Rock Tale Drilling Prototype : An Innovative Design for Investigation of Rock Properties

Rekha Tomar
Academy of Scientific and Innovative Research
CSIR-Central Institute of Mining & Fuel Research
Dhanbad, India

Dilip Kumbhakar
Longwall Mining Division
CSIR-Central Institute of Mining and Fuel Research
Dhanbad, India

Abstract— Assessing the physico-mechanical properties of rock is one of the important factors of concern to the engineers in the general field of rock excavation. Different direct and indirect methods are applied to determine the rock properties. This paper deals with the details of a design concept applied to develop a drilling prototype which generates online drilling parameters and can be used to correlate with various rock properties.

Keywords— Prototype, microcontroller, Infra red, Hall effect, data logger, signal conditioning, signal convertor.

1. INTRODUCTION

In mining industry, the knowledge of physico-mechanical properties of rock types, viz. uniaxial compressive strength, tensile strength, Young's modulus of elasticity, density, Poisson's ratio, etc., is very important for design and stability analysis of different structures, like, pillars, openings and slopes [14, 17]. These properties are also important for optimizing many mining operations, such as, blasting and mechanical excavation of rocks and minerals.

The physico-mechanical properties of rocks are generally determined in the laboratory according to ASTM/ISRM suggested standard methods [2,6] stipulated for each property. However, these methods are time consuming and expensive. To obtain realistic results of rock properties, it requires carefully prepared rock samples. The standard cores cannot always be extracted from weak, highly fractured, thinly bedded, foliated and/or block-in-matrix rocks. Weak to very weak rocks may deteriorate during coring and fail to yield good quality samples.

Worldwide various studies have been conducted which clearly establishes specific relation between the physico-mechanical properties of different rock types and different drilling indices, like, rate of penetration (ROP), specific energy (SE) and heating rate (HR) are calculated from drilling parameters, such as, penetration, drilling speed, current, voltage, load, temperature etc. [1, 4, 7, 8, 10, 11, 13]. Taking cue from the above, an effort has been made to develop an alternative method using the drilling technique to determine different rock properties.

The paper deals with the details of a design concept used to develop a drilling prototype which generates online drilling parameters and can be used to correlate with various rock properties. Such a system is a very useful testing installation from which most of the rock properties can be estimated.

2. DESIGN CONSIDERATIONS

The main considerations to design and develop the proposed drilling prototype are to formulate design criteria; make necessary sensory arrangements in a drilling machine; measure the drilling parameters; integrate the modular units, mechanical units with proper interfacing; and provide appropriate control and data logging mechanism. The methodology adopted for the design and development of the drilling prototype is given in figure 1. The proposed system facilitates calculation of rate of penetration, specific energy and heating rate from which different rock properties can be determined.

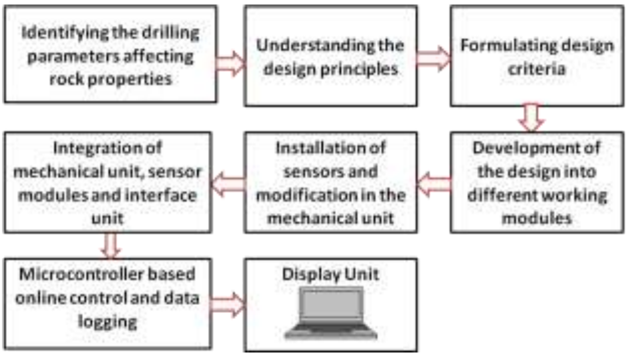

Identifying the drilling parameters affecting rock properties
Understanding the design principles
Formulating design criteria
Development of the design into different working modules
Installation of sensors and modification in the mechanical unit
Integration of mechanical unit, sensor modules and interface unit
Microcontroller based online control and data logging
Display Unit

Figure 1. Flow chart showing the methodology adopted for development of the drilling prototype

2.1 Rate of Penetration

The rate of penetration, also termed as penetration rate or drill rate, is the speed at which a drill bit breaks the rock under it to deepen the borehole [5,7,8]. It is normally measured in meters per hour or meters per minute or meters per second in SI units. It is calculated as:

$$ROP = \frac{D}{\Delta t} \qquad \text{---- (1)}$$

where, D = Depth of drilling, mm or m
Δt = Time duration, sec or min.

2.2 Specific Energy

The concept of specific energy (*SE*) was proposed by Teale [16] as a quick means of assessing rock drillability and defined it as the energy required to remove a unit volume of rock.

SE can be measured in KJ/m^3 or GJ/m^3 and can be expressed as follows:

$$SE = \frac{F}{A} + \frac{2\pi NT}{A*ROP} = E_t + E_r \qquad \text{---- (2)}$$

where, F = thrust/weight on the bit (kN).
A = hole section (m^2).
N = rotation speed (rps).
T = rotation torque (kN · m).
ROP = rate of penetration (m/s).

The first member of the equation, E_t represents the contribution of the thrust (thrust component). It is equivalent to the pressure acting over the cross – sectional area of the hole. The second member, E_r is the rotary component of energy.

It is evident from equation 2, that to calculate the specific energy, the drilling parameters, namely, thrust, torque, penetration rate and rotational speed need to be measured [3, 12, 15, 16]. The torque in equation 2 can be determined in terms of voltage and current as follows:

$$T = \frac{P}{2\pi N} \qquad \text{---- (3)}$$

$$P = V \times I \times \cos \emptyset \qquad \text{---- (4)}$$

where, *T* = motor torque, KNm
P = motor power, KWh
V= voltage, volt
I = current, ampere
cos ϕ = power factor of the motor = 0.71 for the motor under use

Thus equation 2 can be written as

$$SE = \frac{F}{A} + \frac{V * I * \cos(\phi)}{A * ROP} \qquad \text{---- (5)}$$

2.3 Heating Rate

Temperature variation occurs at the drill bit due to the heat produced while drilling [18,19]. The heating rate (HR), defined as the rate of change in temperature with respect to time, has been used in the design scheme for correlation with rock properties. It can be calculated as:

$$HR = \frac{\Delta T}{\Delta t} \qquad \text{--- (6)}$$

where, HR is the heating rate, °C/sec
ΔT is the change in temperature, °C
Δt is the duration of drilling, sec.

The process of drilling invariably increases temperature of either the drill or the job on which it is being operated. The rate of increase in temperature will greatly be influenced by the rock types and their physico-mechanical properties. Hence, this parameter can act as a means to study the rock properties.

3 DETAILS OF THE PROTOTYPE

The complete system comprises mainly of three components. The first one consists of the integrated modules of sensors and interfacing units and the data logger unit housed in a CPU enclosure. The second component includes the drill machine with all modifications incorporated to facilitate controlled testing of the samples. The third component comprises of a computer with the requisite software to configure the machine, controlling the operation and logging and retrieval of data.

The drilling prototype is fabricated using a bench type high speed rotary drill machine, array of sensors, signal convertor and conditioning units, microcontroller based operation unit, suitable interface with computer and an application software for on-line configuration, control and data logging [9]. The block diagram of the entire system is shown in figure 2.

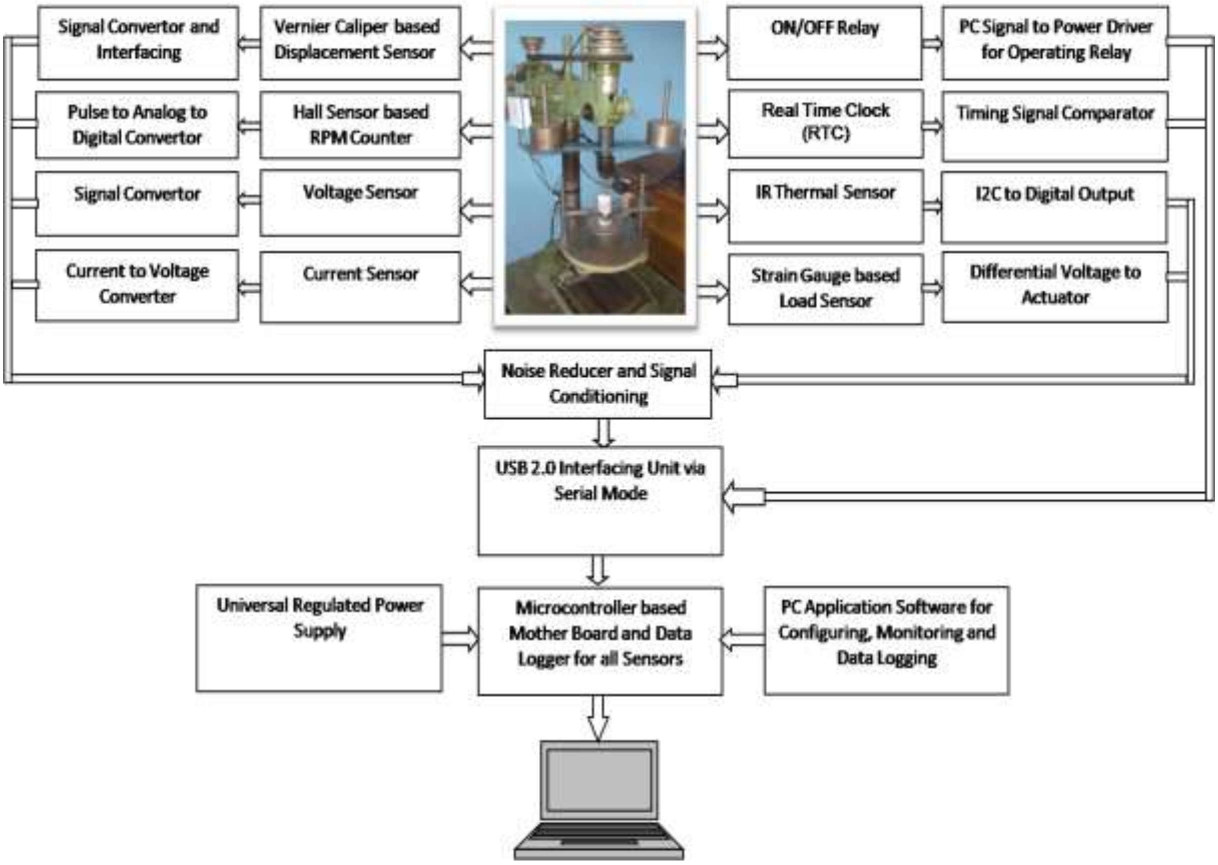

Signal Convertor and Interfacing
Vernier Caliper based Displacement Sensor
ON/OFF Relay
PC Signal to Power Driver for Operating Relay
Pulse to Analog to Digital Convertor
Hall Sensor based RPM Counter
Real Time Clock (RTC)
Timing Signal Comparator
Signal Convertor
Voltage Sensor
IR Thermal Sensor
I2C to Digital Output
Current to Voltage Converter
Current Sensor
Strain Gauge based Load Sensor
Differential Voltage to Actuator
Noise Reducer and Signal Conditioning
USB 2.0 Interfacing Unit via Serial Mode
Universal Regulated Power Supply
Microcontroller based Mother Board and Data Logger for all Sensors
PC Application Software for Configuring, Monitoring and Data Logging

Figure 2: Block Diagram of the Rock Tale Drilling Prototype

3.1 Sensor Network

The system comprises of an array of sensors used for measurement of the drilling parameters.

- Digital vernier caliper has been used to measure the depth of drilling.
- Weight on bit is measured by using a load cell fitted at the base plate.
- Cross-section area is calculated from the bit diameter.
- Rotational speed is measured by the Hall effect sensor based RPM counter.
- ROP is determined as already discussed above in section 2.1.
- Voltage and current are measured by using voltage or current sensors.
- Temperature is measured by using an infra red thermal sensor.
- Real time clock records the time.

Most of the sensors generate analog signals. To enable the microcontrollers to detect these signals, suitable analog-to-digital convertors are used in the sensor modules. However, the signal generated by the sensors have very low voltage levels. Hence, signal conditioning units are also used in the system to amplify the voltage signals generated before they can be digitized accurately and effectively measured.

3.2 Mechanical Arrangements

The laboratory scale experimental setup has been built up from Elliot make bench type high speed rotary drill machine shown in figure 3. Several modifications have been incorporated in the existing drill machines to enable measurements of the desired parameters.

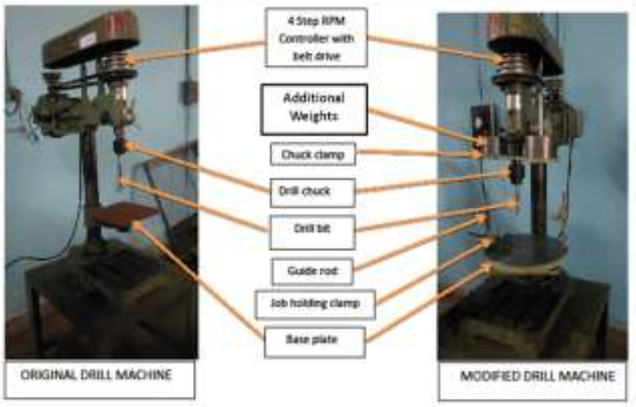


Figure 3: Modifications incorporated in the drill machine

A digital vernier caliper is fixed with the body of the drill machine and the external jaw is connected to the chuck clamp (figure 4) to measure the movement of the clamp when drill penetrates through the sample.

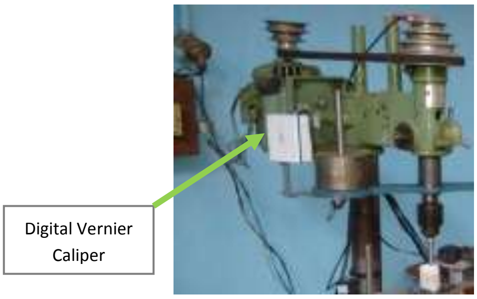


Figure 4: Arrangement showing digital vernier caliper for measurement of penetration

The drill machine has a four step rpm controller using an endless belt. On the top surface of the pulley, the Hall effect rpm sensor is fitted along with the magnetic ring as shown in figure 5.

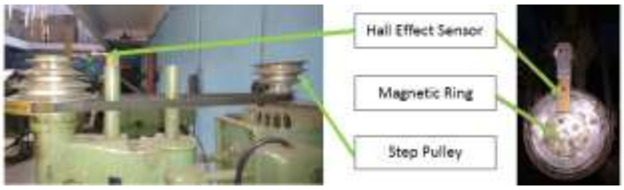


Figure 5: Arrangement showing step rpm controller with Hall sensor

A dumb-bell shaped chuck clamp, shown in figure 6, is fitted in the drill chuck for providing additional weight on its both sides. These weights are used for increasing thrust or weight on the bit.

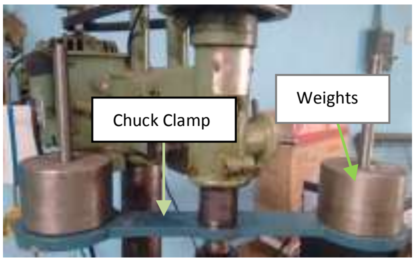


Figure 6: Arrangement showing chuck clamp with provision for additional weights

A guide rod is used for steadying or directing the motion of job holding clamp. A clamp is used in the proposed system to hold the rock samples firmly and only allows free vertical movement. The base plate has been incorporated in the system to place the rock sample over it. It is fitted with the load cell at the bottom to measure the weight of the bit on the sample and the IR sensor for measurement of temperature variation at the bit surface. The arrangement is shown in figure 7.

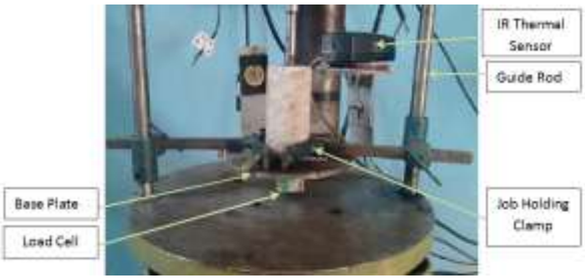


Figure 7: Arrangement showing guide rod with job holding clamp

The integrated system comprising of the mechanical unit, sensory arrangements, control unit, interface unit and display unit with software is shown in figure 8.

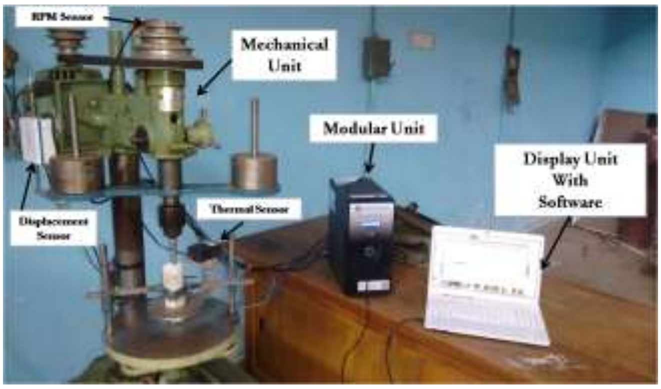
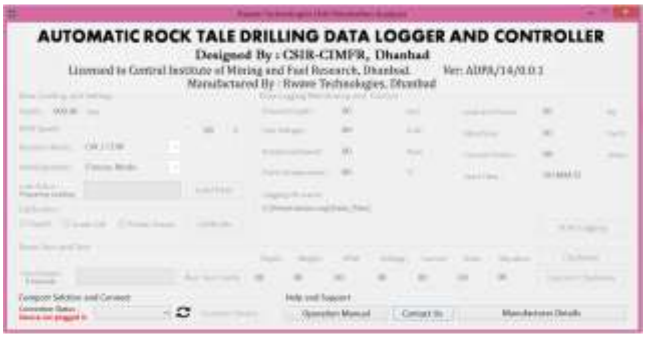


Figure 8: The Integrated Rock-Tale System

3.3 Working of the System

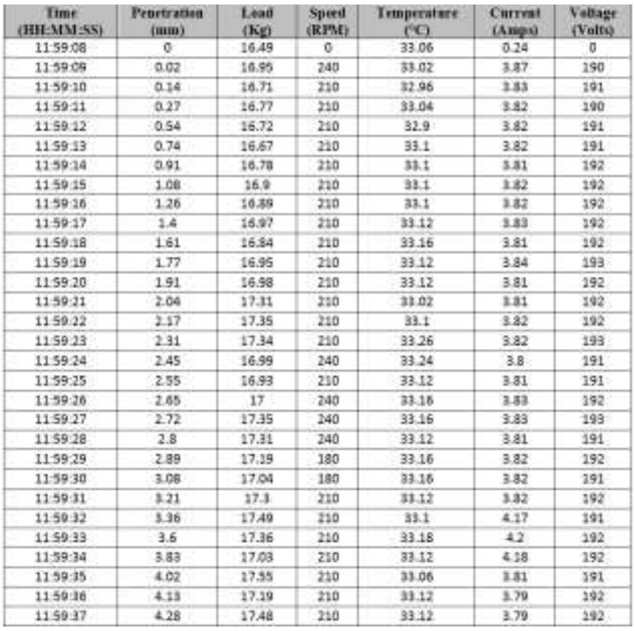
The device is constructed with power feed technology to drill the rock sample up to certain specified depth, programmed through keyboard using the application software. Provision of clockwise and anti-clockwise movement have been made to ensure that the motor moves the drilling machine upward and downward direction while drilling the hole over the rock sample. The facility for calibrating the sensors before start of any test is also provided with the system. The drilling operation is controlled by the microcontroller based operation unit. The data generated during drilling operation were transferred to the computer through an USB interface.

A snap shot of the automatic rock tale drilling data logger and controller is shown in figure 9.



AUTOMATIC ROCK TALE DRILLING DATA LOGGER AND CONTROLLER
Designed By : CSIR-CIMFR, Dhanbad
Licensed to Central Institute of Mining and Fuel Research, Dhanbad. Ver: ADPR/14/0.0.1
Manufactured By : Rwave Technologies, Dhanbad

A typical datasheet generated from a drilling test is shown in figure 10.



Time (HH:MM:SS)	Penetration (mm)	Load (Kg)	Speed (RPM)	Temperature (°C)	Current (Amps)	Voltage (Volts)
11:59:08	0	16.49	0	33.06	0.24	0
11:59:09	0.02	16.95	240	33.02	3.87	190
11:59:10	0.14	16.71	210	32.96	3.83	191
11:59:11	0.27	16.77	210	33.04	3.82	190
11:59:12	0.54	16.72	210	32.9	3.82	191
11:59:13	0.74	16.67	210	33.1	3.82	191
11:59:14	0.91	16.78	210	33.1	3.81	192
11:59:15	1.08	16.9	210	33.1	3.82	192
11:59:16	1.26	16.89	210	33.1	3.82	192
11:59:17	1.4	16.97	210	33.12	3.83	192
11:59:18	1.61	16.84	210	33.16	3.81	192
11:59:19	1.77	16.95	210	33.12	3.84	193
11:59:20	1.91	16.98	210	33.12	3.81	192
11:59:21	2.04	17.31	210	33.02	3.81	192
11:59:22	2.17	17.35	210	33.1	3.82	192
11:59:23	2.31	17.34	210	33.26	3.82	193
11:59:24	2.45	16.99	240	33.24	3.8	191
11:59:25	2.55	16.93	210	33.12	3.81	191
11:59:26	2.65	17	240	33.16	3.83	192
11:59:27	2.72	17.35	240	33.16	3.83	193
11:59:28	2.8	17.31	240	33.12	3.81	191
11:59:29	2.89	17.19	180	33.16	3.82	192
11:59:30	3.08	17.04	180	33.16	3.82	191
11:59:31	3.21	17.3	210	33.12	3.82	192
11:59:32	3.36	17.49	210	33.1	4.17	191
11:59:33	3.6	17.36	210	33.18	4.2	192
11:59:34	3.83	17.03	210	33.12	4.18	192
11:59:35	4.02	17.55	210	33.06	3.81	191
11:59:36	4.13	17.19	210	33.12	3.79	192
11:59:37	4.28	17.48	210	33.12	3.79	192

4. CONCLUSIONS

The rock tale drilling prototype is capable of generating online performance parameters, such as, penetration, drilling speed, current, voltage, load, temperature etc. These parameters can be used to calculate drilling indices, like, rate of penetration, specific energy and heating rate which bear very good relation with different rock properties.. Such a system will be a very useful testing installation from which most of the rock properties can be estimated.

5. ACKNOWLEDGMENTS

Our sincere thanks to Director, CSIR-Central Institute of Mining & Fuel Research, Dhanbad for giving permission to publish this paper and guiding us during execution of the project.

6. REFERENCES

[1] Adamson W.R. 1984, "Correlation of model excavating machine performance with rock properties and rotary drilling performance data", MSc. Thesis, University of Queensland, p. 124.

[2] ASTM 1986, "Standard test method of unconfined compressive strength of intact rock core specimens", ASTM Publication.

[3] Celada B., Galera J.M., Munoz C. and Tardaguila I. 2009, "The use of the specific drilling energy for rock mass characterization and TBM driving during tunnel construction", ITA-AITES World Tunnel Congress, Budapest, Hungary.

[4] Fish B.G. 1968, "The basic variables in rotary drilling", Mine and Quarry Engineering, 27, pp. 74-81.

[5] Hoseinie S.H., Atael M. and Aghababaie A. 2014, "A lab study of rock properties affecting the penetration rate of pneumatic top hammer drills", Journal of Mining and Environment, vol.5, no.1, 25-34.

[6] ISRM 2007, "The Complete ISRM Suggested Methods for Rock Characterization, Testing and Monitoring: 1974-2006", International Society for Rock Mechanics, Commission on Testing Methods.

[7] Kahraman S., Balci C., Yazici S. and Bilgin N. 2000, "Prediction of the penetration rate of rotary blasthole drilling using a new drillability index", Int. J Rock Mech. & Min. Sci., 37: 729-43.

[8] Kahraman S. and Bilgin N. 2003, "Drillability Prediction in Rotary Blast Hole Drilling", International Mining Congress and Exhibition of Turkey-IMCET, ISBN 975-395-605-3.

[9] Lundberg B. 1982, "Microprocessor simulation of percussive drilling", International Journal of Rock Mechanics and Mining Science,19: 229-39.

[10] Pandey A.K., Jain A.K. and Singh D. P. 1991, "An investigation into rock drilling", Int. Journal of Surface Mining Reclamation, 5, pp. 139-141.

[11] Paone J., Madson D. and Bruce W. E. 1969, "Drillability studies-laboratory percussive drilling", US Bureau of Mines, RI 7300.

[12] Reddish D.J. and Yasar E. 1996, "A new portable rock strength index test based on specific energy of drilling", Int. J. Rock Mech. Min. Sci., 33(5): pp. 543-548.

[13] Selmer-Olsen R., Blindheim O.T. 1970, "On the drillability of rock by percussive drilling", In: Proceedings of the Second Congress International Society on Rock Mechanics, p. 65–70.

[14] Singh D.P. 1969, "Drillability and physical properties of rocks", Proc. Rock Mechanics Symp., University of Sydney, pp.29-34.

[15] Sinkala T. 1991,"Improving hole quality by automatic control of drilling process: theoretical and field studies". Min Sci Technol 1991; 12:79-88

[16] Teale R. 1965, "The concept of specific energy in rock drilling", Int J Rock Mech Min Sci, 2: 57–71.

[17] Thuro K. 1997, "Drillability prediction geological influences in hard rock drill and blast tunneling", Geol Rundsch, 86:426-438

[18] Tu, Y. K., Chen, L. W., Ciou, J. S., Hsiao, C. K. and Chen, Y. C. 2013. Finite element simulations of bone temperature rise during bone drilling based on a bone analog, Journal of medical and biological engineering, vol. 33, no. 3.

[19] Zhi-jun, W., Yang-sheng Z., Yuan Z. and Chong W. 2009. Research Status Quo and Prospection of Mechanical Characteristics of Rock under High Temperature and High Pressure, Proceedings Earth and Planetary Science, no 1, 2009, pp. 565–570.

International Journal of Science and Engineering Applications
Volume 4 Issue 6, 2015, ISSN-2319-7560 (Online)

Developing Mobile-Based Restaurant Point of Sales Information System Application

Alexander Setiawan
Informatics Engineering
Petra Christian University
Surabaya, Indonesia

Silvia Rostianingsih
Informatics Engineering
Petra Christian Universit
Surabaya, Indonesia

Hendy Thomas Herman
Informatics Engineering
Petra Christian Universit
Surabaya, Indonesia

Abstract: Point of sales system information is a growing system information and a lot of people is interested in using it especially in the business areas. Nowadays, the mostly used process in restaurant are order process, reservation process, delivering customer;s order to kitchen, and calculating payment bill that are still noted using paper, which makes the process less efficient than it should have been. In this research, a mobile-based point of sales information system application will be developed. The development of this application is using Laravel PHP framework and Javascript.

Result from the research is that the application can show customer's order, record reservation, order's status in kitchen and display daily sales report.

Keywords: Restaurant, Information System, Point of Sales, Mobile.

1. INTRODUCTION

The growth of the technology nowadays enforce the needs of accurate and fast information in restaurant's business process. The already existing process in most restaurant is in need of such information system to help their business process. There are various matters that needs to be addressed inside the taking order, and reservation process, such as to quickly find out how many items are available to order without the need of walking back and forth to kitchen department, mistakenly write the customer's order by the waiters or mistakenly read the waiter's handwriting by the kitchen department.

With the use of mobile-based point of sales information system application, the waiter can quickly find out how many items are available to order, the customer's order will be directed quickly to kitchen department to prevent the human error done by both of the waiter and kitchen department. Thus can save the time required to process the customer's order and prevent the possible human error.

2. BASIC THEORY

2.1 Point of Sales

Point of sales (POS) is the physical location at which goods are sold to customers. The point of sale is often more specific than the general building or store where something is sold, typically indicating the piece of technology which is used to finalize the transaction. In many cases, this is a standard cash register at the front of the store [3].

Restaurant POS refers to point of sale (POS) software that runs on computers, usually touchscreen terminals or wireless handheld devices. Restaurant POS systems assist businesses to track transactions in real time. Typical restaurant POS software is able to print guest checks, print orders to kitchens and bars for preparation, process credit cards and other payment cards, and run reports. POS systems are often designed for a variety of clients [4].

2.2 Laravel Framework

Framework is used to ease the maintenance to website by other developer because the structure of the website is already defined by the framework thus making it easier to understand.

Laravel is an MVC web-development framework written in PHP. It has been designed to improve the quality of your software by reducing both the cost of initial development and ongoing maintenance costs, and to improve the experience of working with your applications by providing clear expressive syntax and a core set of functionality that will save hours of implementation time [6].

2.3 PhoneGap

PhoneGap is a growing technology used to develop cross-mobile platform applications. PhoneGap is a HTML5 application framework that is used to develop native applications through web technologies. This means that developers can develop Smartphone and Tablet applications with their existing knowledge of HTML, CSS, and JavaScript. [2].

2.4 Web Services

In an SOA, applications are made up of loosely coupled software services, which interact to provide all the functionality needed by the application. Each service is generally designed to be self-contained and stateless to simplify the communication that takes place between them.

Web services provides a technology foundation for implementing an SOA. Web services are self-contained software services that can be accessed using simple protocols over a network. Web services can perform a wide variety of tasks, ranging from simple request-reply tasks to full business process interactions [5].

REpresentational State Transfer (REST) is an architecture principle in which the web services are viewed as resources and can be uniquely identified by their URLs. The key characteristic of a RESTful Web service is the explicit use of HTTP methods to denote the invocation of different operations [1].

3. SYSTEM DESIGN

3.1 Analysis of Existing Ordering System

Order process in restaurant is done manually, which means that the waiter write the customer's order in a paper and then goes to the kitchen to deliver it so it can be processed immediately and then to cashier so that how much the customer is obligated to paid later can be calculated. Should the item(s) ordered by the customer are out of stock, the waiter then must go back to customer to inform them about the availability of the item.

3.2 Problem Analysis of Existing Ordering System

Order process in the restaurant is not efficient and inconvenience, because the waiter must goes back and forth to kitchen and cashier every time there is a new order from the customer. If the restaurant is crowded then this process can waste valuable time which can lead to the delay of serving the customer's order.

3.3 Requirement Analysis of Ordering System

Based from the problem analysis of the existing ordering system, it can be identified that the waiter needs more efficient order process system. System that is directly connected to kitchen and cashier is needed in ordering process to increase the waiter's efficiency, to reduce the time needed to process the order, and also to quickly find out the availability of each item.

With the help of the system, it is expected to reduce the time needed to process customer's order until the order is served.

3.4 Information System Application Design

The new information system is created to ease the order process and table selection to help the waiter and to satisfy the customer. The system is a mobile-based application and will be automatically directed to kitchen and to cashier.

3.5 Research Flowchart

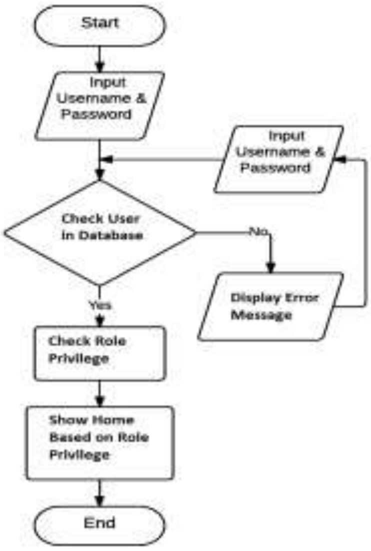

Start
Input Username & Password
Check User in Database
No
Input Username & Password
Display Error Message
Yes
Check Role Privilege
Show Home Based on Role Privilege
End

Figure 1 Application Overview

Figure 1 explain the overview of the application that will be created. This application can be used by the user with the privilege of admin and user. Users with the admin privilege will be able to use all the feature provided in the application, while the user with user privilege will have a limitation that is set by the admin. Before using the application, users are required to login with username and password. The system will then check the login information provided by the user if the login information is existed in database, the system will check for its privilege level and display the home page based on the privilege. If the login information is not existed or false the system will display an error message and the user must login again.

In home page of the application, there are various menus that can be chosen. The hierarchy from each menus can be viewed in Figure 2.

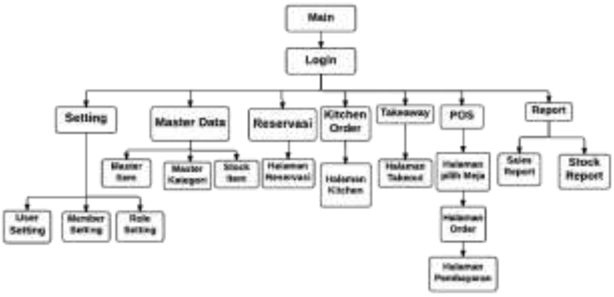


Figure 2 Hierarchy Menu

New order can be added from POS menu by the user by selecting the table beforehand. The flowchart of adding order process can be viewed in Figure 3.

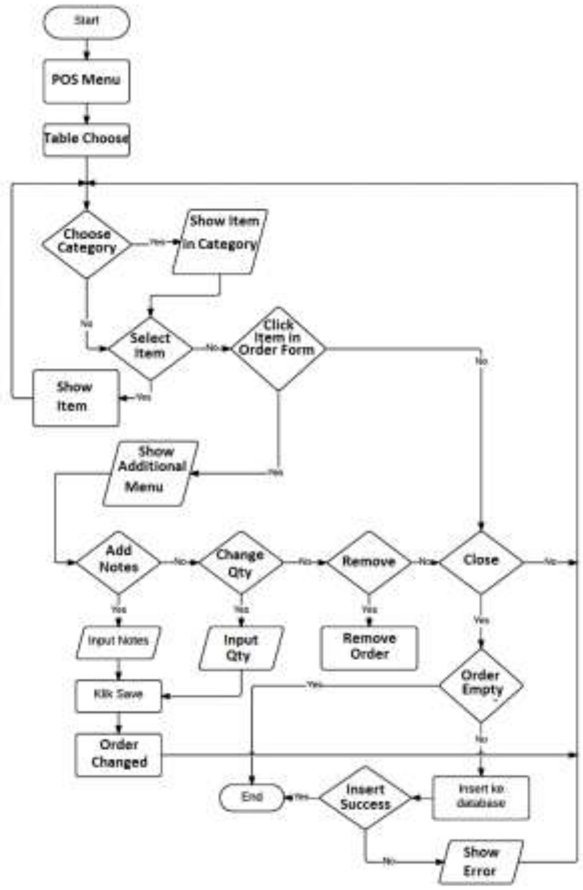


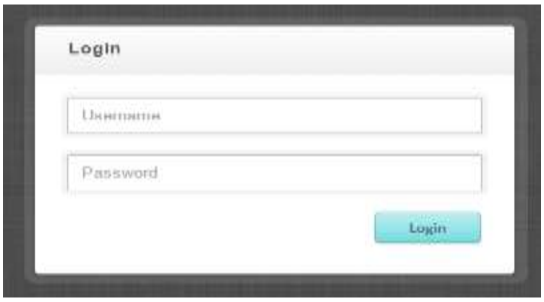
Figure 3 Add Order

4. APPLICATION IMPLEMENTATION

This chapter will explain the implementations of the application.

4.1 Login

Before the application can be used, the user must login first. The login page can be viewd in Figure 4.



Login

Username

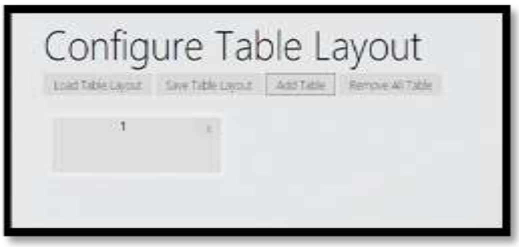
Password

Login

Figure 4 Login Page

4.2 Layout Table

Creating table layout can be done by opening Table Layout menu and then creating the table layout using Add Table button. This process can be seen in Figure 5.



Configure Table Layout

Load Table Layout | Save Table Layout | Add Table | Remove All Table

1

Figure 5 Create Table Layout

The created table layout will be used as the table layout in this application that can be seen in Figure 6.

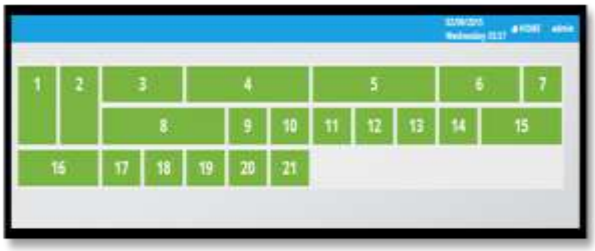


Figure 6 Layout Table

4.3 Ordering

Ordering process is done by selecting POS menu in home page. After the user selects the table, user will be redirected to order form that can be viewed in Figure 7.

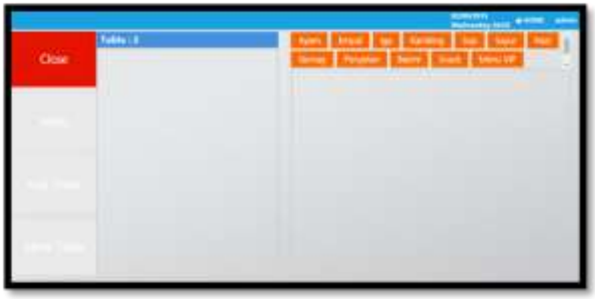


Figure 7 Order Form

To be able to choose item, user must select the category from the item that will be selected, and then choose the item. This process can be viewed in Figure 8.

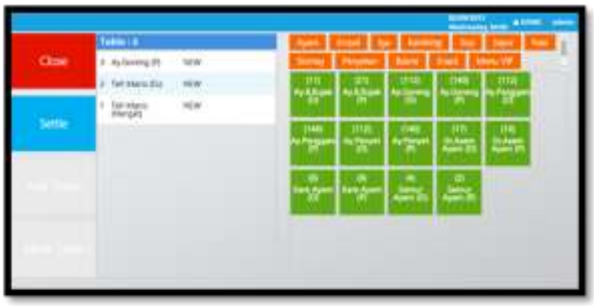
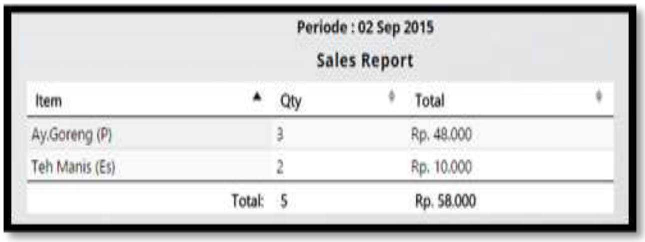


Figure 8 Filled Order Form

4.4 Reporting

Report page display the sales report and item's stock in certain period. Sales report consists of total sales report, total promo discount, total payment type. While the stock report contains stock item report in certain period. Item sales report can be viewed in Figure 9.



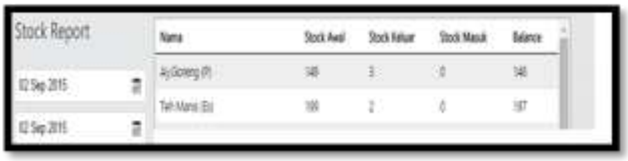
Periode : 02 Sep 2015

Sales Report

Item	Qty	Total
Ay.Goreng (P)	3	Rp. 48.000
Teh Manis (Es)	2	Rp. 10.000
Total:	5	Rp. 58.000

Figure 9 Item Sales Report

Stock item report can be viewed by selecting Stock Report in Report page, can be seen in Figure 10.



Stock Report

02 Sep 2015

02 Sep 2015

Nama	Stock Awal	Stock Keluar	Stock Masuk	Balance
Ay.Goreng (P)	148	3	0	148
Teh Manis (Es)	199	2	0	197

Figure 10 Stock Report

4.5 Mobile Devices

Mobile application can be used in Android mobile devices that runs on Android Jelly Bean operating system. The login page from the mobile device can be viewed in Figure 11.

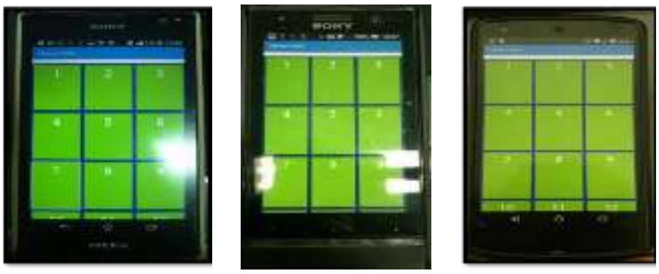
Sony Xperia TX
(i)

Sony Xperia U
(ii)

LG Nexus 5
(iii)

Figure 11 Mobile Login

After a successful login, user will be directed to table selection page. This can be seen in Figure 12.

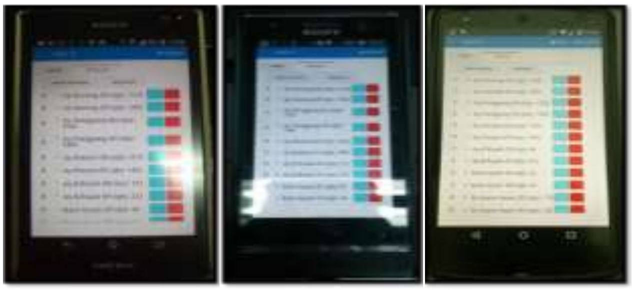


Sony Xperia TX (i) Sony Xperia U (ii) LG Nexus 5 (iii)

Figure 12 Mobile Table Selection

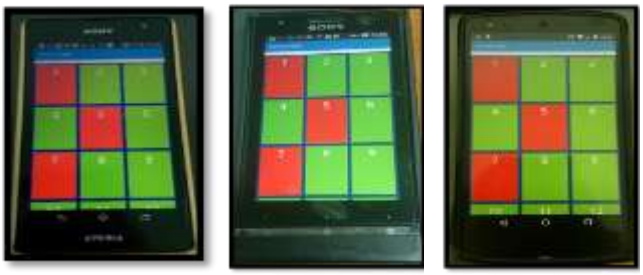
In table selection page, user is required to choose the table before adding a new order. New order form can be viewed in Figure 13 after the user choose the table.

After the successful order, user will be directed to table selection page and the table's colour will change to red, indicating that there is an order in that table. This can be viewed in Figure 14.



Sony Xperia TX (i) Sony Xperia U (ii) LG Nexus 5 (iii)

Figure 13 Mobile Order Form



Sony Xperia TX (i) Sony Xperia U (ii) LG Nexus 5 (iii)

Figure 14 Color Alteration in Mobile Table Selection

5. CONCLUSIONS

Based from the result of the testing, conclusions made are :

- Application can display order, display available item to order, reservation data, sales and stock report, change order status in kitchen, and updating item data and category.
- Application can create table layout in creating table layout page.
- All features from the application works using the local area network connection.
- All feature in mobile device works well.
- Based on the questionnaire's results, 45% of the respondents answered good, 50% of the respondents answered mediocre, and 5% of the respondents answered not good enough for the question does the application's user interface is user friendly. This indicates that the application's user interface is still acceptable.

6. REFERENCES

[1] Dambal, V. 2010. REST, Web services, REST-ful services.http://www.ibm.com/developerworks/library/ws-RESTservices.

[2] Ghatol, R. dan Patel, Y. 2012. Beginning PhoneGap: Mobile Web Framework for JavaScript and HTML5. California: Apress Media LLC.

[3] Investorwords. Point of Sale. URI= http://www.investorwords.com/3725/point_of_sale.html.

[4] Kashima, T., Matsumoto, S., dan Ishii, H. 2010. Recommendation Method with Rough Sets in Restaurant Point of Sales System. Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol III, IMECS 2010.Internet Corporation for Assigned Names and Numbers. n.d. WHOIS Primer | ICANN WHOIS. http://whois.icann.org/en/primer.

[5] Keen, M., Coutinho, R., Lippmann, S., Sollami, S., Venkatraman, S., Baber, S., Cui, H., dan Fleming, C. 2012. Developing Web Services Applications. IBM.

[6] McCool, S. 2012. Laravel Starter . Birmingham : Packt Publishing Ltd. URI= http://www.blog.flds.fr /site/assets/files/1212/laravel_starter.pdf.

Accessing and Modifying Sqlite Remotely for Catering Multi Client Access

Sharayu Lokhande
Department of Computer Engineering
Army Institute of Technology, Pune

Vaishali Ganganwar
Department of Computer Engineering
Army Institute of Technology, Pune

Abstract: SQLite is a lightweight database management system and a Stable serverless database with almost zero difficulty in installations. SQLite does not support client server facility due to the write lock issue. For expedite multi-client access to the central database, multiple instances of the database on the central system can be created and later integrating these instances to give the resultant product. Accessing these instances remotely would be a solution to the write lock issue. As a result of creating multiple instances of the database on the same system, there might be a heavy traffic which could lead to reduce performance. To handle this cloud computing concept of High Availability which refers to a system or component that is continuously operational for a desirably long length of time.

Keywords— Remotely Access, SQLite, High Availability

1. INTRODUCTION

A lightweight database system is a high- performance, application-specific Database Management system. It differs from a general- purpose (heavyweight) [1] DBMS in that it omits one or more features and specializes in the implementation of its features to maximize performance. Although heavyweight monolithic and extensible DBMS might be able to emulate LWDB capabilities, they cannot match LWDB performance.

SQLite is a software library that implements a SQL engine. It has been used with great success as on-disk file format: allows the developer to handle data in a simple way, but also have the use of database features (such as undo, redo, etc.). In embedded device environment, in which there is low-concurrency and there are little or medium size datasets, SQLite is the right choice. If we want to save the data in a common place, i.e., Remote Server until now there is no easy mechanism to implement this.

The need for storing information in remote server exists to have centralized access to data by the users. The idea of storing information in remote server is implemented using Web Services (plugin) which can save the data in the Remote database like SQL Server and retrieve as and when required. When a project is developed, a group of developers/testers are involved. They will need concurrent information for development which can be done using a centralized database. For example feedback is collected from different customers for a product and it is more feasible to store it in a centralized repository that can be used by the entire for improvements and further development. So we require a remote access to SQLite [2]

to be used by all of them.The relevant changes need to be reflected and others discarded. SQLite has write lock issues which have to resolve by creation of different instances of the database. Testers can access and debug the problems directly and provide the information without having to install the entire system or database files.

1.1 High availability

Virtualization, a technique to run several operating systems simultaneously on one physical server, has become a core concept in modern data centers, mainly driven by benefit of application isolation, resource sharing, fault tolerance, portability and cost efficiency. A special middleware, hypervisor, abstracts from physical hardware resources and provides so called virtual machines acting like real computers with their own (virtual) hardware resources. High availability system [3] design approach and associated service implementation that ensures a prearranged level of operational performance will be met during a contractual measurement period. Enabling high availability we can detect any point of failure to propagate reliable crossover, if needed. High availability is a characteristic of a system. The definition of availability is Ao = up time / total time. If (total time - down time) is substituted for up time then you have Ao = (total time - down time) / total time. Determining tolerable down time is practical. From that, the required availability may be easily calculated. Here a small network has made with a master, slave (replica of master) backing up data, controller and a user virtual machine. Controller will be constantly checking the master for downtime and doing crossover to slave in case tolerable down time is exceeded. For this purpose we will use open source tools like heartbeat, pacemaker and DRBD.

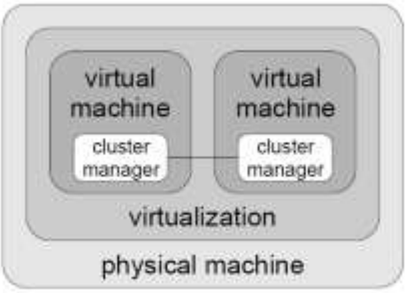


Fig. 1 Virtualization

2. SOLUTION FOR SQLITE

Plugin as an interface has been used for remote accessing of SQLite. A connection to the remote system is made through ssh. As soon as the remote system is accessed the database is copied to the local system and launched through SQLite manager. Now the remote database will be in synch throughout. In case of read operation the local system will not be updated (by copying remote database) as no updations have been made. In case of modification/updation of Database, an instance for it is created corresponding to the developer/ tester which will be used for further development by this particular tester/developer. The local database will be copied again to the remote system. The final product is developed at the remote system by using data from these instances.

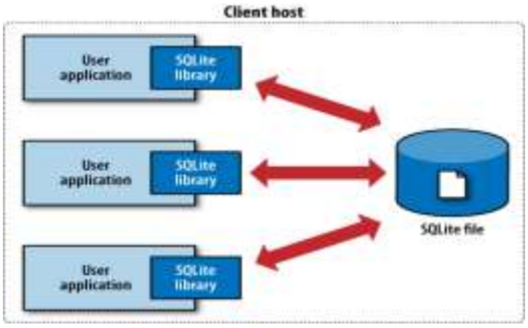


Fig. 2 SQLITE Architecture

3. SOLUTION FOR HIGH AVALABILITY

A controller which sends heartbeat or pace-maker (OS tool) to master, slave and checks the response time.
Availability is calculated by Ao = (total time - down time) / total time. Determining tolerable down time is practical. Using this threshold value is determined. If response time exceeds threshold value, controller shifts from master to slave. All further queries are directed to slave by the controller.
In case master is updated then the last copied time is checked for the slave and synched with the master. For this purpose an open source tool (like DRBD is used). Heartbeat is a daemon that provides services of clustering; this allows the exchange of messages between the machines running Heartbeat and check the health of them. Heartbeat is used for checking if all the nodes are running is recommended to use a dedicated interface for it. Pacemaker is a resource manager that provides a full management of the resources provided by the cluster.

4. GLUSTERFS

GlusterFS [5] is an open source, distributed file system capable of scaling to several petabytes and handling thousands of clients. GlusterFS clusters together storage building blocks over Infiniband RDMA or TCP/IP interconnect, aggregating disk and memory resources and managing data in a single global namespace. GlusterFS [6] is based on a stackable user space design and can deliver exceptional performance for diverse workloads.

Attributes of GlusterFS include:
Scalability and Performance
High Availability
Global Namespace
Elastic Hash Algorithm
Elastic Volume Manager
Standards-based

By considering the advantage of two different features to provide a highly available, scalable NFS and CIFS service. First, the use DNS round robin to have each client use one of the Gluster servers[6] for their mounts. Then, CTDB will provide virtual IPs and failover mechanisms to ensure that, in the case of a server failure, failover is transparent to clients. Define DNS entries for two load balanced services, called glusternfs and glustercifs. Virtual IPs combined with CTDB IP failover; it allows having both load balancing and high availability.

Set a low TTL for the records so, if a virtual IP is down while a client is trying to mount, the client can retry using a different one. To configure CTBD start with a single volume called vol1, configured as distributed + replicated (2 replicas), and export it using NFS and CIFS.

5. DRBD AND DRB DLINKS

5.1 DRBD

One mechanism for sharing data between two machines is to use an external RAID array. The primary drawback to this is cost, with typical array configurations costing no less than $2,000. DRBD is a"Distributed Replicated Block Device"
that allows similar results to be achieved on local discs using a network connection for replication. DRBD can be thought of as a RAID-1 (mirrored drives) system that mirrors a local hard drive with a drive on another computer. DRBD includes mechanisms for tracking which system has the most recent data, "change logs" to allow a fast partial re-sync, and startup scripts that reduce the likelihood that a system will come up in
"split brain" operation.

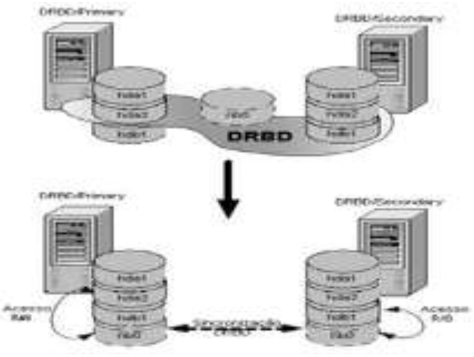


Fig. 3 Overview of DRBD concept

A dedicated network using a direct cross-over network connection is set up between the machines.

5.2 DRBDLINKS

In a typical system running DRBD[8], there will be many directories and files that reside on the shared data partition. A way to handle the data in the HA Cluster is- Link the normal system files and directories into the shared partition. This means that configuration file and data reside in their familiar locations on the primary system. However, links must be set up when the service starts on the primary and returned to normal when the service is not operating. These links can be maintained in the heartbeat startup and shutdown scripts using the standard ln, mv, and rm commands. The DRBD shared partition will be mounted on”/shared”. DRBDLINK Configuration install the”drbdlinks” package Configure the ”/etc/drbdlinks.conf” file setup the directories mentioned in /etc/drbdlinks.conf file in the shared partition restart the DRBD close the database to ensure a good copy of the data is made configure heartbeat resource to start and stop DRB- DLinks by modifying the ”/etc/ha.d/haresources” file DRBDLinks moves the system ”httpd” file to the httpd.drbdlinks” and makes a link to the version in ”/shared.

6. CONCLUSION

Environment, in which there is low- concurrency and there are little or medium size datasets, SQLite is the right choice[1]. The drawback of SQLite can be removed by the proposed solution by creating instances and then integrating the modules. HA is implemented with the help of open source tools such as heartbeat, DRDB, GlusterFS, corosync which helps in achieving availability at all times overcoming any failure at the server end.

7. REFERENCES

[1] D. C. Igweze and E. O. Nwachukwu, Lightweight Database System (Lwdbs): An Overview

[2] Kiran Dhokale, Namdeo Bange,Shelake Pradeep, Sachin Malave,Implementation Of Sql Server Based On Sqlite Engine On Android Platform

[3] High availability clustering of virtual machines- possibilities and pitfalls may 2006 Wiesbaden/germany version 1.01

[4] The Expedient Approach for High Availability in Web Server Services for HPC Attained by Clustering using Virtualization International Journal of Computer Applications, Volume 95 No.20, June 2014

[5] GlusterFS: http://www.gluster.org/documentation/ Architecture/internals/Dougw:ANewbie0 sGuidetoGlusterInternals=; V olume95No:20; June2014

[6] http://blog.gluster.org/about/

[7] http://www.linuxlinks.com/article/20130411160756441/GlusterFS.html

[8] https://www.smartseohosting.com/GlusterFS

The Main Factors Influencing Information Security Behavior

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: This paper attempts to investigate the impacts of main factors influencing information security behavior in improving awareness and performance of ICT departments' staff. According to the extant research, there are four groups of factors influencing information security behavior namely self-efficacy, intention to IT security practice, security practice-care behavior, and security practice-technology. The results of analyzing 220 gathered data from five Iranian universities showed that all factors have significant and positive impact on information security behavior, and the highest impact refers to security practice-care behavior.

Keywords: Self-efficacy, Intention to IT Security Practice, Security Practice

1. INTRODUCTION

Because of managed information system security (IS), emphasize on security of IS studies go further than technical consideration and it has close relationship to organizational and individual perspective to reach key goals in system. Regarding organizational level, there is no gradual growth of the breaches for the information security and also included risks to take place which threat individuals in organizations. Moreover, achieving a better knowledge of information system security within ethical field is according to mentioning it at combination stage of organization and technology. According to (Segev et al., 1998), in order to reach security utilizing technology is not enough but rather the organization itself does matter. Besides, it should be mentioned that IS security at both organizational and technical level (Trom Peter and Eloff, 2001) as well as its implementation has to have cognizance of both human and ethical considerations.

Also the cornerstone of information system security goals which are the foundation of secure system functions in past and critical reasons of methodology developments, were integrity, confidentiality and also data availability that needs to be followed by measures of value in order to avoid any inability issues in managing the IS security. Therefore, in current project, the method of combining different organizational and social variables to make sure IS security has been considered.

The IS security will still present a problem for professionals and also executives. Most of the studies on IS security are in nature technical and have limited emphasize on organizational and individual issues. Today, unfortunately, many firms do not have enough consideration on individual value and so they just emphasize on technical facets. Because of technical failures and human errors, organizations need to be aware about necessity of educating responsible employees in order to reinforce IS security. In this article, ICT departments of many universities in Iran have been chosen as study scope. It means that this study attempts to understand the key influential elements impacting behavior of IS security in universities of Iran.

2. LITERATURE REVIEW

According to Martins and Eloff (2003), guidelines and instructions of awareness are important aspects of maintaining stability. Also each client should be trained through stability awareness with their influential role in protecting possessed details (Lee and Larsen, 2009). It utilizes an ongoing protection awareness program for training as a probable compound in defense system of enterprise property. The specific intention of this program is enhancing the attention of users about risks and also the importance of resource security methods, particular safety of tools as well as related consequences of illegal measurements.

In addition Lee and Larsen (2009) stated that firms have to emphasize on protection awareness and provide their plans as clear as possible for making sure that there is no security problem within organizations (Woon and Kankanhalli, 2007). It will suggest a chaos of customers in protection issues that casually will take the potential risks through specific natural activities. In addition Woon and Kankanhalli, (2007) asserted that a successful firm would be safe if it provides awareness programs in certain considerations. Thus, IS can be very helpful if individuals know how to use them.

The Protection Motivation Theory (PMT) that was presented by Rogers in 1983 elaborated the model of health-related belief within health and social psychology area. Based on theories of expectancy-value and also theories of cognitive processing, PMT has been developed in order to contribute to demonstrate fear appeals. PMT was assumed as one of the best and influential explanatory theories in order to predict the attention of an individual to participate in protective acts (Anderson and Agarwal, 2010). In fact, protection motivation originates from both coping and threat appraisals. The threat appraisal defines the assessment of a person of the danger level imposed by a threatening phenomenon (Woon et al. 2005). It includes the below two items:

(i) Perceived vulnerability is a personal assessment about possibility of threatening phenomenon. In this paper, threats are initiating from non-compliance with ISSP.

(ii) Perceived severity means those severities which are the results of event. Here, imminent threats toward security of information in an organization come from non-compliance with ISSP. The aspect of coping appraisal of the PMT means the individual's evaluation of their capability to deal with and also avert the potential damage and loss originating from a threat (Woon et al., 2005). Such coping appraisals have three main sub-constituents:

(i)

Self-efficacy: this variable focuses on a person's judgment or capability about their abilities to deal with or perform the suggested behavior. In this paper, it means those types of measures and skills which are necessary for protecting the information in an IS context within an organization (Bandura, 1991; Woon et al., 2005 and Pahnila et al., 2007).

(ii)

Response efficacy: it is about those beliefs on perceived advantages of the taken action by people (Rogers, 1983). In this study it means having compliance with ISSP as an effective approach to detect any threat to organizational IS properties.

(iii)

Response cost: this element refers to the perceived opportunity costs of monetary, effort ad time in order to perform the suggested behavior, in this case means complying with ISSP.

Moreover, it was demonstrated that people's behavior in fact is impacted or influenced by what they see as typical within an environment (Chan et al., 2005; Knapp and Marshall, 2006; Johnson and Warkentin, 2010).

Moreover self-efficacy reveals the knowledge and characteristics of an individual to manage any task or maybe contribute to make many alternatives (Bandura, 1991). This concept has been demonstrated to have a remarkable impact on capabilities of a good individual to conduct a task behavior that includes usage too (Compeau and Higgins, 1995; Workman et al., 2008).

Many investigations have coped with remarkable dysfunction since self-efficacy pertinence does not have compliance with conformity behavior intention of ISSP (Bulgurcu et al. 2010; Pahnila et al., 2007; Herath and Rao, 2009a; Larose et al., 2008; Workman et al., 2008).

Previous scholars that employed PMT realized that it is helpful in forecasting the related behaviors to people's computer security behaviors in both organizations and at home (Lee and Larsen, 2009 and Anderson and Agarwal, 2010) and also compliance of ISSP (Herath and Rao, 2009; Pahnila et al., 2007).

Various researchers (e.g. Karamizadeh et al., 2013; Rhee et al., 2009; Richardson, 2007; Proctor et al., 2006; Lee and Kozar, 2005) have highlighted different factors which have high potential to affect information security behavior. These factors are self-efficacy, intention to IT practice, security practices (care behavior), and security practices (technology). It suffices that this study also applies these factors for its scope. The proposed framework of this study is demonstrated figure 1.

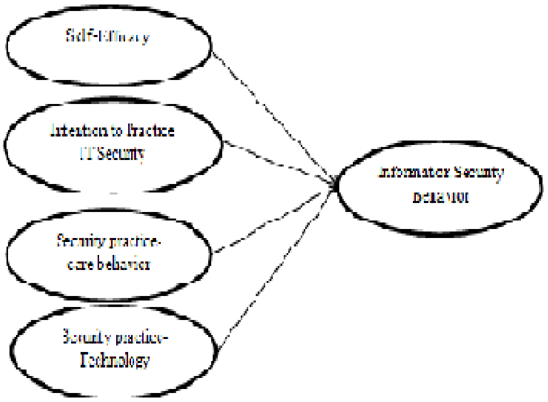

Self-Efficacy
Intention to Practice IT Security
Security practice-care behavior
Security practice-Technology
Information Security Behavior

Figure1: Proposed Framework

3. METHOD AND RESULTS

This study applied quantitative approach to measure the impact of highlighted factors on information security behavior. In this regard, four hypotheses were developed as followings.

H1: Self-efficacy has a significant and positive impact on information security behavior

H2: Intention to practice has a significant and positive impact on information security behavior

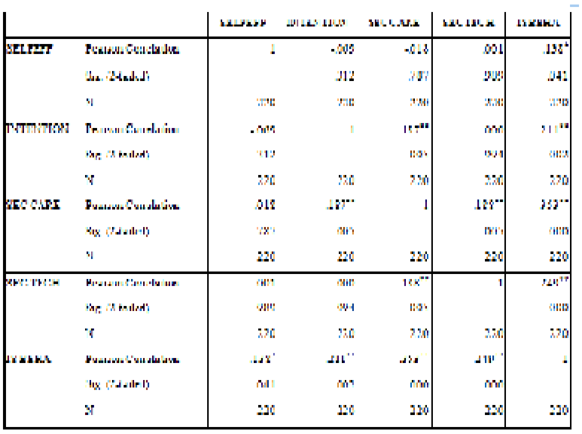
H3: Security practice-care behavior has a significant and positive impact on information security behavior

H4: Security practice-technology has a significant and positive impact on information security behavior

To measure the underlying factors of this study, the questionnaire of the Karamizadeh et al. (2013) were applied. According to their research, self-efficacy consists of two dimensions namely IT knowledge and computing behavior. Intention to practice IT security is measured by IT literacy and security measures. Security practice-care behavior refers to online file-sharing and data protection, while security practice-technology refers to antivirus and spam filtering.

The population of this study was all members of staff (managers, engineers and technicians) who work in ICT departments of 5 large universities located in Tehran. The sample size was 220. The results of reliability test shows that all variables have good or excellent internal consistency. To test above hypotheses, first Pearson correlation test was applied. The results showed that each independent variable has significant relationship with information security behavior. The highest relationship refers to security practice-care behavior, while the lowest relationship refers to the self-efficacy to practice.

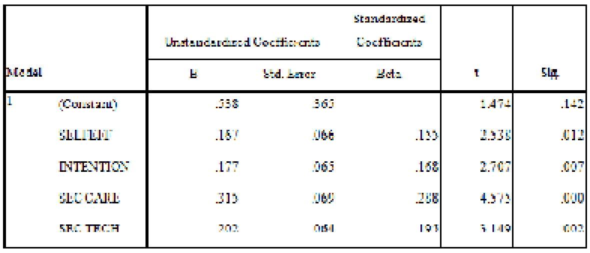
Table1: Correlations



		SELFEFF	INTENTION	SEC CARE	SEC TECH	ISBEHA
SELFEFF	Pearson Correlation	1	-.005	-.018	.001	.138*
	Sig. (2-tailed)		.912	.787	.989	.041
	N	220	220	220	220	220
INTENTION	Pearson Correlation	-.005	1	.187**	.000	.211**
	Sig. (2-tailed)	.912		.005	.994	.002
	N	220	220	220	220	220
SEC CARE	Pearson Correlation	.018	.187**	1	.189**	.353**
	Sig. (2-tailed)	.787	.005		.005	.000
	N	220	220	220	220	220
SEC TECH	Pearson Correlation	.001	.000	.189**	1	.240**
	Sig. (2-tailed)	.989	.994	.005		.000
	N	220	220	220	220	220
ISBEHA	Pearson Correlation	.138*	.211**	.353**	.240**	1
	Sig. (2-tailed)	.041	.002	.000	.000	
	N	220	220	220	220	220

The result of regression analysis shows that 72.3 percent of variation of information security behavior can be accounted by the four existing independent variables because R square is equal to .723.

Table2: Coefficients from Regression Analysis



Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.538	.365		1.474	.142
	SELFEFF	.167	.066	.155	2.538	.012
	INTENTION	.177	.065	.168	2.707	.007
	SEC CARE	.315	.069	.288	4.573	.000
	SEC TECH	.202	.064	.193	3.149	.002

a. Dependent Variable: ISBEHA

As shown in table 2, all of the independent variables have significant impact on information security behavior since all estimated coefficients are less than .05. Hence all of the hypotheses of this study are supported by obtained results. As summary, the outcome of regression analysis can be written as following equation:

IS Behavior =.538+.167 (Self-Eff) + .177 (Intention)+ .315 (Sec-care)+ .202 (Sec-Tech)

4. CONCLUSION AND DISCUSSION

The obtained results demonstrated that all of the highlighted factors have significant influence on information security behavior. On the other hand, ICT departments in Iranian universities can improve these factors in order to reinforce their information security behavior. Since most of the impact is on security practice-care behavior so considering the online file sharing and also data protection are very important. The future studies can test the framework of this research in other scopes. Moreover, the amount of R-Square in this study is not high thus it is possible that other factors also could be added to this framework. Besides, future researches can focus on some factors such as human resource practices and transformational leadership. Using such factors will make a bridge between human resource management and information security.

5. REFERENCES

[1] Anderson, C. L., Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*. 34(3), 613-643.

[2] Bandura, A. (1997). toward a unifying theory of behavioral change. *Psychological review*. 84(2), 191.

[3] Bandura, A(1991). Social cognitive theory of self-regulation. *Organizational Behaviour and Human Decision Processes*. 96(3), 160.

[4] Chan, M. Woon., and Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security*. 1(3), 18-41.

[5] Compeau, D. R., and Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. MIS Quarterly.

[6] Hsu, M. H., and Chiu, C. M. (2004). Predicting electronic service continuance with a decomposed theory of planned behaviour. *Behaviour and Information Technology*. 23(5), 359-373.

[7] Herath, T., and Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*. 18(2), 106-125.

[8] Herath, T., and Rao, HR. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*. 47(2), 154-165.

[9] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 34(3), 549-566.

[10] Knapp, K. J., and Marshall, T. E. (2006).Information security: management's effect on culture and policy. *Information Management and Computer Security*. 14(1), 24-36.

[11] Kankanhalli, A., Tan, B. C. Y., and Wei, K. K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *Mis Quarterly*, 113-143.

[12] Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model For Cloud.International Journal Of Computers & Technology, 10(1), 1186-1191.

[13] Larose, R., and Rifon ,N. J. Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*. 51(3), 71-76.

[14] Lee, Y., and Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. Communications of the ACM.

[15] Lee, Y., and Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems.

[16] Martins, A., and Eloff, J. (2003). Information Security Culture, Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt. IFIP Conference Proceedings.

[17] Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

[18] Pahnila, S., Siponen, M., and Mahomood, A. (2007). Employees' behaviour towards IS security policy compliance. In: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3e6, Los Alamitos, CA.

[19] Proctor, R.W and Proctor, J.D. (2006). Handbook of Human Factors and Ergonomics 3rd ed., John Wiley and Sons, New York

[20] Richardson, R. (2007). CSI Computer Crime and Security Survey. Computer Security Institute. From: retrieved November 16, 2007.

[21] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology*, 153-176.
[22] Segev, A., Porra, J., & Roldan, M. (1998). Internet security and the case of Bank of America. Communications of the ACM, 41(10), 81-87.

[23] Trompeter, C. M., & Eloff, J. H. P. (2001). A framework for the implementation of socio-ethical controls in information security. Computers & Security, 20(5), 384-391.

[24] Torkzadeh, G., and VanDyke, T. P. (2001). *Development and validation of an internet self-efficacy scale Behaviour and Information Technology.*

[25] Woon, I., Tan, G., and Low, T. (2005). A protection motivation theory approaches to home wireless security. In: Avison D, Galletta D, DeGross JI, editors. Proceedings of the 26th International Conference on Information Systems, In Las Vegas, December P.

[26] Woon, I., and Kankanhalli, A. (2007). Investigation of IS professionals' intention to practise secure development of applications. International Journal of Human-Computer Studies.

[27] Workman, M., Bommer, H. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior.* 24(6), 2799-2816.

Information System Security Model for ICT Departments

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: Due to human theft, fraud and error is declining as well as the reduction in computer properties misuse, most of the ICT departments all, should focus on human elements in their models of information system (IS) security. This issue has not been considered in previous studies efficiently. This paper, uses qualitative approach in order to improve IS security models. Usually, in most of the developed models so far, only technical factors are considered. In this regard, an interview was conducted with 6 experts in ICT departments of 6 universities in Iran. After exact review of their ideas and insights, human factors have been identified. All of the achieved results have been added to existed technical models and then the finalized model has been designed, which was verified by experts too later. The identified human factors include staffing, training, reward and compensation system and also performance appraisal.

Keywords: Information System Security, Technical factors, Human Factors

1. INTRODUCTION

Considering so types of threats for example errors, human theft, employee error or technical failure, all are the most critical threats toward IS according to (Whiteman and Mattord, 2005). Thus, training the employees regarding information security appears to be important. Those individuals who are utilizing security monitors should be educated too and should be aware about necessity of security within a certain context since appropriate use of security monitors could be accomplished while the members are aware about security importance (Pfleeger and Pfleeger, 2003). This research, remarkably emphasizes on human and organizational factors within IS system and also computer. There would be a significant impact on information system security if both human and organizational factors influence their employment and usage with not considering the power of technical controls (Bishop, 2002).

Here, the supposed IS juncture and vulnerabilities of computer could be accomplished through a vulnerable computer and information security protection, for example, poor stability or password so as a result many harmful intentions could occur. The results of personal practices and also policies in an organization which are originated in early presumptions of design and also managerial choices would result in many susceptibilities (Besnard and Arief, 2004).

In most of the common models in IT security, the main focus is on technical elements. However, human error also should be considered. This topic has been emphasized in recent studies. However, it is important to develop a model which includes both technical and human factors. Hence, this research attempts to identify which human factors could modify the current IS security models.

2. LITERATURE REVIEW

The data availability, confidentiality and integrity are existed in IS system (Pfleeger, 2003; Bishop, 2003); the three main elements which can ensure the data security. When all of the systems constituent can be accessed only by authorized parties, so there exists confidentiality. To be aware about availability of system constituents, viewing and also printing are existed in access concept (Pfleeger, 2003; Bishop, 2003). To make sure that system's constituents can be modified by just authorized groups or manner is known as integrity. Modifications in fact are altering, forming, writing and erasing the altering position (Pfleeger and Pfleeger, 2003). Those available system constituents for the authorized people during specific times are known as availability. Moreover, denial of services will be against the availability through which accessing into defined sets of objects cannot be accepted in a certain time (Pfleeger and Pfleeger, 2003).

In general, in a framework, the first level of establishing a secured system would be identification of possible dangers. Interception, interruption, fabrication and also modification could be considered as some system dangers. These four mentioned classifications include all types of system dangers which can occur (Pfleeger, 2003). In addition, accessible information to source from the outside without any appropriate authority is known as interception. An outer source, in fact, may or may not be positioned and can be an individual, program or system (Pfleeger and Pfleeger, 2003).

Those wiretappings which are respectively successful or not successful could be the appropriate examples for both traced and non traced interceptions. When the system constituent is lost, the inaccessible and not applicable will be known as interruption (Pfleeger and Pfleeger, 2003). A good example in this regard is when the cables are connected with critical system are purposely damaged, so as a result system's connectivity would be distributed and so internal sources could not be accessible. Alteration is not only about the fact that an unauthorized person accesses a system, but instead it will modify it in such a way that is different from interception. In line with technical changes, such modifications may or may not be identified (Pfleeger and Pfleeger, 2003). The computer virus which modifies the keyboard's output is one of the good examples of what a recognizable modification is like, thus, the user will automatically becomes aware of any alterations within the system.

On the other side, users might not identify any kind of alterations in output of systems or experience if the same system is being attacked by root kit, although there are alterations of system kernel. Besides, the inclusion of counterfeit objects from an illegitimate individual is called as fabrication (Pfleeger and Pfleeger, 2003). It might not be complicated to identify due to they are the added factors, but also it is dependent on the capability of attackers too. For instance, a malevolent user, for each single transaction can credit to his account, a very small and might be not a traceable amount by an enclosed module at server of database in a bank.

2.1. Security Threats in Information System

The threat concept is considered as all of the unexpected or potential causes of a not favorable incident that has negative impact on a system or an organization. In general, there are three main categories of threat resources:

- Natural Threats: Those events that are forces of nature such as floods, earthquakes, tornados, landslides as well as electrical storms.
- Human Threats: Those events that are both enabled or caused by humans including the intentional actions which encompass some deliberate actions and inadvertent information entry for example network based attacks, harmful software and also unauthorized access to confidential data.
- Environmental Threats: It includes those incidents or conditions such as pollution, chemical spills and also liquid leakage.

A suitable developed classification of threats would be required for explaining challenges in information security context. So far, there have been many efforts to categorize threats information system. They could be arranged according to actions or consequences. Actions might be as following types: observe, destroy, modify and emulate the threats. In addition, consequences consist of disclosure, execution, misrepresentation and repudiation of threats and also integrity threats. Moreover, the security threats can be grouped according to their involved asset types.

The other subject is about penetration techniques. Such penetration techniques could be procedural, hardware, software, physical or personal related. Other studies also defined 12 different classifications for threats such as human error acts or failure, deliberate software attacks, hardware failures and technical errors, technology obsolescence and finally natural forces.

In addition, information system threats could be assumed from two separated perspectives. The first viewpoint is according to threat agents. Such agents are authorized or classified, unauthorized groups and also environmental elements.

. 2.2. Human Errors

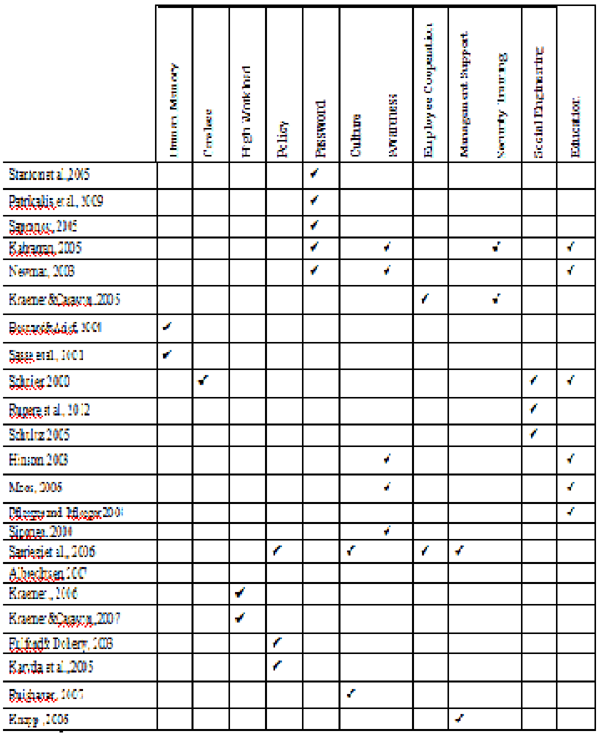
Because of human errors occurring by computer users, the breaches of information security might take place in many different ways. Without having any effective computer knowledge, technical errors and also careless users of computer will make many failures. Moreover, the expanding population can use computer in internet age. But also many people just describe basic facets of computer usage such as web browsing, forward email and word processing.

The significant dimensions of security measures such as firewalls, antivirus, software and patches and in addition general updates are not emphasized by most of the users (Roberts, 2004). This type of users, later easily become the main target of hackers and harmful software. Their errors might lead to compromised computers and utilized as a pad for developing major attacks of unsecured systems.

One of the important and harmful causes resulting from human failure on information security context is possibly not being careful enough. A lot of security breaches such as those users who put password on notes next to keyboards, entering into harmful websites or not assuming the demonstrated warnings by browser, as well as those workers are not able to abide security procedures and policies that could be linked to their carelessness.

In addition, more lethal dangers for firms are not emphasized and educated by the insiders. There are many dissatisfied and malevolent workers and staffs who are the victims of such attacks from social engineering. A lot of businesses could be lost because of breaches in security and many of them are linked to human errors. Moreover, many organizations may deal with more security risks initiating from not considering physical and investing on software security devices. In order to reduce human failure risks in an organization, there could be a balance among procedures, policies, technology and training (See Table 1).

Table1: Human errors by different scholars



	Human Memory	Careless	High Workload	Policy	Password	Culture	Awareness	Employee Competition	Management Support	Security Training	Social Engineering	Education
Stanton et al.,2005					✓							
Patrikalis et al., 2009					✓							
Sasse et al., 2005					✓							
Kahraman, 2005					✓		✓			✓		✓
Newman, 2008					✓		✓					✓
Kraemer &Carayon,2005								✓		✓		
Besnard&Arief, 2004	✓											
Sasse et al., 2001	✓											
Schrier 2000		✓									✓	✓
Rogers et al., 2012											✓	
Schultz 2005											✓	
Hinson 2008							✓					✓
Mcoa, 2006							✓					✓
Dhillon and Moores 2006												✓
Siponen, 2000							✓					
Samejeh et al., 2006				✓		✓		✓	✓			
Albrechtsen 2007												
Kraemer., 2006			✓									
Kraemer &Carayon,2007			✓									
Fulford& Doherty, 2003				✓								
Karyda et al.,2005				✓								
Ruighaver, 2007						✓						
Knapp ,2006									✓			

Source: Asadi (2014)

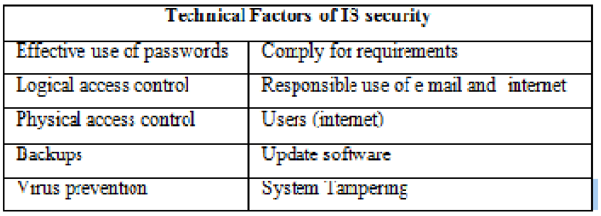
According to mentioned points above, it can be concluded that human error is a very critical factor. In following section, we will discuss on how to highlight appropriate human factors.

3. METHOD AND RESULTS

This paper applied qualitative approach to highlight the main human factors which have potential to improve information system security model. For this purpose, 6 experts were selected from ICT departments of 6 Iranian universities. They were chosen because they have enough knowledge and experience in term of information system security.

The interview process will be conducted with face to face method and open question. The questions are mainly emphasized on available technical factors and also human factors. After the interview process, all of the answers have been exactly reviewed and examined. The highlighted technical factors and human factors together with proposed model, again, have been presented to them and it was accepted by all of them. The technical factors are listed in Table 2.

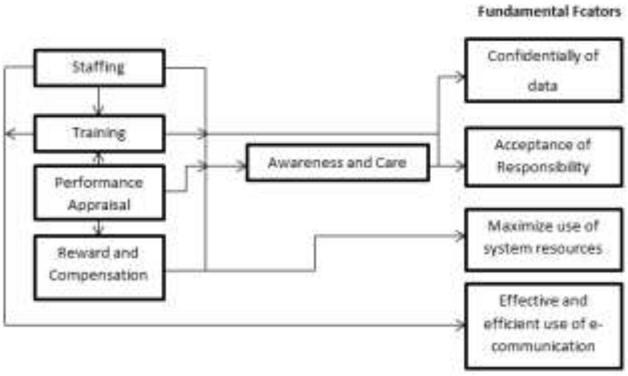
Table 2: Technical factors of IS security model



Technical Factors of IS security	
Effective use of passwords	Comply for requirements
Logical access control	Responsible use of e mail and internet
Physical access control	Users (internet)
Backups	Update software
Virus prevention	System Tampering

Since size of this model is large, this paper will not demonstrate the technical factors and their relationship with each other in this developed model. Finally, the proposed model of this research will be as follows:

Figure2: Proposed model based on the human factors



Also other factors such as availability and integrity of data have been identified (as the fundamental factors). Because of the fact that these factors cannot be impacted by human factors, they are not included in this model.

4. CONCLUSION

The achieved results from this study demonstrated that in ICT departments of 6 located universities in Iran, human error can be declined through some of the human resource practices such as training, staffing, and reward system and performance appraisal. These practices, first impact information system security and care and finally will result in maximizing the fundamental factors (data confidentiality, responsibility acceptance, using the system resources and efficient and effective e-communication usage).

Moreover, integrity of data and availability of data are among those fundamental factors which are only being impacted by technical factors. In Table 2, all of the technical factors are listed. Future studies can compare the impacts of human factors and technical factors with each other. Moreover, the proposed model of current study can be adapted in healthcare industry as well.

5. REFERENCES

[1] Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.

[2] Besnard, D., &Arief, B. (2004).Computer security impaired by legitimate users. *Computers & Security*, *23*(3), 253-264.

[3] Bishop, M. A. (2002). The art and science of computer security.

[4] Fulford, H., & Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation.*Information Management & Computer Security*, *11*(3), 106-114.

[5] Hinson, G. (2003). Human factors in information security. *IsecT Ltd*.

[6] Kahraman, E. (2005). Evaluating IT security performance with quantifiable metrics. *Master's thesis, DSV SU/KTH*.

[7] Karyda, M., Kiountouzis, E., &Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246-260.

[8] Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24-36

[9] Kraemer, J. A., &Zawadowskiy, A. (2006). *U.S. Patent Application 11/499,460*.

[10] Kraemer, S., &Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), 143-154.

[11] Kraemer, S., &Carayon, P. (2005, September). Computer and information security culture: findings from two studies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, No. 16, pp. 1483-1488).SAGE Publications.

[12] Moos, T. T. (2006). Cisco-sponsored security survey of remote workers reveals the need for more user awareness.

[13] Newman, E. (2003). Refugees, international security and human vulnerability: Introduction and Survey. *Refugees and Forced Displacement*, 3-30.

[14] Patrikakis, C. Z., Kyriazanos, D. M., Voulodimos, A. S., & Nikolakopoulos, I. G. (2009).Trust and security in Personal
[15] Network environments. *International Journal of Electronic Security and Digital Forensics*, *2*(4), 365-376.

[16] Pfleeger, C., &Pfleeger, S. L. (2003).Security in Computing 3rd.

[17] Roberts, A. S. (2004). National security and open government. *Georgetown Public Policy Review*, *9*, 69-85.

[18] Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, *26*(1), 56-62.

[19] Rupere, T., Mary, M., &Zanamwe, N. (2012).Towards Minimizing Human Factors In End-User Information Security. *International Journal of Computer Science and Network Security*, *12*(12), 159-167.

[20] Stanton, J. M., Stam, K. R., Mastrangelo, P., &Jolton, J. (2005).Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

[21] Sarriegi, J. M., Santos, J., Torres, J. M., Imizcoz, D., &Plandolit, A. (2006). Modeling security management of information systems: analysis of a ongoing practical case. In *The 24th international conference of the system dynamics society. Nijmegen, The Netherlands*.

[22] Sasse, M. A., Brostoff, S., &Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security.*BT technology journal*, *19*(3), 122-131.

[23] Sapronov, K. (2005). The human factor and information security.

[24] Schneier, B. (2000). Software complexity and security.

[25] Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*(6), 425-426.

[26] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

[27] Whitman ME, Mattord HJ., (2005) Principles of information security.2nd ed. Thomson.

Mediating role of Information System Security Awareness in the relationship between Self-Efficacy, Security Practice and Information System Security Behavior

Hanieh Yaghoobi Bojmaeh
London Metropolitan University
London,United Kingdom

Abstract: Through reviewing the previous conducted studies, we can find enough evidence in order to support the relationship between self-efficacy and security practice with information system security behavior. The main issue which is discussed in this research is the key role of information system security awareness. According to the data analysis results on 230 collected data from 10 universities in Iran, located in Tehran, it was revealed that the relationship between mentioned factors with information system security can be mediated by information system security awareness

Keywords: Self-Efficacy, Security Practice, Information System Security Behavior, Information System Security Awareness

1. INTRODUCTION

In fact, security awareness is the attitude and knowledge of organizational members toward the protection of informational as well as physical organizational assets. Many firms need to have some formal security awareness education programs for all of their staffs while they are being employed in organization and thereafter periodically, mainly annually.

Still, information system security is a challenging issue for executives and professionals. A lot of investigations on this topic are technical in nature and so would not focus on individual and organizational issues. Currently, unfortunately, a lot of companies do not have sufficient emphasize on individual values, thus, they just focus on technical aspects. Due to human errors and technical errors, firms should be aware about importance of training responsible workers for reinforcing the IS security. In this paper, ICT departments of many Iranian universities have been selected as scope of study. It demonstrates that this research puts effort to recognize the main influential factors which impact IS security behavior within the Iranian universities.

However, this research believes that some factors such as self-efficacy and security practices (technology and care behavior), at first will increase IS security and then impact the IS security behavior. The influence of self-efficacy and also security practices on awareness and behavior in ICT universities of Iran is an important subject which should be studied exactly. Therefore, this study aims to find how IS security awareness affects the relationship between self-efficacy, security practices and IS security behavior.

2. LITERATURE REVIEW

The information security management in an organization includes a set of actions which have both technical and organizational implications. For example, establishing an IS security management system according to ISO/IEC 270001 (ISO, 2005), standard, involves those actions that impact organizational structure, introducing processes and policies, practices and change responsibilities as well as introducing defined technical and functional specification. One of the critical practices of any type of IS security management system is awareness of information security. Joining different methods together, security awareness could be explained as a continuous attempt of raising the attention of audiences into importance of information security for stimulating the security-oriented behaviors (Peltier, 2005; European Network and Information Security Agency (ENISA, 2008).

Previous conducted studies by (CSI, 2009; Ernst and Young, 2008; BEER, 2008), demonstrate the importance of awareness actions revealing that a main part of security losses are the results of non-malicious, totally careless behaviors of the insiders as well as the fact that security has a key role in developing a strategic perspective of information security.

The survey conducted by Ernst and Young (2010), asserts that a lot of existed security awareness and training programs are not functioning well as they can be.

According to the Computer and Crime Security Survey (CSI, 2009), the longest continuous survey running in field of IS, almost 43.4% of participants noted that less than 1% of their total security budget was devoted to awareness training programs. It seems logical to assume that effective trainings on awareness usually are less costly than security technology armory which is used by most of the companies to apply defense appropriately. Also, 55% of participants mentioned that the made investment on such training programs was not efficient. Similar phenomenon occurred in 2008 CSI Computer Crime and Security Survey (CSI, 2008). There it was found that little amount of money has been pushed toward efforts of information security awareness. It is not east to explain why these amounts are lower than some discussions about necessity of security awareness training programs may offer (CSI, 2008, P.9).

2.1. Approaches to IS system Awareness

Most of the frameworks of IS awareness offer or implement some awareness approaches and methods, for example techniques for conveying security messages, computer games, artificial intelligence devices, etc., with no justification of their specific choices and also defining their theoretical foundations (Tsohou et al., 2008; Puhakainen, 2006). In addition, those research methods which are in nature theoretical and test the problems and challenges of security awareness, exclusively draw from behavioral and physical theories. However, these behavioral and psychological theories are not capable of mentioning organizational and social dimensions of security awareness appropriately, therefore, cannot offer a perspective on the direction of this process in an organizational environment and demonstrate those events which result in specific consequences.

In addition, Thomas and von Solms (1998) referred to social psychological theories and used psychological rules for developing an effective security awareness program. They defined an attitude system that based on it the attitude of a user can be impacted by behavior cognitions, behavior intentions as well as affective responses. In this regard, scholars concentrated on three approaches which can impact attitude of a person via persuasion: the first approach is changing their behavior directly; second is employing a change in behavior for impacting the attitude of a person and lastly changing the attitude of a person by means of persuasion and also offer a series of psychological techniques and rules in order to change the overall attitude of a person. Siponen (2000) suggested a conceptual foundation regarding security awareness based on theories of planned behavior, reasoned action, technology acceptance model and intrinsic motivation.

According to mentioned points above, Siponen (2000), presents practical principles and approach with respect to motivation: emotions, logic, ethics and morals, rationality, feeling of security and well being.

Also, Qing et al., (2007) used model of elaboration likelihood as their framework for recognizing the degree of effectiveness of persuasive communications. They reviewed effectiveness of security messages and also impacts of various messages related to modifying behavior of recipients. Besides, Puhakainen 92006) investigated on behavioral changes and compliance of IS users with information system security, instructions and policies through employing instructional and attitudinal theories. D' Archy et al., (2009) tested the counter measures of security awareness from a general perspective of deterrence theory and studied how security policy awareness, security awareness, education and theory programs as well as computer monitoring are related to misuse intention of IS.

Even though research methods to security awareness are limited in social and managerial perspectives, Spears and Barki (2010), recently, in their study examined participation of users in information system security risk management and also its impact in field of regulatory compliance. Based on their research, participation of users in security risk management helps to better organizational awareness of IS security.

Many scholars (Karamizadeh et al., 2013; Rhee et al., 2009; Richardson, 2007; Proctor et al., 2006; Lee and Kozar, 2005) have demonstrated various variables that have a high potential to impact information security behavior. These variables include, self-efficacy, security practices (care behavior, technology) and also IT practice intention. It would be efficient if this study only measures self-efficacy, security practices and care behavior. Because according to technology acceptance model, intention has the capability to generate behavior. However, this study focuses on intervening role of IS system awareness. Figure 1 illustrates the proposed framework of this research.

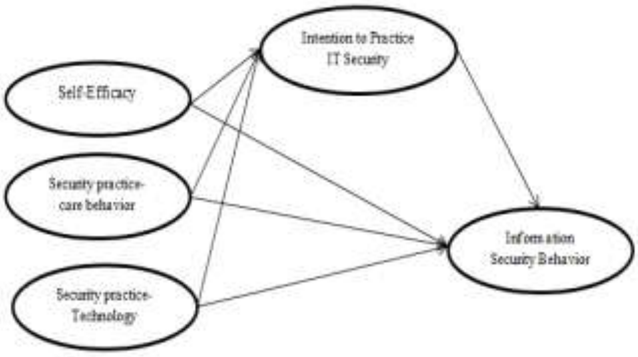


Figure 1: Proposed framework of this study

3. Methodology and Results

At the first this study developed 10 hypotheses as follow:

H1: IS security awareness is affected by self-efficacy significantly

H2: IS security awareness is affected by security practice-care behavior significantly

H3: IS security awareness is affected by security practice-technology significantly

H4: IS security behavior is affected by self-efficacy significantly

H5: IS security behavior is affected by security practice-care behavior significantly

H6: IS security behavior is affected by security practice-technology significantly

H7: IS security behavior is affected by security awareness significantly

H8: IS security awareness mediates the relationship between self-efficacy and IS security behavior

H9: IS security awareness mediates the relationship between security practice-care behaviorand IS security behavior

H10: IS security awareness mediates the relationship between security practice-care behaviorand IS security behavior

In order to evaluate all of the underlying elements of this research, the designed questionnaire by Karamizadeh et al., (2013) was utilized. Based on their study, self-efficacy includes two main aspects known as computing behavior and IT knowledge. Having intention to practice security of IT can be evaluated by security measures and IT literacy. The concept of security practice-care behavior means sharing files online and also data protection. In addition, security practice-technology means spam and antivirus filtering. Moreover, in order to measure IS security awareness; we used the conducted studies by Tshou et al., (2012).

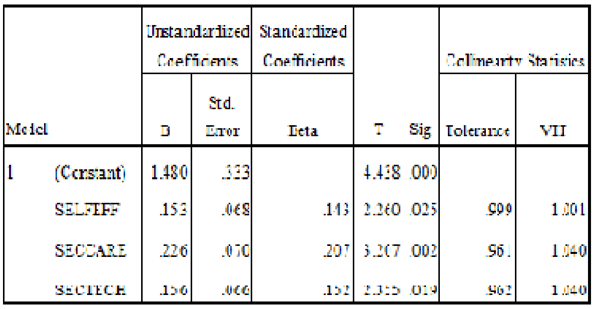
The population of this research is all of the employees (technicians, engineers and managers) who are working in ICT departments in 10 large Iranian universities. Sample size was equal to 230. Also, the reliability test results demonstrated that all of the factors have excellent or good internal consistency. To examine the formulated hypotheses, first we applied the Pearson Correlation test.

The outcome of the Pearson correlation test showed that all independent variables have significant relationship with IS security awareness and IS behavior. The highest correlation with IS security awareness refers to security practice-care behavior while the lowest refers efficacy. The results were inverse for IS security behavior. Besides, the relationship between IS security awareness and IS security behavior was significant (.723).

The result of regression analysis shows that 72.3 percent of variation of information security behavior can be accounted by the four existing independent variables because R square is equal to .723.

Table 1 demonstrates the results of first multiple regression analysis of this study:

Table1: Coefficients[a]



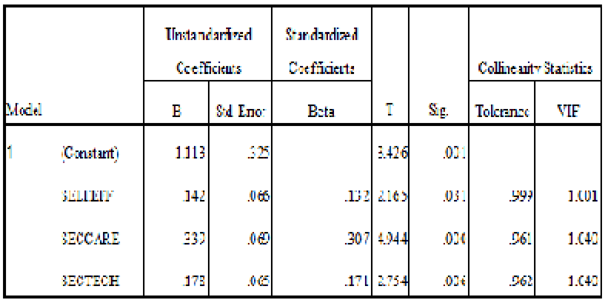
Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig	Tolerance	VIF
1	(Constant)	1.480	.333		4.438	.000		
	SELFEFF	.153	.068	.143	2.260	.025	.999	1.001
	SECCARE	.226	.070	.207	3.207	.002	.961	1.040
	SECTECH	.156	.066	.152	2.355	.019	.962	1.040

a. Dependent Variable: ISAwarness

The estimated R-square for the first regression analysis was equal to .659. In other words, 65.9% of variation of IS security awareness can be accounted by self-efficacy, security practice-care behavior, and security practice-technology. As shown in table 1, all variables (self-efficacy, security practice-care behavior, and security practice-technology) have significant impacts on IS security awareness. Henc, H1, H2, and H3 are supported by this study. The results of this regression can be written as following equation:

IS security awareness= 1.48+ .153 (Self-Eff)+ .226 (SEC-CARE)+ .156 (SEC-TECH)

Table2: Coefficients[a]



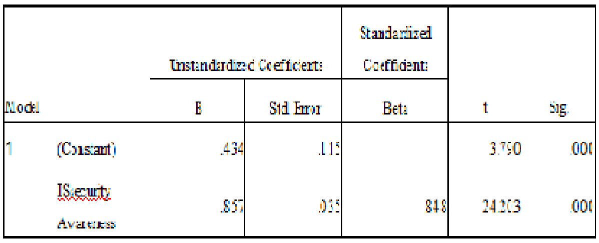
Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig.	Tolerance	VIF
1	(Constant)	1.113	.325		3.426	.001		
	SELFEFF	.142	.066	.132	2.165	.031	.999	1.001
	SECCARE	.339	.069	.307	4.944	.000	.961	1.040
	SECTECH	.178	.065	.171	2.754	.006	.962	1.040

a. Dependent Variable: ISBEHA

The estimated R-square for the second regression analysis was equal to .754. In other words, 75.4% of variation of IS security behavior can be accounted by self-efficacy, security practice-care behavior, and security practice-technology. As shown in table 2, all variables (self-efficacy, security practice-care behavior, and security practice-technology) have significant impacts on IS security behavior. Henc, H4, H5, and H6 are supported by this study. The results of this regression can be written as following equation:

IS security behavior= 1.13+ .142 (Self-Eff)+.339 (SEC-CARE)+.178 (SEC-TECH)

Table3: Coefficient



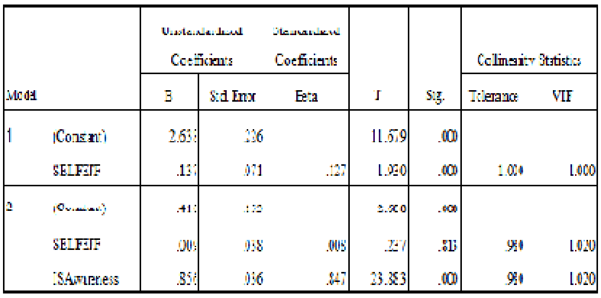
Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.434	.115		3.790	.000
	ISsecurity Awareness	.857	.035	.848	24.203	.000

a. Dependent Variable: ISBEHA

The estimated R-square for the third regression analysis was equal to .821. In other words, 82.1% of variation of IS security behavior can be accounted by IS security awareness. As shown in table 3, IS security awarenesson IS security behavior. Hence, H7 is supported by this study. The results of this regression can be written as following equation:

IS security behavior= .434+ .857(IS security behavior)

Table 4: Coefficients[a]

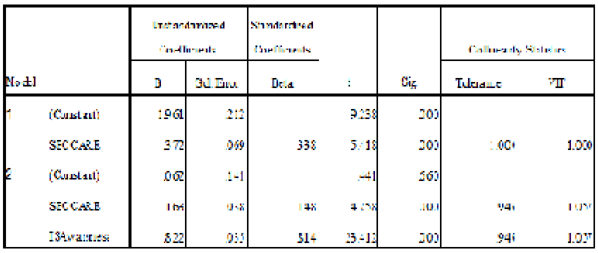


Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig.	Tolerance	VIF
1	(Constant)	2.633	.226		11.579	.000		
	SELFEFF	.137	.071	.127	1.930	.000	1.000	1.000
2	(Constant)	.413	.132		2.900	.000		
	SELFEFF	.009	.038	.008	.237	.813	.980	1.020
	ISAwareness	.856	.036	.847	23.383	.000	.980	1.020

a. Dependent Variable: ISBEHA

According to the table 4, in the first regression analysis self –efficacy has a significant impact on IS security behavior (p-value is equal to zero which is less than .05). In the second regression self- efficacy does not have significant impact on IS security behavior while the impact of IS security awareness is significant. So, IS security awareness fully mediates the relationship between self-efficacy and IS security behavior. Therefore, H8 is accepted by this study.

Table 5: Coefficients[a]

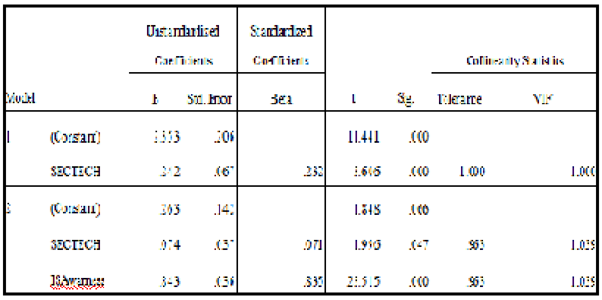


Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	1.961	.212		9.258	.000		
	SECCARE	.372	.069	.338	5.418	.000	1.000	1.000
2	(Constant)	.062	.141		.441	.660		
	SECCARE	.164	.038	.148	4.258	.000	.946	1.057
	ISAwarness	.822	.033	.814	25.412	.000	.946	1.057

a. Dependent Variable: ISBEHA

According to the table 5, in the both regression analyses security practice-care behavior have significant impacts on IS security behavior (p-value is equal to zero which is less than .05). So, IS security awareness partially mediates the relationship between security practice-care behavior and IS security behavior. Therefore, H9 is accepted by this study.

Table 6: Coefficients^a



Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	2.353	.206		11.441	.000		
	SECTECH	.242	.067	.232	3.616	.000	1.000	1.000
2	(Constant)	.263	.142		1.848	.066		
	SECTECH	.074	.037	.071	1.996	.047	.963	1.039
	ISAwareness	.843	.036	.835	23.315	.000	.963	1.039

a. Dependent Variable: ISBEHA

According to the table 6, in the both regression analyses security practice-technology have significant impacts on IS security behavior (p-value is equal to zero which is less than .05). So, IS security awareness partially mediates the relationship between security practice-technology and IS security behavior. Therefore, H10 is accepted by this study.

3. CONCLUSION AND DISCUSSION

The achieved outcomes revealed that all of the mentioned elements have a remarkable impact on IS behavior and also information system security awareness. Moreover, IS security awareness can mediate the relationship between dependent and independent factors. Therefore, ICT departments in universities of Iran could improve such factors for reinforcing the awareness and IS security behavior. The future investigations can examine the developed framework of this research in other scopes too. Besides, the R-Square amount in current research is not high, therefore, it can be possible that other elements also can be added to this developed framework.

4. REFERENCES

[1] BERR (2008), "Information Security Breaches Survey", technical report, PricewaterhouseCoopers, in association with Symantec, HP and The Security Company, available at: www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf (accessed October 10, 2010).

[2] Computer Security Institute (CSI) (2008), "Computer Crime and Security Survey 2008", Computer Security Institute, available at: http://www.cse.msstate.edu/Bcse6243/readings/CSIsurvey2008.pdf (accessed July 5, 2012).

[3] D'Archy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information security misuse: a deterrence approach", Information Systems Research, Vol. 20 No. 1, pp. 79-98.

[4] Ernst & Young (2008), "Annual Global Information Security Survey", available at: www.arc-tc.com/pages/documents/ErnstandYoung2008.pdf (accessed February 9, 2011).

[5] Ernst & Young (2010), "12th Annual Global Information Security Survey: outpacing change", available at: www.ey.com/Publication/vwLUAssets/12th_annual_GISS_pub/$FILE/ 12th_annual_GISS_AU0383.pdf (accessed February 9, 2011).

[6] European Network and Information Security Agency (ENISA) (2008), "A new users' guide: how to raise information security awareness", ENISA, Heraklion, available at: www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf (accessed October 10, 2010).

[7] ISO (2005), Information Technology – Security Techniques – Information Security Management Systems – Requirements, ISO/IEC 27001, ISO, Geneva.

[8] Karamizadeh, S., Shayan, J., Alizadeh, M., &Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model ForCloud.International Journal Of Computers & Technology, 10(1), 1186-1191.

[9] Lee, Y., and Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems.Communications of the ACM.

[10] Peltier, T.R. (2005), "Implementing an information security awareness program", Information Systems Security, Vol. 14 No. 2, pp. 37-48.

[11] Proctor, R.W and Proctor, J.D. (2006). Handbook of Human Factors and Ergonomics 3rd ed., John Wiley and Sons, New York

[12] Puhakainen, P. (2006), "A design theory for information security awareness", doctoral dissertation, Department of Information Processing Science, University of Oulu, Oulu, available at: http://herkules.oulu.fi/isbn9514281144/ (accessed January 10, 2010).

[13] Qing, H., Hart, P. and Cooke, D. (2007), "The role of external and internal influences on information systems security a neo institutional perspective", Strategic Information System, Vol. 16 No. 2, pp. 153-72.

[14] Rhee, H. S., Kim, C., &Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

[15] Richardson, R. (2007). CSI Computer Crime and Security Survey. Computer Security Institute. From: retrieved November 16, 2007.

[16] Siponen, M. and Willison, R. (2007), "A critical assessment of IS security research between 1990-2004", in O ̈ sterle, H., Schelp, J. and Winter, R. (Eds), Proceedings of the Fifteenth European Conference on Information Systems, University of St Gallen, St Gallen, pp. 1551-9.

[17] Siponen, M.T. (2000), "A conceptual foundation for organizational information security awareness", Information Management & Computer Security, Vol. 8 No. 1, pp. 31-41.

[18] Spears, J. and Barki, H. (2010), "User participation in information systems security risk management", MIS Quarterly, Vol. 34 No. 3, pp. 503-22.

[19] Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: research and practice gaps", Information Security Journal: A Global Perspective, Vol. 17 Nos 5-6, pp. 207-27.

[20] Tsohou, A., Karyda, M., Kokolakis, S., &Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. Information Technology & People, 25(3), 327-352.

Corrosion Behaviour of 6061 Al-SiC Composites in KOH Medium

Arun V K
Assistant Professor
Mechanical Engineering
Ilahia School of Science & Technology
Cochin, India

Arun T A
M.Tech
Metallurgy and Materials
National Institute of Technology
Mangalore, India

Abstract: The present research work deals with the corrosion behaviour of 6061 Al-15% (vol) $SiC_{(P)}$ composites. The addition of the reinforcement like SiC to Aluminium has been reported to decrease the corrosion resistance of the matrix due to several reasons, one of them being galvanic action between the reinforcement and the matrix. In the present work, the corrosion behaviour of 6061 Al-15% (vol) $SiC_{(P)}$ composites in KOH at different concentration (0.5M, 1M, 1.5M) and different temperature (30^0C, 35^0C, 40^0C, 45^0C, 50^0C) was determined by Tafel extrapolation technique. The inhibition action of 8-Hydroxyquinoline on corrosion behaviour of 6061 Al-15% (vol) $SiC_{(P)}$ composites in KOH at different concentration of inhibitor (200ppm, 400ppm); different concentration of medium (0.5M, 1M,1.5M) and different temperature (30^0C, 35^0C, 40^0C, 45^0C, 50^0C) was investigated. The results indicate that corrosion rate of Al-SiC composite in KOH increases as the concentration of medium increases and also as temperature of medium increases. The results indicate that the inhibitor is moderately effective in inhibiting the corrosion of 6061 Al-15% (vol) $SiC_{(P)}$ composites. As the inhibitor concentration increases, the corrosion rate decreases. The surface morphology of the metal surface was investigated using scanning electron microscope (SEM). Activation energy was evaluated using Arrhenius equation, and enthalpy of activation and entropy of activation values were calculated using transition state equation.

Keywords: Corrosion, 6061 Al-SiC composite, KOH, 8-Hydroxyquinoline, Tafel.

1. INTRODUCTION

The word Corrosion stands for material or metal deterioration or surface damage in an aggressive environment. Corrosion is a chemical or electrochemical oxidation process, in which metal transfers electrons to environment and undergoes a valence change. It is a natural process which occurs with all metals except the least active noble metals like Gold and Platinum. Most metals are found in nature in the form of chemical compounds such as oxides, sulphides, carbonates, chlorides etc. In the refining process energy is added to the ore to extract the metal. The same amount of energy needed to extract metals from their ores is liberated during the chemical reactions that produce corrosion. Corrosion returns the metal to its combined state in chemical compounds that are similar to the ores from which metals were extracted. Corrosion is theoretically equivalent to the reverse of extractive metallurgy, if the material getting deteriorated is a metal. It must be noted that the deterioration by physical cause is not corrosion, but it termed as erosion, galling, wear etc. Corrosion of structural elements is a major issue for any industry because of the chemical environment of the chemical processing such as cleaning, pickling, descaling, acidizing acid pickling.

Al-SiC is a metal matrix composite consisting of Silicon carbide particles dispersed in a matrix of Aluminium alloy. The Silicon carbide reduces the density of Al and improves its stiffness and wear resistance. Aluminium matrix composite possess high Young’s modulus/ density and yield strength/ density ratios together with tailorable coefficient of thermal expansion and high thermal conductivity and hence look very promising and find applications in aerospace, military and automobile industries. However, one of the main draw backs of Aluminium matrix composite is the decrease in corrosion resistance compared to the base alloy. Base alloys inherently develop a protective oxide surface film which imparts corrosion resistance ; but, addition of reinforcing phase leads to in homogeneities and can cause discontinuities in the surface film, increasing the number of sites where corrosion can be initiated and making the composite more venerable to corrosion attack. The preferential localized attack has been based on factors, such as reactive silicon carbide matrix, presence of crevices and pores, processing routes, presence of secondary phases and the volume percentage of reinforcement. It is therefore important to add corrosion inhibitors to decrease the corrosion rate of Al composites. So a detailed study on the corrosion behaviour of this composite is relevant.

Inhibitors are substances, which can retard the rate and extent of corrosion, when added to a corroding environment in small concentration. Hundreds of organic and inorganic compounds have been studied and recommended as inhibitors of corrosion for various metals in various environments i.e. aqueous, non-aqueous, molten salt and dry atmospheres. Inhibitors properties are reported at various temperatures, ranging from very low to very high values. A wide variety of compounds are reported as inhibitors for metal matrix composites and these are mainly organic compounds usually containing N, S or O atoms and rare earth compounds.

The investigation was mainly focused to study the corrosion behaviour of 6061 Al-SiC composite in Potassium Hydroxide solution at three different concentrations viz. 0.5M, 1M, 1.5M at five different temperatures like 30, 35, 40, 45, 50^0C by Tafel extrapolation technique. Meanwhile, to add corrosion inhibitors to decrease the corrosion rate of the composite and 8-Hydroxyquinoline is selected as inhibitor in the present work to understand the effect of temperature on the inhibition action coupled with the study of influence of thermodynamic and kinetic parameters on the corrosion inhibition.

2. EXPERIMENTAL PROCEDURE

2.1 Material Preparation

The 6061 Al-SiC composites were cast in the form of 10 cylinders each of 90 mm diameter and 240 mm length by stir casting technique at NIIST (formerly RRL), Thiruvananthapuram. These cylinders were extruded at 430^{0}C-480^{0}C with extrusion ratio of 30:1 (two rods each of 11.5 mm diameter) at Serval Engineers, Mangalore. The experiments were performed with composite in extruded rod form. Reinforced SiC (average particle size is about 25 micron) has 99.8percentpurity. The extruded material is in the form of cylindrical rods of 1.15cm in diameter. The samples were cut from these rods and metallographically mounted up to 20mm height using cold setting resin. This exposed flat surface of the mounted part was polished using 1/0, 2/0, 3/0, 4/0 grit level and finally disc polished using diamond paste.

2.2 Medium

The corrosion studies were conducted in a Potassium Hydroxide solution of different concentrations viz. 0.5M, 1M and 1.5M. KOH pellets and distilled water were used to prepare the KOH solution for all experiments. 0.5M, 1M, 1.5M KOH solutions were prepared by dissolving28, 56, 84g of KOH pellets in 1litre of distilled water respectively.

2.3 Temperature

The corrosion studies were conducted in five different temperatures such as 30, 35, 40, 45 and 50^{0}C. A water thermostat was used to maintain the required constant temperature.

2.4 Inhibitor

8-Hydroxyquinoline was used as the inhibitor for corrosion inhibitor studies at different concentrations viz.200 and 400ppm.

2.5 Method

Tafel polarization studies were carried out by using CH instrument's electrochemical analyzer and a three electrode Pyrex glass cell with Platinum counter electrode and saturated Calomel electrode as reference electrode. An area of 1.038 cm^2 of the polished Al-15% (vol) SiC composite specimens were exposed to alkaline solution of concentration 0.5M at 30^{0}C with and without inhibitor. The polarization studies were made from -0.250V to 0.250V against open circuit potential (OCP) with a scan rate of 0.01V/sec and the corresponding corrosion currents, i, recorded. From the potential, E Vs log i plots, corrosion potential, E_{corr}, and corrosion current density, i_{corr}, were determined. The corrosion rate (C.R), in mpy, is calculated using the relation:

$$\text{Corrosion Rate (mpy)} = 0.129 \times EW \times i_{corr}/D \qquad (1)$$

Where, I_{corr}= corrosion current density in µA/cm^2, D=density of the corroding material, 2.77 g/cm^3, E.W=9.15g/mol,equivalent weight of corroding material (atomic weight/oxidation number).

The surface coverage (θ) is calculated as

$$\theta = (i_{corr} - i_{corr\ (inh)}) / i_{corr} \qquad (2)$$

Where, $i_{corr}$is the corrosion current density in the absence of inhibitor and $i_{corr\ (inh)}$ is the corrosion current density in the presence of inhibitor.

$$\text{The percentage inhibition efficiency (\%IE)} = \theta \times 100 \qquad (3)$$

The experiments were repeated for the temperatures such as 35, 40, 45 and 50^{0}C and for the concentrations such as 1M and 1.5M with 8-Hydroxyquinoline as inhibitor. E_{corr}, i_{corr}, C.R, θ and %IE for each experiment were determined.

2.6 Microstructural Studies

6061 Al-SiC composite specimens were polished as per standard metallographic practice, belt grinding followed by polishing on emery papers, finally on polishing wheel using diamond paste to obtain mirror finish. After polishing the specimens were etched with kellar's reagent and observed under Scanning Electron Microscope (SEM).

The microstructure of corroded samples of 6061 Al-SiC composite at three different concentrations of KOH with and without the addition of inhibitor, were examined under SEM to obtain the type of corrosion.

3. RESULT AND DISCUSSIONS

3.1 Corrosion Behaviour in KOH Medium

The corrosion rates were determined using Tafel extrapolation technique. Typical Tafel plots are shown in figures 1 to 12.

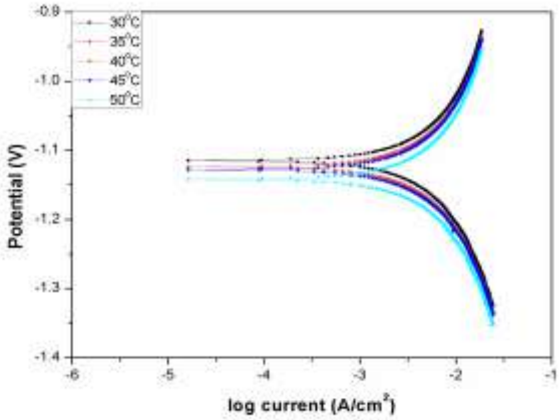


Figure 1. Tafel plot for 0.5M KOH solution at different temperatures

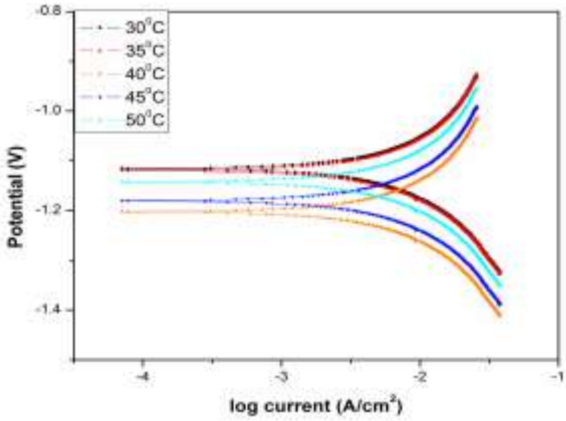


Figure 2. Tafel plot for 1M KOH solution at different temperatures

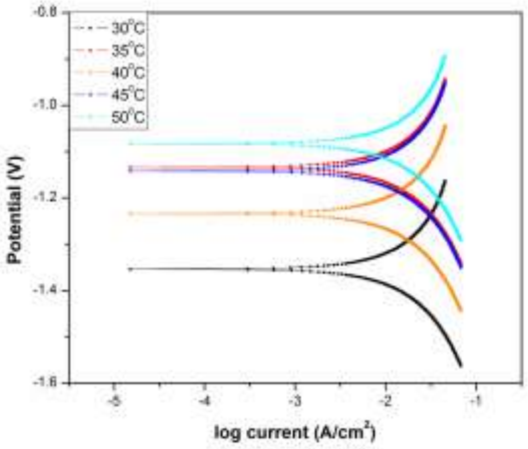


Figure 3. Tafel plot for 1.5M KOH solution at different temperatures

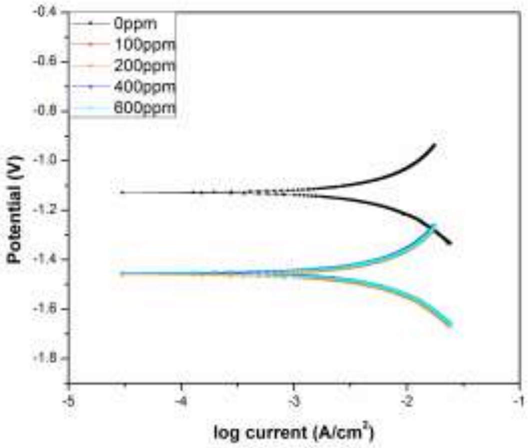


Figure 4. Tafel plot for 0.5M KOH at 30^{0}C with different concentrations of 8-Hydroxyquinoline

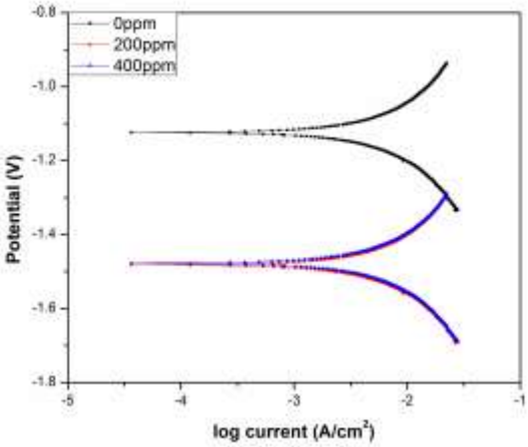


Figure 5. Tafel plot for 0.5M KOH at 40^{0}C with different concentrations of 8-Hydroxyquinoline

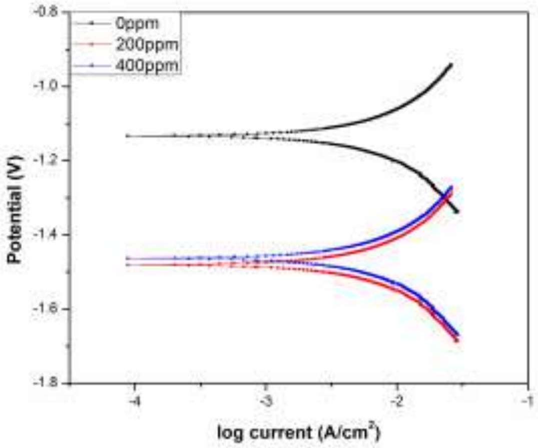


Figure 6. Tafel plot for 0.5M KOH at 50^{0}C with different concentrations of 8-Hydroxyquinoline

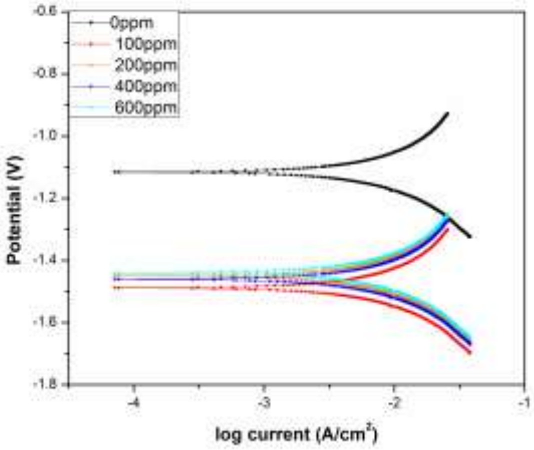


Figure 7. Tafel plot for 1M KOH at 30^{0}C with different concentrations of 8-Hydroxyquinoline

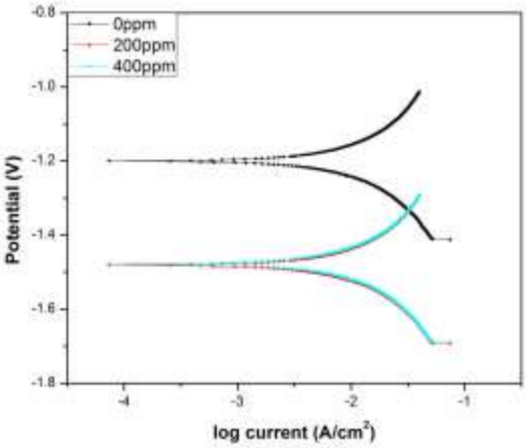


Figure 8. Tafel plot for 1M KOH at 40^0C with different concentrations of 8-Hydroxyquinoline

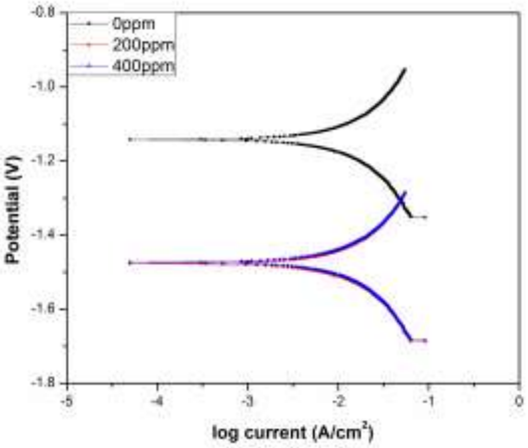


Figure 9. Tafel plot for 1M KOH at 50^0C with different concentrations of 8-Hydroxyquinoline

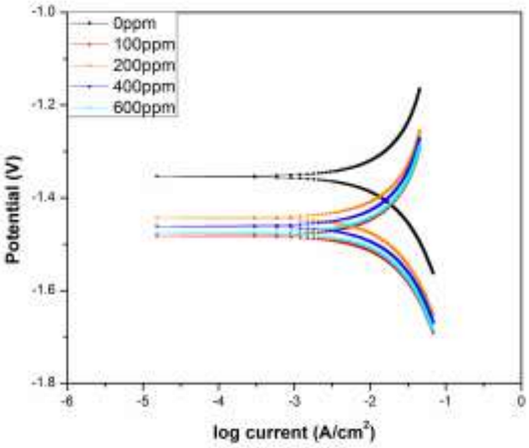


Figure 10. Tafel plot for 1.5M KOH at 30^0C with different concentrations of 8-Hydroxyquinoline

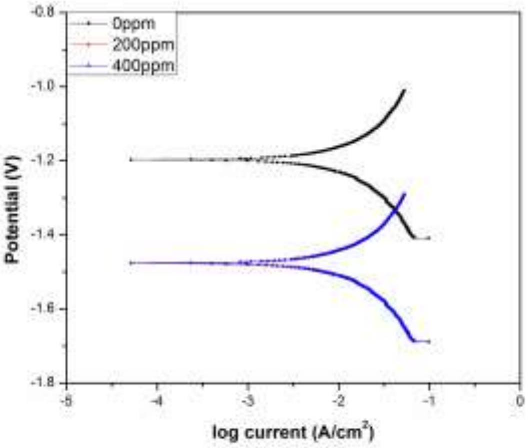


Figure 11. Tafel plot for 1.5M KOH at 40^0C with different concentrations of 8-Hydroxyquinoline

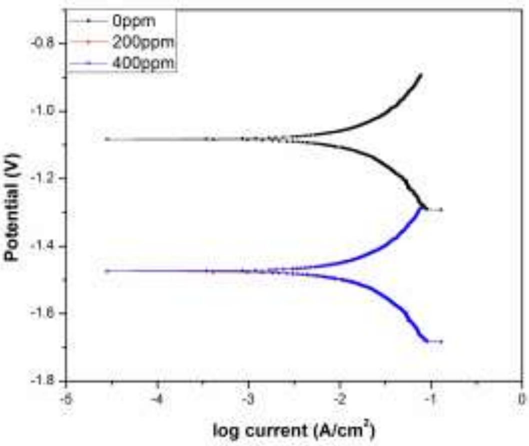


Figure 12. Tafel plot for 1.5M KOH at 50^0C with different concentrations of 8-Hydroxyquinoline

The corrosion rates are calculated for various experiments from these plots and tabulated. Values of corrosion rates in KOH solution obtained for different temperatures are presented in the Table 1.

Table 1. Corrosion rates of 6061Al-SiC Composite in different concentrations of KOH and at temperatures

Medium	Temperature (^{0}C)	Corrosion Rate (mpy)
0.5M KOH	30	37.982
	35	40.372
	40	45.714
	45	49.550
	50	54.572

1M KOH	30	65.718
	35	75.760
	40	85.885
	45	93.759
	50	105.629
1.5M KOH	30	97.535
	35	112.860
	40	117.199
	45	134.894
	50	150.822

3.2 Inhibition Behaviour of 8-Hydroxyquinoline

Corrosion rates obtained for different concentrations of 8-Hydroxyquinoline and the inhibition efficiency of 8-Hydroxyquinoline are tabulated in tables 2, 3 and 4.

Table 2. Corrosion rates of 6061Al-SiC Composite in KOH solutions with inhibitor 8-Hydroxyquinoline at 30^{0}C

Medium	Corrosion Rate (mpy)				
	0 ppm	100 ppm	200 ppm	400 ppm	600 ppm
0.5M KOH	37.98	37.01	35.01	31.91	31.79
1M KOH	65.71	62.98	55.79	52.56	51.95
1.5M KOH	97.53	85.80	82.02	61.28	55.39

Table 3. Corrosion rates of 6061Al-SiC Composite in KOH solutions with inhibitor 8-Hydroxyquinoline

Medium	Temperature (^{0}C)	Corrosion rate (mpy)		
		Inhibitor concentration		
		0ppm	200ppm	400ppm
0.5MKOH	30	37.982	35.009	31.915
	40	45.714	40.582	34.814
	50	54.572	46.514	37.550
1M KOH	30	65.719	55.798	52.560
	40	85.885	75.300	64.535
	50	105.629	81.547	72.107
1.5M KOH	30	97.535	82.029	61.280
	40	117.199	89.340	74.550
	50	150.822	132.685	116.453

Table 4. Inhibition Efficiency of 8-Hydroxyquinoline in KOH

Medium	Temperature(^{0}C)	Inhibition efficiency (%)	
		Inhibitor concentration	
		200ppm	400ppm
0.5M KOH	30	7.825	15.971
	40	11.226	23.843
	50	14.760	31.914
1M KOH	30	15.095	20.020
	40	12.320	24.850
	50	17.110	31.730
1.5M KOH	30	15.890	37.159
	40	23.770	36.390
	50	12.025	22.780

3.3 Thermodynamic Parameters

The effect of temperature on the corrosion rate of 6061 Al-SiC composite was studied by measuring the corrosion rate at different temperature between 30^{0}C to 50^{0}C. Activation energy (Ea) for the corrosion process of 6061 Al-SiC composite in KOH was calculated from the Arrhenius equation.

$$\ln(\nu_{corr}) = B-(Ea/RT) \qquad (4)$$

Where B is a constant which depends on the metal type and R is the universal gas constant. The plot ofln(ν_{corr})versus reciprocal of absolute temperature (1/T) gives a straight line whose slope = -Ea/R, from which the activation energy values for the corrosion process were calculated. Arrhenius plots are shown in the figure 13 to 15.

The enthalpy of activation (ΔH#) and entropy of activation (ΔS#) values for the corrosion process were calculated from transition state theory equation.

$$\nu_{corr} = (RT/Nh)\exp(\Delta S\#/R)\exp(-\Delta H\#/RT) \qquad (5)$$

Where h is Planck's constant, and N is Avagadro's number and R is the ideal gas constant. A plot of ln(ν_{corr}/T) versus (1/T) gives a straight line with slope= -ΔH#/R and intercept = ln(RT/Nh) + (ΔS#/R). The free energy of adsorption of inhibitor is calculated using formula as,

$$\Delta G_{ads} = -RT\ln\left[\frac{55.5\times\theta}{C\,(1-\theta}\right] \qquad (6)$$

Where, ΔG_{ads}= Free energy of adsorption (J/mol), R = Real gas constant, T = Temperature (K), C = Concentration of inhibitor (mol/dm^3), θ = Surface coverage.

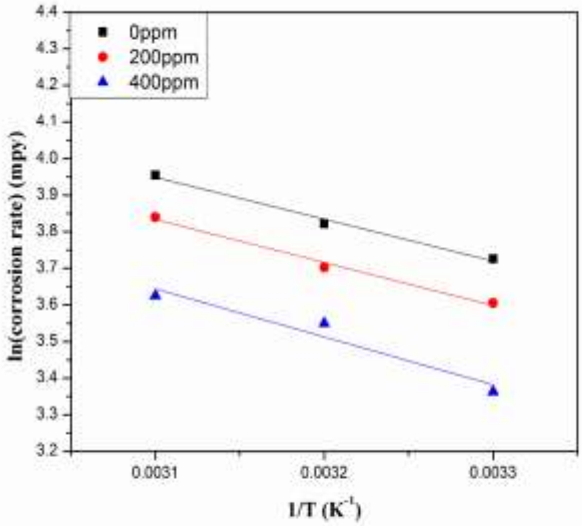


Figure 13. Arrhenius plots for 0.5M KOH

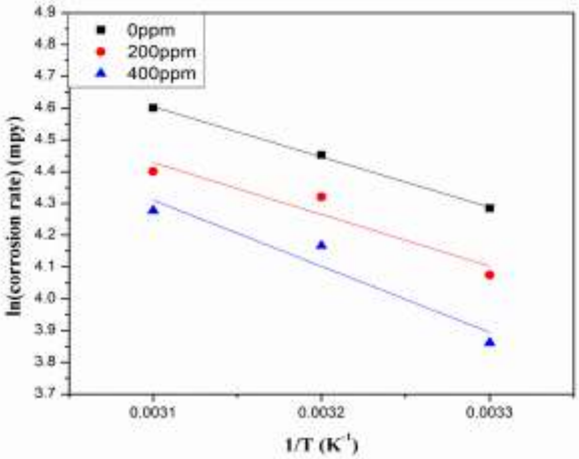


Figure 14. Arrhenius plots for 1M KOH

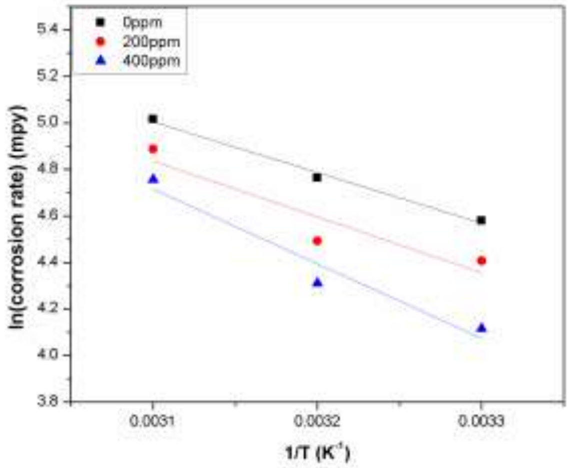


Figure 15. Arrhenius plots for 1.5M KOH

The plot of ln(ν_{corr}/T) versus (1/T) are shown in Figure 16 to18.

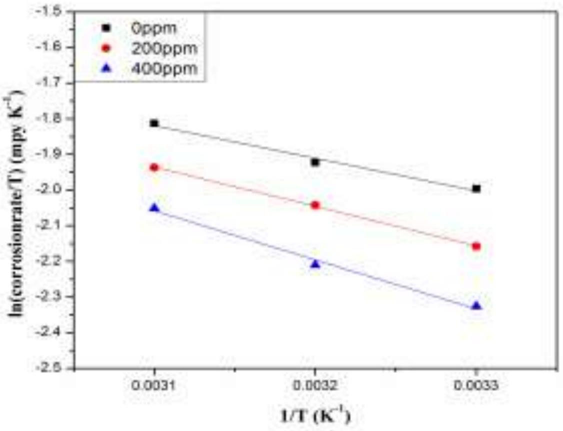


Figure 16. Plot of ln(ν_{corr}/T) versus (1/T) in 0.5M KOH

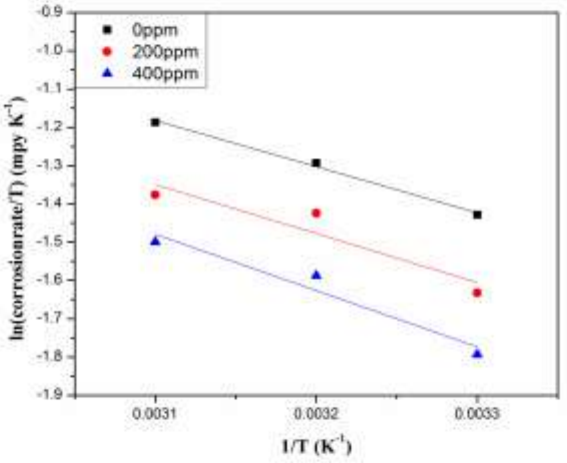


Figure 17. Plot of ln(ν_{corr}/T) versus (1/T) in 1M KOH

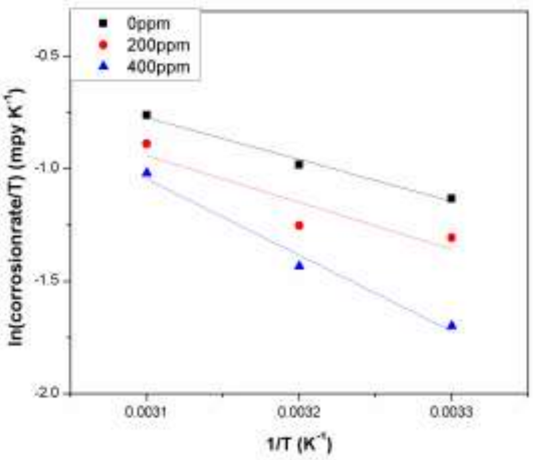
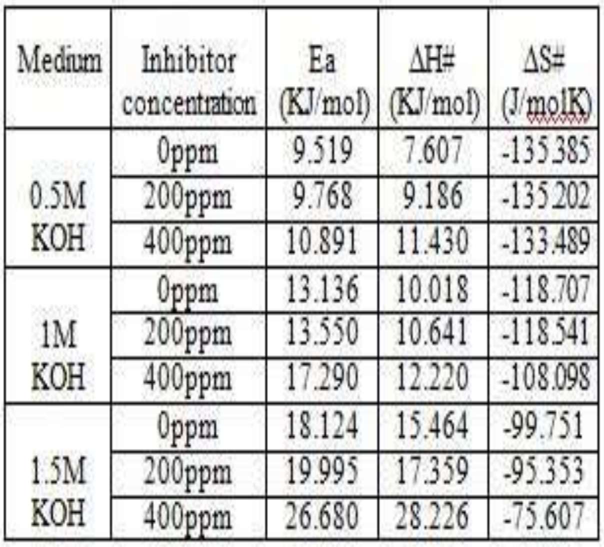


Figure 18. Plot of ln(ν_{corr}/T) versus (1/T) in 1.5M KOH

The value of Ea, ΔH#, ΔS# and ΔG# for 8-Hydroxyquinoline on 6061 Al-SiC composite in different KOH concentrations and temperatures is listed in Table 5 and 6.

Table 5. Activation parameters for the corrosion of 6061Al-SiC Composite in KOH solution



Medium	Inhibitor concentration	Ea (KJ/mol)	ΔH# (KJ/mol)	ΔS# (J/molK)
0.5M KOH	0ppm	9.519	7.607	-135.385
	200ppm	9.768	9.186	-135.202
	400ppm	10.891	11.430	-133.489
1M KOH	0ppm	13.136	10.018	-118.707
	200ppm	13.550	10.641	-118.541
	400ppm	17.290	12.220	-108.098
1.5M KOH	0ppm	18.124	15.464	-99.751
	200ppm	19.995	17.359	-95.353
	400ppm	26.680	28.226	-75.607

Table 6. Standard free energy (ΔG#) values

Medium	Temperature (^{0}C)	Standard free energy (ΔG#)		
		0 ppm	200 ppm	400 ppm
0.5M KOH	30	48.572	50.181	51.850
	40	49.924	51.534	53.184
	50	51.276	52.887	54.518
1M KOH	30	45.923	46.607	44.944
	40	47.108	47.794	46.024
	50	48.293	48.981	47.104
1.5M KOH	30	45.688	46.250	51.134
	40	46.685	47.203	51.980
	50	47.683	48.157	52.647

The table 7 shows the free energy of adsorption of inhibitor (8-Hydroxyquinoline) for corrosion of 6061 Al-SiC composite in KOH at different concentrations.

Table 7. Free energy of adsorption (ΔG_{ads}) of inhibitor

Medium	Temperature (^{0}C)	Free energy of adsorption (KJ/mol)	
		200ppm	400ppm
0.5M KOH	30	-20.498	-20.754
	40	-22.221	-22.761
	50	-23.753	-24.577
1M KOH	30	-22.362	-21.473
	40	-22.481	-22.903
	50	-24.236	-24.552
1.5M KOH	30	-22.516	-23.636
	40	-24.551	-24.337
	50	-23.124	-23.333

4. DISCUSSIONS

4.1 Corrosion Behavior in KOH Medium

The results indicate that the 6061 Al-SiC composite is highly susceptible to corrosion in 1.5M KOH while its corrosion rate is comparatively lower in 0.5M KOH even at 50^{0}C. Corrosion rate is high at 50^{0}C and is lower at 30^{0}C for every concentrations of KOH. Corrosion rate of the 6061 Al-SiC increases with increase in temperature. It would be possible because of the increased kinetics of the reaction. As the KOH concentration increases from 0.5M to 1.5M, corrosion rate shows an increase, because the loss of passivity of the specimen due to thinning of primary oxide layer by the chemical dissolution action of hydroxide ions(OH^-) on increasing the concentration of the alkali. The hydroxide ions formed increase the pH at the film/solution interface considerably; the increased local pH on the metal surface accelerates the corrosion reaction, and damage the passive film.

4.2 Inhibition using 8-Hydroxyquinoline

8-Hydroxyquinoline is moderately effective in bringing down the corrosion rate as its presence brings down the corrosion rate considerably. Among the 2 concentration studied, the lowest corrosion rate was obtained at 400ppm of 8-Hydroxyquinoline in all alkali concentrations. Since, 8Hydroxyquinoline is adsorption type inhibitor its spread over the surface of the metal like an umbrella and protects the metal from corrosion. However, if sufficient quantity is not added then the surface of the metal is left uncovered which results in severe corrosion attack. It has been observed from the figures 4 to 12 that the inhibitor 8-Hydroxyquinoline acts as a cathodic inhibitor. It displaces the corrosion potential in the negative direction and reduces corrosion current, there by retard cathodic reaction and suppresses the corrosion rate. Inhibition efficiency increases with the increase in inhibitor concentration in all media. A maximum inhibition efficiency of about 37% could be achieved with 400ppm of inhibitor addition in 1.5M KOH at 30^{0}C. The inhibition efficiency of 8-Hydroxyquinoline in different KOH concentration is shown in figures 19 to 21.

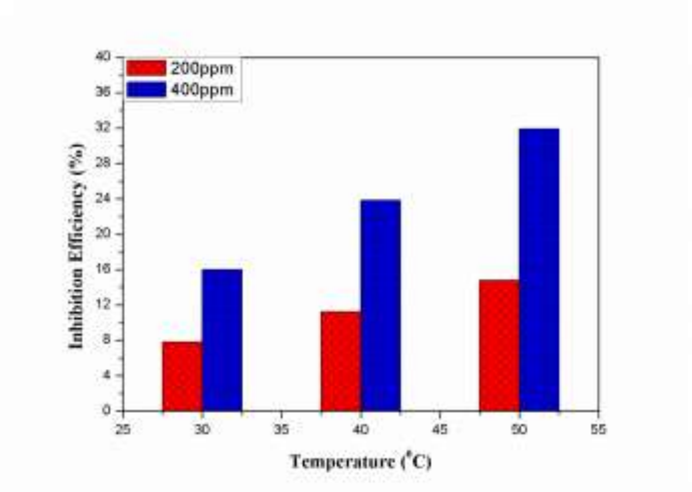


Figure 19. Inhibition efficiency of 8Hydroxyquinoline in 0.5M KOH

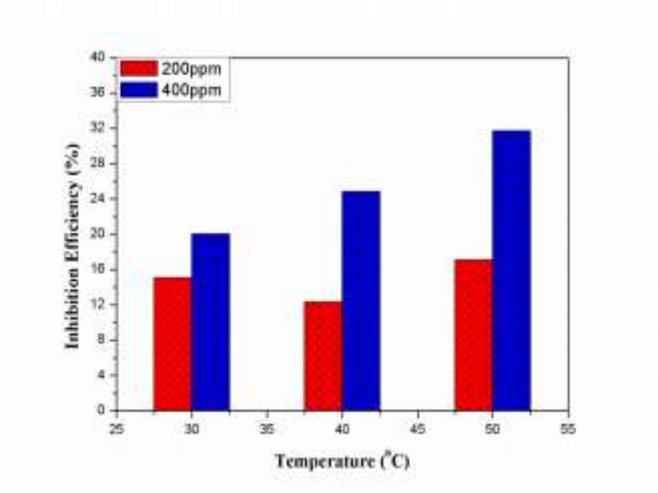


Figure 20. Inhibition efficiency of 8Hydroxyquinoline in 1M KOH

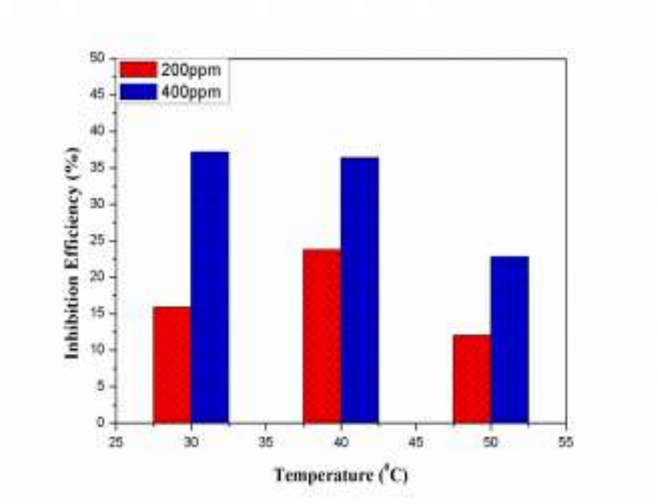


Figure 21. Inhibition efficiency of 8Hydroxyquinoline in 1.5M KOH

Table 8. Adsorption isotherms

SI. No	Name	Verification plot
1	Langmuir	c/ θ vs c
2	Frumkin	θ vs log c
3	Bockris-Swinkels	θ/(1- θ) vs log c
4	Temkin	θ vs log c
5	Virial Parson	θ vs log (θ/c)
6	Flory Huggins	log (θ/c) vs log (1- θ)
7	El-Awady	log [θ/(1- θ)] vs log c
8	Freundlich	log θ vs log c

Various adsorption isotherms are listed in the above table 8. Verification plots were plotted for each isotherms and it was found that Temkin adsorption isotherm exhibits straight line.

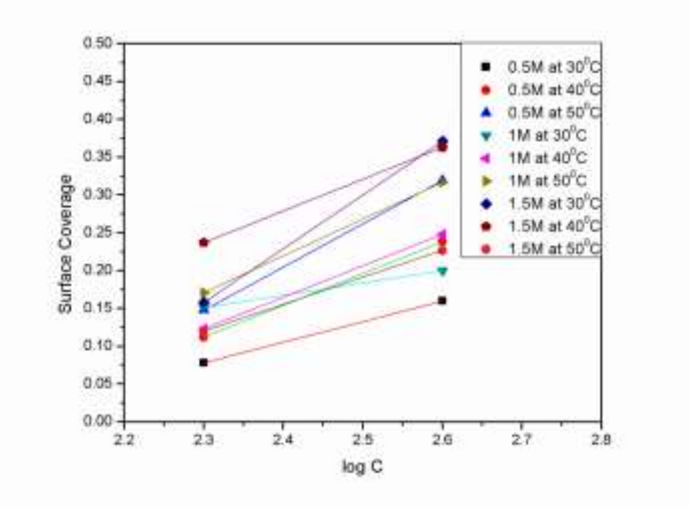


Figure 22. Temkin adsorption isotherm for corrosion of 6061 Al-SiC composite

From the table 7 it is clear that the ΔG_{ads} values for 8-Hydroxyquinoline (C_9H_7NO) ranges between -20KJ/mol to -25KJ/mol and it is observed that the inhibition efficiency decreases with increase in temperature. From these two observations it can be concluded that this inhibitor get adsorbed on the metal surface by mixed adsorption, which is also supported by enthalpy of activation shown in table 5.

4.3 Characterization Using SEM

The SEM images of the surface of the Al-SiC composite are shown in figures 23 to 25. The figure 23 shows the SEM micrograph of corroded sample without inhibitor and the figure 24 and 25 show the SEM micrographs of corroded sample with inhibitor at 30^0C.

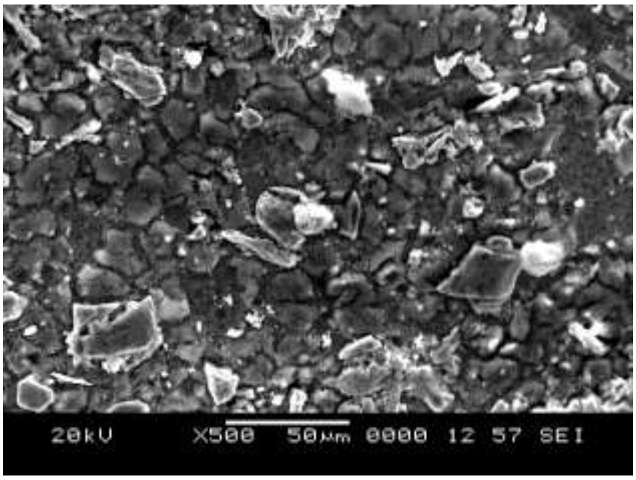


Figure 23. SEM micrograph of corroded 6061 Al-SiC composite in 0.5M KOH at 30^0C

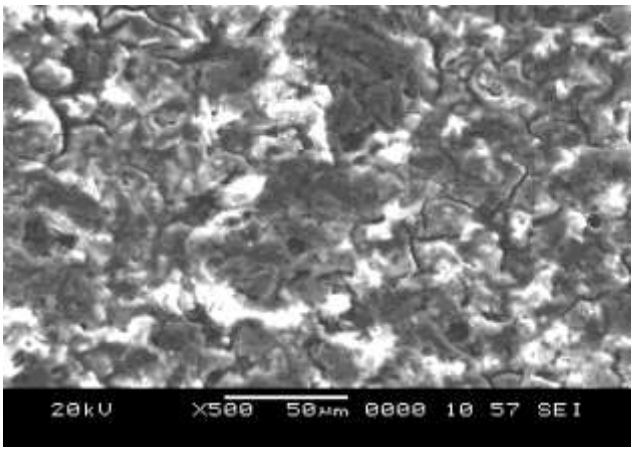


Figure 24. SEM micrograph of corroded 6061 Al-SiC composite in 1.5M KOH with inhibitor (200ppm) at 30^0C

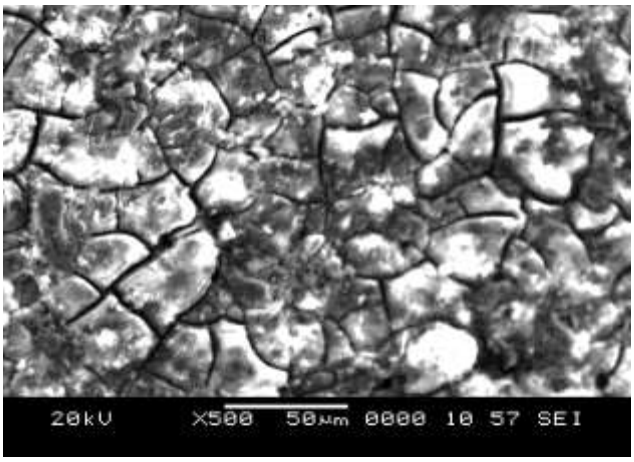


Figure 25. SEM micrograph of corroded 6061 Al-SiC composite in 1.5M KOH with inhibitor (400ppm) at 30^0C

The SEM images shown that Al-SiC composite have undergone both uniform and galvanic corrosion. The galvanic corrosion is due to presence of SiC particles in Al matrix which act as cathode site. This can be seen in the SEM images where the matrix adjacent to the SiC particle has been corroded.

5. CONCLUSIONS

1. 6061 Al-SiC composite is highly susceptible to corrosion in KOH.

2. Corrosion rate of the sample increase with increase in concentration of the solution. Also, corrosion rate of the sample increases with increase in temperature because of the increased kinetics of reaction.

3. 8-Hydroxyquinoline is found to be moderately effective as a corrosion inhibitor and the inhibition efficiency increases with inhibitor concentration for a given set of conditions.

4. The highest efficiency of 37% was observed at 400ppm concentration of the inhibitor.

5. The standard free energy values confirm that inhibitor molecules get adsorbed on to the surface of the composite by mixed adsorption.

6. ACKNOWLEDGMENTS

We are grateful to Dr Jagatnath Naik, HOD, Department of Metallurgy and Materials Engineering NITK Surathkal Inda Inda, for his keen interest and support during the course of the investigation. Also the authors gratefully acknowledge the assistance provided by the Metallurgy department staffs of NITK surathkal India for carrying out heat treatments and corrosion experiments.

7. REFERENCES

[1] Aprael, S. Y. and Huda, A. D.,"Corrosion Inhibition of Aluminum Alloy 5083". Iraqi Joumal of Chemical and Petroleum Engineering,Vol.10 *No.4* (December 2009) 19-25.

[2] ASM Handbook.(2005).Volume13B, Corrosion: Materials, ASM International, Ohio.

[3] Bhat, M. S. N., Surappa, M. K. and Nayak, H. V. S. (1991)."Corrosion Behaviour of Silicon Carbide particle reinforced 6061/Al alloy composites." J. Mater. Sci., 26, 4991-4996.

[4] Bockris, J. O. M. and Swinkels, D. A. J. (1964)."Adsorption of n-Decylamine on solid metal electrodes."J. Electrochem. Soc., 111(8), 736-743.

[5] Candan, S. and Bilgic, E. (2004). "Corrosion behavior of Al-60 vol. % SICp composites in NaCl solution."Mater.Lett., 58, 2787-2790.

[6] Chawla, K. K. (1998). Composite Materials- Science and engineering, *S*pringer, Newyork.

[7] Davis, J. R. (1993). Aluminium and Aluminium Alloys. ASM International, Ohio.

[8] Fischer, H. (1972). "The Inhibition of Vapor-phase Corrosion."Werkst.Korros, 23, 445-465.

[9] Fontanna, M. G. (2005). Corrosion Engineering,3rd Edition,McGraw Hill, USA.

[10] Ghali, E. (2010). Corrosion Resistance of Aluminium and Meganesium Alloys Understanding, Performance and Testing, John Wiley & Sons, Inc., Publication, New Jersey.

[11]Hausler, R. H. (1983). Paper 19, International Conference on Corrosion Inhibition. National Association of Corrosion Engineers, Dallas, paper 19.

[12]Hollingsworth, E. H. and Hunsicker, H. Y. (1987). Metals Hand Book, Vol.13, 9th Edition, 583-609, ASM International, Metals Park, Ohio.

[13]Lamakaa, S. V., Zheludkevich, M. L., Yasakau, K. A., Montemorb, M. F. and Ferreira, M. G. S., "High effective organic corrosion inhibitors for 2024 Aluminium alloy."ElectrochimicaActa52 (2007) 7231–7247.

[14]Lloyd, D. J. (1994). "Particle Reinforced Aluminium and Magnesium Matrix Composites." International Metals Review. 39(1), 1-3.

[15]Lorenz, K., Zellner, B. and Ber.Bunsenges.(1984). "Laser Photolysis/resonance fluorescence study of the rate constants for the reactions of Hydroxyl radicals with ethane and propene."Phys. Chem., 88, 1128-1231.

[16]Lorenz, W. J and Mansfield, F. (1983).Paper 2, International Conference on Corrosion Inhibition. National Association of Corrosion Engineers, Dallas.

[17]Nayak, J. and Hebbar, K. R. (2008).Trans. Indian. Inst. Met., 61, 221-224.

[18]Paciej, R. C. and Agarwala, V. S. (1986)." Metallurgical Variables Influencing the Corrosion Susceptibility of a Powder Metallurgy SiCw/ Al Composite." Corrosion, 42, 718-728.

[19]Philip, A. S. (2007). Corrosion of Linings and Coatings-Cathodic and Inhibitor Protection and Corrosion Monitoring, Taylor and Francis group, USA.

[20]Reena, K. P. D., Nayak, J. and Shetty, N. A., "Corrosion behavior of 6061/Al-15 vol. pct. SiC(p) compositeand the base alloy in sodium hydroxide solution." Arabian Journal of Chemistry (2012).

[21]Roberge, P.R. (2000). Handbook of Corrosion Engineering, McGraw, USA.

[22]Sun, H., Koo, E. Y. and Wheat, H. G. (1991)." Corrosion behaviour of SiCp/6061 Al Metal Matrix Composites." Corrosion, 47, 741-753.

[23]Trzaskoma, P. P., McCafferty, E. and Crowe, C. R. (1983). "Corrosion behaviour of SiC/Al Metal Matrix Composites."Electrochem Soc. J, 130, 1804-1809.

[24]Uhling, H. H. and Revie, R. W. (2008).Corrosion and corrosion control, John Wiley & Sons, Inc., Publication, New Jersey.

[25]Winkler, S. L., Ryan, M .P. and Flower, H. M. (2004). "Pitting corrosion in cast 7XXX Aluminium alloys and fibre reinforced MMCs." Corrosion Science., 46, 893-902.

[26]Winston, R. R (2011).Uhligs Corrosion Hand Book,John Wiley & Sons, Inc., Publication, New jersey.

[27]Zaki, A. (2006). Principles of Corrosion Engineering and Corrosion Control,Elseveir, UK.

Effect of Heat Treatment on Corrosion Behaviour of Spring Steels

Arun V K
Assistant Professor
Mechanical Engineering
Ilahia School of Science & Technology
Cochin, India

Roshith Raghavan
M.Tech
Metallurgy & Materials
National Institute of Technology
Mangalore, India

Abstract: The experimental work deals with the effect of heat treatment on the corrosion behaviour of spring steels. In this study the heat treatments like hardening, normalizing and tempering were done for spring steels to obtain martensitic matrix, pearlitic structure and tempered martensitic matrix respectively. After heat treatment the microstructural studies were carried out for the samples using SEM. Hardness measurements were done. The corrosion behaviour of all heat treated samples in HCl at different concentration (1.5N, 2N and 2.5N) was determined using Tafel extrapolation technique. The variation in the corrosion rates due to the effect of heat treatment was noted. The results indicate that for fully martensitic matrix the corrosion rate is minimum and for pearlitic structure its maximum. As tempering time is increased the corrosion rate increases correspondingly. The corroded microstructural images were also taken using SEM and analysed.

Keywords: corrosion, spring steel, leaf spring, HCl, Tafel

1. INTRODUCTION

The word Corrosion stands for material or metal deterioration or surface damage in an aggressive environment. Corrosion is a chemical or electrochemical oxidation process, in which metal transfers electrons to environment and undergoes a valence change. Corrosion returns the metal to its combined state in chemical compounds that are similar to the ores from which metals were extracted. Corrosion of structural elements is a major issue for any industry because of the chemical environment of the chemical processing.

Today steel is the most important resource in this industrialized world. It forms the basic building material of today’s structure. Moreover steels with large chromium and vanadium percentage can be used as spring steels which form the suspension system. Prevention of wear and increase in steel life depends principally on the design and operation on the component, but providing some pre-use treatment on steel can also improve the quality to a great extent. It has been seen that most of the study focuses on the experimental testing of the steel component and very few focuses on the material testing and improving its properties beforehand. One of the processing routes to alter the properties is heat treatment. Nearly 90% of the springs are used in heat treated conditions. The major requirement for the conventional spring steel is toughness, strength & hardness [11].

Increasing demands of automotive industry on performance improvement , weight reduction and cost savings place a lot of pressure on vehicle components , which require new design concepts and further material development. In this respect, weight reduction is very important as it reduces costs, but more importantly it reduces fuel consumption and CO_2 pollution. The biggest fuel consumers and polluters are trucks, where redesign and use of lighter high strength leaf springs can bring considerable benefits. Parabolic leaf springs used in suspension systems of truck front axles are usually made of two leaves, and serve two main purposes: support the weight of the trailer and provide the spring function in the suspension system. Improved strength of spring steel can be achieved through control of alloy composition, effective heat treatment, micro-alloying, thermo mechanical treatment and shot-peening The main objectives of current research work are to investigate the corrosion behavior of spring steel in acid medium, investigate the effect of concentration of medium on corrosion behavior of spring steel and investigate the effect of heat treatment on the corrosion behavior of spring steel.

2. EXPERIMENTAL PROCEDURE

2.1 Material Preparation

There are many grades of steels used for manufacturing of leaf springs like 9260, 4068, 4161, 6150, 8660, 5160, and 51B60. The leaf spring used in this experiment is 51B60.

The samples were cut from leaf spring and metallographically mounted using cold setting resin. This exposed flat surface of the mounted part was polished using 1/0, 2/0, 3/0, 4/0 grit level and finally disc polished using levigated Alumina, and etched using 2% Nital which was prepared by adding 2 Milliliter of Nitric acid to 98 Milliliter of ehtyl alcohol.

2.2 Medium

The corrosion studies were conducted in Hydro chloric acid solution of different concentrations viz. 1.5N, 2N and 2.5N.

The solutions were prepared from concentrated HCl(almost 32N). 1.5N HCl was prepared by adding 150ML of concentrated HCl to 850ML of distilled water. 2N HCl was prepared by adding 200ML of concentrated HCl to 800ML of distilled water. Finally the 2.5N HCl was prepared by adding 250ML of concentrated HCl to 750ML of distilled water.

2.3 Temperature

The corrosion studies were conducted at room temperatures.

2.4 Heat treatment

The samples were subjected to heat treatments like hardening, normalizing and tempering. The leaf spring of the automobile was first cut into rectangular pieces of area 1.1×1.1 cm^2 and height of 1 cm. One sample was taken and heated to 920^0C, holding at that temperature for 45 minutes for homogenizing in a resistance furnace. After 45 minutes the sample was taken out and air cooled to obtain Normalized structure for leaf spring. Another sample was taken and heated to 920^0C and after holding 45 minutes at that temperature it is immediately oil quenched to obtain Hardened microstructure for spring steel. Five samples were heated to 920^0C and after holding there for 45 minutes the samples were oil quenched immediately. These samples were reheated to a temperature of 200^0C. After one hour one sample was removed from furnace and oil Quenched immediately. That sample is tempered for 1 hour sample. Like this after each hour one sample is removed and oil quenched. So that we will get Tempered 1 hour, tempered 2 hour, tempered 3 hour, tempered 4 hour, tempered 5 hour samples.

2.5 Microstructural Examination

These heat treated samples were finely polished using 1/0, 2/0, 3/0, 4/0 grit level and finally disc polished using levigated Alumina, and etched using 2% Nital. SEM images were taken before and after corrosion for the samples.

2.6 Hardness Test

All the heat treated samples were subjected to hardness test. The hardness of the samples was determined using Rockwell c scale.

2.7 Method

Tafel polarization studies were carried out by using CH instrument's electrochemical analyzer and a three electrode cell. An area of 1.1×1.1 cm^2 of the polished leaf spring specimens were exposed to acid solution (1.5N, 2N and 2.5N) at room temperature. The polarization studies were made from -0.250V to 0.250V against open circuit potential (OCP) with a scan rate of 0.01V/sec and the corresponding corrosion currents, i, recorded. From the potential, E Vs log i plots, corrosion potential, E_{corr}, and corrosion current density, i_{corr}, were determined. The corrosion rate (C.R), in mpy, is calculated using the relation:

$$\text{Corrosion Rate (mpy)} = 0.129 \times EW \times i_{corr}/D \qquad (1)$$

Where, i_{corr} = corrosion current density in µA/cm^2, D=density of the corroding material, 7.16 g/cm^3, E.W=27.398g/mol,equivalent weight of corroding material (atomic weight/oxidation number). The experiments were repeated for the hardened, normalized and tempered (1-5 hours) samples. E_{corr}, i_{corr} and C.R for each experiment were determined.

3. RESULT AND DISCUSSIONS

3.1 Microstructural Examination

The spring steel samples were heat treated and the microstructures were viewed under SEM. The results of SEM are shown below.

By analyzing the scanning electron microscopy images of the hardened sample, the lath shape martensite formed due to the hardening process can be clearly seen. The samples were oil quenched after austenizing.

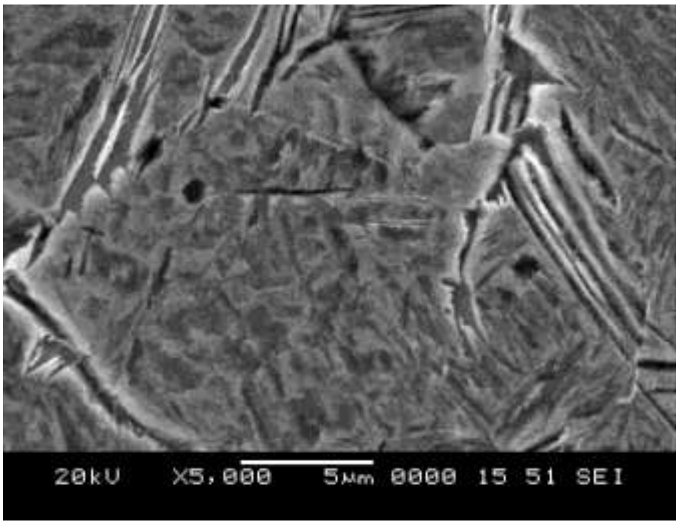


Figure 1. SEM images for hardened sample

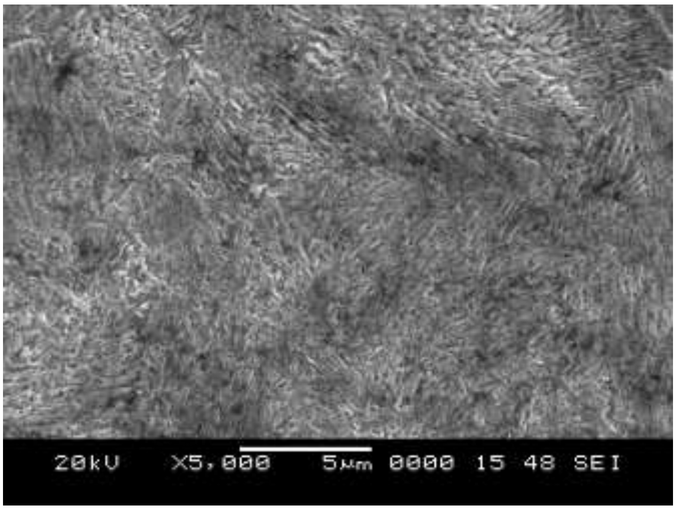


Figure 2. SEM images of a normalized sample

Looking at the scanning electron microscopy images of the normalized sample, the layers of ferrite and pearlite can be clearly seen.

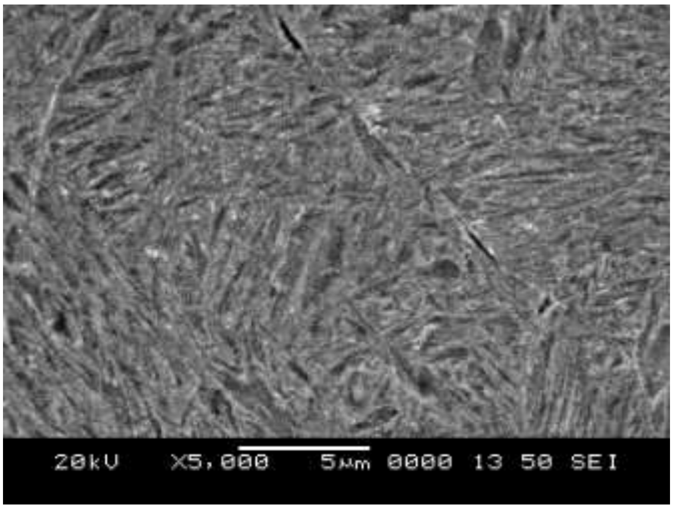


Figure 3. SEM images of a sample tempered for 1 hour

Looking at the scanning electron microscopy images of the tempered 1hour sample, carbides are distributed along previous martensitic laths.

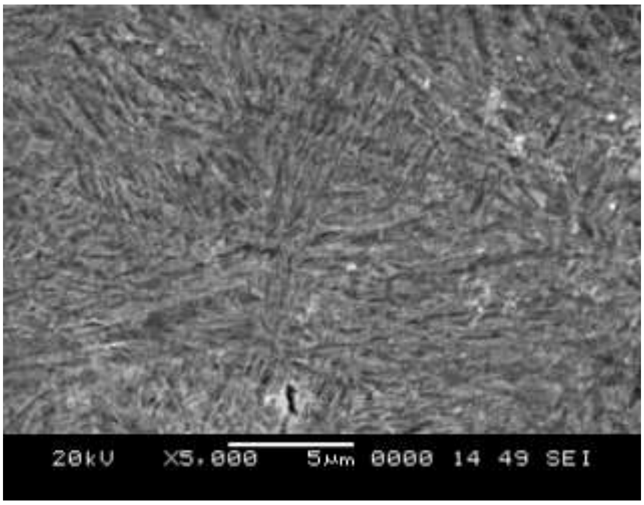


Figure 4. SEM images of a sample tempered for 2 hour

Looking at the scanning electron microscopy images of the 2 hour tempered sample, it is clearly seen that the along with martensite the carbides are also there but the intensity of carbides has increased as compared with samples tempered for 1 hour.

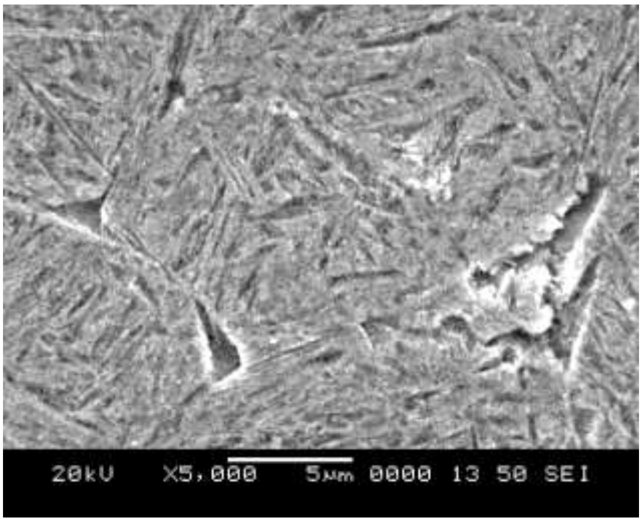


Figure 5. SEM images of a sample tempered for 3 hour

Looking at the scanning electron microscopy images of the 3 hour tempered sample, it can be clearly seen that the intensity of carbides is increasing as the tempering time is increased.

In figure 6, Looking at the scanning electron microscopy images of the 4 hour tempered sample, it can be clearly seen that the intensity of carbides is increasing as compared to samples tempered for 3 hour.

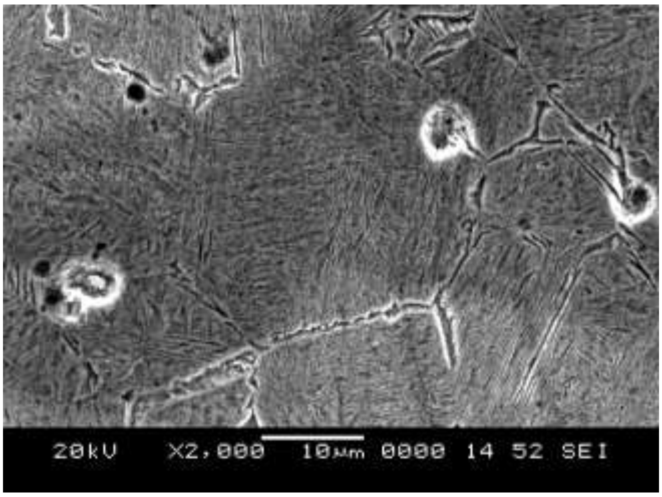


Figure 6. SEM images of a sample tempered for 4 hour

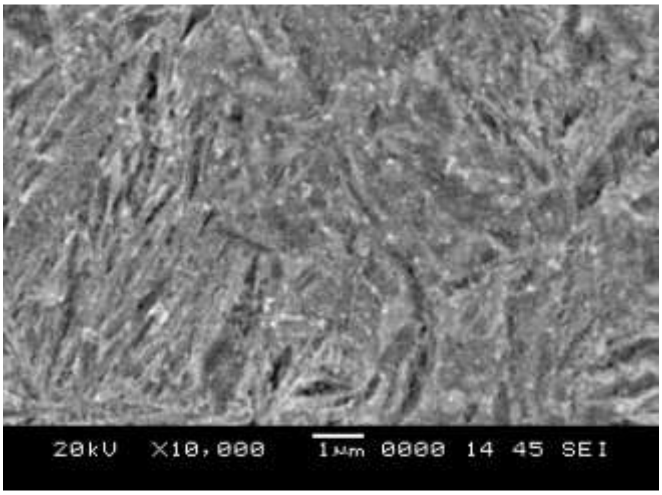


Figure 7. SEM images of a sample tempered for 5 hour

Looking at figure 7, it can be clearly seen that the distribution of carbides along the martensitic laths is very high. The coarsening of the carbides may occur along the ferritic grain boundaries.

3.1.1 Microstructures after corrosion (in 2.5N HCL)

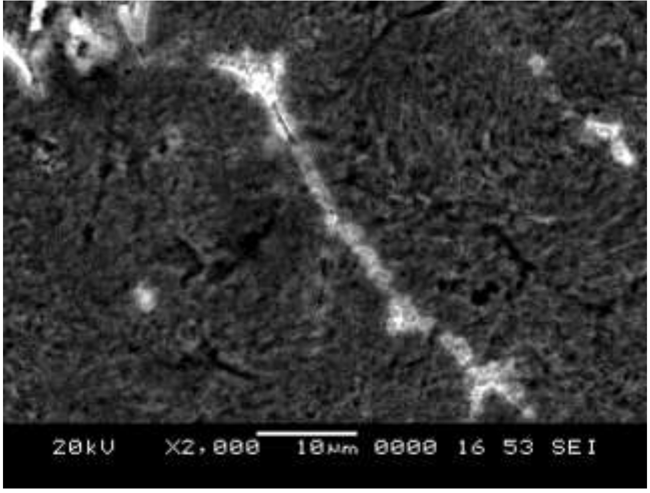


Figure **8.** Microstructure of the normalized spring steel after corrosion in 2.5N HCl

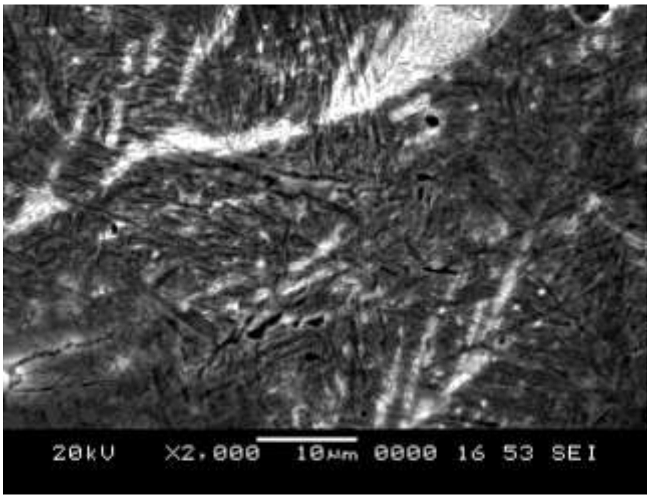


Figure 9. Microstructure of the hardened spring steel after corrosion in 2.5N HCl

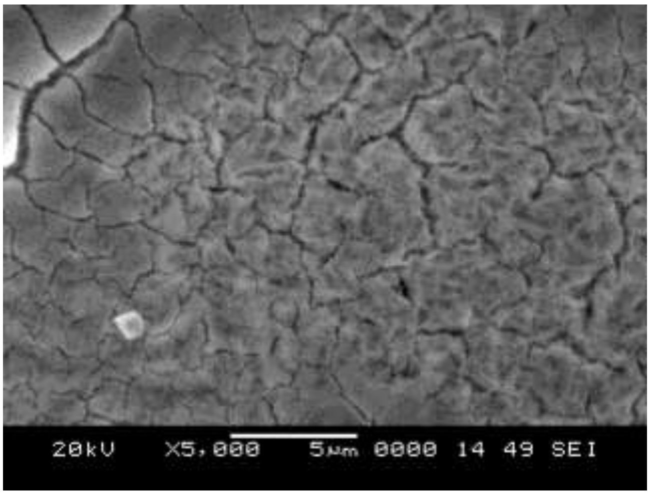


Figure 10. Microstructure of the tempered 1 hour spring steel after corrosion in 2.5N HCl

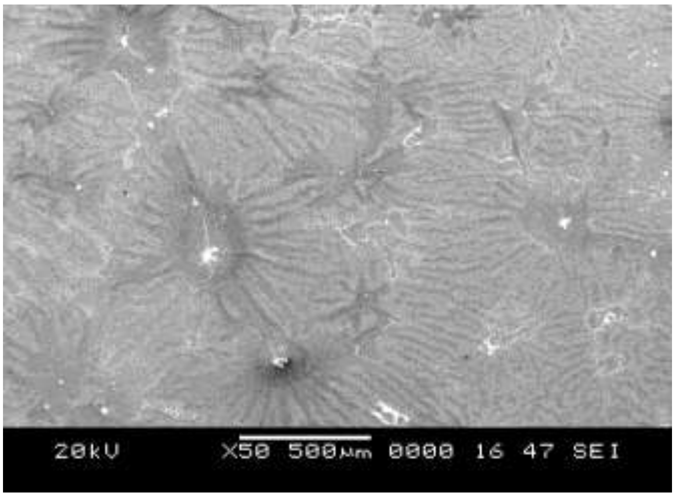


Figure 11. Microstructure of the tempered 2 hour spring steel after corrosion in 2.5N HCl

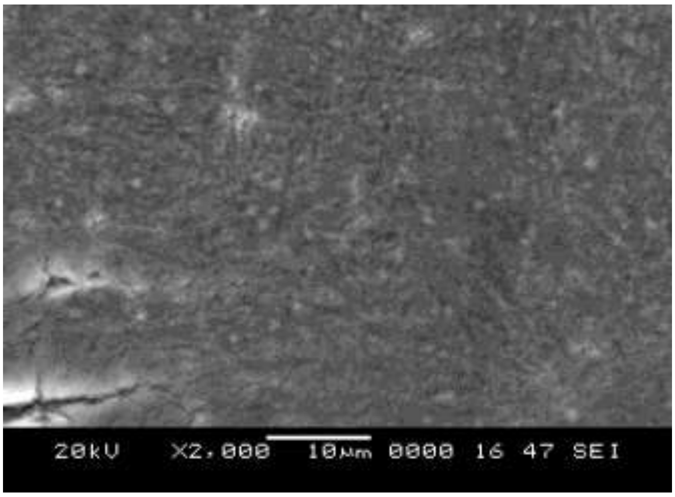


Figure 12. Microstructure of the tempered 3 hour spring steel after corrosion in 2.5N HCl

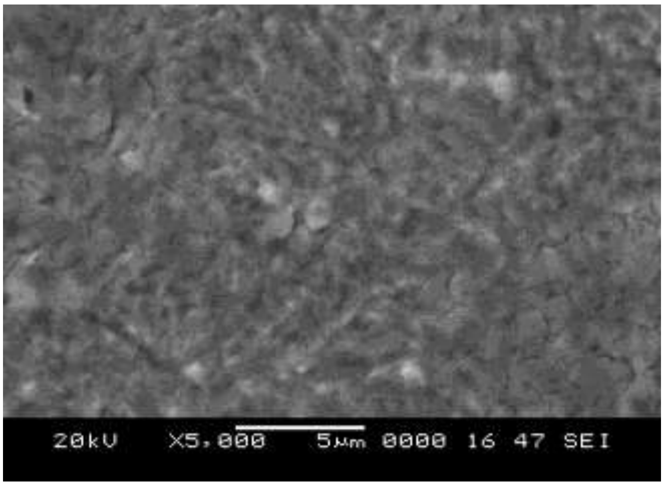


Figure 13. Microstructure of the tempered 4 hour spring steel after corrosion in 2.5N HCl

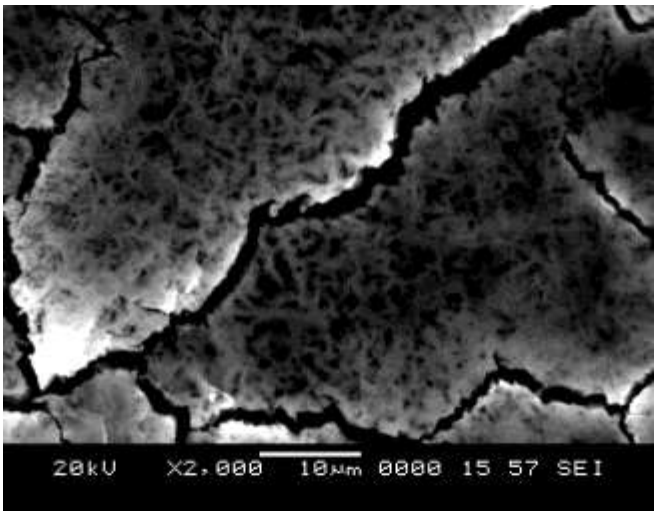


Figure 14. Microstructure of the tempered 5 hour spring steel after corrosion in 2.5N HCl

The microstructures of the heat treated specimens of spring steel were observed. Microstructures are of martensitic structures with some carbides at the grain boundaries,cabides may be occurred due to incomplete austanitization. After tempering for 1 hour the microstructure consist of tempered martensite and the carbides precipitates (epsilon carbides) are seen along the grain boundaries. As the carbon atoms are diffusing from the martensite to form the ε-carbides the overall hardness decreases as the tempering time increases. The main aim of the heat treatment is to modify the strength and toughness of the spring steels. Tempering of hardened steel reduces the brittleness or increase the toughness of the spring steel. So the tempering is selected in such a way to obtain the desired product required for automobiles.

3.2 Hardness Test

After the heat treatment the hardness is measured by using Rockwell c scale. The Figure 15 shows the decrease in hardness as we increase the tempering time. As expected the hardness of the hardened sample is high. The martensite formed due to heat treatment increases the hardness of the leaf spring sample. As we are tempering the sample the hardness of the sample goes on decreasing. This is due to the loss of carbon in the martensite due to formation of carbides.

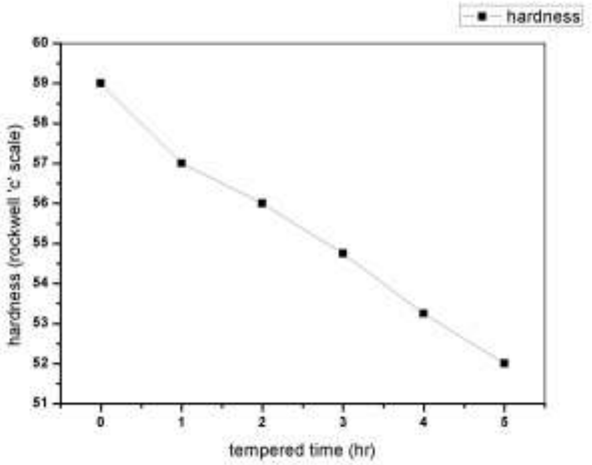


Figure 15. Variation of hardness with tempering time

3.3 Results Of Corrosion Tests

The Tafel Plots were drawn for each heat treated samples for different normalities of HCl solution as shown below.

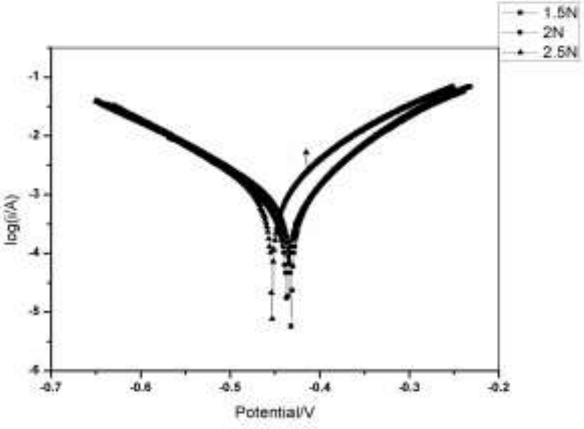


Figure 16. Tafel plot for the normalized sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

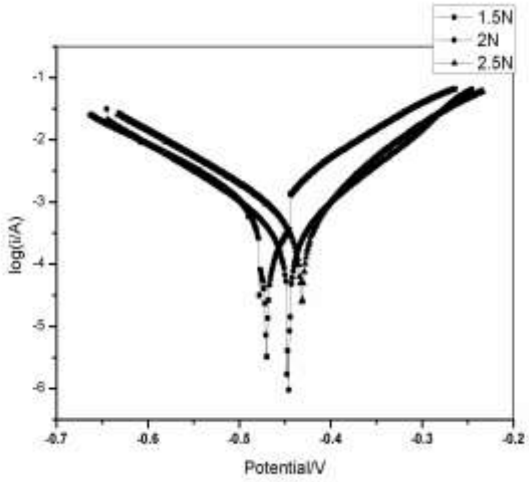


Figure 17. Tafel plot for the hardened sample. Plot is drawn for three normalities(1.5N,2N and 2.5N)

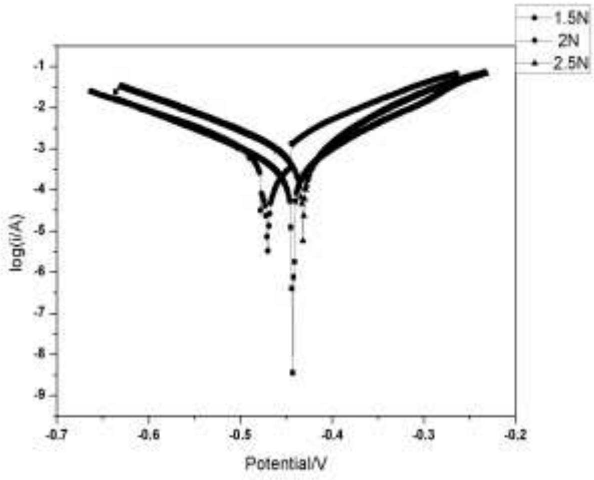


Figure 18. Tafel plot for 1 hr tempered sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

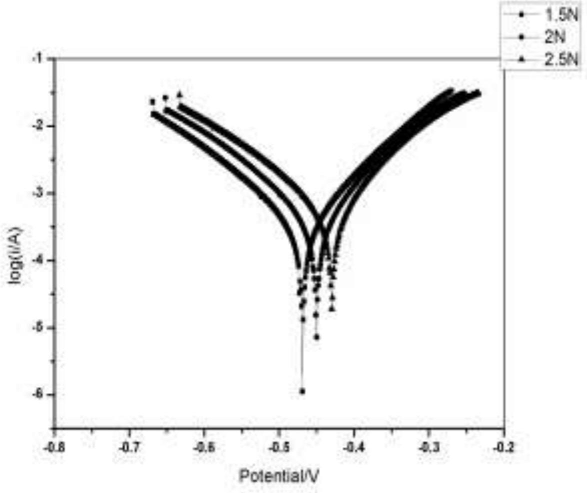


Figure 19. Tafel plot for the 2 hr tempered sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

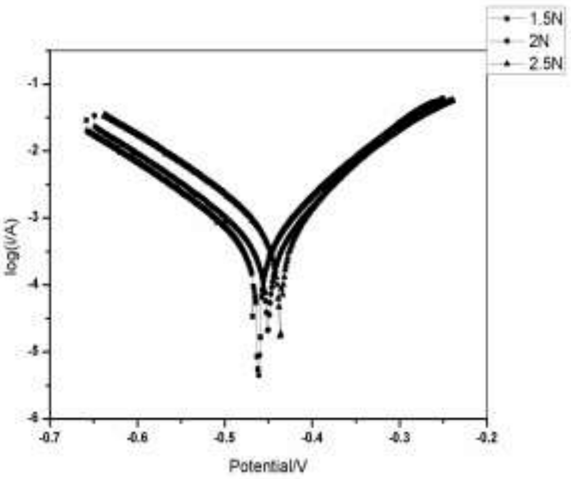


Figure 20. Tafel plot for the 3 hr tempered sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

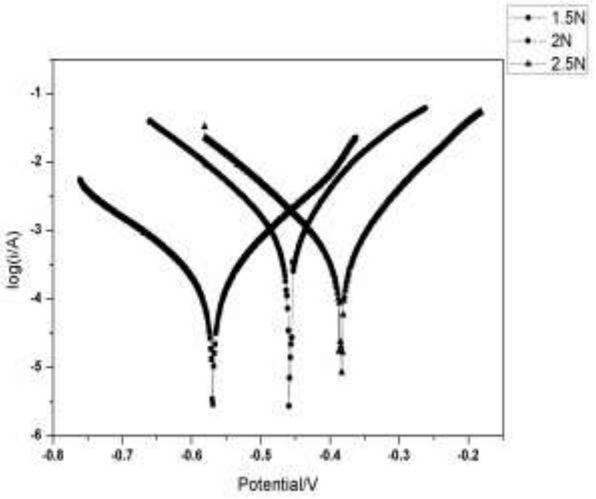


Figure 21. Tafel plot 4 hr tempered sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

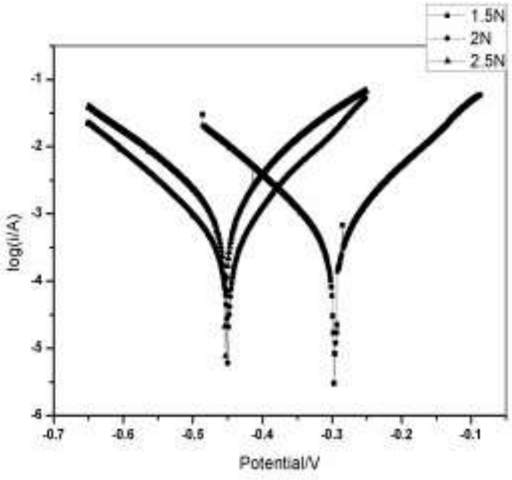


Figure 22. Tafel plot for the 5 hr tempered sample. Plot is drawn for three normalities(1.5N,2N and 2.5N).

From the Tafel plots it can be seen that the corrosion rates are increasing with the increase in normalities of hydrochloric acid and also the corrosion rates increases with the increase in the tempering time. As we can see the i_{corr} increases with the increase in normalities.

The corrosion rates for the hardened sample is minimum and the corrosion rate of 5 hour tempered sample is maximum. This is because during hardening the microstructure formed is martensitic and as tempering is done carbides start precipitating from the martensite and martensite changes to low carbon martensite. Due to presence of carbides it is more prone to corrosion.

The table 4.2 shows the corrosion rates obtained for various samples. From the table it can be seen that the corrosion rate is maximum for the 5 hour tempered sample. It is evident from the table that with increase in tempering time and the concentration of HCl the corrosion rate in spring steel is increasing.

Table 4.2 Corrosion rate of heat treated samples

Sl no	Type of sample	Corrosion rates(mpy)		
		1.5N	2N	2.5N
1	Hardened	9.97	10.63	17.22
2	Tempered for 1 hour	10.35	12.76	21.09
3	Tempered for 2 hour	13.10	13.97	22.35
4	Tempered for 3 hour	13.92	16.10	24.65
5	Tempered for 4 hour	13.69	17.86	24.20
6	Tempered for 5 hour	11.65	20.72	37.05
7	Normalized	22.25	23.33	37.52

Fig.4.23 & Fig.4.24 shows the variation of corrosion rate with tempering time and variation of corrosion rates with increase in concentration of HCl.

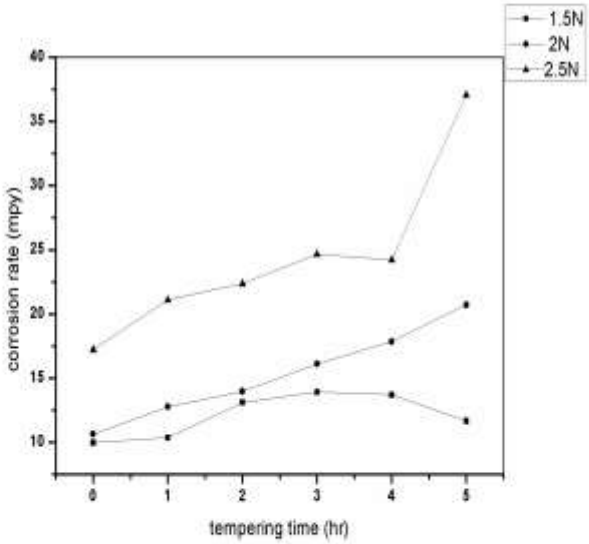


Figure 23. Variation in corrosion rates with tempering time.

It can be also seen that corrosion rates are increasing with increasing concentration.

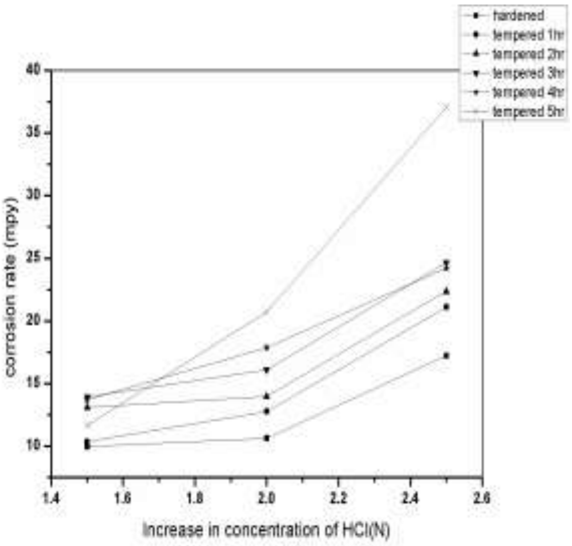


Figure 24. Corrosion rate with increase in concentration.

In a metal, anodic dissolution starts at the grain boundaries since they are amorphous regions and have high defect energy. Thus, the grain boundaries anodically dissolve as a function of time in an aggressive media having Cl– ions, and corrosion proceeds along the grain boundaries leaving the steel surface covered with corrosion products such as metallic oxides. In this case its inevitable that the original matrix loses weight. The grain boundaries rapidly react with aggressive Cl– ions and form pits. Therefore these regions can be seen as dark regions in the images of corroded sample [3].

As the time progresses, the amount of grain boundaries for anodic dissolution decreases and lath interfaces become new regions to be corroded. The ferrite phase which is having lower hardness behave as anode and cementite phase which is a kind of ceramic component behaves like cathode in corrosive media.

In the case of hardened spring steel there martensite and in some cases retained austenite will also be there, the retained austenite phase act as anode and the martensite which is having a body centered tetragonal structure act as cathode. The corrosion occurs only when both anodic and cathodic reactions are simultaneously taking place. If any of the reaction is delayed the corrosion rate decreases. In hardened case the carbon is not available for the cathodic reaction to take place. So the corrosion rate is very low.

In the case of normalized spring steel there will be only ferrite and pearlite present in the microstructure. So the ferrite will act as anode and cementite in pearlitic structure eases the cathodic reaction so corrosion rate is high in the case of normalized steel compared to hardened and tempered case.

In the case of tempered martensitic steels consist of ferrite laths and micron sized iron carbides and nano sized alloy carbides at the boundaries of laths or within the laths. In this case the corrosion rates gradually increases corresponding to tempering time, this is because on tempering it will form low carbon martensite(metastable state) and $Fe_{2.4}C$ and cathodic reaction takes place. As the tempering time increases the corrosion rate also increases.

4. CONCLUSION

The following conclusions can be drawn from the results obtained by experimental work:

1. The corrosion rate of spring steel increases with increase in concentration of corrosive media.

2. The hardened spring steel is having maximum corrosion resistance whereas the normalized sample shows least corrosion resistance.

3. The hardness of the spring steel decreases with increase in tempering time. This is due to loss of carbon in martensite.

4. The microstructure observation clearly shows that the corrosion is initiated in the grain boundaries and is propagated.

5. The corrosion of spring steel is increasing with increasing tempering time.

5. ACKNOWLEDGMENTS

We are grateful to Dr Jagatnath Naik, HOD, Department of Metallurgy and Materials Engineering NITK Surathkal Inda Inda, for his keen interest and support during the course of the investigation. Also the authors gratefully acknowledge the assistance provided by the Metallurgy department staffs of NITK surathkal India for carrying out heat treatments and corrosion experiments.

6. REFERENCES

[1] ASM Handbook. 2005. Volume 1, spring steels, ASM International, Ohio.

[2] ASM Handbook, 2005. Volume 13B, corrosion: Materials, ASM International, Ohio.

[3] Atapek,S.A, Seyda Polat and Sibel Zor.2013. "Effect of Tempering Temperature and Microstructure on the Corrosion behavior of a Tempered Steel" Protection of

Metals and Physical Chemistry of Surfaces, Vol. 49, No. 2, 240–246.

[4] Digges,T.G, Samuel, J. R, and Glenn ,W. G.1966. “Heat Treatment and Properties of Iron and Steel.” U.S. Government Printing Office, Washington, D.C. ,12-15.

[5] Fontana, M.G. and Greene, N. D.1978. Corrosion Engineering, McGraw Hill, USA.

[6] Fontana,M.G.1987. “Corrosion Engineering” McGRAW-HILL Series in Material Science and Engineering, 39-198.

[7] Gariboldi.E,Nicodemi,W,Silva,G. and Vedani,M.1994. “Mechanical Properties Of spring steels at room and low temperatures.”,11-14.

[8] Lee,C.S et al. 1998. “ Microstructural influence on fatigue properties of a high-strength spring steel.” J.Materials Science and Engineering A241,30-37.

[9] Podgornik,B.,Leskovšek,V.,Godec,M. and Senčič,B. 2014. “Microstructure refinement and its effect on properties of spring steel.” J.Materials Science and Engineering A599,81–86.

[10] Rajan,T.V, Sharma,C.P and Ashok Sharma. 2011. “Heat Treatment: principles and techniques” PHI learning private limited, New Delhi. Heat treatment processes for steel, 94-104.

[11] Sharma,S.S et al. 2013. “Effect of Heat Treatment on Mechanical Properties of AISI 4147 Spring Steel” 3rd International Conference on Mechanical, Automotive and Materials Engineering (ICMAME'2013) April 29-30,102-104.