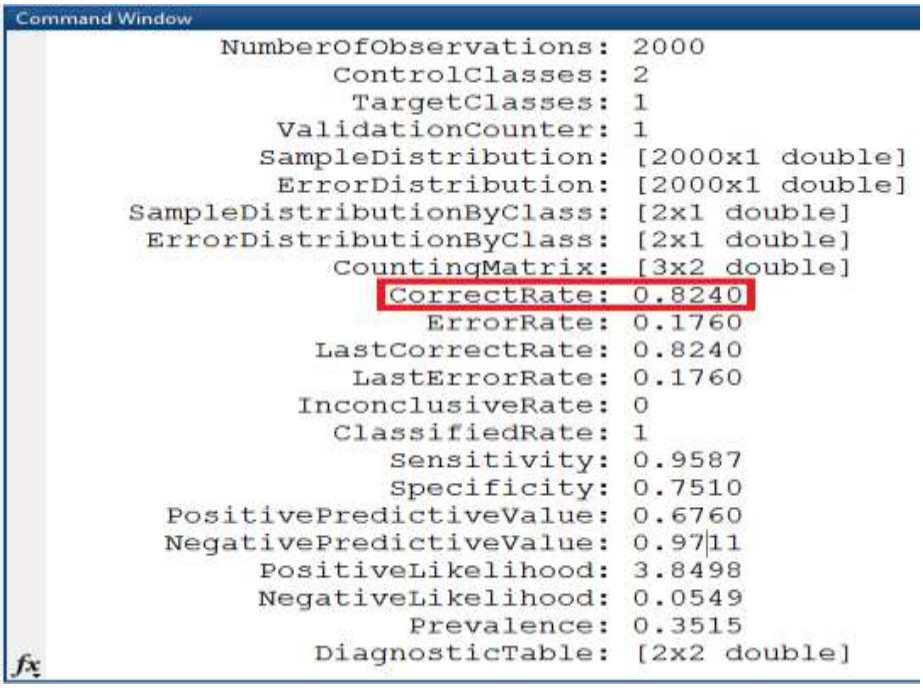


Figure 14. Performance of the built fault tree

From figure (10), it is shown that decoding of detecting and correcting error is suitable in case of high SNR values. But, in case that its values are low, it fails and error rate increases, which in turn directly leads –according to figure (12)– to an error in connection if the error rate exceeded X1=0.128, while the detected fault tree demonstrates that the error rate coefficient is the key factor in the connection's failure. If it is more than 0.128, the connection fails immediately. If the number of sent bits is less than 1000 bits and the number of received bits is more than 500 bits, then the connection fails. Otherwise, it would be successful.

ACKNOWLEDGMENT

This paper research provided a reference study for wireless digital communications system under study in the Syrian Arab Republic with regard to communications and services that it is supposed to provide for investors. It also tackled the problems resulted from investment, which was analyzed and in which fault tree was abstracted. It considered as well the simulation of the physical layer using Matlab.

REFERENCES

[1] E. NASCIMENTO JUNIOR, H. T. D. SANTOS FILHO, E.C. ROLIN, T.M.S. OTOBO, C.A. DARTORA, and J.R. DESCARDECI, "Performance Analysis of 380-470 MHz Band Radio Systems for Brazilian Public Safety". IEEE Latin America Transactions. Vol. 13, No. 3, March 2015, 5

[2] 13-622.

[3] M. CHENG, H. LI, X. NING, "A Priority-Based Preemptive Channel Resource Allocation Mechanism for TETRA System". IEEE U.S.A, Third International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2013, 1708-1711.

[4] H. LIU, D. YAO, and J. LIAO, "Research on Downlink Synchronization for TETRA". IEEE U.S.A. 13th International Conference on Instrumentation, Measurement, Computer, Communication and Control. 2012, 582-585.

[5] E. JAFARIAN, and M.A. REZVANI, "Application of fuzzy fault tree analysis for evaluation of railway safety risks: an evaluation of root causes for passenger train derailment". Proceedings of the Institution of Mechanical Engineers F: Journal of Rail and Rapid Transit Iran. vol. 226, No. 1, 2012, 14–25.

[6] R. FERDOUS, F. KHAN, R. SADIQ, P. AMYOTTE, and B. VEITCH, "Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations". Risk Analysis Canada. Vol. 31, No. 1, 2011, 86–107.

[7] R. DUAN, and J. FAN, "Reliability Evaluation of Data Communication System Based on Dynamic Fault Tree under Epistemic Uncertainty". Hindawi Publishing Corporation, Mathematical Problems in Engineering. Vol 2014, Article ID 674804, 2014, 9 pages.

[8] N. LIMNIOUS, "Fault Trees". 1st. ed, ISTE, U.S.A, 2007, 224

Satellite Derived Sea surface temperature fronts in relation with Tuna catch In the EEZ of Pakistan

[1]Muhammad Abdullah, Saad Malik, Muhammad Danish Siddiqui. Department of Remote Sensing & GISc, Institute of Space Technology, Karachi and Aftab Ahmed Khan, Global Change Impact Studies Center (GCISC), Islamabad

***Abstract*- Sea surface temperature (SST) is an important parameter in marine ecosystem studies as its relations of Fishery and other marine resources. In this study SST fronts have also been studied with relate to tuna fish catch data of April and August 2014 was acquired. Satellite derived MODIS daily products have been used to derive thermal fronts in the exclusive economic zone (EEZ) of Pakistan. Research results indicated that the Sea surface temperature gradually changed from 22C to 24C where Tuna catch is high and By Catch is low in frontal region. The further Relationship between these two data are discussed in this study and also made recommendations for in what way these two datasets should be handled. Remote sensing data and GIS tools are efficient and less time consuming for mapping and classifying sea surface temperature in a broader way. Survey of fishing resources is really time consumed and costly, Satellite Remote sensing data shows a promising tool to monitor fishery resources in a cost effective manner. Satellite data play an important role to identify fish aggregation zones and these techniques could also be used to forecast potential fishing zones by measuring oceanic parameters which influence on fish distribution on a broader scale and these techniques can help to local fisherman and fishery organizations to observe fishery resources.**

Keywords: SST, Remote Sensing, GIS, EEZ, SST Fronts.

I. INTRODUCTION

One of the important variable for the assessment of the world climate is sea surface temperature (SST) [7]. SST is considered as one of the important variables by WMO (World Meteorological organization). For various application such as weather prediction, ocean estimating, climate research studies, marine fishery resources high quality of SST datasets are necessary. Sea surface temperature can be obtain with different sensors but these sensors do not provide a similar estimation of the SST because of each sensor type [1]. Sea surface temperature maps are important for commercial and fishing communities as well as provide critical information for gases between ocean and atmosphere [8]. In ocean, fronts are narrow zones of gradients of biological, chemical and physical properties [29]. Frontal zones are abundant in the marine water with spatial measures from 1 to 1000km [9]. Frontal regions are very dynamically active and its presence in location where large energy scale

[1] mabdullahsiddiqui88@gmail.com

transfer to small scale is most strong. Such as upwelling process, water mass interleaving happening at frontal region that share to vertical exchange of ocean properties [29]. So high biological productivity present in frontal regions due to vertical fluxes of nutrients et al [11, 21]. Species Distribution identification and its relations to particular marine habitat features is important for marine conservation and efficient marine management [24]. So, Considerable attention needed at classifying marine biological hotspots and relation with ecologically significant zones et al [20, 27, 17]. Many Studies mentioned that Sea surface temperature (SST) fronts are vital habitat features that effect the distribution of pelagic species, marine ecologist have been interested in SST fronts because of productivity associated with Fronts [24]. Frontal regions are characterize by upwelling events, but change over a short time period. Upwelling event power will also impact the distribution of food resources [5]. So techniques of defining the locations of marine fish while considering SST coverage in these frontal areas would be a good utility. Because of the spatial range and dynamic environment of Upwelling areas, it is tough to map from ships because it do not allow ships to sample the whole point of interest within a specific time. In modern era different image processing techniques have been developed such as edge detection analysis and automated features extraction using SST imagery [14, 26, 4]. The visible and infrared spectrum of the satellite image has great potential to study fronts [15]. Satellite based remote sensing methods seems to be cost and time effective for examining the biological and physical relations between the fish species and their environment at temporal and high resolution datasets [13].

In National economy fishery plays an important contribution, marine fisheries sector provide a key role in contributing approx. 57% in terms of fish production. For local fisherman fishing provides an important source of income. Fishery provides economic benefits and sole source of employment to the community living along the coast. On the basis of repeated experiments and local knowledge, fishermen employ fishing. Due to the lack of information, fishermen face problems about the particular potential fishing grounds which in turns cause problems in terms of money, time and fishermen's incomes.

The prime objective of this research is to identify aggregated hotspots of fish resources by evaluating different environmental factors in EEZ of Pakistan. Remote sensing and GIS techniques in connection with the usage of GPS allow us to predict hotspots for fish catching by using ocean parameters, which primarily include sea surface temperature. However, this method is helpful in improving the fish yield.

I. Material And Methods

In this study, Pakistan Exclusive Economic Zone (EEZ) has been selected as shown in (Fig 1). The continental shelf area of Pakistan is about 50,270km2 [28] and coastline length of Pakistan is 1,050 km [16]. Coastline of Pakistan is separated into two states, one is Sindh coast and the other one is Baluchistan coast. Sindh coast is about 250km including Indus delta region and Karachi coast. Balochistan coastline is spreading approximately 800kmand the Pakistan Exclusive Economic Zone (EEZ): It is about 240,000 km2 [16]. Jiawani, Gwadar, Pasni, Ormara and Sonmiani are regions of Baluchistan's coastline having a population of about one million [23]. For this research daily Tuna fish catch data of 2014 year have been acquired from World wild Fund (WWF) Pakistan. Satellite data MODIS product such as Sea surface temperature (SST) of same year 2014 daily product acquired from NASA ocean color (oceancolor.gsfc.nasa.gov) to correlate with in situ data as shown in (Table 1).

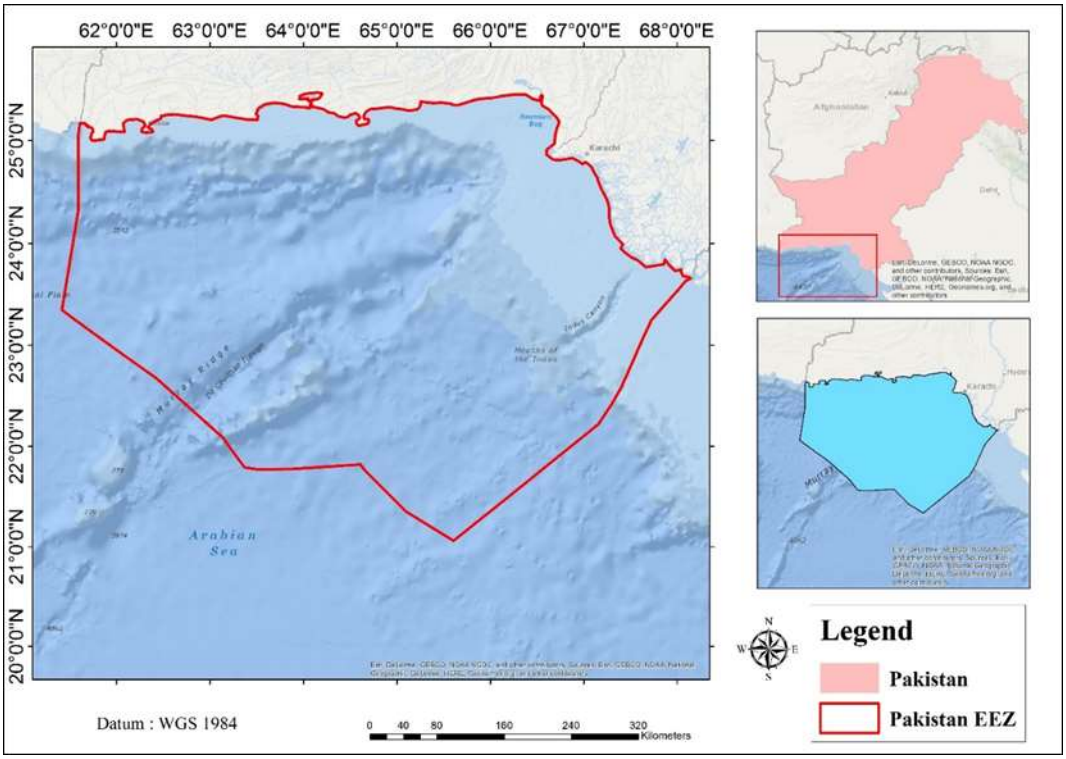


Figure 1: Study Area the EEZ of Pakistan

TABLE I
FISH CATCH GIS DATABASES WITH DIFFERENT SPECIES: TOTAL CATCH AND SST VALUE

Other[Kg]	Dolphins[Kg]	Turtle[Kg]	Bycatch[Kg]	Total Catch[Kg]	Raster value[C°]
16	0	14	111	199	24.93
224	0	0	129	248	25
21	0	0	506	558	24.96
5	0	0	81	107	25.03
10	7	0	161	309	25.02
16	0	0	185	329	24.83
7	0	0	98	168	24.5
8	0	0	69	150	24.83
1	0	15	88	160	25.06
0	0	0	95	172	24.73
0	0	0	115	208	24.27
30	0	0	92	135	24.34
12	0	0	93	180	24.4
16	0	0	72	134	24.38
12	0	0	118	263	24.32
1	0	12	93	270	24.27
28	0	0	127	206	24.2
20	0	0	120	260	24.39
14	0	0	75	233	0
26	0	0	137	216	0
0	0	0	89	330	0
0	0	0	69	232	0
37	0	0	114	229	0
49	0	0	143	314	0
12	0	0	139	287	0
28	0	0	225	363	0
4	0	0	135	220	23.89
12	0	12	61	113	23.92
24	0	0	66	324	23.97
7	0	0	80	240	24
18	0	12	53	134	23.82
12	0	0	65	111	1

3	0	0	100	202	23.51
18	0	4	76	134	23.5
6	0	0	103	195	22.95
3	0	0	321	387	22.78
16	0	0	168	393	22.83
20	0	0	98	239	22.78
12	0	0	131	217	22.78
1	0	0	161	328	22.95
35	0	0	139	186	22.57
9	0	0	53	112	22.65
9	0	0	133	202	23.04
0	0	0	57	111	23.01
6	0	0	104	200	23.18
0	0	0	37	119	23.15
3	0	14	134	204	23.11
12	0	0	54	301	23
0	0	0	98	248	22.94
0	0	0	31	182	22.99
28	0	0	225	363	23.55
4	0	0	36	204	22.96
3	0	12	43	134	22.97
3	0	0	37	173	22.92

A. Methodology

The workflow of the study is shown in (Fig 2). A detailed description of each step is presented in the following subsections.

B. Fish Catch Data

Daily in situ data of year 2014 acquired from WWF Pakistan in the excel sheet form this data includes many species of fish and turtle, fish data include Tuna fish, jelly fish and other species for whole year excluding breeding months i.e. June and July as shown in Fig 3.

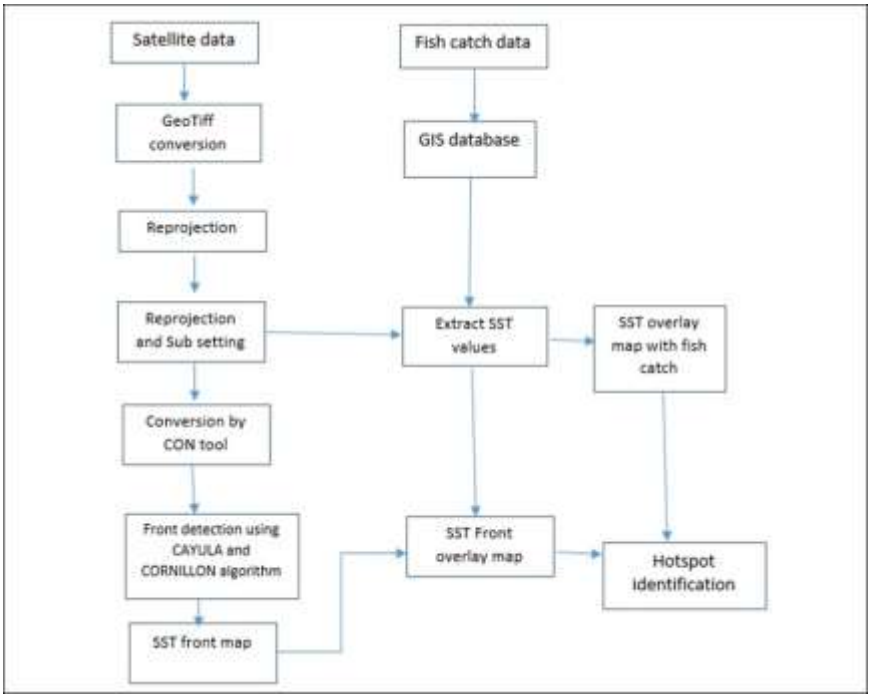


Figure 1: Workflow Diagram

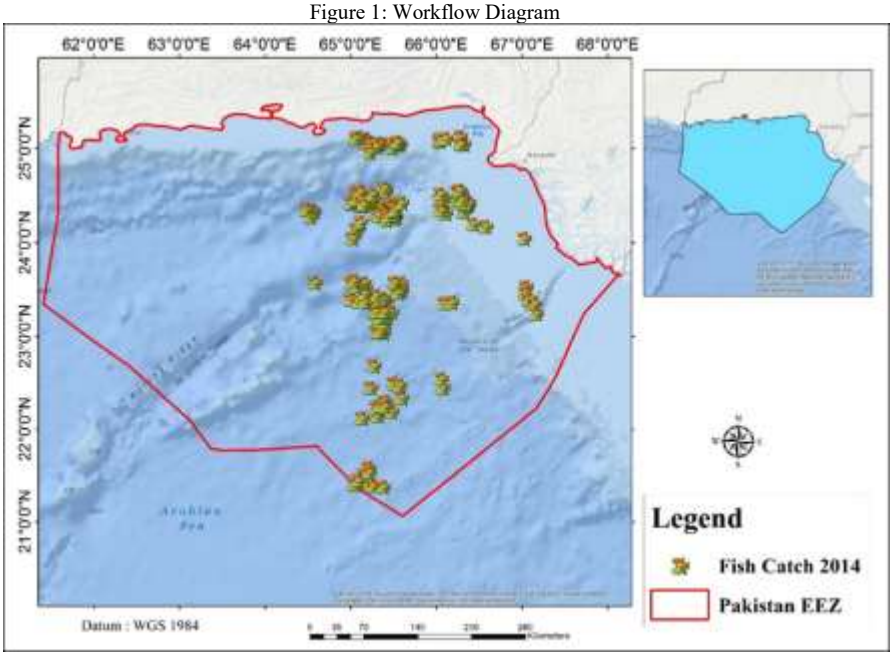


Figure 3: Fish Catch GIS Database

C. Raw data to GIS

As mentioned above the date was in excel form which was exported in GIS to make GIS database of daily fish catch with detailed attribute of each species with date, Location and catch frequency as shown in Fig 4.

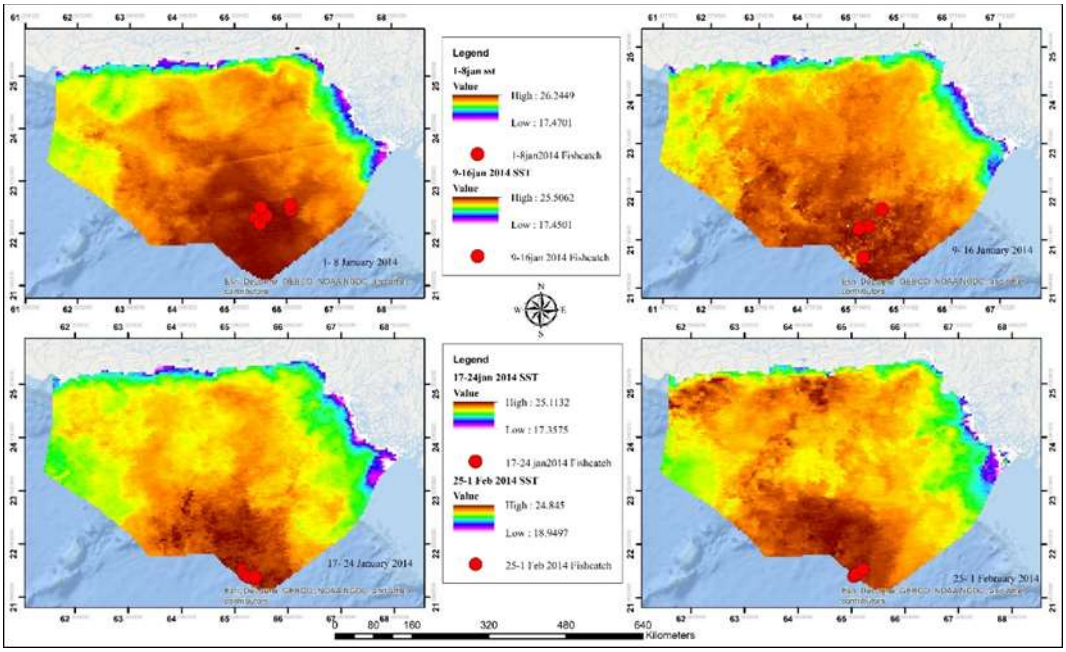


Figure 4: Sea surface Temperature (SST) overlay on respective Fish Catch data

D. Satellite data processing

MODIS data cover 36- Bands in visible and infrared spectrum to produce land and ocean products such as vegetation, cloud, aerosol, chlorophyll and SST. The product from Ocean color data used in different aspects to study coral reef ecological health, algal bloom monitoring and water quality of coast and estuarial water and this satellite data help fish resources management [18]. 45 images of MODIS 8 day satellite data of sea surface temperature were acquired. The data has been filter by excluding fish breeding months (June and July).

E. Re-projection and Sub setting

Images were converted into Geo-Tiff format, which can be readable in GIS software and then applied reprojection tool on these images using SeaDas which was an open source software and

downloaded from ocean color website. After Conversion and re-projection the next step is to extract Pakistan Exclusive economic zone (EEZ) from all forty five images of MODIS by Extraction of the study area.

F. Extract SST values

GIS database was use to extract sea surface temperature values from MODIS product and identify temperatures values with respect to fish catch data as shown in Fig 5. And further overlay on fish catch data.

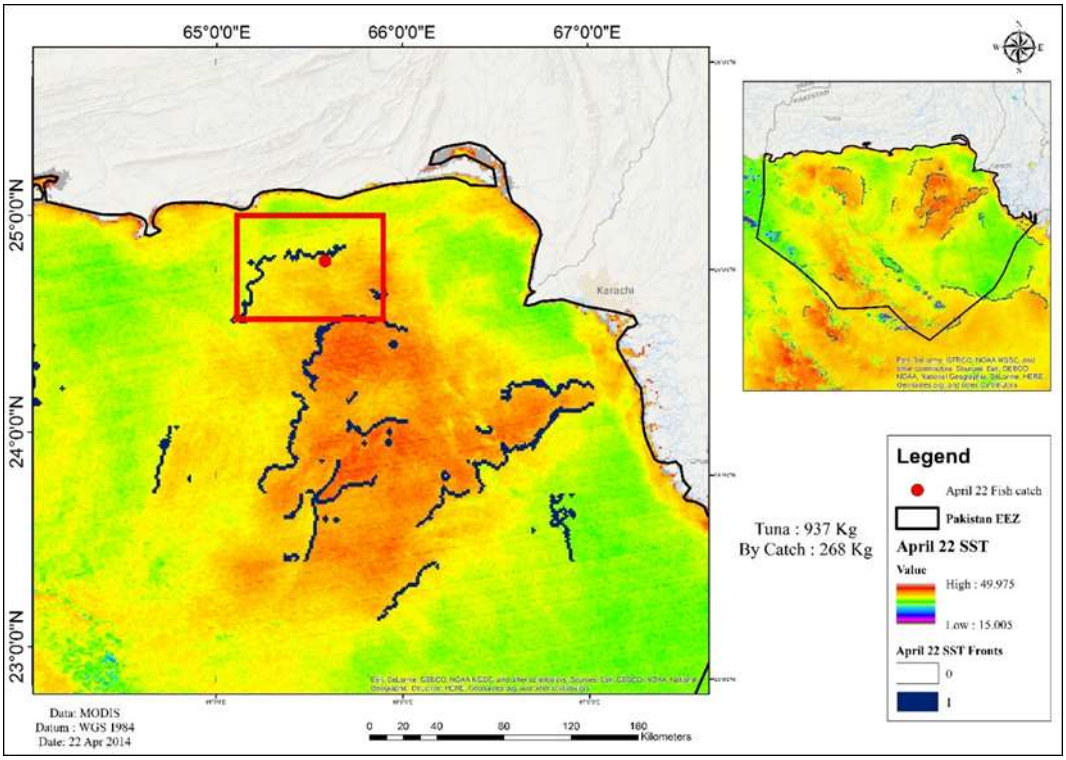


Figure 5: Ocean front Sea surface temperature map with Fish catch data (22 April, 2014)

G. Con Tool

After Re projections in GIS software. The Con tool allows to manage the output values of raster datasets. This tool helps you to control the result values of each raster cell, which based on whether the value of the cell is estimated as true or false in a quantified conditional statement

H. Front Detection

In this study thermal front were identified along the EEZ of Pakistan using MODIS satellite imagery. The SIED algorithm, which was used in this study for Front detection were developed by [2]. This algorithm shows the region where there is a gradient change in SST. The statistical sequence of single image edge detection (SIED) algorithm on temperature field is within 32*32 pixel window to detect the presence of front.

III. Results And Discussion

Since the main objective of this research is to identify the thermal fronts regions with respect to tuna fish catch. Hence, a database of 2014 was created of fish catch provided by WWF-Pakistan, which includes various species of fish. With the assistance of this database, raster values of SST of each point were extracted. Once the points were extracted, no data values were deleted and exported to excel in order to get the knowledge of the best value of SST as shown in Fig 3. GIS based fish catch were comprised of daily data of 2014, each species of Tuna fish and other fish species were defined with Total Tuna Catch , By Catch of whole 2014 year excluding June July months due to fishing season off as shown in Fig 4.

Sea surface temperature (SST) 8 Day composite images of 2014 year were analyzed. All satellite images were preprocessed and extracted sea surface temperature values by overlaying fish catch data of 2014. Fig 4 shows the SST map from January 1st, 2014 to February 1st, 2014: 8 day composite.

During analysis, it has been noted that on 1- 8 January, 2014, Total Tuna fish catch was 577 kg and Total By Catch 1173kg was observed at 24 C to 25C. The highest Tuna fish catch of 148kg which was recorded on January 6th, 2014 was observed at 25.02C and highest by catch of 506 kg, which was recorded in January 4th, 2015 which was observed at 24.98C as shown in below mentioned Table 2.This relation method applied on all MODIS SST images and relate with respective Tuna fish catch data as shown in graphical format in Fig 6. During analysis it has been observed that the maximum Fish catch were observed at 25C to 27C. [3] Mentioned in his research that the physical and climatological parameters are seriously inclined the Fish abundance and other marine organisms. World climate changes affect the marine resources such as fishery production due to sea surface temperature, currents and other ocean parameter changes and this also can be affect on species and food distribution.

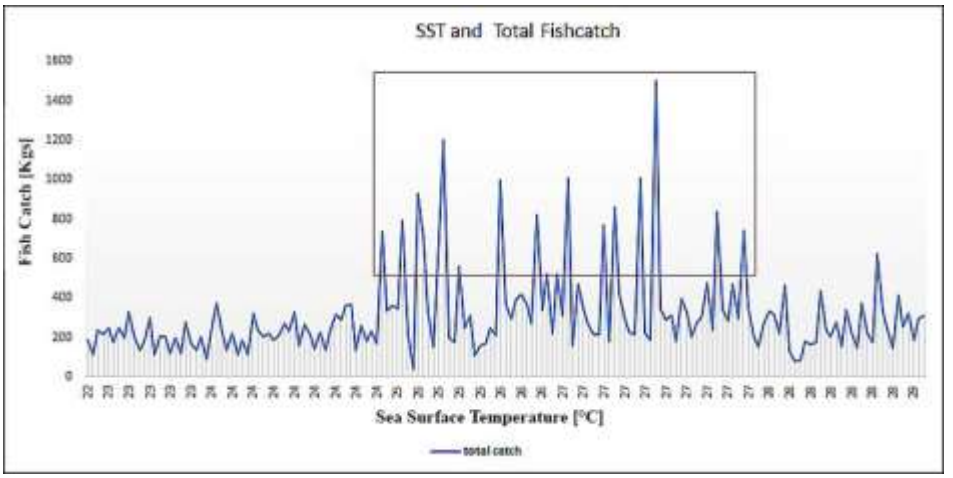


Figure 6: Sea surface Temperature values and Red Highlighted box shows Tuna Fish Catch

Thermal fronts have been analyzed and incorporate with fish catch data for understanding the ocean parameter such as Sea surface temperature relation with Tuna fish. Fish abundance of species like Swordfish, Tuna and Billfish with fronts have been used for establishing relationships [30]. [30] Determined a relationship of predator variety with ocean fronts. [22] Applied the fronts techniques to define the strong relationship between the shark and thermal front. In this study fronts area identified on Sea surface temperature (SST) daily L2 dataset has been used. Ocean front detected on Sea surface temperature L2 daily image of April 22, 2014 and overlaid fish catch datasets which revealed the strong relationship between SST and Tuna catch. During analysis, it is observed that the Tuna fish catch which around 937kg was found on front edge as shown in Fig 5.

On August 20th, 2014 Satellite image shows ocean front detect on the point where tuna catch about 610kg and temperature were gradually changed from 22C to 24C as shown in Fig 7. Results also showed that the by catch frequency was very low as compared to tuna fish catch on frontal regions. According to et al [6, 10] the features of ocean circulation which include fronts, eddies show higher biological productivity as compared to other region which are more inactive or calm flow and these features are strongly related to SST gradients.20th August, 2014 image also showed high tuna catch 601kg on sea surface temperature fronts region it is noted that the by catch very low as compared to tuna catch. [19]. Also mentioned in study that the fish-catch estimations indicated that the Potential fishing zone located by detecting the ocean features using satellite data produce high fish catch data. August 21st, 2014 also showed a good relation between tuna fish catch and Sea

surface temperature (SST) as shown in Fig 8. Tuna catch was recorded around 798kg whereas by catch data was recorded 37kg on frontal regions. These areas might be further evaluated as Potential location for MPA (marine protected areas) [12]

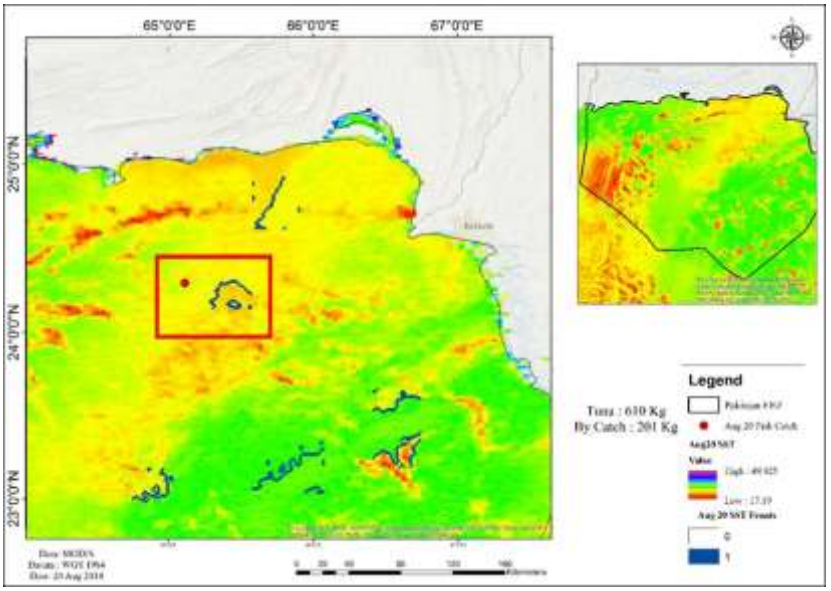


Figure 7: Ocean front Sea surface temperature map with Fish catch data (20 Aug, 2014)

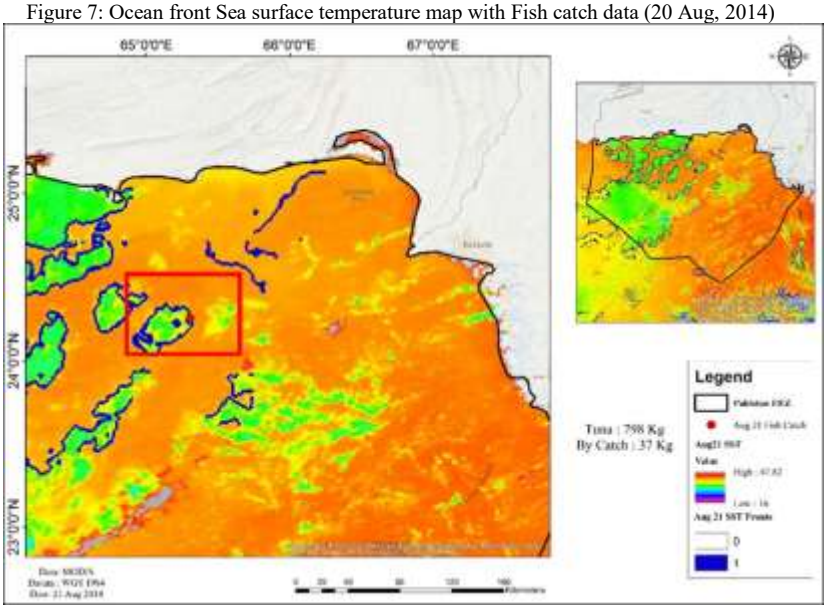


Figure 8: Ocean front Sea surface temperature map with Fish catch data (21 Aug, 2014)

IV. CONCLUSION

By concluding this research, it is assured that, the thermal fronts in a marine upwelling phenomena; although lasting for a very short time but it provide a suitable environment for tuna fish in EEZ of Pakistan. Additional datasets and sampling would need to understand Tuna fish association with thermal fronts. By identifying the location of thermal fronts in coastal waters this could be beneficial for marine management and conservations. As mentioned above SST fronts are important for fish species in marine upwelling areas so remote sensing play a vital role in monitoring of these features. There is an alarming need to obtain information on temporal and spatial variability of ocean processes for managing fish resources in Pakistan.

ACKNOWLEDGMENT

Author would like to Thank to Dr. Moazamm Khan (WWF-Pakistan) for providing valuable information and data. I would also like to thank Mirza Muhammad Waqar for the guidance throughout the research.

REFERENCES

[1] Alvera-Azcárate, A., Troupin, C., Barth, A., &Beckers, J. M. (2011). Comparison between satellite and in situ sea surface temperature data in the Western Mediterranean Sea. Ocean Dynamics, 61(6), 767-778.
[2] Barton, I. J. (1995). Satellite-derived sea surface temperatures: Current status. Journal of Geophysical Research: Oceans (1978–2012), 100(C5), 8777-8790.
[3] Biswas BK, Svirezher YUM, Bala BK, Wahab MA (2009). Climate Change impacts on fish catch in the world fishing grounds. Clim. Change 93:111-136.
[4] Cayula, J-F., and Cornillon, P. 1992. Edge detection algorithm for SST images. Journal of Atmospheric and Oceanic Technology, 9: 67–80
[5] Chavez, F. P., and Messie´, M. 2009. A comparison of eastern boundary upwelling ecosystems. Progress in Oceanography, 83: 80–96.
[6] D'Asaro, E., Lee, C., Rainville, L., Harcourt, R., & Thomas, L. (2011). Enhanced turbulence and energy dissipation at ocean fronts. Science,332(6027), 318-322.
[7] Donlon, C., Casey, K. S., Robinson, I. S., Gentemann, C. L., Reynolds,R. W., Barton, I., Arino, O., Stark, J., Rayner, N., Le Borgne, P., Poulter,D., Vazquez-Cuervo, J., Armstrong, E., Beggs, H., Llewellyn-Jones, D.,Minnett, P. J., Merchant, C. J., Evans, R., (2009). The GODAE High-Resolution Sea Surface Temperature Pilot Project. Oceanography 22 (3),34–45.
[8] Emery, W., Baldwin, D. J., Schl¨ussel, P., Reynolds, R., 2001a.Accuracy ofin situ sea surface temperatures used to calibrate infrared satellite mea-surements. Journal of Geophysical Research 106 (C2), 2387–2405
[9] Fedorov, K. N., The Physical Nature and Structure of Oceanic Fronts, Springer-Verlag, New York, 1986
[10] Ferrari, R. (2011). A frontal challenge for climate models. Science, 332(6027), 316-317.
[11] Fournier, R. O., Biological aspects of the Nova ScotJanshelfbreak fronts, in Oceanic Fronts in Coastal Processes, edited by M. J. Bowman and W. E. Esaias, pp. 69-77, Springer-Verlag, New York, 1978
[12] Game E. T., Grantham H. S., Hobday A. J., Pressey R. L., Lombard A. T., Beckley L. E., Gjerde K., et al. Pelagic protected areas: the missing dimension in ocean conservation. Trends in Ecology and Evolution 2009; 24:360-369. doi:10.1016/j.tree.2009.01.011.
[13] Gauldie R. W., Sharma S. K., Helsley C. E. Lidar applications to fisheries monitoring problems. Canadian Journal of Fisheries and Aquatic Sciences 1996;53:1459-1468. doi:10.1139/f96-070.
[14] Holyer R. J. and S. H. PECKINPAUGH (1989) Edge detection applied to satellite imagery of the oceans. IEEETransactions on Geoscience and Remote Sensing, 21, 46-56.
[15] Horstmann U. (1983) Distribution patterns of temperature and water colour in the Baltic Sea as recorded inSatellite images: indicators of plankton growth. BerichteInstitutfiirMeereskundeUniversitiit Kiel, 106, l-147.
[16] http://www.niopk.gov.pk/intro-1.html (Web Access: October 2016)

[17] Hughes, T. P., Bellwood, D. R., and Connolly, S. R. 2002. Biodiversity hotspots, centres of endemicity, and the conservation of coral reefs. Ecology Letters, 5: 775–784.
[18] Hyun Jung Cho, Deepak Mishra and John Wood (2012). Remote Sensing of Submerged Aquatic Vegetation, Remote Sensing - Applications, Dr. Boris Escalante (Ed.)
[19] Nayak, S. R., Solanki, H. U. and Dwivedi, R. M. 2003. Utilization of IRS P4 Ocean colour data for potential fishing zone-A cost benefit analysis. Indian J. Mar. Sci., 32(3): 244-248
[20] Piatt, J. F., Wetzel, J., Bell, K., DeGange, A. R., Balogh, G. R., Drew, G. S., Geernaert, T., et al. 2006. Predictable hotspots and foraging habitat of the endangered short-tailed albatross (Phoebastriaalbatrus) in the North Pacific: implications for conservation. Deep Sea Research II, 53: 387–398.
[21] Pingree, R. D., P.M. Holligan, and G. T. Mardell, The effects of vertical stability on phytoplankton distributions in the summer on the northwest European shelf, Deep Sea Res., 25, 1011-1028, 1978.
[22] Priede, I.G. & Miller, P.I. (2009) A basking shark tracked by satellite with simultaneous remote sensing: reveals orientation to a thermal front. Fisheries Research, 95(2-3), 370-372
[23] Qureshi, R. M., Mashiatullah, A., Fazil, M., Ahmad, E., Khan, H. A., &Sajjad, M. I. (2002).
[24] Reese, D. C., O'Malley, R. T., Brodeur, R. D., &Churnside, J. H. (2011). Epipelagic fish distributions in relation to thermal fronts in a coastal upwelling system using high-resolution remote-sensing techniques. ICES Journal of Marine Science: Journal du Conseil, 68(9), 1865-1874.
[25] Seawater pollution studies of the Pakistan coast using stable carbon isotope technique. Science Vision, 7, 224-229.
[26] Simpson J. J. (1990) On the accurate detection and enhancement of oceanic features observed in satellite data.Remote Sensing of the Environment, 33. 17-33.
[27] Sydeman, W. J., Brodeur, R. D., Grimes, C. B., Bychkov, A. S., and McKinnell, S. 2006. Marine habitat “hotspots” and their use by migratory species and top predators in the north Pacific Ocean: introduction. Deep Sea Research II, 53: 247–249.
[28] trtapakistan.org/wp-content/uploads/.../OIE-PVS-Pakistan-FINAL.pdf, (Web Access: 26 February 2016)
[29] Ullman, D. S., &Cornilion, P. C. (1999). Satellite-derived sea surface temperature fronts on the. Journal of Geophysical Research, 104(C10), 23-459.
[30] Worm B, Sandow M, Oschlies A, Lotze HK, Myers RA (2005) Global patterns of predator diversity in the open oceans. Science 309(5739): 1365-1369

Advancement in GSM Network to Access Cloud Services

[1]Muhammad Tanveer Meeran, Asif Raza, Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan and Muizzud-Din, Department of Computer Science Khawaja Fareed University, RYK, Pakistan

***Abstract*- Cloud services are offering a large number of utilities to the mobile users. Mobile users can share, store, develop, compute and many other services on the cloud. Due to extensive utilization of cloud services by the mobile users, security concerns are also evolving with the same pace. Among different security problems, secure access to the cloud services (cloud data utilization, data storage) is also a difficult and challenging task. This paper highlights the security concerns, particularly addresses the issue of secure access to cloud infrastructure, Such as access the cloud services securely by the mobile users. As Elastic Cloud Computing is valid only for Amazon, MLaden model is theoretical based model and not implemented practically, Wayne model enhances the end user security but not proposed tool for practical implementation. Intention of this paper is to propose mechanism to securely access the cloud services using GSM band. Only defined frequency band of GSM will provide the access to the cloud services. Users will be restricted to use the particular frequency to access the cloud services.**

Keywords: Multi-Tenancy, Elasticity, Identity Spoofing, HLR, VLR and MSC.

I. INTRODUCTION

Cloud companies are offering different services. Such as: Saas (Software as a Service): This is consumer use app and don't control/manage by network. It reduces expenses e.g. Flicker, Amazon, Cloud Drive. Paas (Platform as a Service): In this service cloud user or consumer deploy their apps on cloud computing system. But they can't control, Manage, Storage Server. Iaas (Infrastructure as a Service): In this service consumer gets access of deployment of application, but don't manage or control infrastructure. Instead of these it can manage and control storage and apps e.g. Elastic Cloud Complete (ECR).

Cloud computing concept is started in 1950's with the mainframe computing. In which numbers of users or clients trying to access the mainframe through dumb terminals. But it is not feasible for each employee to install a mainframe [1]. After some time, nearly in 1970 the virtual machine concept generated [2] [3]. Through this different software used such as VMware software through this different operating system executed on the single physical hardware in different environment. Cloud computing helps the enterprises in different angle, it help the enterprises in reducing the

[1] 1tanveer_miran@yahoo.com

upfront cost of infrastructure deployment, helps the enterprises to focus only on their core business, helps in reducing the deployment time and costs, also provides the flexibility to the enterprises to meet their requirements on demand and enterprises only need to "pay as you go" basis.

Security concerns are increasing rapidly due to the extensive list of services for mobile user offered by cloud. Among different security problems, secure access to the cloud services is also a tough and noticeable task. By the analysis of previous models and techniques presented by researchers, their drawbacks are given in TABLE 1.

TABLE I
SHORTCOMING OF PREVIOUS MODELS

Model/ Technique	Drawbacks
EC2 [4]	Is valid only for Amazon.
DS2 [5]	Provides end-to-end verification of data but their work is no longer valid.
TCPS [6]	Improved security, transparency mechanism but it is not deployed in professional cloud computing system.
Rongxing [7]	Presented mathematical model , system will be secured in all sense; but its implementation is difficult due to complex mathematical techniques.
MLaden [8]	It is theoretical based model and not implemented practically.
Provetrack.R.La [9]	Implemented a security capture device It is useful for end users or small systems; but it is not feasible for large scale companies.

By the viewing previous models or techniques and their drawbacks, proposed a new mechanism which is implemented by using the Paas (Platform as a Service) layer for secure access to cloud services over GSM network. By this approach previous shortcomings will be minimized.

The rest of this paper is organized as follows. In section II describes the security attributes and threats to the cloud services. In section III previous solutions of security will be discussed. Section IV elaborates the proposed solution for the cloud services. In section V results and analysis will be mentioned. Section VI pop out the conclusion in a best way.

II. SECURITY ATTRIBUTES AND THREATS TO THE CLOUD SERVICES

Basic security attributes are authentication, confidentiality, and integrity. Where authentication ensures that allowed person is accessing the data or only authorized person or devices can participate in communication within the network. Authentication is achieved either using digital signatures or certificates. Mostly RSA algorithm is used to ensure authentication [10].

Confidentiality ensures that data is confidential between intended parties and no one can see or read it without authentication of doing so. Different mechanisms and techniques are applied to the data to achieve the confidentiality [11].

Integrity ensures that data is original and real and data is not changed either during communication or in data storage. Different techniques [12] are applied to the data to maintain the integrity of data for examples hashes are generated for the data, which are the mathematical function. Hash functions not only ensure the integrity of data during communication but also during the store time over the data storage in cloud.

A. Threats to Cloud Services

In cloud computing data located at different places or locations. Because each server contains same type of data such as Mail server, File Server, Mom Server etc. The main purpose is to facilitate the user to access data from anywhere and anytime. But the scope of cloud is increasing constantly and security issues and risks are also increasing with respect to time [13].

List of threats to cloud services are given in TABLE II [14] [15] [16].

TABLE II
THREATS TO CLOUD SERVICES

Name of Threats	Description
Tampering	An attacker may change the data which is stored in local file
Information disclosure / eavesdropping	In which attacker enter in the tunnel of traffic
Repudiation	Attacker tries to disprove the sender statement
Elevation of privileges	Attacker get access unauthorized to inform
Man in the middle attack	Attacker involve the third party deployment
Replay attack	After some delay of time data sent
Identity spoofing	Attacker destroy the identity of node or server
Viruses and worms	In which attacker slow down the performance of hardware and software as possible
Insider attacks	Low level of security due to illiterate staff working in cloud
Outsider attacks	Every hacker try to penetrate in API interfaces and break down the connection
Malware injection attacks	Attacker attacks in the form of any file type which is unknown for us
Flooding attacks	When system overloaded data not secured so,attacker access easily
Differential analysis threats	It occurred on the basis of old and new security codes

III. Formal Solution Of Threats And Attacks

Table III below is showing formal solutions from the literature.

TABLE III
FORMAL SOLUTIONS

Solutions	Description
DS2 [17]	Declarative secure distributed system (DS2) which provides end to end verification of data
EC2 [4]	EC2 Amazon and Python for Access security and Privacy in cloud computing. But drawback is that it is valid only for Amazon
TCPS [6]	TCPS) transparent Cloud Protection System. Presented model has improved security, transparency, and Intrusion detection mechanism. But their works not validated because it is not deployed in professional cloud computing system
Jinpeng [18]	Jinpeng (Jinpeng et al, 2009) they proposed an Image Management System model which provides Image filter, scanner to detect malicious images. But drawback is that image filter is not accurate sometime legitimate images may also be detected as malicious/ virus.
Mirandasiani [19]	Mirandasiani proposed a model in which many features were implemented like preference setting, data access and feedback but drawback is that it is not generalized and not implemented in all scenarios.
Rituik [20]	A simulation program is developed for eBay. It verifies billing detail and prevention of security attacks. But it is only applicable to sales application.
Dan and Anna [21]	Dan and Anna introduced a new framework with three key components, first is policy ranking, second is policy integration and finally policy enforcement. These components provide correctness, time efficiency, scalability, reliability and robustness. Drawback is that this model is not validated.

IV. Proposed Solution For Cloud Services

This section provides the illustration of proposed work. A general scenario is presented below to depict the properties of proposed work. Scenario is based on the GSM architecture. Because overdue reports brought from the FCC [22] in the US and Ofcom [23] in the Uk have discovered the regular use within approved frequency bands is really as reduced as 5%.Due to availability of spectrum holes in GSM spectrum band, GSM network is involved in this approach. In this intention first section provides the brief overview of GSM architecture and second section provides the details of integration of proposed work with the GSM scenario. General GSM architecture can be shown in Figure 1.

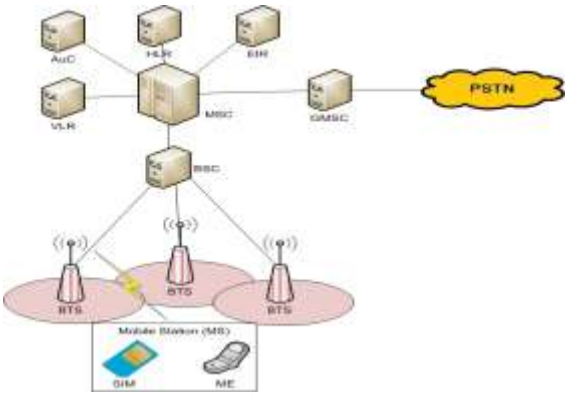


Figure 1: General GSM Architecture

Figure 1 illustrates the general influence of signals through GSM architecture. Where, as per requirement cloud services can be accessed and managed by the server. In this architecture accessed services and data flow will be less secure due to less security implementation. Other reason of the less secure of GSM network as GSM is public network so any one can utilize this network. The encryption methods, hashing techniques [24] may secure the network but hackers also have the ability to decrypt these methods as well. The pictorial view of mentioned scenario is given in Figure 2.

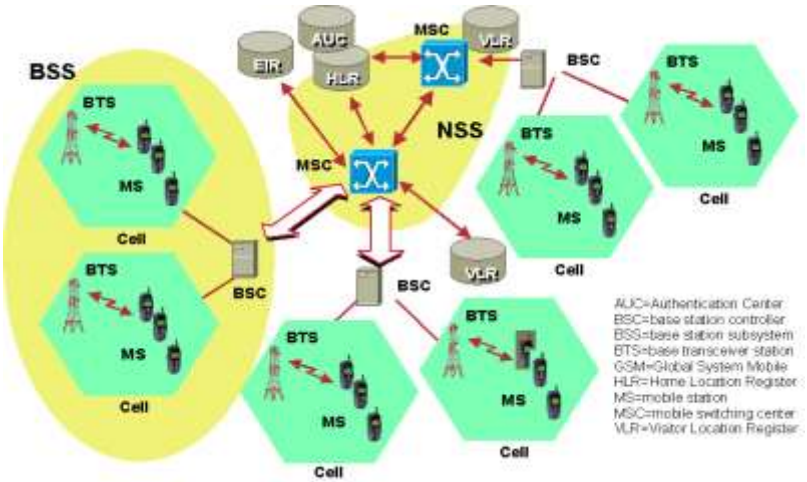


Figure 2: GSM Network in Detail Working

Figure 2 illustrate the detail mechanism of the GSM architecture. This architecture describes the complete detail of each part of the GSM network. First part describes the registers which are using in GSM. There are two types of registers that are commonly used. (i) Home Location Register (HLR) saved the permanent address of the subscribers. (ii) Visitor Location Register (VLR) saved the temporary data of the visitors. Figure2 shows that Mobile Station (MS) directly linked with Base transceiver Station (BTS) and BTS connected with Base Station Centre (BSC) and BSC with Mobile Switching Centre (MSC) and MSC send or receive the data or services through clouds or any public or private networks or via internet.

Figure 3: GSM Network and Proposed Scenario

Figure 3 shows the communication between MS and cloud. According to this secure access method adopted by implementing the digital filter which is software defined radio (SDR) module which can filtered out the particular frequency from a GSM band spectrum. This particular frequency used only for a specific purpose. This frequency utilized only for cloud services (data storage, data integration, and data analytics). Software defined radio module (Digital filter) communicate between MS and GSM. MS and BTS communicate by using the Um interface and BTS communicate with BSC via Abis interface. Same as above mentioned BSC communicate with MSC through an interface

Digital filter (SDR) is connected with BTS terminal. When MS want to communicate with cloud or want to access cloud services then it use the particular frequency which can be extracts from GSM band spectrum by using the digital filter (SDR). MS has the mobile equipment (ME) and subscriber identity module (SIM).MS send the request to the GSM spectrum for attaining the specific filtered frequency; BTS send the acknowledgement to the MS and send the message to the SDR to filter out the required frequency. After receiving the message SDR starts to perform its functionality and acknowledges the BTS. After that, BTS send the acknowledgement to the MS and MS tune the application according to the required frequency, so through this method secure cloud services accessed between MS and cloud.

GSM have the different parts which can communicate with each other. Cloud services which we want to access, these services may be data storage, data integrity and data analytics. Secure access method might be possible by using these different devices but for implementing the proper statistical and mathematical equations we can justify and explain the proposed work. For the justification and explanation of this model we should equate the proper equations, which are in the form of general

equation and in the form of statistic. Now, the general and static form of given model is given below.

GSM=f(MS, CLOUDS) --------- (1)

In the equation1 GSM is the main variable which is the functionality of MS and clouds.MS and clouds depends on GSM because if GSM not exist/implemented then communication between MS and clouds is not possible. Basically these are all the variables which is dependent on GSM and GSM is independent variable. On the other hand MS and clouds are dependent variables. If we separately discuss these dependent and independent variables, then these variables have the different communicating parts, such as the dependent variables MS have the ME and SIM. Clouds have the junk of data and have a many more parts but our concern is only related to data storage, data integrity and data analytics. Independent variable is GSM which have the BTS, BSC, MSC, HLR, VLR, AUC, EIR etc.

Second form of equation which we are elaborate in this model is Statistic form of equation that is

$$GSM = \alpha_{\circ} + \alpha_1(MS) + \alpha_2(CLOUDS) + \mu_{\circ} \text{ ---------- (2)}$$

The equation2 shows the statistical form of the cloud scenario/model. $\alpha_{\circ}$ shows the intercept and α1 shows or denoted the slope of the given variables.

GSM=f(BTS,BSC,MSC,HLR,…….N) -------- (3)

In this Eq. 3 GSM is a dependent variable which has been used in this model that represents BTS, BSC, MSC, HLR, VLR, AUC, EIR, OMC and others. Specifically GSM is interrelated with all this functions such as BTS, BSC, and MSC and so on.

MS=f(S,M) ------- (4)

MS is interconnected with the mobile Sims and mobile equipment. Cloud includes storage, integrity and analytics. It means that

CLOUDS=f(data storage, data ,integrity, data analysis)..... (5)

V. Results and Analysis of Proposed Work Simulation

For accessing cloud services using GSM Network concept of SDR as digital filter is designed. To access services, a signal of particular frequency in licensed band of GSM is generated. For this purpose a licensed band created. After that, define signal will propagate in defined frequency ranges with other undefined signals. In last our digital filter extract out defined signal. The detail of this

entire scenario, i.e. defined signal frequency, licensed GSM band, multiple signal propagation, extraction of defined signal is depicted step by step with all requirements.

A. Signal Generating and Conceptualization

In Figure . 4 contiguous blue lines describe the defined signal using mathematical equation cos(2*pi*t* frequenc l/20) for time period 1 sec at frequency 1000Hz. Basically it is the generation defined signal for accessing cloud services.

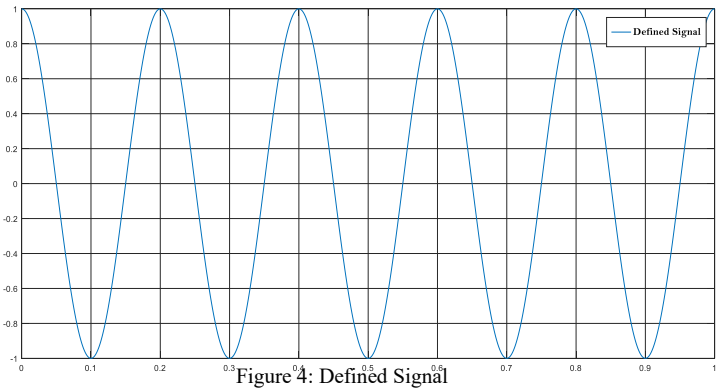


Figure 4: Defined Signal

In Figure . 4 contiguous blue lines describe the defined signal using mathematical equation cos(2*pi*t* frequenc l/20) for time period 1 sec at frequency 1000Hz. Basically it is the generation defined signal for accessing cloud services.

B. Spectrum Generating and Conceptualization

After defined signal generation next step goes to Spectrum generation .On the basis of scenario, Spectrum is generated with sampling frequency 1000 Hz and having frequency range 0 to 1000 Hz, is shown in Figure 5.

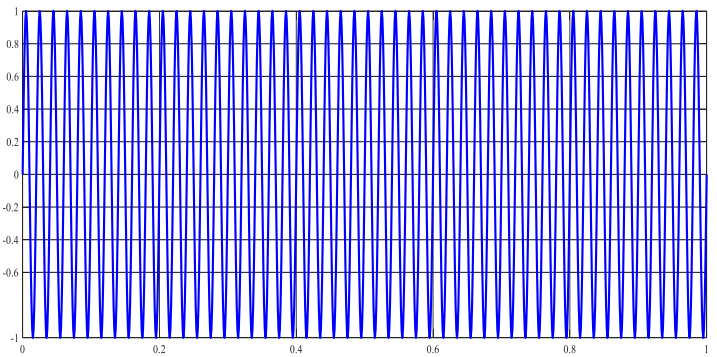


Figure 5: Spectrum Generation

C. Multiple Signals Broadcasting in Same Spectrum

As spectrum holes are there in GSM band, to enhance the efficiency of spectrum, a number of users utilized band. So in the same spectrum band defined signal broadcast with other signals. This phenomenon is shown in Figure 6.

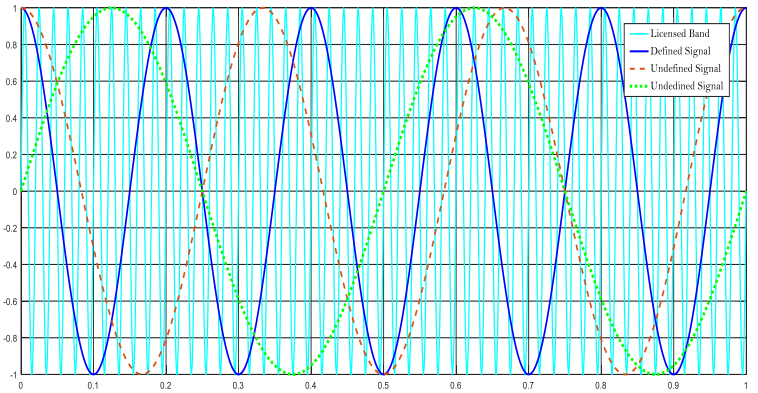


Figure 6: Multiple Signals Broadcasting

D. Extracting Defined Signal through SDR (Digital Filter) from GSM Band Spectrum

When defined signal broadcast in defined GSM band then defined signal modified due to addition of noise. Where blue spark lines in Figure 7 show this. Whereas black dotted lines shows the undefined signal. After removing the noise from defined signal to carry out cloud services , blue dotted lines in Figure 7 obtained after the filtration of defined signal from noise.

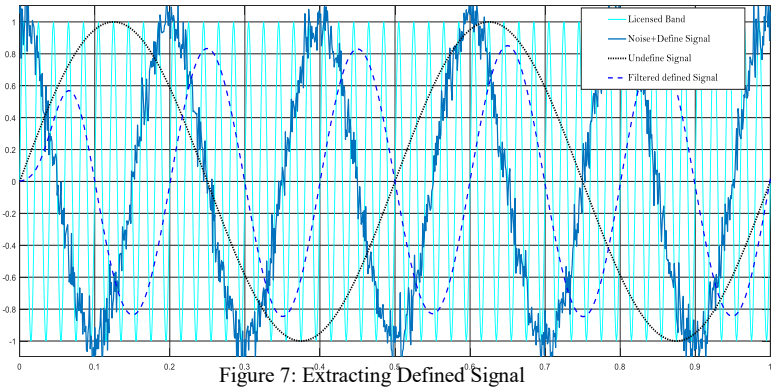


Figure 7: Extracting Defined Signal

D. Analysis on Defined Signal

Analysis is performed on defined signal. Analysis of signal is performed in term of spectral power density, Autocorrelation.

i. Power Spectral Density

Power spectral density is a very valuable tool. Power spectral density exposes the intensity of frequencies variations and at whatever variations are feeble by utilizing the strength of the alterations (energy) as a function of frequency.PSD integrating within frequency range, energy within that specific frequency range is gained. Inspection of variation in frequency domain is reliable way to noticing time series data variations and frequency transformation of time. PSD demonstrates which frequency dimensions alteration are intense and for further analysis that would be quite useful. Table4 demonstrate the PSD of defined signal that is extracted from GSM band spectrum. PSD calculated at different frequencies are listed in TABLE 4.

TABLE4
PSD OF EXTRACTED DEFINED SIGNAL

Frequency (Hz)	Power (dB)	Power MilliWatts
10	-18.83	13.0918
20	-44.61	.03459
40	-52.14	.006109
60	-61.7	.000676
80	-59.75	.001059
100	-58.98	.001265

In similar way Table 5 demonstrate the PSD of original defined signal before propagation.

TABLE 5
PSD OF ORIGINAL DEFINED SIGNAL

Frequency (Hz)	Power (dB)	Power MilliWatts
10	-18.81	13.1522
20	-44.61	.03459
40	-52.14	.006109
60	-61.9	0.000645
80	-59.75	.001059
100	-58.96	.001270

Both extracted defined signal PSD and original signal PSD graphical representation can be view in figure 8 which depict that defined signal that is propagating in licensed GSM band after implementation of proposed technique PSD of it remain same without interfering other signals.

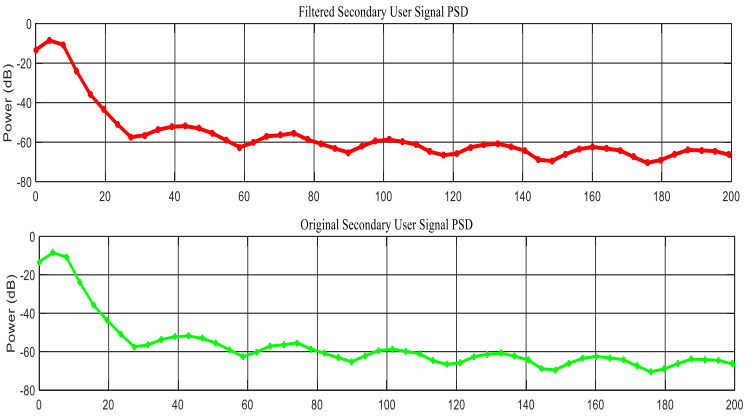


Figure 8: Comparative Analysis of Power Spectral Density

ii. Auto Correlation

Correlation is a relationship that exists between signals. Correlation procedures are broadly utilized as a part in signal processing with numerous applications in media communications, material science, stargazing, geophysics and many more.

Numerous valuable properties of correlation has been given, for example the ability to

- Perceive designs within analogue, discrete-time or digital signals.
- Correlation is an examination procedure
- The correlation between two functions is a measure of their comparability.

When measuring the correlation between two functions, the result is often expressed as a correlation coefficient, ρ, within the range –1 to +1.

ρ = - 1	ρ = 0	ρ = +1
Similar but opposite	No similarity	Exactly similar

For periodic functions, with period T, the correlation function is given by [25]

$$R_{12}(\tau) = \frac{1}{T}\int_{\frac{-T}{2}}^{\frac{T}{2}} v_1(t)v_2(t-\tau)dt \qquad \text{---------- (6)}$$

R12(τ) is the correlation function and is a measure of the similarity between the functions v1(t) and v2(t). The measure of correlation is a function of a new variable,τ, which represents a time delay or time shift between the two functions. That correlation is decided by multiplying one signal, v1 (t), by someone else shifted in time, v2 (t-τ), and finding the integral of the product, in this fashion correlation concerns multiplication, time shifting (or delay) and integration

Autocorrelation, identified as serial correlation. In signal, the perception of autocorrelation has meaningful aspect of tragedy. Autocorrelation action of signal suggests the generic dependence of codes of samples at one time on codes of sample at other time. Informally, it is similarity between considerations as a function of the time lag between them. The ACF (Autocorrelation function), R (τ), is noticed as by [25]

$$R(\tau) = \frac{1}{T} \int_{\frac{-T}{2}}^{\frac{T}{2}} v(t)v(t-\tau)dt \quad \text{---------- (7)}$$

For auto correlation, the correlation coefficient is given by [25]

$$\rho = \frac{R(\tau)}{\sqrt{R(0).R(0)}} = \frac{R(\tau)}{R(0)} \quad \text{----------(8)}$$

Resultant correlation coefficient of original signal and filtered signal are computed in MATLAB**,** which are given below

$$\rho = \begin{vmatrix} 1.000 & 0.8732 \\ 0.8732 & 1.000 \end{vmatrix}$$

As all calculated correlation coefficients are close to 1, as a result there is a strong positive correlation between each one pair of data which depict that signal extracted from licensed band is similar to original signal. No one can access the cloud services without knowing the frequency of defined signal. If anyone get to know the frequency of defined signal successfully, then digital filter is programmable which can alter the frequency of defined signal simultaneously. Further encryption techniques enhance the security. So by this eaves dropping, outsider attack and malware injection are minimized.

VI. Conclusion and Future Directions

Proposed developed scenario will be helpful in providing the secure access to the cloud services (cloud data utilization, data storage). Secure access to the cloud services provided by implementing

the signal of defined frequency in licensed GSM band which is generated by using software defined filter. Only defined frequency range will provide the access to the cloud services. Users are restricted to use the particular frequency range to access the cloud services. In this way security threats to cloud computing can be minimized and access to the cloud services can be restricted.

More research is required to develop New and modern techniques to remove vulnerabilities found in licensed bands for quick and efficient access to cloud services.

REFERENCES

[1] Curran.K, Carlin.S and Adams. M. Security issues in cloud computing- published in August 2011, Elixir Network Engineering.
[2] Malgey.S, and Chauhan.P. A Review on Security Issues and their Impact on Cloud Computing Environment, 2016
[3] Mell.P and Grance.T, The NIST Definition of Cloud Computing, Version 15, October 7, 2009.
[4] Soren Bleikertz et al, ―Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds‖, CCSW 2010, Chicago, USA.
[5] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada.
[6] Flavio Lombardi& Roberto Di Pietro, ―Transparent Security for Cloud‖, SAC‘10 March 22-26, 2010, Sierre, Switzerland.
[7] Rongxing et al, ―Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing‖, ASIACCS‘10, Beijing, China
[8] Mladen A. Vouch, ―Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246.
[9] R. La‘Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA.
[10] B. Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C,Wiley India Edition, 2nd edition, 2007.
[11] Behrouz A. Forouzan, Cryptography & Network Security, McGraw- Hill, Inc., New York, NY, 2007.
[12] The Cryptography Guide: Triple DES". Cryptography World. Retrieved 2010-07-11.
[13] Issa M.Khalil et al,security concern in cloud computing,2013 10th international conference on information technology:NewGenertaion.
[14] Flavio Lombardi and Roberto Di Pietro, “Transparent Security for Cloud”, March 2010, Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415.
[15] A Review on Security Issues and their Impact on Cloud Computing Environment Sadhana Malgey1, Mr. Pranay Chauhan
[16] A Survey on Cloud Security Issues and Techniques Garima Gupta1, P.R.Laxmi2 and Shubhanjali Sharma
[17] Wenchaoet al, ―Towards a Data-centric View of Cloud Security‖, CloudDB 2010, Toronto, Canada.
[18] Jinpeng et al, ―Managing Security of Virtual Machine Images in a Cloud Environment‖, CCSW, 2009, Chicago, USA.
[19] Miranda &Siani, ―A Client-Based Privacy Manager for Cloud Computing‖, COMSWARE‘09, 2009, Dublin, Ireland.
[20] R. Balasubramanian, Dr.M.Aramuthan (2012) Security Problems and Possible Security Approaches In Cloud Computing.
[21] Dan Lin & Anna Squicciarini, ―Data Protection Models for Service Provisioning in the Cloud‖, SACMAT‘10, 2010, Pittsburgh, Pennsylvania, USA.
[22] Federal Communications Commission (FCC), "Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Tech-nologies," ET Docket No. 03-108, Mar. 2005.
[23] Cognitive Radio Technology, [Online] Available: http: //www. of corn. org.uk/ research/technology / overview / emer_tech / cograd / cograd_main.pdf
[24] W.Stallings, “Cryptography and Network Security”, 5th Edition, Prentice Hall, 2011.
[25] Fabrice Gens, Jean-Pierre Remenieras and Stephane. Diridollou .” Estimation of the Correlation Amplitude of RF Signals in Small Cutaneous Vessels”.IEEE transactions on ultrasonics, ferroelectrics, and frequency control, vol. 47, no. 6, november 2000

Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 7, No 1, June 2017

Performance Comparison of DSR and AODV Routing Protocols for Soft Delay Deadlines in Wireless Multimedia Sensor Network

[1]Sana Sarwat, Ayesha Tahir, Salman Afsar Awan and Mudassar Ahmed

***Abstract*- Wireless Multimedia Sensor Network (WMSN) is a collection of the vast amount of different types of sensors like camera sensor, video and scalar sensors which are involved in retrieving multimedia data from the large environment. The real-time sending of video and audio content to the destination before a strict playout deadline has been necessary for multimedia environment. Otherwise, it will be dropped at the destination. In WMSN sending real time multimedia data with soft play deadlines is a challenging task to solve this challenge, routing protocols play an important role in WMSN. Routing demands of multimedia content of WMSNs need to be perfect routing protocols to optimize path selection and guarantee communication. This paper presents a performance comparison between two reactive routing protocols; namely AODV and DSR, with soft delay deadlines and efficient utilization of resources in WMSN. The objective is to assess the real-time behavior of these two protocols upon sending multimedia content. Here, we evaluate the performance with respect to the use of these matrices like latency, Average jitter, Average delay and throughput and factors includes are CBR and multimedia traffic with varying packet size and bandwidth. DSR perform better as compared to AODV routing protocol since it discovers the routes more efficiently. AODV is better in term of Jitter than DSR. NS-2 simulator tool used for the purpose of this comparison.**

Keywords: WMSN, AODV, DSR, NS2, Average Delay, Latency, Average Jitter, Throughput.

I. INTRODUCTION

The wireless networks provide portable customers with ubiquitous processing capabilities and data, giving little attention to the user area. They are order in two types: Infrastructure and Infrastructure-less systems (multi-hop). The infrastructure system is associated with covering a lid (one computer) to another sink. In any case, Infrastructure-less has no stable routers, each node may be like a router [5]. All nodes are armed for progress and can be progressively linked in a discretionary manner. The infrastructure-less systems are otherwise called or Mobile-Ad-Hoc Networks (MANET) or Ad-Hoc Networks [13].

Wireless Multimedia Sensor Network (WMSN) are multi-hop networks collective a huge amount of sensor. It may be camera sensors or scalar sensors which scattered with the enormous

[1] sanasarwat@hotmail.com

environment to gather multimedia contents by means of different concern like audio, image, and video [10, 15]. Each sensor has the ability to connect with several other sensors to reach a Base Station (BS) that is the whole network escape in the digital world in WMSN [1, 3]. Samples of WMSNs application consist of environmental monitoring, smart health-care, and security surveillance [14]. Therefore, the volume of power consumption, detection coverage area, transmission / reception latency and fault tolerance are most of the characteristics that must be measured in WMSNs [17].

Here we clarify the three primary system models for WMNS in this architecture. Essentially wireless multimedia sensor network (WMSN) arrange engineering. It is comprehensively characterized in three classifications as shown in Fig. 1, relying upon way with focusing on the application [16, 4].

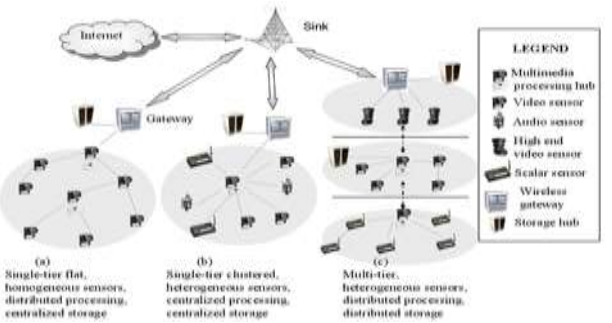


Fig. 1 Architecture of WMSN

The ad hoc routing protocol is divided into the following types. The protocols with flat routing protocol classification are basically alienated into two categories. First, reactive routing protocols. Second Proactive routing protocols. For both protocols, one thing is generic which is every node that is interested in routing plays the same role [7].

In reactive routing protocol route is determine when we need them. When a node tries to transmit a packet, it may have to wait for route discovery. Examples of such schemes are Dynamic Source Routing, Ad-Hoc On-Demand Distance Vector Routing (AODV) etc. However, in the proactive routing protocol, the path is predefined; so the routes are already present whenever needed. Route Discovery overheads are large in such schemes. Examples of such schemes are the conventional routing schemes, Destination Sequenced Distance Vector (DSDV) [12].

The real-time sending of video and audio contents to the destination before a strict playout deadline has been necessary for multimedia environment. Otherwise, it will be drop by destination. In WMSN, it is challenge task to provide soft delay deadlines for optimization of multimedia data. To solve the soft play deadlines challenge routing protocols, play an important role in WMSN. For this purpose, routing protocols are use to maintain the routes and communication in the network to choose potential forwarding nodes for soft play deadlines. Therefore, satisfy routing demands of multimedia contents need to be perfect routing protocols for WMSNs, for path selection.

To understand the importance of real-time sending of multimedia contents in this paper, we have built comparison of performance for reactive routing protocols for soft delay deadlines with use of efficient resources are AODV and DSR in WMSNs. These protocols performed the diverse type of behaviors and performance in different mobility rate of packet size in the WMSN. Here, we evaluate the performance with respect to measuring performance metrics like latency, average jitter, average delay and throughput using CBR and multimedia traffic in the above comparison of these two protocols. We compare the performance by using of NS-2 simulator tool.

The remainder of the paper is organized as follows: section 2 describes two routing protocols AODV and DSR of MANETs. Section 3 describes working methodology. The simulations and results of simulations present in section 4. Finally, section 5 concludes the paper.

II. LITERATURE REVIEW

We briefly explain the studied routing protocols in this section and discussed the detail of working the routing protocols that we used in this paper.

A. Ad-Hoc On-Demand Distance Vector (AODV)

The Ad-hoc on-demand distance vector (AODV) routing algorithm is a routing protocol designed for Ad-hoc mobile devices. AODV is a combination of DSR and DSDV. It has a basic on-demand mechanism of Route Discovery and Route Maintenance similar to DSR, and the use of hop by hop routing, sequence numbers and periodic beacons similar to DSDV. It does not keep routes from each node to each of the other nodes in the network, but is discovered when needed, and is maintained only when needed. The AODV used an algorithm for creation of unicast routes. At a point, during the sending the packets to the target center, the node will have checked the entries in the routing table to confirm that it is available some routes to the target center in the routing table then if there, it will send the information of packets to the right next node near the goal. If it is not available, it used the route discovery method for finding the routes. AODV send a packet, Route Request

(RREQ) and Route Reply (RREP) by using the route discovery method [18]. AODV occupies less overhead on a simple protocol. It keeps up the complete routes in its table for the source host to the target host has some greatest advantages for this protocol. The packet of RREQ and RREP messages responsible for routing discovery where it cannot significantly increase the overhead of these control messages. The routing maintenance is the responsibility of Hello messages that are inadequate. So, it doesn't make needless overhead in the network [8]. The details of elementary operations with respect to AODV routing protocol are describe including routing creation, deletion, and maintenance.

B. Dynamic Source Routing (DSR)

Dynamic source routing (DSR) is refined instances of on-demand routing protocols based on source routing concepts. The nodes keep the routing cache that contains the source route it knows and updates the entries when learning new routes in the routing cache [9]. It is specifically intended for multi-hop and self-organizing networks for mobile nodes. This allows the network to fully self-organize and self-configuration. It does not need slightly current network organization and management. DSR routing protocol does not utilize periodic routing messages (such as AODV) and dipping overall network bandwidth, redeemable battery power and evading a huge number of routing apprises. Route Discovery and Route Maintenance are two routes contained by DSR routing protocol. It is effort both for sense to the node. It keeps up the source routes from randomly to the last stop goal is an exclusive advantage of it. It detects the routes as rooting is part itself, can be detected directly [2,6]. It works when there is demand available, where data does not send like path announcements occasionally. Due to this traffic produced by DSR protocol may be reduced. Therefore, overhead packets evaded. It has only two main stages: the first one is route discovery and second is route maintenance.

III. WORKING METHODOLOGY

In this section, the research work will have performed using from the start to selection of techniques and framework for network performance to explain as well.

A. Simulation Model

We use the different network parameters SHOWN in table 1 for our simulation by using the NS-2. Network Simulator (NS-2) is an acknowledge the correct development of every node, correct act of

every node started to record, and additionally the correct time for every adjustment in movement or gathering for simulation shown in Fig. 2.

TABLE I
SIMULATION PARAMETERS

Parameter	Details
Simulator	NS-2.35
Area of simulation	1800 m * 840 m
MAC protocol	802.11
Radio Propagation model	Two Ray Ground
Routing Protocol	AODV, DSR
Traffic Type	CBR, Multimedia
Number of nodes	22
Network interface Type	Phy/wirelessphy
Channel type	Channel/Wireless channel
Interface queue type	QueuelDrop Tail
Antenna	Antenna/omni antenna
Maximum packet in ifq	50
Packet size	1000 to 8000
Bandwidth	54Mb, 108Mb,300Mb

Trace files are create made for every time of simulation as shown in Fig 2 is stored on disk and examined utilizing different scripts, specifically a record file named (* .tr) consist of the quantity of packets effectively conveyed and the length of the packet path and other information of each execute script. Use AWK and perl files and Microsoft Excel files to further analyzed this data to generate charts [7].

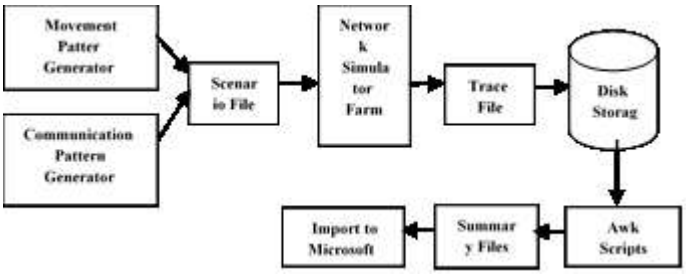


Fig. 2 Model of NS-2

The Network Simulator tool (NS-2) version 2.35 used to build the simulation model. There are create three cases run at a nominal bit rate with 54Mbps, 108Mbps, 300Mbps. The experiments conducted with use of packet size are 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000. There is 22 fixed number of source nodes and 50 queue size takes for every simulation used by simulation. A packet rate transmits the packet to 54Mb, 108Mb and 300Mb were takes. The area for this simulation used is 1800m x 840m with 22 stations expected as to consistently scattered in the area. CBR and multimedia traffic are use for this simulation. Alike CBR and Multimedia traffic are also use for both protocols to get fair results. Testbed model that we used to perform the simulation results are shown in Fig. 3 below.

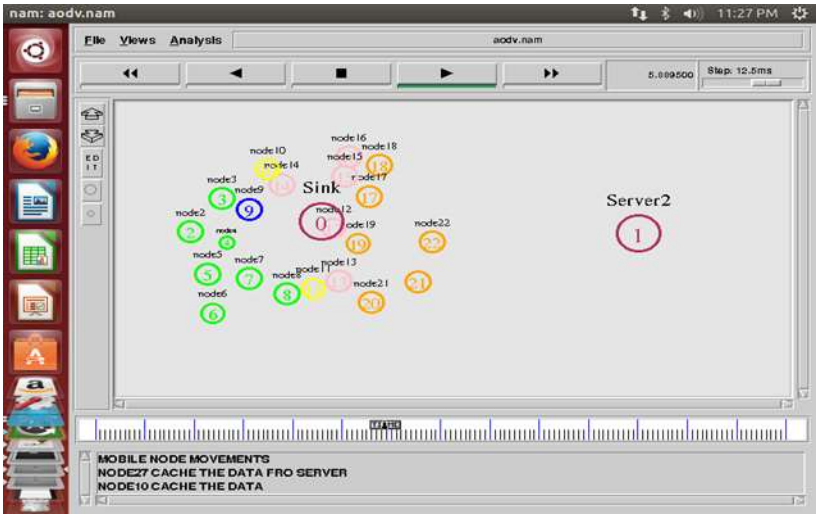


Fig. 3 Testbed Model of NS-2

B. The Simulation Scenarios

The following assumptions are made when we wrote the Tcl script.

1. We take three kinds of cases of bandwidths with 54Mb, 108Mb and 300Mb with the basic rate of 5Mb, 10Mb, and 27Mb.
2. Every sender node has constant bit rate (CBR) traffic and Multimedia traffic (VBR and CBR) with a packet size of 1000, 2000, 3000, 4000, 5000, 6000, 7000 and 8000 the rate of data rate is 54Mb ,108Mb, and 300Mb (number of stations send packet).
3. Two kinds of routing protocol DSR and AODV are used to implement the wireless multimedia sensor network environment and compare with one by one to both traffic model and with all cases of bandwidths with 2.472e9 frequency rate.

4. 22 sensor source nodes and 50 Queue size take are created fixed in every scenario for simulation environment.
5. Comparing all result with other assumption and draw the result with tables and design graphs in MS Excel.

C. *Performance Metrics*

Some important performance metrics discussed in this section for these two routing protocol simulators. These metrics are listed below:

1) Latency

It is the time that is required to distribute the packets in the networks. It is calculated in many diverse points of view like round trip and one way but I use round trip.

2) Throughput

Throughput successfully delivered a number of the message as a per unit of time. The throughput was calculated in bits per second (bps), megabits per second (Mbps) or maybe gigabits per second (Gbps).

3) Average Delay

It is mentioned, the time has taken from source station to destination for transmitting them across the network. It was measured in millisecond and seconds.

4) Average Jitter

The variation in the delay of received packets is called avg jitter. Jitter has been measured in millisecond and second.

Those parameters are explained in detail and clearly plotted with its graphical representation in next section.

IV. SIMULATION AND RESULTS

The Wireless multimedia sensor network (WMSN) simulation performed to evaluate different types of performance metrics for AODV and DSR routing protocols with network simulator (NS-2) tool. The performance matrices are performed in this research are latency, Jitter, throughput, and delay. Latency, jitter and delay parameter is calculating in millisecond unit through awk file in NS-2 and throughput result was shown in kbps. The tables are made against these parameters to displays the corresponding values. Simulation setup and performance metrics description is also given. The

table displays the values of AODV and DSR protocols for varying Packet Size with CBR and Multimedia Traffic, different bandwidths cases with different basic rates for latency, delay, jitter, and throughput. We are analysis and compare the effect of these performance parameters with changing the several packet sizes with varying bandwidths and traffic model. The analysis results display in shape of graphs. Two types of network scenario for CBR and Multimedia traffic are generated.

A. Performance On CBR Traffic

In this section, we analyze the results of AODV and DSR routing protocol in term of latency, jitter, throughput and delay with a varying packet size and 54, 108, 300Mb bandwidths in CBR traffic. We show that results of latency shown in Fig. 4, with 54 bandwidths of AODV and DSR routing protocols below where latency of DSR protocol takes low as compared to other protocol.

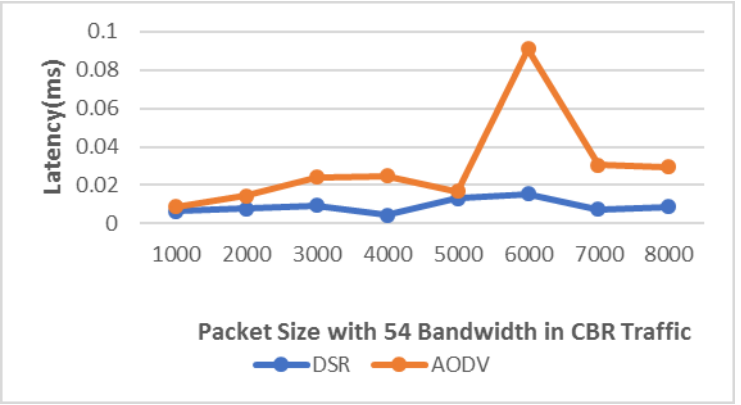


Fig. 4 Latency Vs packet size

We analyze the results of jitter that show in Fig. 5, with 108 bandwidths, which tell the AODV routing protocol is better than DSR protocol.

Fig. 5 Jitter Vs Packet Size

The throughput was better in the DSR routing protocol as shown in Fig. 6, as compared to AODV protocol in form of taking the 54 bandwidths.

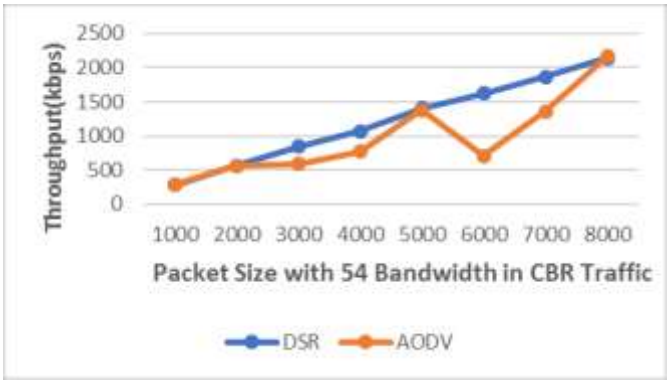


Fig. 6 Throughput Vs Packet Size

In Fig. 7, As the analysis of delay metrics with 300 bandwidths is better for the DSR routing protocols as compared to AODV routing protocol.

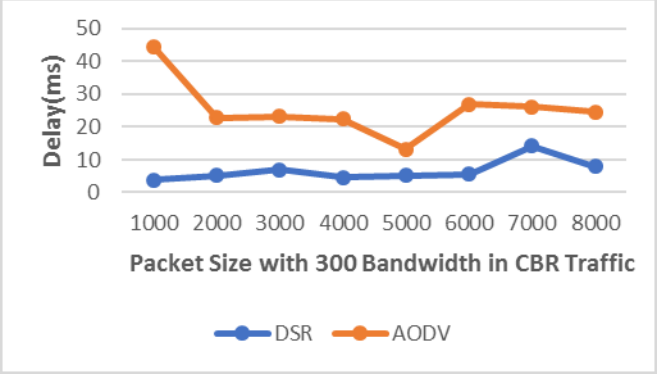


Fig. 7 Delay Vs Packet Size

In this experiment Fig. 8, show that DSR takes low latency as compared to AODV protocol in all cases of bandwidths with CBR traffic and varying packet size. DSR takes less latency to start the process. It has less latency with 300 Mb bandwidths as compared to others bandwidths. DSR routing protocol is better for routing purpose in the matrices of latency.

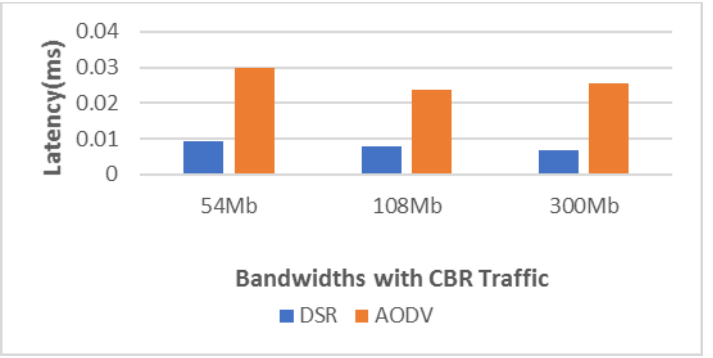


Fig. 8 Latency Vs Bandwidths

In this experiment Fig. 9, shown jitter where AODV takes less jitter as compared to DSR protocol in the all cases of bandwidths in 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000 packet size scenarios. This is because AODV contain routing information in its routing table this reduce the search for new routes. In jitter AODV is best for routing purpose.

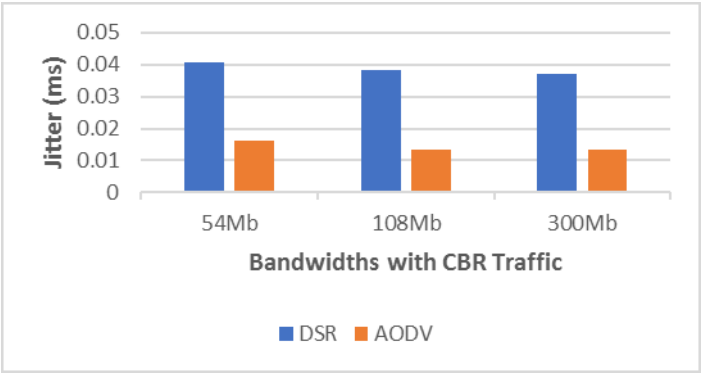


Fig. 9 Jitter Vs Bandwidths

In this experiment Fig. 10 shows where DSR has high throughput as compared with AODV protocol in the all cases of bandwidths with respect to varying packet size. It is observed that throughput for DSR protocol is increases when packet size increase. DSR is better for routing purpose in case of throughput.

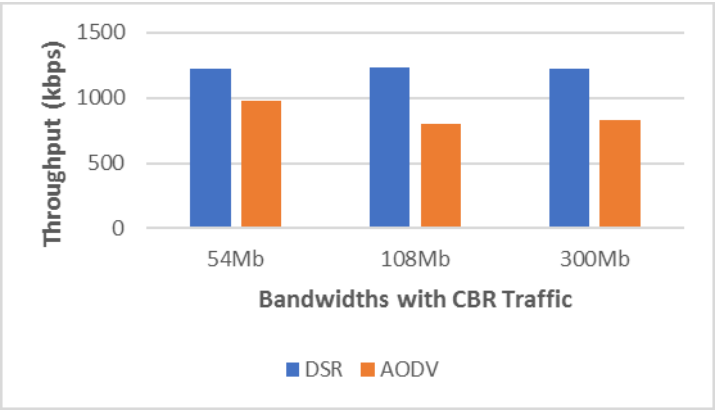


Fig. 10 Throughput Vs Bandwidths

In this experiment Fig. 11 shows variation in delay with respect to 1000, 2000, 3000, 4000, 5000, 6000, 7000 and 8000 packet sizes for variation of routing protocol where DSR has less delay as compared with AODV protocol in the all cases of bandwidths within increases the different packet size because of reactive nature.

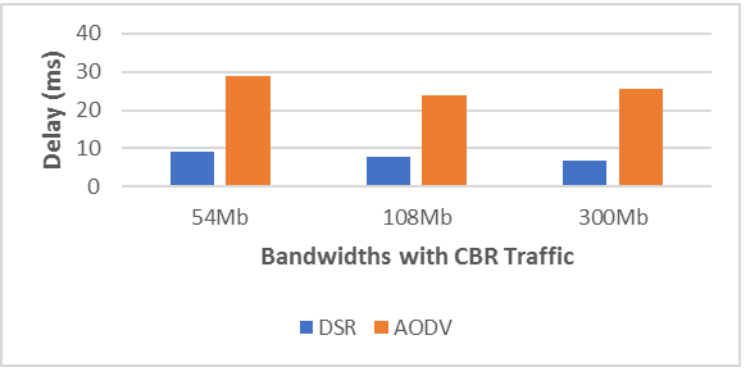


Fig. 11 Delay Vs Bandwidths

B. Performance on Multimedia Traffic

In this section, we compare the performance of AODV and DSR routing protocols for the soft delay in term of multimedia traffic with 54, 108 and 300 Mb bandwidths and varying packet size. Here we use the performance metrics are latency, delay, jitter and throughput for comparing the performance of AODV and DSR protocols in WMSN. In the analysis of latency with multimedia traffic in 300 bandwidths shows in Fig. 12 the results that DSR routing protocol is better than AODV protocols.

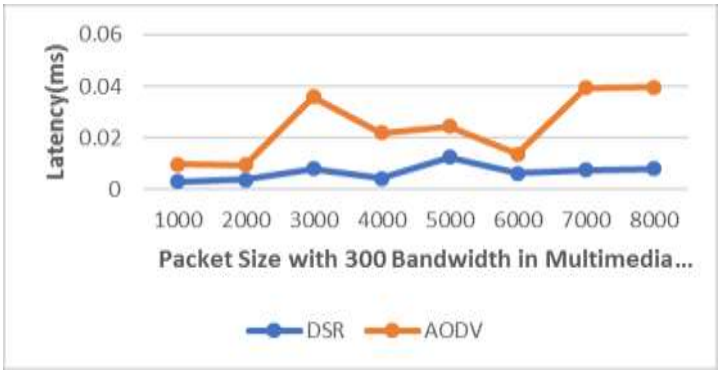


Fig. 12 Latency Vs Packet Size

In this experiment Fig. 13 shown the graph of jitter in millisecond unit not more jitter on DSR side with 54 bandwidths. The DSR has taken high jitter as compared to AODV protocol.

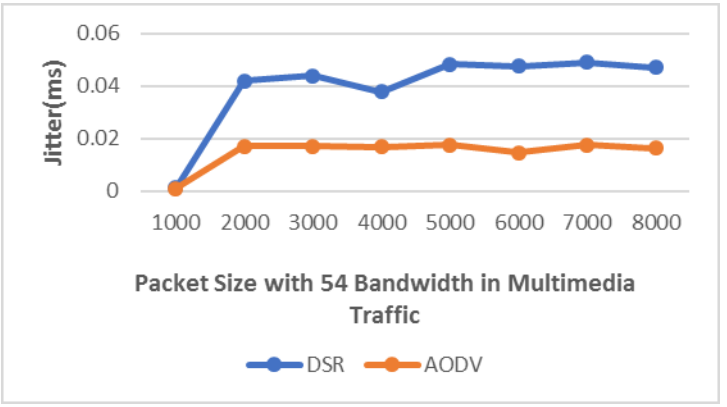


Fig. 13 Jitter Vs Packet Size

In this graph Fig. 14 below for throughput of DSR and AODV routing protocols. It measured for varying of packet sizes 1000, 2000, 3000, 4000, 5000, 6000, 7000 and 8000. The throughput for DSR protocols is high as compare to AODV. DSR has more throughput overall as compared to AODV in data transmit.

Fig. 14 Throughput Vs Packet Size

In this experiment of delay Fig. 15 shows graph below for AODV and DSR protocol with Multimedia traffic and 300 Mb bandwidths. AODV take more delay for transfer data as compare to DSR. DSR protocol is performed well as compared to AODV and has less delay in this experiment.

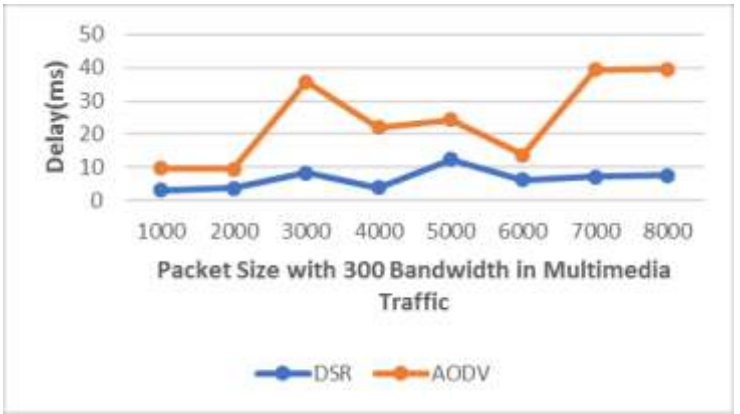


Fig. 15 Delay Vs Packet Size

In this experiment Fig. 16 shown that DSR has less latency as compared with AODV protocol in all cases of bandwidths with varying packet size.

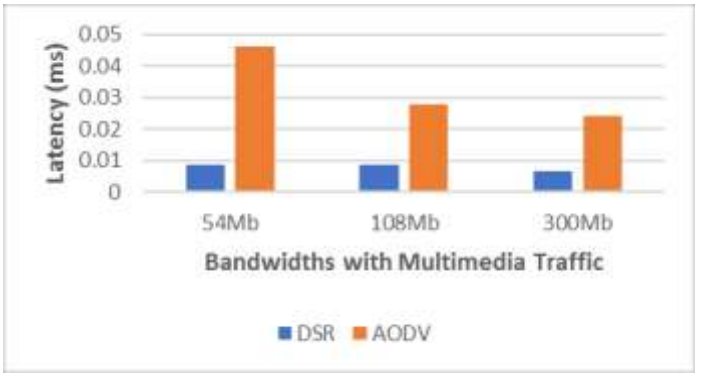


Fig. 16 Latency Vs Bandwidths

In this experiment where AODV has less jitter as compared with DSR protocol in all cases of bandwidths that shown in Fig. 17, DSR take more jitter in 300Mb and 54Mb bandwidth as compared to other bandwidths.

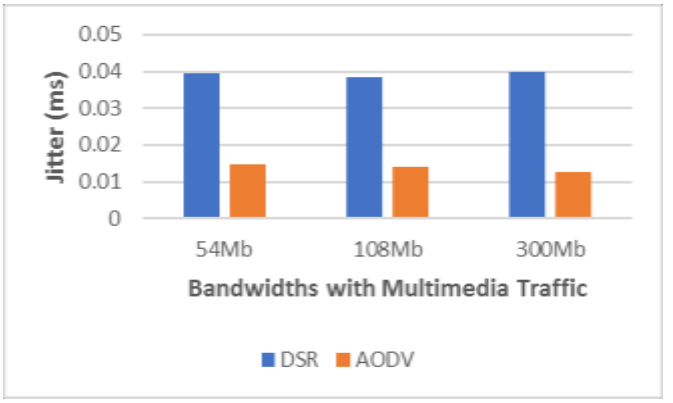


Fig. 17 Jitter Vs Bandwidths

In this experiment Fig. 18 shows throughput for DSR is more as compared to AODV protocol in all cases of bandwidths with multimedia traffic and with varying packet size.

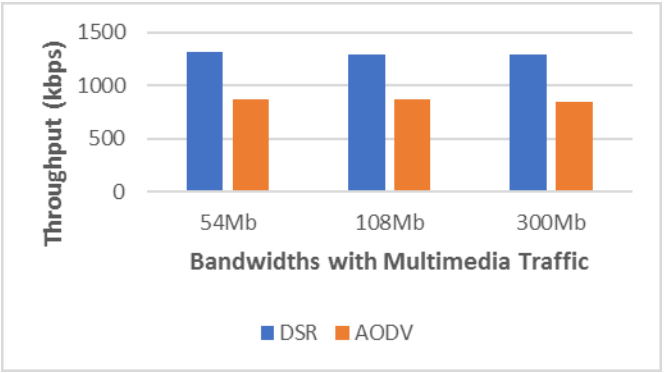


Fig. 18 Throughput Vs Bandwidths

In this experiment, Fig.19 shows where DSR has less delay in all variation of packet size as compared with AODV protocol in all cases of bandwidths. DSR take less delay in 300Mb bandwidth as compared to other bandwidths with respect to multimedia traffic.

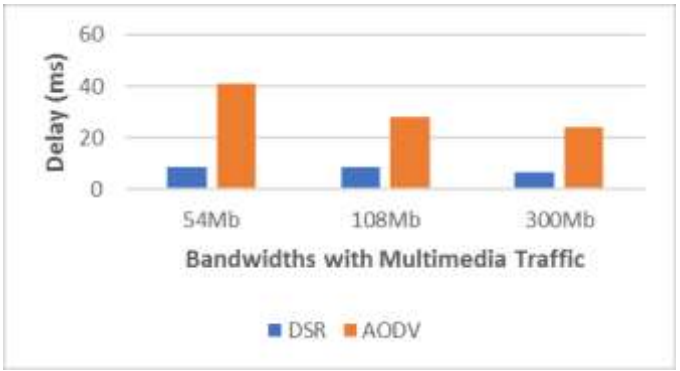


Fig. 19 Delay Vs Bandwidths

In this paper, we analysis that DSR overall is performing well as compared to AODV for routing purpose with respect to performances matrices latency, average delay and throughput with a case of CBR and Multimedia traffic and all scenarios of bandwidths in WMSN for soft playout deadline.

V. CONCLUSION

This paper is an attempt to evaluate the performance of two commonly used mobile ad hoc routing protocols namely AODV and DSR in Wireless Multimedia Sensor Network (WMSN). Performance evaluation did in NS-2 simulator by doing many simulations. The comparison was based on Throughput, Average Jitter, Latency and Average Delay and factors include are CBR and

multimedia traffic with varying packet size and bandwidths. Simulation results are shown in many figures. By using simulation results, we can understand that DSR gives better performance with CBR and Multimedia both traffic simulation conditions as compared to AODV in WMSN. DSR perform better in term of latency, throughput and delay for routing purpose but in case of jitter, it not performs well. To decrease the jitter in case of DSR routing protocol we increase the buffer size to decreases the packet loss. DSR routing protocol is overall best protocol to satisfy the routing demands for multimedia contents for soft play out deadlines in WMSN. In future, a specific type of routing protocols can be designed that provides optimized results with security in all the above performance metrics for WMSN.

REFERENCES

[1] Abuarqouba, A., M. Hammoudehb, B. Adebisib, *S. Jabbar*, A. Bounceurd, and H. Al-Bashara. 2017. Dynamic Clustering and Management of Mobile Wireless Sensor Networks. *Computer Networks*. 117: 62-75.

[2] Ade, S. and P. Tijare. 2010. Performance comparison of AODV, DSDV, OLSR and DSR routing protocols in mobile ad hoc networks. *International Journal of Information Technology and Knowledge Management*. 2(2): 545–548.

[3] Ahmad, A., *S. Jabbar,* A. Paul, and S. Rho. 2014. Mobility aware energy efficient congestion control in wireless sensor network. *International Journal of Distributed Sensor Networks*. 1:10-23.

[4] Akyildiz, IF., T. Melodia, and KR. Chowdhury. 2007. A survey on wireless multimedia sensor networks. *Elsevier Comput Netw*. 51: 921–960.

[5] Amjad, K., M. Ali, S. Jabbar, M. Hussain, S. Rho, and M. Kim. 2015. Impact of Dynamic Path Loss Models in an Urban Obstacle Aware Ad Hoc Network Environment. *Journal of Sensors.* 1(5): 1-8.

[6] Borin, J. F. and N. Fonseca. 2008. Simulation Modelling Practice and Theory Simulator for WiMAX networks. *Simulation Modelling Practice and Theory.* 1:817-833.

[7] Ghadi, M., L. Laouamer, and T. Moulahi. 2016. Securing data exchange in wireless multimedia sensor networks : perspectives and challenges. *Multimedia Tools Application*.1:3425-3451.

[8] Gowrishankar, S., T. Basavaraju, M. Singh and S. Sarkar. 2007. Scenario-based Performance Analysis of AODV and OLSR in Mobile Ad hoc Networks. *International Journal*. 1:1-6.

[9] Gupta, A. K., H. Sadawarti, and A.Verma. 2010. Performance analysis of AODV, DSR & TORA routing protocols. *International Journal of Engineering and Technology (IACSIT)*. 2(2): 226-231.

[10] Hammoudeh, M., R. Newman, C. Dennett, S. Mount, and O. Aldabbas. 2015. Map as a Service: A Framework for Visualising and Maximising Information Return from Multi-Modal Wireless Sensor Networks. *Sensors*. 1:15.

[11] Hassan, Y. K., M. El-Aziz, and A. El-Radi. 2010. Performance evaluation of mobility speed over MANET routing protocols. *International Journal of Network Security*. 11(3): 128-138.

[12] *Jabbar*, S., M. A. Habib, A. A. Minhas, M. Ahmad, R. Ashraf, S. Khalid, and K. Han. 2017. Analysis of Factors Affecting Energy Aware Routing in Wireless Sensor Network. *Wireless Communication and Mobile Computing*. 1(6):1-10.

[13] Kale, R., and Gupta. R. 2013. an Overview of Manet Ad Hoc Network. *International Journal Of Computer Science And Applications*. 6(2): 223-227.

[14] Mbarushimana, C. and A. Shahrabi. 2007. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. *21st International Conference on Advanced Information Networking and Applications Workshops.* 1:679-684.

[15] Minhas, A., S. Jabbar, M. Z. Aziz, and W. Mahmood. 2010. Query-Based Energy-Aware Real-Time Routing for Wireless Sensor Network. *IEEE*. 1(5): 1-5.

[16] Sharif, A., V.Potdar, and E.Chang. 2009. Wireless multimedia sensor network technology: A survey. *7th IEEE International Conference on Industrial Informatics*, 606-613.

[17] Surayati, N. and M. Usop. 2009. Performance Evaluation of AODV , DSDV & DSR Routing Protocol in Grid Environment. *Journal of Computer Science and Network Security*. 9(7): 261-268.

[18] Taneja, S., A. Kush, and A. Makkar. 2010. Experimental Analysis of DSR , AODV using Speed and Pause time. *International Journal of Innovation, Management, and Techn*

Relationship of Social Progress Index (SPI) with Gross Domestic Product (GDP PPP per capita): The moderating role of Corruption Perception Index (CPI)

Bilal Qaisar, [1]Sajid Nadeem, Muhammad Usman Siddiqi, School of Business and Economics, University of Management and Technology, Lahore and Ahmed F. Siddiqi, Institute of Business Management, University of Engineering & Technology, Lahore

***Abstract*- This study investigated the impact of social progress on economic development in 119 countries, while taking their individual corruption perception into consideration. Simple linear regression was use on the secondary data for 119 countries and 5 continents while the SPSS PROCESS macro was used to test the moderating effect of corruption perception. As hypothesized, a positive relationship of the social progress index (SPI) with gross domestic product (GDP) PPP per capita was observe. This means that countries, which fulfill basic human needs, foundations of wellbeing and foster availability of opportunities have enhanced economic development. Moreover, the moderating role of corruption perception between the relationship of social progress and economic development was confirmed; thus indicating that countries with better corruption perception rating possess a stronger relationship of SPI and GDP (PPP) per capita and vice versa. When checked for continents, moderation results showed that the continents that have higher values of corruption perception index (CPI) are more socially and economically developed.**

Keywords: Social Progress, Economic Development, Corruption Perception, SPI, GDP, CPI.

I. INTRODUCTION

Economists have been skeptical about the sufficiency of gross domestic product (GDP) to measure national economy. Stiglitz, Sen, and Fitoussi [1] called GDP a "wrong metric" for the economy, and that it forces us to set and strive for irrelevant economic goals. This lead to the development of the social progress index (SPI), also called social progress imperative. It is a comprehensive measure of social progress with inclusive growth, i.e. the combination of economic and social progress, including environmental performance. This measure was developed by Michael E. Porter and his colleagues [2]. SPI focuses on three aspects of social progress, i.e., citizen wellbeing, basic human needs, and opportunities available. SPI country scores are calculated through 54 indicators [2]. The literature also shows divergence in theoretical perspectives for the

[1] sajid.nadeem@outlook.com

relationship between corruption and social as well as economic growth. Some authors argue that corruption enhances economic growth while others contend that corruption result in wastage of resources [3].

Corruption Perception Index (CPI) was first developed by Transparency International in 1995. It is a composite measure of corruption [3]. Scores ranging from 100 (very clean) to 0 (highly corrupt) which rank countries based on the perceived level of corruption as evaluated by expert opinions and surveys [4]. There is an ongoing debate within the literature on the relationship between GDP and corruption. Results from several empirical studies assert that corruption does not have a negative consequences for GDP per capita growth [5].

Primarily, this study aims to explore how the social progress influences economic development of a country and promote skill development. In addition, this research investigates the impact of corruption perception on social progress and economic development of a country.

A higher GDP does not necessarily show that the government has succeeded to provide for the basic human needs, standard of living and sense of security to the citizens. Therefore, GDP can not be used as an exclusive measure of social progress of any country. To overcome this flaw, Porter et al. [2] developed a multi-dimensional scale which could gauge the performance of countries on the underpinnings, i.e., basic human needs, environmental sustainability and opportunities for its citizens to provide a more holistic picture of their society. As per the statistics, SPI and GDP (PPP) per capita had 88% correlation with non-linear relationship [2]. The SPI measures a country's absolute performance along with its relative performance by comparison with economic peers to understand the economic progress and the social outcomes. This encourages improved public policies and investment.

SPI is a relatively new index and was first released in 2014 [2] as compared to GDP (PPP) per capita and CPI. Consequently, there is a lack of literature on SPI and its relationship with other variables. On the contrary, a considerable amount of research has been conducted around the construct of GDP. The relationship between economic development and social progress is complex, so this study probed into the relationship of SPI and GDP (PPP) per capita with CPI as a moderator. The SPI quantifies the degree to which countries cater for their citizen's social and environmental needs by ranking them on 54 indicators related to social performance, health services, basic and higher education, security situation, communication facilities, environment sustainability, access to

information and tolerance in society [2]. The scoring criteria can facilitate government to identify their strong and weak areas for corrective actions.

This research aims to fill the prior stated research gap in the literature and verify the predicting power of recently developed SPI scale. The core objectives of this study are to quantify the relationship between SPI and GDP (PPP) per capita and to demonstrate to governments, the benefits associated with social progress. Another objective is to assess the superiority of using social indicators like SPI for social prosperity rather than economic measures and lastly to assess the role of corruption in economic development and social progress of any country.

The organization of this paper is as follows. The next section integrates the existing literature on the study variables and the aforementioned research gap for the proposed hypotheses. Later section followed by research methodology. The fourth and fifth sections report and discuss the study results. Then study limitations will briefly discussed in section six. The study concludes with future research, implications for practitioners and conclusion sections.

II. Literature Review

GDP (PPP) per capita is use as an economic indicator of a country to measure its standard of living and productivity as compared to other countries. It is considered as an accurate measure to assess the total value of an economic activity instead of merely value added by the activity. This is especially helpful to note outputs of individual industries and sectors. It was developed during the great depression by economist Simon Kuznets [6].

Recognizing the shortcomings of GDP, the United Nations Human Development Index (HDI) was developed almost 25 years ago, but it incorporated only a few indicators. HDI also did not cater for environmental sustainability. This lead to the development of the SPI, a comprehensive measure of social progress with inclusive growth, i.e. the combination of economic and social progress, including environmental performance.

The previous literature lacks consensus on s specific definition of corruption. The term is commonly conceptualized as ‘the misuse of public office for private gain’. Some researchers have differentiated various forms of corruption for conceptual clarity, e.g. petty corruption, grand corruption, public office-centered corruption, market-centered corruption, public interest-centered corruption [3].

Ahmad and Arjumand [7] empirically studied the impact of corruption, specifically on GDP per capita through international migration in 94 countries. The results showed that high corruption level

in any country negatively affects GDP per capita. A significant positive association between GDP per capita and migration was found in literature, while a decrease in corruption will directly increase in migration.

Mauro [8] and Grabova [9] found empirical evidence showing significant negative correlation between corruption and GDP growth. Researchers have therefore claimed that corruption deters growth by lowering private investment. Kim and Lim [10] also found a negative correlation between corruption and other growth variables such as private investment, but did not find strong statistical evidence to support the same claim between corruption and economic growth. Shao et al. [11] found a negative correlation between corruption levels and the long-term growth of a country. Podobnik et al. [12] showed that a one-unit increase in CPI value (or lower corruption) led to a 1.7% increase in GDP per capita growth rate.

As corruption is usually a concealed act, therefore it is not easy to obtain or access it through primary data [3]. Some researchers and international bodies tend to estimate the level of corruption, whereas others use the survey method to quantify the corruption perception of residents or combine both types of measures [13].

Purchasing power parity (PPP) in GDP per capita is an estimated measuring scale of living conditions in a particular country. It is calculated using World Development Indicators (WDI) [7]. A comparison study was conducted by Ram [14] to estimate the GDP (PPP) per capita published by international comparison program (ICP) from World Bank. The study advised the users to be cautious while using this data for cross-country studies in which GDP (PPP) per capita is used as a core variable. This caution is suggested due to the existence of significant differences between the correlations of ICP and World Bank PPP GDP per capita in 73 of the 163 countries [14, p. 9].

Ahmad and Arjumand [7] mentioned that in previous literature, arguments have been made in support of corruption as it “greases the wheels” of commerce by avoiding non-industry friendly government regulations. The counter argument in literature, tested by few researchers, is that corruption always “sands the wheels” of commerce as the government starts trying to impose more restrictions and barriers.

Corruption is one of the fundamental factors affecting economic growth of countries and costs more than 1 trillion US dollars annually worldwide [3], [15]. It is inevitable in almost every society, but differs across countries due to their economic status and political systems [16]. Economists have been studying the phenomenon of corruption and its impact on economic growth for a long time [9].

There is a lack of theoretical consensus in the empirical literature while explaining the effects of corruption on economic growth in GDP per capita [3], [7]. Méon and Sekkat [17] empirically confirmed the destructive impact of corruption on economic growth. Xu [3] cited previous literature that justified the existence of corruption as a positive thing in developing countries where bureaucrats are unmotivated and corruption cuts the red tape, thus helping entrepreneurs [18]–[22]. The other side to this coin is lowered tax revenues generated, embezzlement frauds, and waste of human talent [3].

SPI differs from GDP by two of its core features, i.e. it excludes economic variables and uses outcomes instead of inputs for the economic process measurement. SPI offers the foundation for understanding the underlying relationship between social progress and economic development. The social progress is subdivided into three dimensions, i.e. a country's capacity to meet basic human needs, has the institutional support system to improve the quality of life and cultivate an environment in which the general populous has the opportunity to flourish.

The following research questions were developed after reviewing the literature and analyzing the limitations of previous researches.

1. Does SPI of a country result in higher GDP (PPP) per capita?
2. Does CPI have a moderating effect within the relationship of SPI and GDP (PPP) per capita?

Figure 1. Proposed Conceptual Framework (Author's Formulation)

The literature suggests the presence of a directional relationship between these study constructs. Two reports, Social Progress Index 2015 and Corruption Perception Index 2015 were used to operationalize the constructs. Two directional hypotheses were formulated as per opinion of Forza [23]. In these two hypotheses, SPI score and GDP (PPP) per capita are independent variable and dependent variables respectively. CPI will be used as a moderator between the relationship of SPI score and GDP (PPP) per capita.

A. SPI and GDP (PPP) per capita

To evaluate the relationship between social progress and economic development, all dimensions of social progress must be taken into account. Dimensions of social progress include basic human needs, foundations of wellbeing and opportunity. Basic human needs are likely to improve rapidly with GDP (PPP) per capita at relatively low levels of income. These needs include nutrition and basic medical care, water and sanitation, shelter and personal safety, which may improve with higher GDP at lower levels of income. Foundations of wellbeing are likely to improve marginally with higher levels of income. This marginal increase can be contributed to the fact that economic progress may also lead to new challenges, such as obesity and environmental degradation. Opportunities are also less likely to improve with GDP (PPP) per capita because many aspects of opportunities, such as rights and freedoms, do not necessarily require large resource investments, but are influenced by norms and policies [2].

Hypothesis 1: *Social Progress Imperative score of each country positively impacts Gross Domestic Product (PPP) Per Capita.*

B. CPI as Moderator in the relationship of SPI and GDP (PPP) Per Capita

A country with a less corrupt system, where public power prevails, will be economically more developed and prosperous. Basic human needs such as appropriate nutrition, water, public health care system, sanitation, shelter and personal safety can be met if resources for such public initiatives are available. Foundations of wellbeing such as access to education and communications, health and ecosystem sustainability are all possible if the country's system is free from corruption. Opportunity includes having access to personal rights, personal freedom, choice, tolerance, inclusion and access to advanced education, if the masses are given access to these rights, without the use of unfair means, this can ensure that people from that country can excel ultimately making that country economically developed and socially progressive [2].

Hypothesis 2: *CPI will moderate the relationship between SPI and GDP (PPP) per capita.*

III. Research Methodology

This study was conducted using the quantitative research method. This method was used so that the results of quantitative research can be depicted in a numerical form [24], with more generalizability and consistency. The results are likely to be free of researcher bias [25] as secondary data was used to test the proposed research hypotheses. The data was collected from two sources,

i.e. Social Progress Index 2015 [2] for GDP (PPP) per capita and SPI scores and the Corruption Perception Index 2015 [4] for CPI scores of each country.

A. Data Processing and Analysis

For 126 countries, secondary data was available for all three variables from the aforementioned reports and indices. This data was entered into SPSS (version 23) for statistical analysis. Descriptive statistics were calculated for central tendency and dispersion. Conditions of data normality [26] were observed for the data set. To achieve normality in the data, 7 countries were removed from the data set. Regression analysis was run to test hypothesized relationships between variables. The assumptions of regression analysis were tested and found to be satisfied. Hypothesis contains one dependent and independent variable; therefore, simple regression analysis was conducted to evaluate the relationship between two variables. To test the second hypothesis, which intends to measure CPI score's moderating effect between the relationship of SPI and GDP (PPP) per capita, SPSS "PROCESS" macro was used, which was developed by Andrew F. Hayes [27].

B. Assumptions for Regression Analysis

Several assumptions need to be fulfilled before using regression analysis [26]. The first condition is fulfilled, as the data used was quantitative in nature. Shapiro-Wilk test (significance level=0.05) was used to check the normality of both outcome and the predictor. Initially, value of significance was below 0.05; therefore, certain entries were removed in order to achieve normal distribution. Consequently, a significance value was calculated to be 0.067. Shapiro-Wilk value for the relationship between SPI and GDP (PPP) per capita was found to be 0.383. This study has only one independent variable, which will not raise any issue of multi-collinearity. Durbin-Watson statistic was used to check the condition of auto-correlation. Initially, first-order auto-correlation was found, but was removed. The value of Durbin-Watson statistic was 1.971 shows that a negligible auto-correlation is present between the observations.

IV. RESULTS

Descriptive statistics were used to find out the central tendency and dispersion. Results of the mean and standard deviation were generated (see Table 1).

TABLE I
DESCRIPTIVE STATISTICS OF STUDY VARIABLES FOR 119 COUNTRIES

Variable	*M*	*SD*
Social Progress Imperative	63.9695	13.63430
Corruption Perception Index	42.46	19.525
Gross Domestic Product (PPP) Per Capita	14590.94	13021.645

*Note: The values for SPI, CPI and GDP (PPP) Per Capita are for the year 2015.

Similarly, data was split based on continents and the mean and standard deviation values for all variables are presented in Table 2.

TABLE II
DESCRIPTIVE STATISTICS OF STUDY VARIABLES FOR FIVE CONTINENTS

Variable	Continent	*M*	*SD*
Social Progress Imperative	Asia	58.725	10.4383
	Africa	50.8343	9.32131
	Europe	75.4353	8.10188
	South America	69.1027	5.95153
	North America	68.4860	8.46891
Gross Domestic Product (PPP) Per Capita	Asia	11387.21	9909.371
	Africa	4445.20	4454.637
	Europe	24786.58	12263.364
	South America	11537.73	6413.484
	North America	14132.90	11206.988
Corruption Perception Index	Asia	33.86	14.593
	Africa	33.77	11.793
	Europe	54.92	820.395
	South America	38.73	17.465
	North America	42.50	16.608

A. Hypothesis Testing

Since this study's predictor and outcome variables both are quantitative, and the direct relationship between SPI and GDP (PPP) per capita under study is a linear one, therefore simple linear regression was used to test the first hypothesis [28]. For second hypothesis, the moderating effect of CPI on the relationship between SPI and GDP (PPP) per capita was tested.

B. Social Progress Index and Gross Domestic Product PPP Per Capita

Simple linear regression was used to predict the dependent variable based on the independent variable (see table 3).

TABLE III
REGRESSION ANALYSIS OF SPI WITH GDP (PPP) PER CAPITA (119 COUNTRIES)

Variable	R^2	*B*	*SE*	*β*	*t*	*p*
Social Progress Imperative	*0.*749	839.3	43.7	0.866	19.16	0.000

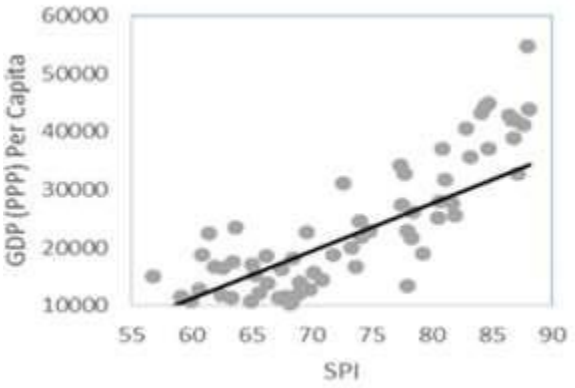


Figure 2. Regression Model for the relationship between SPI and GDP (PPP) per capita

A significant regression equation was F (1, 123) = 367.2, p <0.000, with an R^2= 0.749. The result of regression analysis showed the value of the un-standardized coefficient is not zero which indicates a relationship between SPI and GDP (PPP) per capita. R-square value shows that this relationship is in fact strong. Results show that the variation in value of GDP (PPP) per capita explained by SPI is nearly 75%. Further, SPI's significance value is also below 0.05, which indicates strong generalizability. Moreover, the standardized coefficient (Beta) has a positive sign which implicates a positive relationship between both variables. The value of the un-standardized coefficient (*B)* was 839.305, which mean that a unit increase in the value of SPI causes an approximately 840 unit increase in GDP (PPP) per capita. This also supports our hypothesis that GDP (PPP) per capita is positively dependent on the SPI.

Similarly, a simple linear regression was calculated by splitting the data based on continents to predict the dependent variable based on independent variable. Summary of regression analysis with data split as per continents is given below (see Table 4).

TABLE IV
REGRESSION ANALYSIS OF SPI WITH GDP (PPP) PER CAPITA (4 CONTINENTS)

Variable	R^2	*B*	*SE*	*β*	*t*	*P*
Asia	0.637	757	112.224	0.798	6.75	0.000
Africa	0.695	398	45.952	0.834	8.66	0.000
Europe	0.860	1421.7	97.110	0.927	14.6	0.000
South America	0.645	0.001	0.000	0.803	3.56	0.009

A significant regression equation for Asia was F (1, 26) = 45.5, p <0.000, with an R^2=0.637. Whereas for Africa F (1, 33) = 75.15, p <0.000, with an R^2=0.695, Europe F (1, 35) = 214.3, p <0.000, with an R^2=0.860 and South America F (1, 7) = 12.70, p <0.009, with an R^2=0.645. The value of the un-standardized coefficient *(B)* was 757, 398 and 1421.7 for Asia, Africa and Europe, which mean that a unit increase in the value of SPI causes an approximately 757, 398 and 1421.7 units increase in GDP (PPP) per capita. Whereas the value of the un-standardized coefficient *(B)* was 0.001 for South America, which mean that a unit increase in the value of SPI causes almost no increase in GDP (PPP) per capita of South America. A strong, statistically significant relation of SPI and GDP (PPP) per capita was found in European Countries with R^2 value of 0.860. Further, small variations in the value of Beta were observed for all continents showing relatively homogenous sensitivity of SPI. Standardized coefficients (β) contain positive values for all continents which shows that a favorable relationship exists between SPI and GDP (PPP) per capita for all continents. No regression analysis was performed for North American Countries because even after removing second order auto correlation, Durbin Watson value (1.489) was below the acceptable range of 1.75 and 2.25.

C. Moderating Role of CPI on Relationship between SPI and GDP (PPP) Per Capita

To test the moderating role of CPI, PROCESS macro for SPSS was used [27]. As stated earlier, the value of R^2 between SPI and GDP (PPP) per capita is 0.749, however, with the inclusion of CPI, a statistically significant increase in the value of R^2 = 0.795 was found. This shows the inclusion of CPI causes a change of 0.046 in the value of R^2. The moderator reduces the value of the un-standardized coefficient from 8393.05 to 588.801.

Moderation analysis shows that CPI remains statistically significant both at the lower and higher value in this model. The statistics of conditional effect on SPI and GDP (PPP) per capita in the presence of CPI as moderator is shown in Table 5.

TABLE V
MODERATING ROLE OF CORRUPTION PERCEPTION INDEX ON RELATIONSHIP BETWEEN SPI AND GDP (PPP) PER CAPITA (119 COUNTRIES)

Corruption Perception Index	*Effect*	*SE*	*t*	*p*
19.3977	408.5039	56.8274	7.1885	0.0000
0.0000	668.9661	50.2026	13.3253	0.0000
-19.3977	929.4284	73.211	12.6951	0.0000

At higher values of CPI, the effect size of SPI on GDP (PPP) per capita increases from 408.5 to 929.4. This shows the conditional effect of SPI on GDP (PPP) per capita is more at a higher value of CPI or in simpler words; the relationship between SPI and GDP (PPP) per capita is stronger at higher value of CPI. Additionally, better corruption perception rating of countries leads to stronger relationship of SPI and GDP (PPP) per capita.

D. Moderating Role of CPI on Relationship between SPI and GDP (PPP) Per Capita (4 Continents)

By including CPI as a moderator in the model, the value of R2 increased by 0.033 and the significance value of SPI becomes 0.04. CPI moderation was found statistically insignificant for Asian Countries; however, it increased the value of the un-standardized coefficient at higher values of CPI (see Table 6).

TABLE VI
PROCESS MACRO RESULTS FOR MODERATING ROLE OF CPI ON RELATIONSHIP BETWEEN SPI AND GDP (PPP) PER CAPITA (4 CONTINENTS)

Continent Wise Moderation	Corruption Perception Index	*Effect*	*SE*	*T*	*P*
	-14.5925	416.1185	193.8227	2.1469	0.0421
	0.0000	634.2235	211.8223	2.9941	0.0063
Africa	14.5925	852.3286	311.7566	2.7340	0.0116
	-11.7925	268.1255	98.8846	2.7115	0.0108
	0.0000	443.2182	63.7189	6.9558	0.0000
	11.7925	618.3109	67.6810	9.1357	0.0000
Europe	-20.4281	1000.1013	288.0914	3.4715	0.0015
	0.0000	1202.6332	256.4390	4.6897	0.0000
	20.4281	1405.1652	272.5902	5.1546	0.0000
South America	-19.2614	328.3542	332.7635	0.9867	0.3691
	0.0000	595.4692	369.4219	1.6119	0.1679
	19.2614	862.5843	750.2778	1.1497	0.3023

The value of R2 increases by 0.014 for African countries. Unlike previous results, CPI was insignificant at lower value while it was significant for average and higher values. Also, it increased the value of the un-standardized coefficient at higher values of CPI. This shows that for African countries, no relationship between SPI and GDP (PPP) per capita exists at lower values of CPI. However, a relationship is present at higher values. The value of R2 slightly increases by 0.007 for European countries. Unlike the previous results, CPI is significant both at all values, and it increases the value of the un-standardized coefficient at higher values of CPI.

Using CPI as moderator in the model, minor change in the value of R^2 was observed. For South American countries, when the result of moderation of CPI was tested using PROCESS macro, CPI was insignificant for all values. However, it increases the value of the un-standardized coefficient at higher values of CPI. This shows that for African countries, no relation between SPI and GDP (PPP) per capita exists at lower values of CPI, but a relation is present at higher values.

Moderation testing was not performed for North American countries because after removing second order auto correlation, the value of Durbin Watson (1.489) was below the acceptable range of 1.75 and 2.25.

V. Discussion

This research explored the effect of country's SPI on its GDP (PPP) per capita. Further, the moderating effect of CPI on SPI and GDP (PPP) per capita was also investigated.

A. Social Progress Index and GDP (PPP) per capita

The results of the regression analysis show a strong relation between both SPI and GDP (PPP) per capita. A large portion of variability in the value of GDP (PPP) per capita was shown by SPI, which explains that socially progressive societies focus on offering quality education and health facilities to its nationals who benefit from social progress and earn higher per capita income.

This study found similar results for all continents. The value of R^2 for Europe is 0.860 which highlights the reason why European nationals have higher per capita income and better health and education facilities. On the other hand, Asian, African and South American countries have been unable to capitalize on social progress to cultivate human development initiatives.

B. *Moderating Role of CPI on Relationship between Social Progress Index and GDP (PPP) Per Capita*

Similarly, when moderating relationship between SPI and GDP (PPP) per capita was checked for all countries, there was no relationship found in Asian countries and South America. In African countries, it was not found at lower values of the CPI. However, significant relationship with all values of the CPI for European Countries was found, which shows that European nationals have access to basic human rights. Moderating relationship and regression analysis for North American countries was not run because the data did not fulfill basic assumptions for regression and moderation analysis.

VI. Limitations

The secondary data from two reports was used due to time constraint and lack of monetary resources as suggested by Bordens and Abbott [29, p. 68], Saunders, Lewis, and Thornhill [30] and Matthews and Ross [31, p. 285]. The authors also highlighted a con of using secondary data extensively that the information presented in it may not be complete and accurate thus leading to incorrect inferences. Matthews and Ross [31, p. 52] highlighted a pitfall in using secondary data that the data might be collected for some specific purpose only. These concerns were addressed by choosing the secondary data reports issued directly by the prestigious institutes of Transparency International and Social Progress Imperative. The data published by the selected international bodies was in public domain and was used to evaluate countries and their economies.

Previous literature such as Johnston [32] has supported secondary data analysis while highlighting drawbacks such as choosing only the research questions that can be answered through existing secondary data. Due to shortage of time, this particular paper utilized this drawback to researcher`s advantage and answer only specific research questions.

VII. Future Research

This research proposes some suggestions for the future researchers to address the gap and discrepancies observed. In SPI and GDP (PPP) per capita relationship, no relationship was observed between both variables for Asian and South American nations. Likewise, moderating relationship and regression analysis for North American countries was not analyzed because the data from these countries did not fulfill basic assumptions

for regression analysis and moderation analysis. These two statistical deviancescan be explored by statisticians to identify the underlying reasons.

Another measure of corruption developed by International Country Risk Guide (ICRG) provides data for 140 countries, including North American Countries [3, p. 87]. ICRG data can be used as an alternative to CPI to check moderating effect and regression analysis for North American countries which CPI failed to answer.

As shown in table IV, the value of the un-standardized coefficient (B) was 0.001 for South America, which shows that a unit increase in SPI value causes almost no increase in GDP (PPP) per capita for South America. Although significance value (i.e. P-value=0.009) shows CPI does moderate the GDP (PPP) per capita and SPI relationship, further investigation is needed to understand why the unstandardized Beta (B) is so low.

The secondary data used for this study can be used to conduct a longitudinal research for different regions and countries around the world to gain more in-depth insight. Further, the scores of SPI or GDP (PPP) per capita are available countries wise. Respective indicators of both measures might be used at city, province or region level to measure these constructs within a country.

VIII. IMPLICATIONS

A country's GDP does not necessarily guarantee a prosperous society. States such as Iran and Saudi Arabia, etc. have high GDPs but have poor social performance [2, p. 17]. For this reason, an alternate measure, i.e. SPI was developed to provide a better measure of social progress. Social progress is an important metric as it shows that a socially progressive society will help develop the capabilities of its citizens.

Regardless of their importance, these indices should not be thought of as some construct, but a metric to recognize the economic conditions of a country to identify societal lags such as health and educational facilities, environmental sustainability, quality of life, employment opportunities for societal development. The governmental and regulatory policy makers should consider both social progress as well as the economic progress for policy development. Countries across the world are starting to realize the importance of complementing economic and social developing, for instance, Paraguay`s national development plan 2030 explicitly targets economic growth as well as social progress [2, p. 88]. The combination of this two-sided development can have widespread economic for the society. Such bold and thoughtful initiatives on national levels can help achieve the dream of a true welfare state.

VIII. CONCLUSION

This study used secondary data for SPI, GDP (PPP) per capita and CPI that was collected from Social Progress Index 2015, and the Corruption Perception Index 2015 respectively. The study results show that the better corruption perception rating of countries led to stronger relationship of SPI and GDP (PPP) per capita. This means that the socially progressive countries arrange for superior health and education facilities for its nationals. Also, when checked for continents, it was found that the nationals of the European countries have high per capita income and enjoy better health and education facilities. Contrarily, people belonging to South American, Asian, and African states lack social progress, i.e. their population does not have a better quality of health, life and educational facilities.

Governments should now turn their focus on making socially progressive societies (as per SPI) instead of making economic developments as dictated by GDP. Further research is required to better realize and highlight the superiority of SPI over economic development (GDP) as an economic indicator for the economic researchers and practitioners.

ACKNOWLEDGMENT

The authors would like to thank Dr. Ahmad Faisal Siddiqui, University of Engineering and Technology, Lahore, for his motivation and mentorship during the conceptualization of this study. Our thanks also goes to the anonymous reviewer for his/her valuable comments that helped in further improving this manuscript.

REFERENCES

[1] J. Stiglitz, A. Sen, and J.-P. Fitoussi, Mismeasuring Our Lives: Why GDP Doesn't Add Up. The New Press, 2013.
[2] M. E. Porter, S. Stern, and M. Green, "Social Progress Index," Social Progress Imperative, 2015.
[3] X. Xu, "Corruption and economic growth: an absolute obstacle or some efficient grease?," Econ. Polit. Stud., vol. 4, no. 1, pp. 85–100, 2016.
[4] Transparency International, "Corruption Perceptions Index 2015," Transparency International, 2015.
[5] M. T. Rock and H. Bonnett, "The Comparative Politics of Corruption: Accounting for the East Asian Paradox in Empirical Studies of Corruption, Growth and Investment," World Dev., vol. 32, no. 6, pp. 999–1017, Jun. 2004.
[6] A. Maddison, "A comparison of levels of GDP per capita in developed and developing countries, 1700–1980," J. Econ. Hist., vol. 43, no. 01, pp. 27–41, Mar. 1983.
[7] N. Ahmad and S. Arjumand, "Impact of corruption on GDP per capita through international migration: an empirical investigation," Qual. Quant., vol. 50, no. 4, pp. 1633–1643, Jul. 2016.
[8] P. Mauro, "Corruption and Growth," Q. J. Econ., vol. 110, no. 3, pp. 681–712, 1995.
[9] P. Grabova, "Corruption impact on Economic Growth: An empirical analysis," J. Econ. Dev. Manag. IT Finance Mark., vol. 6, no. 2, p. 57, 2014.
[10] C.-U. Kim and G. Lim, "Corruption and Economic Growth: A South Korean Study," J. Rev. Glob. Econ., vol. 4, p. 1, 2015.
[11] J. Shao, P. C. Ivanov, B. Podobnik, and H. E. Stanley, "Quantitative relations between corruption and economic factors," Eur. Phys. J. B, vol. 56, no. 2, pp. 157–166, Apr. 2007.
[12] B. Podobnik, J. Shao, D. Njavro, P. C. Ivanov, and H. E. Stanley, "Influence of corruption on economic growth rate and foreign investment," Eur. Phys. J. B, vol. 63, no. 4, pp. 547–550, Jun. 2008.

[13] P.-G. Méon and L. Weill, "Is Corruption an Efficient Grease?," World Dev., vol. 38, no. 3, pp. 244–259, Mar. 2010.
[14] R. Ram, "PPP GDP Per Capita for Countries of the World: A Comparison of the New ICP Results with World Bank Data," Soc. Indic. Res., vol. 127, no. 3, pp. 1057–1066, Jul. 2016.
[15] N. N. Anh, N. N. Minh, and B. Tran-Nam, "Corruption and economic growth, with a focus on Vietnam," Crime Law Soc. Change, pp. 1–18, 2016.
[16] I. Ehrlich and F. T. Lui, "Bureaucratic corruption and endogenous economic growth," J. Polit. Econ., vol. 107, no. S6, pp. S270–S293, 1999.
[17] P.-G. Méon and K. Sekkat, "Does corruption grease or sand the wheels of growth?," Public Choice, vol. 122, no. 1–2, pp. 69–97, 2005.
[18] P. Bardhan, "Corruption and development: a review of issues," J. Econ. Lit., vol. 35, no. 3, pp. 1320–1346, 1997.
[19] S. P. Huntington, Political order in changing societies. Yale University Press, 2006.
[20] N. H. Leff, "Economic development through bureaucratic corruption," Am. Behav. Sci., vol. 8, no. 3, pp. 8–14, 1964.
[21] C. Leys, "What is the Problem about Corruption?," J. Mod. Afr. Stud., vol. 3, no. 02, pp. 215–230, 1965.
[22] F. T. Lui, "An equilibrium queuing model of bribery," J. Polit. Econ., vol. 93, no. 4, pp. 760–781, 1985.
[23] C. Forza, "Survey research in operations management: a process-based perspective," Int. J. Oper. Prod. Manag., vol. 22, no. 2, pp. 152–194, 2002.
[24] V. L. P. Clark and J. W. Creswell, Understanding research: a consumer's guide, Second edition. Boston: Pearson, 2015.
[25] J. W. Creswell, Research design: qualitative, quantitative, and mixed methods approaches. Los Angeles: Sage, 2009.
[26] S. B. Green and N. J. Salkind, Using SPSS for Windows and Macintosh: analyzing and understanding data, Seventh edition. Boston: Pearson, 2014.
[27] A. F. Hayes, Introduction to mediation, moderation, and conditional process analysis: a regression-based approach. New York: The Guilford Press, 2013.
[28] A. P. Field, Discovering statistics using SPSS: (and sex, drugs and rock "n" roll), 3rd ed. Los Angeles: SAGE Publications, 2009.
[29] K. S. Bordens and B. B. Abbott, Research design and methods: a process approach, Ninth edition. New York, NY: McGraw-Hill Education, 2014.
[30] M. Saunders, P. Lewis, and A. Thornhill, Research methods for business students, 5th ed. New York: Prentice Hall, 2009.
[31] B. Matthews and L. Ross, Research methods: a practical guide for the social sciences, 1st ed. New York, NY: Pearson Longman, 2010.
[32] M. P. Johnston, "Secondary data analysis: A method of which the time has come," Qual. Quant. Methods Libr., vol. 3, pp. 619–626, 2014.

Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 7, No 1, June 2017

CYBER SECURITY AND INTERNET OF THINGS

Muhammad Saad Department of Computer Science, SZABIST Dubai Campus and [1]Tariq Rahim Soomro, College of Computer Science & Information Systems, IoBM, Karachi

***Abstract*- Internet has become a vital part of our lives. The number of Internet connected devices are increasing every day and approximate there will be 34 billion IoT devices by 2020. It is observed that security is very weak in these devices and can be easily compromised by hackers as some manufactures failed to implement basic security. Current devices use standards that are easy to implement and works for most forms of communications and storage. There is no such standard solution that will work on every device within the Internet of Things, because of the varied constraints between different devices; resulting in classifications within the Internet of Things. This study addresses security challenges in the Internet of Things (IoT); first will discuss the IoT evolution, architecture and its applications in industries. Further, classify and examine privacy threats, including survey, and pointing out the challenges that need to be overcome to ensure that the Internet of Things becomes a reality.**

Keywords: Internet of Things, Cybersecurity, Cybersecurity Challenges.

I. INTRODUCTION

The Internet of things (IoT) period began from 2000 and onwards. In IoT everything is connected with the Internet, this concept changed the concept of everything. This concept will create ease in our life style. In IoT, things are interconnected and can be manage through other connected devices i.e. from office you can switch on and off your room temperature. Home, vehicle, workplace and even our shoes will be IoT connected. Although currently everything is not connected with IoT, but gradually as time is passing things are adding to the IoT. Data will generate by these connected devices. These devices will not only generate data, but also behave as well on the basis of collected information [1]. Things will be interconnected and ability to see everything in this life would be possible with just few clicks. This scenario raises the importance of security of data and connected things. If there are loopholes in the security, then malicious actors in society can see, access and misuse the same information too, for example Smart TV with camera, and there are cases that one's TV camera is hacked [2] [3]. By realizing the importance of IoT, investors are making huge investment in it but they are investing on the things that can be marketed and the can get quick return. There is not much or equal level of investment in security of IoT. As more things will add into IoT, concern about the things security will increase too.

[1] tariq.soomro@iobm.edu.pk

According to ITU, cybersecurity is “The collection of security principles, protection, guidelines, chance management processes, actions, education, practices, guarantee and technology that may be used to protect the cyber environment and organization and person's property” [4]. On the other hand according to IoT-SRA “The IoT is a large scale system with self-arranging abilities in view of standard and interoperable conventions and configurations which comprises of heterogeneous things that have characters, physical and virtual traits, and are flawlessly and safely integrated into the Internet” [5].

1.1. Evolution of IoT

The early period of IoT began with Machine-to-Machine (M2M). M2M once referred to communication between devices using any communications channel, including wired and wireless but currently it is typically use to refer machine communications using cellular or satellite networks. In telephony systems, information was exchanged through different end-points i.e. caller identity. This information was sent between the endpoints and no one required starting the transmission. M2M is still majorly wise used in the alarm panels, industrial sector and more. IoT is typically known as superset of M2M and currently overtaken the M2M market as shown in Figure 1 from Google.

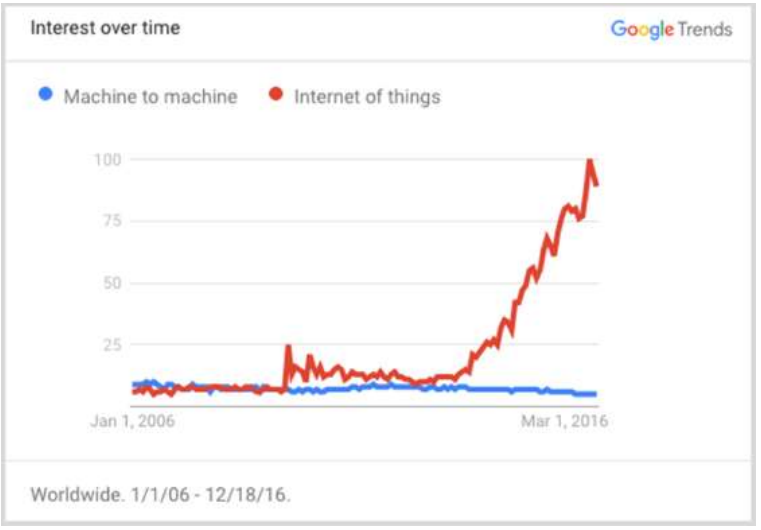


Figure 1: M2M to IoT - Interest over Time on Web Search [6]

Gartner highlight IoT as potential technology in 2013. Onwards from 2014 to 2016, it has been moved from initial stage to peak of inflated as shown in Figure 2 [7] [8] [9] [10].

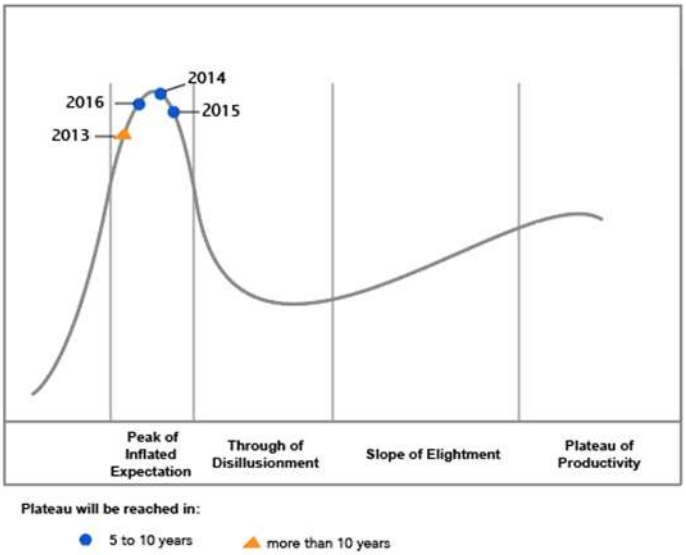


Figure 2: IoT Gartner's Hype Cycle from 2013-16

Everyday IoT umbrella is getting bigger as things are adding into it. According to Business Insider, there will be more than 24 billion IoT devices that mean everyone is going to keep more than 4 devices as shown in Figure 3 [11]. Gradually, this revolution will change everything from personal devices to smart cities.

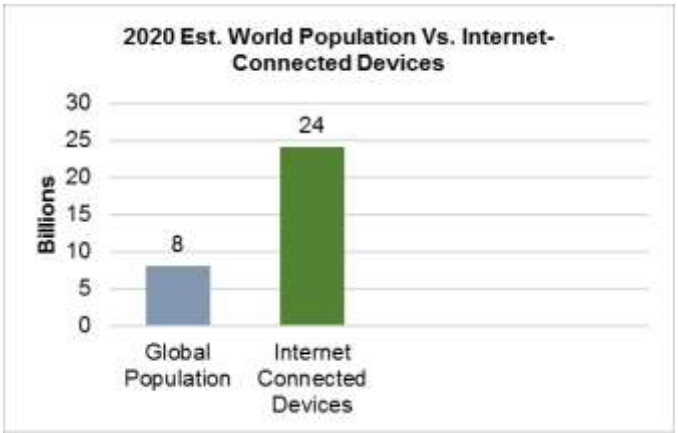


Figure 3: The IoT Growth Forecast

1.2. Cybersecurity in the Internet of Things

With IoT speedy growth, new security threats and challenges are rising in all industries. IoT is going the change the businesses and customer interaction with the world. IoT devices growth prediction is from 10 billion in 2016 to 24 billion in 2020 [11]. Sharing information with everything is an enormous cybersecurity challenge. When billions of IoT devices will connect to the other networks, malicious attacks will increased. Cyber criminals can use IoT devices as a door to enter business networks and cloud environment [12]. Cybersecurity is the primary challenge of IoT implementation. Cyber-attacks already have started on connected devices such as ability to hack connected vehicle. Nowadays, customers have realized their choices can be analyze by their information and they have started to think about who has access to their data and who is responsible to secure it. When different systems will interact, there will be fight among them on competitive intelligence. As it will create new cybersecurity challenges and these challenges will raise the importance of security. Also data security is a major concern for IoT devices and it should be taken seriously. Every second day, there is news about data breaches [13]. Every connected thing generates data and volume of generated data is in zeta bytes. Malicious actors can access this sensitive data. Let's take an example of thermostat data; it can be used to count total number of person and their availability. GPS can use to track your position and your availability at a certain position [14]. This information doesn't seem very important but it is enough for criminal to misuse it against anyone. Business data can misuse in the same way. Nowadays several companies are collecting social data i.e. Google, Yahoo and Facebook etc. and this data can be hacked by hackers. On 14 Dec 2016, Yahoo accepted their 1 billion accounts were compromised [15]. IoT Device manufactures need to understand that data privacy begins at the source. Information should not leave the sensor without protection. Data needs to be encrypted before moving to cloud for processing and storage.

This paper is organized as follows; section 2 will discuss IoT architecture, along with security attacks during 2015 to 2016; section 3 will explore the finding from literature; section 4 will discover the finding from survey done for this study; finally, discussion and future work will be covered.

II. IoT Architecture

IoT standard architecture consisting of things, local network, the Internet and back end services, as shown in Figure 4 below.

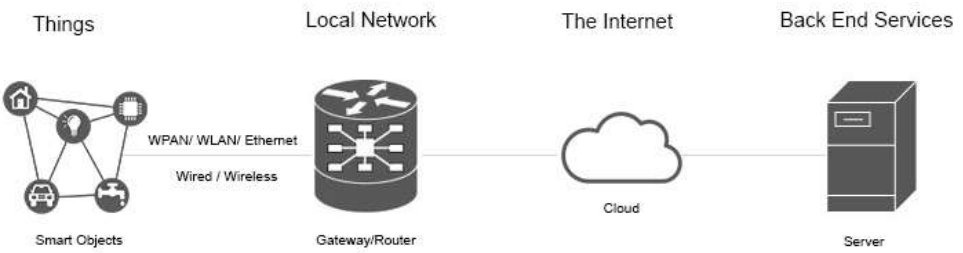


Figure 4: IoT Standard Architecture [16]

Following are the IoT architectures purposed by leading IT companies in the world.

2.1 IoT Architecture by Microsoft

Figure 5 shows the IoT architecture by Microsoft Azure [17]. There are three major areas in it:

- Device connectivity
- Data processing, analytics, and management
- Presentation and business connectivity

By using a gateway, devices can connect directly or indirectly. This architecture is designed for large-scale IoT environments.

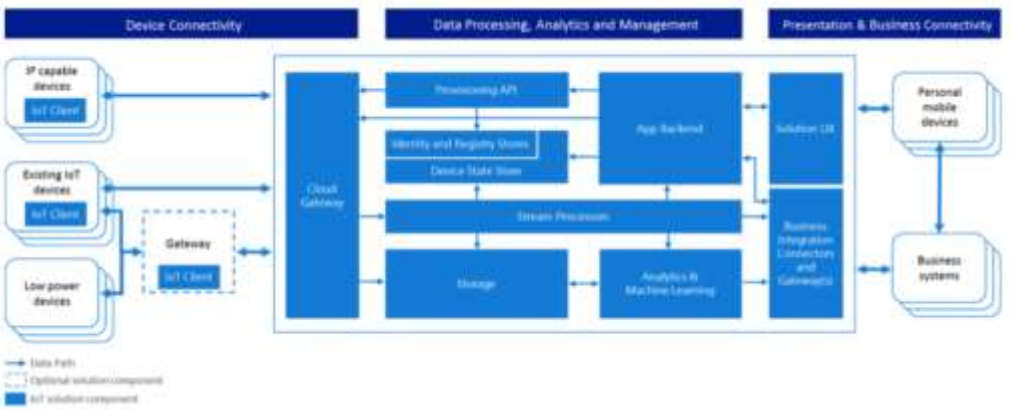


Figure 5: IoT Architecture by Microsoft [17]

2.2 IoT Architecture by Intel

Intel along with its ecosystem partners defined IoT architecture with name of system architecture specification (SAS) for all things whether they are connected with the Internet or not as shown in Figure 6 below. This architecture has 3 components:

- Things
- Network
- Cloud

Intel also released various IoT products along with ecosystem. This architecture provides data and device security [18].

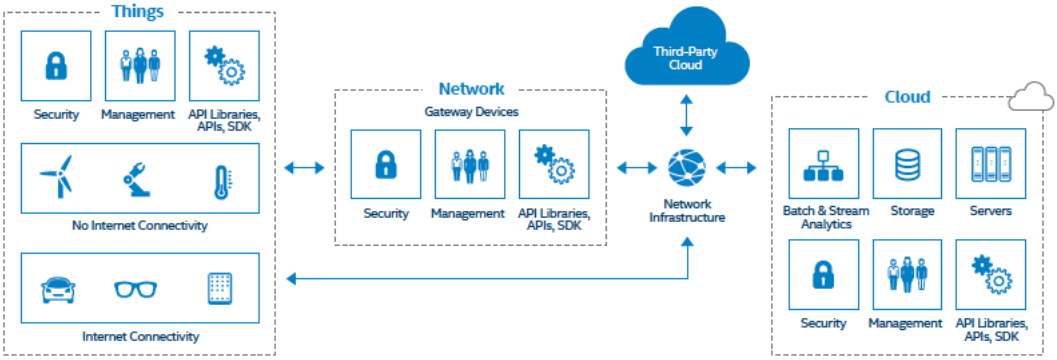


Figure 6: IoT Architecture by Intel [18]

2.3 IoT Architecture by Google

Google architecture is based on three main components.

- Device
- Gateway
- Cloud

Devices can communicate with other devices and these are Internet connected directly or indirectly. Devices, which do not have direct Internet connection, can be accessed by gateway [19]. Gateway also control network traffic that use various protocols. Cloud Platform is used to store, process and analyze data from all devices as shown in Figure 7 below.

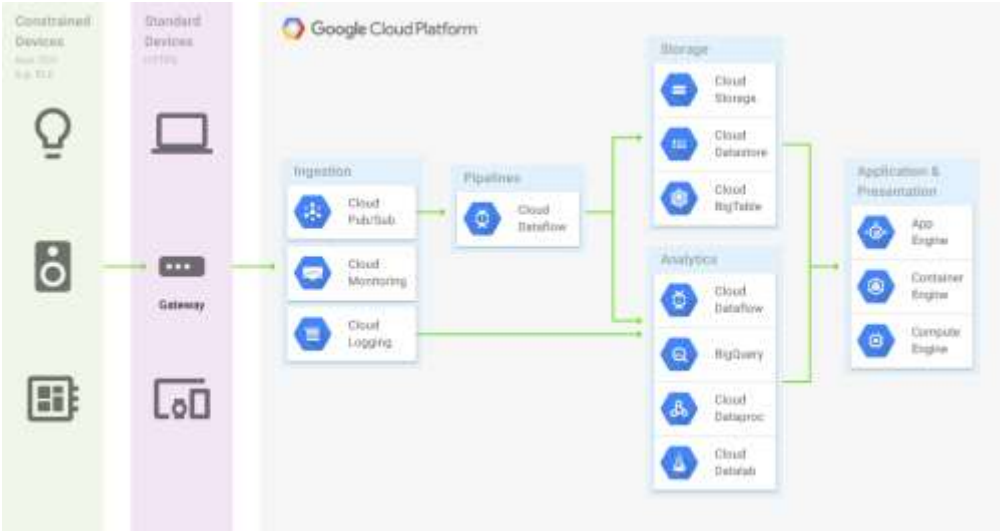


Figure 7: IoT Architecture by Google [19]

2.4 Exploitation of an IoT Device

Integrated circuit can be used as a gateway to control an IoT device. It has been observed from past, IC security is not strong. IoT device can also be accessed by insert-unauthorized device into the network. This technique has been applied to Google nest during a cyber security conference in US [20] [21]. IoT applications can be hacked by malicious code and gain access to device and server. Gateway/router can be used to gain access to network. By gaining network access, fake content can be published on devices as shown in Figure 8 below.

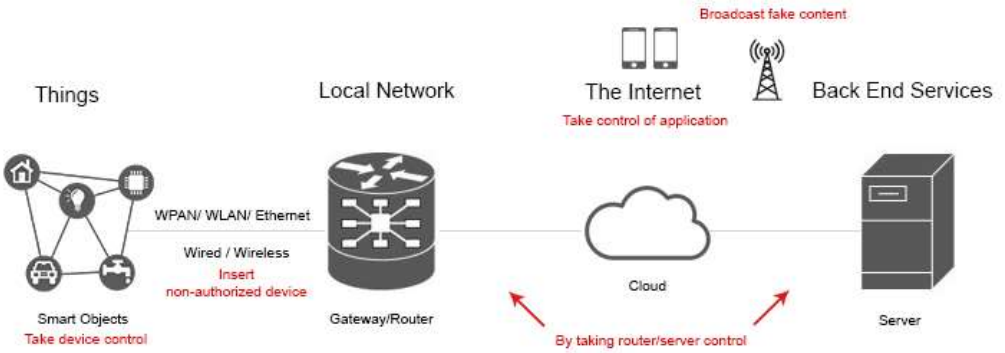


Figure 8: Exploitation of an IoT Device [20]

2.5 IoT Industries & Breach Incidents

IoT will cover everything in every industry [22]. Following are the possible major industries in IoT:

- Connected Home
- Food Services
- Utilities
- Hospitality
- Healthcare
- Government
- Transportation
- Defense
- Infrastructure
- Retail
- Logistics
- Banks
- Oil, gas, and mining
- Insurance
- Agriculture

Health industry is leading 1st half of 2016 with highest number of breaches 263. It has been observed that attacked on this industry has been increased from 2014 [23]. Next highest number breaches 137 happened in Government. Financial services were on third with 118 breaches. Retail, education, technology and other industries cited 102, 102, 90 and 162 respectively. Table 1 shows the breach incidents in IoT industries from 2013 to 1st half of 2016.

TABLE I
BREACH INCIDENTS IN IOT INDUSTRIES [**23**]

IoT Industries	1st Half 2013	2nd Half 2013	1st Half 2014	2nd Half 2014	1st Half 2015	2nd Half 2015	1st Half 2016
Healthcare	172	168	237	208	233	211	263
Finance	78	86	85	126	153	123	118
Government	127	64	109	180	161	135	137
Retail	56	41	81	113	130	108	102
Education	7	27	86	87	102	63	102
Technology	55	55	72	66	58	62	90
Other Fields	151	111	138	136	181	142	162

2.6 IoT Cyber Security Attacks from 2015-2016

As things are adding in IoT umbrella, numbers of breaches are increasing. Following are the 2015-2016 top cyber security attacks.

A. San Francisco's Railway System

On 29 Nov 2016, San Francisco Municipal Transportation Agency (SFMTA) system hacked by ransom-ware attack with a message: "You are hacked. All Data Encrypted". Cyber-criminal encrypted the data by ransom-ware as shown in Figure 9 below [24].

Figure 9: Hackers message on San Francisco's Railway System [24]

B. Ransomware hits Los Angeles hospital

Hollywood Presbyterian Medical Centre is one of the oldest private hospitals in Los Angeles, US. On 15 Feb 2016, a major cyber-attack happened and it blocked everything. This attack was very similar to ransom-ware. Medical staff were unable to access important patient data, which include medical reports and laboratory scan etc. Hackers asked 3 million dollars for this data [25]. On 04 Oct 2016, a name in medical Johnson & Johnson also warned customers that their diabetics insulin pumps can be hacked, which can cause an overdose [26].

C. Security Researchers killed Jeep Cherokee 2014

In 2015, Charlie Miller and Chris Valasek demonstrated the vulnerabilities in connected vehicle Jeep Cherokee 2014 [27]. They were able to increase/decrease vehicle speed, switch on and off radio and stop it anywhere in mid. In past they have compromised other famous models Toyota Prius and

Ford Escape too. They are not the first one, in past University researchers also demonstrated their access to major components in vehicle [28].

D. Hacking in Aviation

The wave of cyber-crimes also hit aviation industry. On 29 Apr 2015, glitch in iPad app delayed more than fifty American Airlines flights. It is also informed to aviation authorities that flight Wi-Fi could leads to hijack a flight. Also passenger cabin and cockpit electronics use the same network as shown in Figure 10 [29].

Figure 10: American Airlines Tweet About an Incident [29]

On Mar 2015 German Airbus A320 crashed. Aviation experts said this plane has vulnerabilities and could be electronically hacked. In past, criminal used fake boarding passes too. Air miles and loyalty programs are also soft target for cyber criminals [29] [30] [31].

E. ATM Skimming Attacks

ATM skimming attacks are rising worldwide. In 2015, 300 million euros were reported [32]. FICO Card Alert Service in US observed 546% increase in skimming attacks in 2015 and warned costumers about it. Usually these are happening in offsite ATMs as shown in Figure 11 below.

Figure 11: ATM Skimming Techniques [32]

2.7 Leading Sources of Data Breach Incident

Malicious outsiders are the biggest source of data breach incidents with 668 data breaches in 1st half of 2016 similar to previous periods as shown in Table 2 below. Malicious outsider is any unauthorized person in the organization who may or may not be recognizable [23]. Accidental loss cited second with 178 breaches in 1st half of 2016. When a person unintentionally shares important data is known as Accidental Loss. Malicious Insiders, hacktivist and state sponsored attacks cited 83, 29 and 14 breaches. Malicious Insider is a person in the organization, who has access to all confidential data. Hacktivist is a person who hacks system for social and political reasons while state sponsored attacks are govt. sponsored and supported attacks.

TABLE II
TABLE 2: LEADING SOURCES OF DATA BREACH INCIDENT [23]

Breach Sources	1st Half 2013	2nd Half 2013	1st Half 2014	2nd Half 2014	1st Half 2015	2nd Half 2015	1st Half 2016
Malicious Outsider	335	317	466	482	608	474	668
Accidental Loss	158	138	189	222	228	208	178
Malicious Insider	114	78	125	156	142	126	83
Hacktivist	20	7	4	16	18	18	29
State Sponsored	3	9	20	40	20	16	14

2.8 Cyber Security Challenges in IoT

Following are identified as cyber security challenges in IoT [33]:

- Insecure mobile & web interface
- Insufficient authentication/authorization
- Poor physical security and Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insufficient security configurability
- Insecure software/firmware

III. FINDINGS FROM LITERATURE

Following are the results and findings from literature:

3.1. Healthcare Industry is Top Target in 2016

The healthcare industry has been a big target of attackers in recent years and that did not change in the first half of 2016 [23]. Next highest in the number of breaches was in government with 137 breaches. Financial services were next with 118 data breaches. The retail and education sectors each had 102 data breaches and the technology industry experienced 90 data breaches, shown in Figure 12 below:

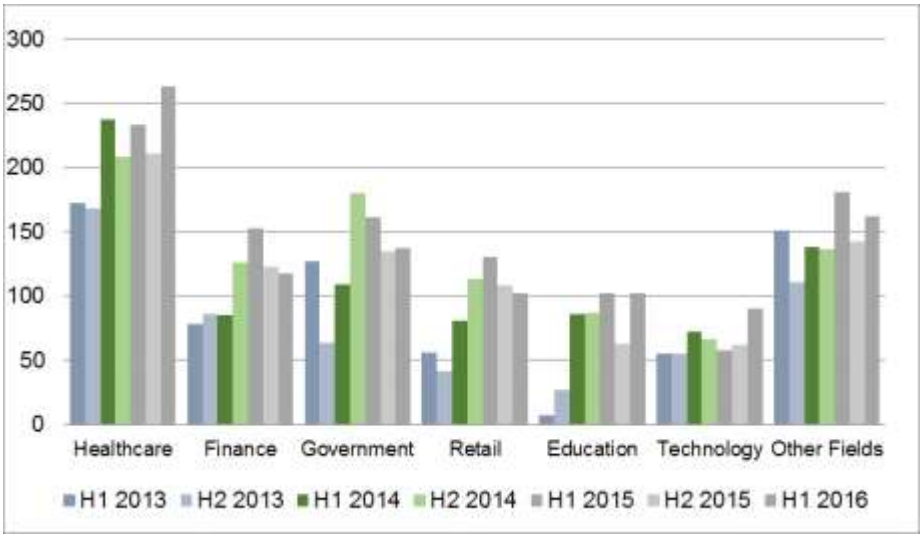


Figure 12: Cybersecurity incidents in different industries over time

3.2. *Leading Sources of Data Breaches*

Malicious outsiders were the biggest source of data breach incidents with 668 data breaches in 1st half of 2016 similar to previous periods as in Figure 13 below [23].

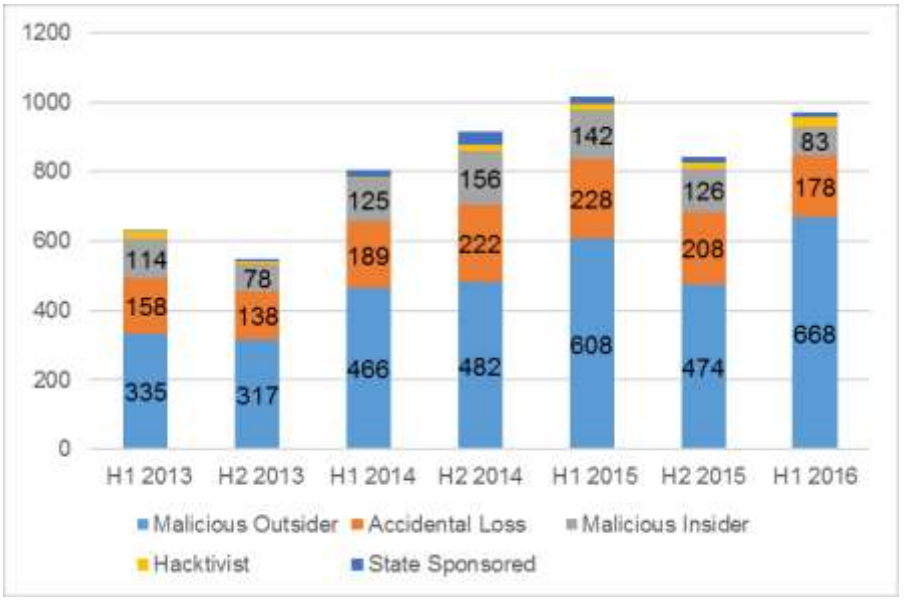


Figure 13: Leading Sources of Cybersecurity Threats from 2013 to 2016

IV. FINDINGS FROM SURVEY

Web based survey was conducted and 100 responses were received; sampling method was random. Survey study shows that the users have strong believe in the potential of IoT. Following are the key findings of this survey study.

4.1. *Familiarity with IoT*

Respondent's knowledge about the survey technology is very important. 96.7% respondents were familiar and very small ratio, 3.3% had no idea about IoT at all.

4.2. *Adaptors of IoT*

The majority of the respondents were from North America 41.4% and Europe 31%. Some 17.2% were in Asia, 6.9% in Africa and 3.4% were in Australia as shown in Figure 14.

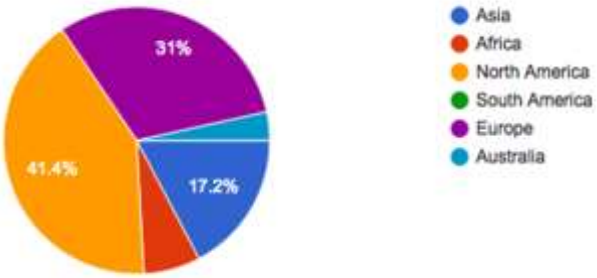


Figure 14: Survey Demographics

4.3. Survey Respondents

Survey respondents came from various industries, as shown in Figure 15. The single largest vertical was technology, at just over 48.3%.

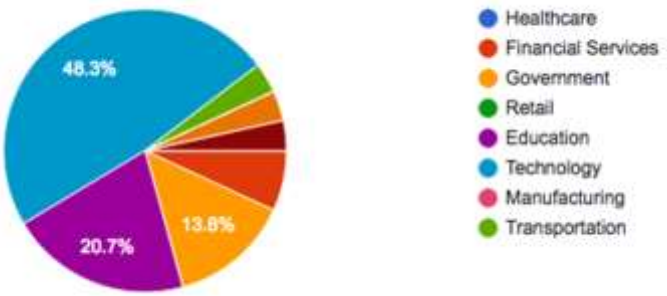


Figure 15: Survey Respondents

The next three largest verticals were education, government, financial services with 20.7%, 13.8% and 6.9% followed by equally spread transportation, hospitality and other fields cited 3.4%.

4.4. Lack of confidence in IoT device security

86.2% respondents feel that IoT devices security is weak. Only 13.8% are slightly more optimistic and satisfied with IoT devices security. Although cybersecurity in IoT is a big challenge but it is an opportunity as well for new ways of thinking.

4.5. Cybersecurity is important to business

Organizations were aware with vital importance of their data and concerned about cybersecurity. 90% respondents from major organizations think cybersecurity is more important than cost, data analytics, performance and integration with hardware as shown in Figure 16.

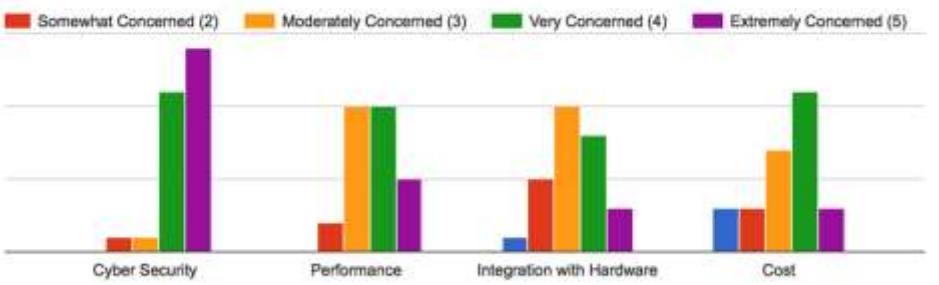


Figure 16: Cyber security is important to business

4.6. Impact of Cyber Security Concerns on Business

65.5% respondents indicate that cybersecurity concerns would discourage them from purchasing an IoT device while 34.5% respondents still want to use the latest technology products despite cyber security concern.

4.7. Awareness about Device Vulnerabilities

Cybersecurity concern is growing along with IoT growth. Only 3.7% are confident about IoT device security, rest 96.6% IoT devices are soft target for hackers.

4.8. Belief in the power of IoT

89.7% respondents have positive thoughts about IoT, they can feel the impact of IoT in their life, business and industries as compare 10.3%, who think IoT is not beneficial for them.

4.9. Most Popular IoT Devices

Smartphones, laptops and tablets were the most popular IoT devices in 2016 cited 100%, 97% and 83% respectively as shown in Figure 17. All respondents own a smartphone of some kind. Desktop computers and TV are the next-most popular devices among those measured cited 75% and 65%. Gaming consoles and wearable are the next with 31%. Rest of the devices popularity is low as compare to other devices that includes radio with 28%, health related devices 24%, kitchen appliances 7% and PDA 4%.

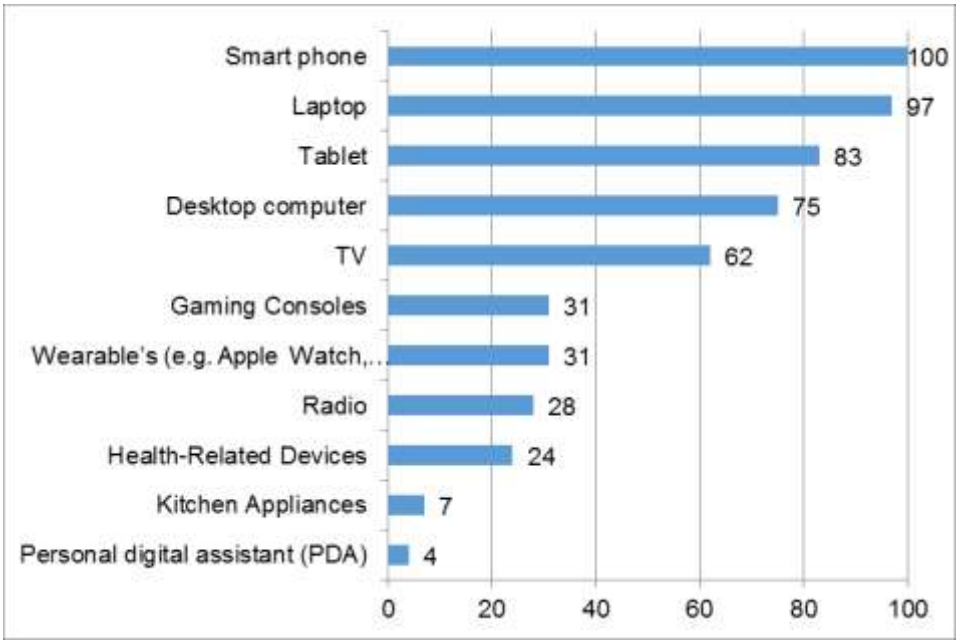


Figure 17: Most Used IoT Devices in 2016

4.10. Use of Credit/Debit Cards on Internet

58.6% respondents were willing to use debit/credit card during online or offline shopping because of ease in payment mode while 41.4% still don't prefer online payments.

4.11. Public Awareness of Credit Card Breach

10.3% feel use of credit/debit cards is safe while 89.7% respondents are aware that their cards have the potential to be hacked. Credit/Debit card hacking is still an unsolved problem but good part in this problem is people awareness about the problem.

4.12. IoT Manufacturers Security Concerns

User awareness about cyber-crimes improved in recent years. 79.3% respondents think IoT manufactures can improve security in their devices, as they don't provide enough security while only 20.7% are satisfied.

4.13. Most Sensitive Data in IoT

Everyone likes to keep personal things private. So, it isn't surprising that 62.1% of the respondents rated Personal data as the most sensitive in IoT as shown in Figure 18. Because so many devices will be connected with IoT and linked with password so passwords were next most frequently cited 24.1%, with concerns about Business data 10.3% and emails with 3.4% rounding out the list.

4.14. Top Security Threat in IoT

The vast majority with 51.7% of respondents felt the DDOS attack as the primary responsible party as shown in Figure 19. Phishing the next most highly cited selection with 48.3%. However, 31% respondents cited Ransom-ware is spreading across the organizations. Similarly, cyber espionage cited 27.6% while inside threats and nation state attacks were cited 20.7%.

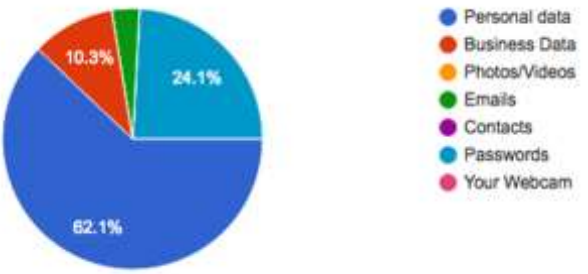


Figure 18: Most Sensitive Data in IoT

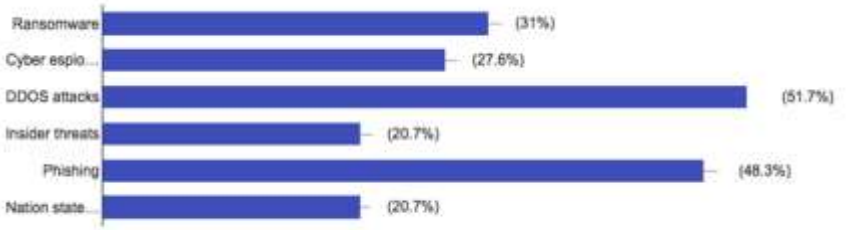


Figure 19: Top cybersecurity threats in IoT

4.15. Leading Sources of Cyber Threats

Malicious outsiders and accidental loss were the biggest sources of data breaches cited 31% and 17.2%. This finding is very close to literature finding. Next on the list of most common sources miscellaneous attacks, which cited for 17.2%? Malicious insiders were the next most common

source of breaches, accounting for 13.8%. Hacktivists and state sponsored attacks were cited 10.3% as shown in figure 20.

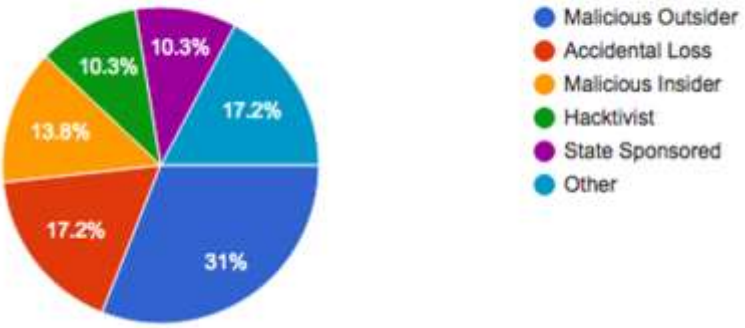


Figure 20: Leading Sources of Cybersecurity Threats in 2016

V. Discussion and Future Work

This study shows that IoT trends is growing up and 97% internet users already have awareness about it. 1st generation of connected things is already in the market and by passing everyday more devices are adding under IoT umbrella. Cybersecurity professional are already making strategies for IoT challenges. 89.7% survey respondents, think IoT will create ease in life and business. Almost majority of the IoT device users have high concerns about IoT device security. Furthermore, they believe it can be improve from manufacturer end; as they do not provide enough security. In recent year's cyber security attacks has been increased on the Internet connected medical devices. Healthcare industry faced 263 data breaches which is highest in all industries and it is 25% up as compare it with previous half [23]. Smart phone, iPad and laptops are the most popular devices while PDA, kitchen appliances and wearable are not much popular among users in 2016.

Cyber security is the main barrier for IoT, because of connected things; users have more awareness about everything that is happening in the world. IoT user awareness about device vulnerabilities is high. More than 90% feel IoT devices are soft target for hackers and 65% users indicate they will not purchase a device that have cybersecurity concerns. Organizations are aware with the impact of cybersecurity on their businesses. Survey results showed that cybersecurity more important than other issues i.e. cost, data analytics, performance and integration with hardware etc. Organizations should review their cybersecurity infrastructure that where they are lacking security

measures and plan ahead of cyber-attacks. This study will help IoT manufacturers to use these results as a key to build more secure products in future.

5.1. Key Recommendations for IoT Users

Cyber security is heart of our devices [33]. Suggested security measures below will improve device security:

- Use HTTPS, two factor authentication option i.e. touch ID, firewall.
- Change or replace default name and password with strong characters and change them after every 30 days
- Don't share your personal information i.e. date of birth or home address unless it is very important.
- Activate pin or password on your device.
- Enable Logs on your device.
- Enable notifications for security alerts.
- Verify software and firmware update before install them on device.
- Disable unused physical ports.

REFERENCES

[1] Nermin Hajdarbegovic. (2014, Oct) https://www.toptal.com/i. [Online]. https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
[2] Kristina Flüchter Felix Wortmann, "Internet of Things," Business & Information Systems Engineering, vol. 57, no. 3, pp. 221–224, June 2015.
[3] Jiafu Wan, Caifeng Zou, Jianqi Liu Hui Suo, "Security in the Internet of Things: A Review," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, Hangzhou, China , 2012, pp. 648 - 651.
[4] ITU. itu.int. [Online]. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[5] Domenico Rotondi, Roberto Minerva Abyi Biru. (2015, Dec) http://iot.ieee.org. [Online]. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
[6] Google. (2016, Dec) https://www.google.com/trends/. [Online]. https://www.google.com/trends/explore?date=2006-01-01%202016-12-18&q=%2Fm%2F0b42qh,%2Fm%2F02vnd10&hl=en-US
[7] Ms. Fenn Mr. LeHong. (2013, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/2575515
[8] Betsy Burton. (2014, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/2819918?_ga=1.51071721.1904172021.1401730474
[9] Betsy Burton. (2015, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/3114217
[10] Amy Ann Forni. (2016, Aug) http://www.gartner.com/. [Online]. http://www.gartner.com/newsroom/id/3412017
[11] BI Intelligence. (2016, June) http://www.businessinsider.com/. [Online]. http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5
[12] W. David Stephenson Christopher J. Rezendes. (2013, June) https://hbr.org/. [Online]. https://hbr.org/2013/06/cyber-security-in-the-internet
[13] Hong Liu, Laurence T. Yang Huansheng Ning, "Cyberentity Security in the Internet of Things," Computer , vol. 46, no. 3, pp. 46 - 53, March 2013.
[14] C. Warren Axelrod, "Enforcing security, safety and privacy for the Internet of Things," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, Farmingdale, NY, USA.

[15] NICOLE PERLROTH VINDU GOEL. (2016, Dec) http://www.nytimes.com. [Online]. http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=
[16] (2014, Feb) http://architectcorner.yolasite.com. [Online]. http://architectcorner.yolasite.com/products.php
[17] Microsoft. (2016, Mar) https://azure.microsoft.com. [Online]. https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/
[18] Intel. (2016, Feb) http://www.intel.com/. [Online]. http://www.intel.com/content/www/us/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html
[19] Google. (2016, Oct) https://cloud.google.com/. [Online]. https://cloud.google.com/solutions/iot-overview
[20] Lawrence Miller, IoT Security for Dummies, Carrie A. Johnson, Ed. Chichester, West Sussex, United Kingdom: John Wiley & Sons, Ltd, 2016.
[21] Eric Gross, Ryan Chinn, Samantha Forbis, Leon Walker, Hsinchun Chen Mark Patton, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," in Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, The Hague, Netherlands , 2014, pp. 232 - 235.
[22] Andrew Meola. (2016, Aug) http://www.businessinsider.com. [Online]. http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8?IR=T
[23] Gemalto. (2016) http://breachlevelindex.com. [Online]. http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf
[24] Krebs On Security. (2016, Nov) https://krebsonsecurity.com/. [Online]. https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060
[25] Jason Murdock. (2016, Feb) http://www.ibtimes.co.uk/. [Online]. http://www.ibtimes.co.uk/los-angeles-hackers-demand-3m-ransom-hospital-unlock-vital-files-1543962
[26] BBC News. (2016, Oct) http://www.bbc.com. [Online]. http://www.bbc.com/news/business-37551633
[27] Andy Greenberg. (2015, Aug) https://www.wired.com. [Online]. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[28] Peter Mell and Tim Grance. (2009, July) www.nist.gov. [Online]. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf
[29] Adam Pasick. (2015, Apr) http://qz.com. [Online]. http://qz.com/393909/american-airlines-planes-are-grounded-because-their-pilots-ipads-have-crashed/
[30] SHAWN HELTON. (2015, April) http://21stcenturywire.com. [Online]. http://21stcenturywire.com/2015/04/13/remote-control-aviation-expert-says-germanwings-9525-could-have-been-hacked-electronically/
[31] Drew Harwell. (2015, May) https://www.washingtonpost.com/. [Online]. https://www.washingtonpost.com/business/economy/fbi-probe-of-plane-hack-sparks-worries-over-flight-safety/2015/05/18/8f75e662-fd69-11e4-805c-c3f407e5a9e9_story.html?utm_term=.66213252e33d
[32] Brian Krebs. (2016, Apr) https://krebsonsecurity.com/. [Online]. https://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/#more-34596
[33] OWASP. (2014, Sep) https://www.owasp.org. [Online]. https://www.owasp.org/index.php/IoT_Security_Guidance
[34] Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak Charles Brookson Scott Cadzow. (2016, July) https://www.enisa.europa.eu/. [Online]. https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Pakistan Journal of Engineering Technology and Science (PJETS)
Volume 7, No 1, June 2017

Prospects & Challenges of Implementing Knowledge Management System in IT Industry

[1]Syed Mubashir Ali, Asim Iftikhar
College of Computer Science & Information Systems,
Institute of Business Management

***Abstract*- Recent past has seen an epidemic growth in the adoption of strategic information systems. In order to be successful, enterprises are putting in huge investments into implementation of information technology (IT) and knowledge management systems (KMS). KMS implementation in an IT industry has been discussed in this paper. Several challenges including multiple information sources, access control, and employee's mistrust among others are being identified along with their possible solutions. Later foreseen benefits of KMS implementation including quicker problem identification, faster response time, and cost saving among others are being highlighted. The paper concludes with revealing future research possibilities.**

Keywords: Knowledge management, service industry, information technology implementation.

I. INTRODUCTION

Good governance and efficiency are the two major drivers for organization's progress. Academicians, scholars and practitioners; all of them have highlighted the significance of knowledge [1-3]. Organizations have been using the shoulders of knowledge and technology not only to survive, but to gain strategic competitive advantage [4]. This has resulted in extensive KMS implementation in various industries worldwide.

Enterprises in order to ensure well-organized flow of knowledge from both inside as well as outside the organization are employing KMS. This not only helps organizations in achieving their goals, but also facilitates in having better organizational output. According to [5]; a revamp in strategy, business processes, configuration and technologies is required to make the best out of KMS. Even the organizations that are unaware of KMS, also requires the supervision of knowledge systematically. This creates a challenge when a particular knowledge is required such as: (1) from where to look for the knowledge, (2) from whom to get it and (3) how to finally have it.

[1]mubashir.ali@iobm.edu.pk

In order to tackle the above challenges, KMS is the way to go. KMS streamlines the end-to-end flow of information within an organization [6] [7].The systematic storage of information in a KMS makes desired information retrieval a facile task.

The next section will briefly discuss KM. After this, company background has been discussed where the KMS is being implemented. Section 4 will highlight few of the challenges being faced by the company during and after the KMS implementation. Section 5 will discuss about the perceived benefits that are expected after successful KMS implementation. In the end, paper is concluded along with identifying future research direction.

II. KNOWLEDGE MANAGEMENT

In order to understand what KM is, we need to understand the definition of knowledge. Although knowledge is considered as an important strategic asset of any modern-era organization, its definition is still being defined [8]. Numerous definitions of knowledge have been devised by a number of researchers. According to [9]; knowledge is the observation, skills and know-how of an individual that comes with experience. Nonaka et al. [10] defines knowledge as the actuality of skillful action and the potentiality of defining a situation to take desired decision.

Now we have understood what knowledge is, we can better understand what KM is. The process to generate, expand, deliver, and exploitation of the use of knowledge is referred to as KM [11]. KM is being utilized to enhance organizational productivity along with gaining strategic competitive advantage [12] [13].

Very often, an individual's knowledge or perception can have complete disparity to the knowledge structure of the organization. Therefore, it is imperative to perform business process re-engineering in a way that aligns individual's knowledge to the organization's knowledge. In order to achieve this, KMS is being implemented. This includes generation, accumulation, retrieval and transfer of knowledge [14] [15].

III. COMPANY BACKGROUND

XYZ Company is the trendsetter in the fields of time management, authentication & authorization, access control and security management solutions. The company focuses on delivering superior technology for workforce management with the help of its world-class top technology vendors. Technology solutions provider sells business problems solutions instead of selling technology itself. Having presence at multiple locations within Pakistan, XYZ Company has a clientele of more than

10,000. In order to give improved customer service, the company decided to implement KMS. Due to privacy issues, the name of the company has been kept anonymous.

IV. Challenges And Issues

The data was gathering from two engineers working for the case company. Many brain-storming sessions were being conducted during the planning and designing phase of KMS. All the stakeholders were involved included but not limited to board of directors, managers and senior managers, engineers and staff from various departments such as maintenance, system support, supply chain and others. After several meetings, the company identified following challenges and issues:

A. Diverse Information Sources

When a client faces an issue in the solution being implemented by the XYZ Company, any available support engineer is assigned by the company to resolve the issue of client. As it is almost next to impossible for the company to always assign the same engineer to a particular client to resolve its issue, knowledge is being generated by multiple support engineers over the course of service level agreement (SLA) with the client. It is imperative that KMS gets updated with the knowledge from only the authorized support engineers in a systematic in order to avoid unnecessary information stored in KMS.

B. Information Inaccuracy

Sometimes, during a remote support given to the client, the client's description of a particular issue is ambiguous or inaccurate. For example, if a client reports an issue that one employee is not being authenticated using the face-detection system being implemented is because system is malfunctioning. However, in actual the problem was not exactly the malfunctioning of the system, instead the employee when got registered had a beard and later he got his beard cleaned which caused the system to not recognize the employee. There is a possibility that this problem gets stored in KMS detailing malfunction as the core reason, which will be incorrect information. Therefore, there needs to be some mechanism in KMS or some standardized procedure, which avoids recording of avoidable and inaccurate information to be entered into KMS.

When a client faces an issue in the solution being implemented by the XYZ Company, any available

C. Unstructured Information

Since, KMS gets information from multiple clients and from multiple support engineers. The information needs to be recorded into KMS accumulate as a huge pile of data. This multiple source of information if entered into the system without proper classification and tags leads to inefficient knowledge retrieval later on. In order to address this issue, the company believed that may employ some classification or statistical techniques along with developing Meta data which may helps in overcoming this challenge.

D. Employees' Mistrust

It is an organizational culture that a technical person sometimes hinders in sharing his knowledge about a particular problem that only he knows how to resolve. The reason is to have some employees / engineers fears that if their knowledge is being transferred to other engineers, they are vulnerable to being fired from the company or in other words become dispensable. This was ranked as the major issue by the company's top management. In order to rectify this issue, top management suggested that the most useful employee who provides with the most legitimate input of information into KMS will be provided maximum annual appraisal.

E. Data Redundancy

The duplication of data is referred to as data redundancy [16]. There is a very high possibility of storage of multiple instances of the same information in KMS. This will result in data redundancy which may make system slow with the passage of time and also the information search could become tedious too. This issue can be resolved by stream lining the process of data entry into KMS by allowing less manual input and more pre-defined input using dropdown menus and combo boxes. This will eventually help KMS in identify and avoid data repetition data duplication.

F. Access Control

Open access to the KMS will be a threat to the information being shared. If all engineers and support staff will have access to update or modify information in KMS, there is a high chance of data inconsistency and / or data loss. In order to take care of this issue, the KMS should be having a provision to give appropriate and different access level to each user who can access or alter the information within KMS.

G. *Stamp Marking / Approval of Imperative Knowledge*

At the time of writing this paper, the KMS was still in the initial phase of its implementation. Initially each and every issue and its solution including unnecessary information were used to be recorded in the KMS. Therefore, this was a need to ensure only the appropriate and necessary information being stored in KMS. But the question was; who will be responsible to approve the source information as "the knowledge". This issue can be addressed by having some provision in the software to register some administrators or special users, which acts as a data or information verifier instead of a data source.

V. BENEFITS OF KMS

According to [17]; product and service efficiency and productivity can only be achieved by having proper knowledge management. It is believed that the implementation of KMS will result in increased customer satisfaction and company's revenue. A number of benefits were being identified by the company as a result of KMS implementation which are discussed below:

A. *Problem Identification*

One of the main reasons of implementing KMS is to identify client's problems and issues as early as possible so as to provide better and improved customer service. Having combined and centralized solutions to all the problems in the KMS will enable the company in better and quicker problem recognition and identification that may be faced by its clients in the future.

B. *Data Mining and Knowledge Engineering*

The science and theory to reveal hidden patterns and trends in a large and complex collection of data is referred to as data mining [18]. KMS having a lot of centralized data and information will enable the company to perform data analytics and make use of knowledge engineering principles. This will enable the company in improving their decision-making capabilities. The company may also be able to forecast problems that may arise with a particular product or particular client.

C. *Quicker Troubleshooting*

As discussed earlier, the use of KMS enables rapid identification of problems. As each problem along with its appropriate solutions are being saved in KMS, this will enable the company is faster troubleshooting and problem rectification.

D. *Reduced Response Time*

As discussed in previous paragraphs, quick problem identification and faster troubleshooting results in reduced response time. Rather than investigating every problem and its solution from scratch, the KMS will enable the company to just search the particular problem from within the system along with the tried and tested solution thus resulting in reduced response time to the customer issues.

E. *Remote Support and Cost Saving*

KMS will change the way how support is being provide to the customers. The requirement to visit the client/customer premise in person will be reduced because of KMS especially for software related issues. As all the solutions to the problems would be single click away, company can easily provide remote support to its client over telephone or by remotely logging in to the client's system. This will ultimately result in saving time by reducing the frequency of visiting in person to the clients' premise and also the various costs of factors such as transportation, user engagement etc associated with it.

F. *Customer Satisfaction*

The perceived performance of a product or service with respect to the customer's own expectations is referred to as customer satisfaction [19]. Company's ultimate goal was to have satisfied customers. They will be able to achieve this goal by KMS implementation. Quicker problem identification, faster troubleshooting and quick problem resolution will ultimately result in satisfied and happy customers, which will further result in company's growth.

VI. Conclusion And Future Research Direction

Every technological implementation comes at a cost of some challenges and issues [20]. These issues need to be addressed and rectified efficiently in order to have that implementation a success [21]. This paper identified and discussed several challenges and issues. Some of these can be generalized. But majority of them are specific to service industry especially IT service industry as discussed. Similarly, some the benefits discussed are the ones, which were expected or experienced by XYZ Company and may not be applicable to other organizations belonging to different industry. Further research can be done by comparing various KMS implementations case studies belonging to other industries in order to verify and or generalize the results of this research study. Furthermore, future research may also reveal some additional challenges or benefits of KMS.

ACKNOWLEDGMENT

We would like to thank all the managers, engineers and support staff that provided us with their valuable feedback and writing this research paper. In addition, we would like to thank Ms. Fatima Khalid for proofreading and correction of grammatical errors.

REFERENCES

[1] Wu, Ing-Long, and Han-Chang Lin. "A strategy-based process for implementing knowledge management: An integrative view and empirical study." *Journal of the Association for Information Science and Technology* 60, no. 4 (2009): 789-802.
[2] McAdam, Rodney, and Sandra McCreedy. "A critical review of knowledge management models." *The learning organization*6, no. 3 (1999): 91-101.
[3] López-Nicolás, Carolina, and Ángel L. Meroño-Cerdán. "Strategic knowledge management, innovation and performance." *International journal of information management* 31.6 (2011): 502-509.
[4] Holsapple, Clyde, ed. *Handbook on knowledge management 1: Knowledge matters*. Vol. 1. Springer Science & Business Media, 2013.
[5] Rasula, Jelena, Vesna Bosilj Vuksic, and Mojca Indihar Stemberger. "The impact of knowledge management on organisational performance." *Economic and Business Review for Central and South-Eastern Europe* 14, no. 2 (2012): 147.
[6] Nazari, Eslam, Ayoub Sarafraz, and Somayeh Naser Amini. "The Effect of Key Factors of Knowledge Management Success on improving Customer Relationship Management (Case study: financial and credit institutions of Parsabad)." *International Journal of Humanities and Cultural Studies (IJHCS)* ISSN 2356-5926 (2016): 915-923.
[7] Baharuddin, Mohammad Fazli, Tengku Adil Tengku Izhar, Ahmad Nadzri Mohamad, and W. M. H. W. Hasnol. "A Framework based Knowledge Management System (KMS) for Dynamic Decision-Making (DDM)." *International Journal of Academic Research in Business and Social Sciences* 6, no. 4 (2016): 287-294.
[8] Lindner, Frank, and Andreas Wald. "Success factors of knowledge management in temporary organizations." *International Journal of project management* 29, no. 7 (2011): 877-888.
[9] Koskinen, Kaj U., and Pekka Pihlanto. "Why Knowledge Management in Project-Based Companies?." In *Knowledge Management in Project-Based Companies*, pp. 1-6. Palgrave Macmillan, London, 2008.
[10] Nonaka, Ikujiro, and Georg Von Krogh. "Perspective—Tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory." *Organization science* 20, no. 3 (2009): 635-652.
[11] Içten, Elçin, Girish S. Joglekar, Arun Giridhar, and Gintaras V. Reklaitis. "Application of a Knowledge Management System to a Dropwise Additive Manufacturing System for Pharmaceuticals." In *Computer Aided Chemical Engineering*, vol. 38, pp. 619-624. Elsevier, 2016.
[12] Chalmeta, Ricardo, and Reyes Grangel. "Methodology for the implementation of knowledge management systems." *Journal of the American Society for Information Science and Technology* 59.5 (2008): 742-755.
[13] McAdam, Rodney. "Knowledge management as a catalyst for innovation within organizations: a qualitative study." *Knowledge and process management* 7, no. 4 (2000): 233.
[14] Back, Andrea, Georg von Krogh, and Andreas Seufert, eds. *Putting knowledge networks into action: Methodology, development, maintenance*. Springer Science & Business Media, 2005.
[15] Natek, Srečko, and Moti Zwilling. "Student data mining solution–knowledge management system related to higher education institutions." *Expert systems with applications* 41, no. 14 (2014): 6400-6407.
[16] Song, Qinbao, Jingjie Ni, and Guangtao Wang. "A fast clustering-based feature subset selection algorithm for high-dimensional data." *IEEE transactions on knowledge and data engineering* 25, no. 1 (2013): 1-14.
[17] R.Young. (2010). *From knowledge to innovation.* http://www.knowledge-management-online.com/from-knowledge-toinnovation.html (Accessed on August 16, 2015)
[18] Lior, Rokach. *Data mining with decision trees: theory and applications*. Vol. 81. World scientific, 2014.
[19] N. Torres, Edwin, and Sheryl Kline. "From customer satisfaction to customer delight: Creating a new standard of service for the hotel industry." *International Journal of Contemporary Hospitality Management* 25, no. 5 (2013): 642-659.
[20] Ali, Syed Mubashir. "Challenges and security issues in future IT infrastructure components." International Journal of Computers & Technology 8, no. 2 (2013): 845-847.
[21] Ali, Syed Mubashir. "Challenges and Benefits of Implementing Tablets in Classroom for e-Learning in a K-12 Education Environment–Case Study of a School in United Arab Emirates." *Research Inventy: International Journal of Engineering and Science* 3, no. 4 (2013).