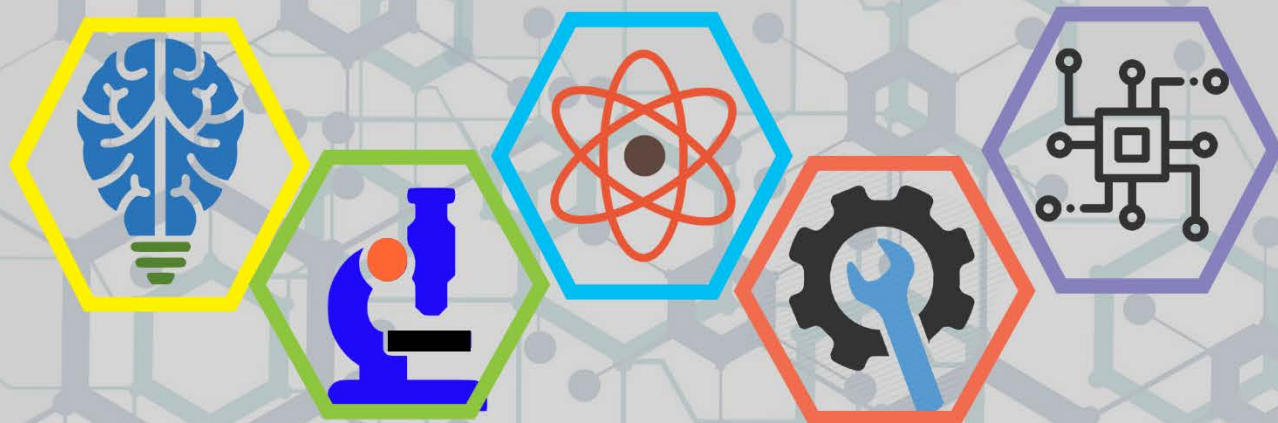


ISSN: 2687-2153

IJEIR

International Journal of Engineering & Innovative Research



Volume: 3 Issue: 2

International Journal of Engineering and Innovative Research (IJEIR)

Year: 2021

Volume: 3

Issue: 2

Editor in Chief

Dr. Ahmet Ali SÜZEN
Isparta University of Applied Sciences

Editorial Board Secretaries

Osman CEYLAN
Isparta University of Applied Sciences

Ziya YILDIZ
Isparta University of Applied Sciences

Correspondence Address

International Journal of Engineering and Innovative Research (IJEIR)
Secretaries Office
Isparta University of Applied Sciences
Uluborlu Selahattin Karasoy Vocatioal School
Uluborlu / Isparta / Turkey

Phone and e-mail

Tel: +90 0246 531 26 21 - 0246 531 26 22

E-mail: ijeirturkey@gmail.com

e-ISSN: 2687-2153

International Journal of Engineering and Innovative Research (IJEIR)

Year: 2021

Volume: 3

Issue: 2

Editorial Board

Prof. Dr. Narita Md Norwawi Universiti Sains Islam Malaysia University- MALAYSIAN
Prof. Dr. Shivam Mishra Dr. A.P.J. Abdul Kalam Technical University- INDIA
Prof. Dr. Fu Jianzhong Zhejiang University – CHINA
Prof. Dr.Hans-Jörg Trnka Fusszentrum Wien – AUSTRIA
Prof. Dr. Arif Emre ÖZGÜR Isparta University of Applied Sciences - TURKEY
Assoc. Prof Dr. Deniz KILINÇ İzmir Bakırçay University - TURKEY
Asst. Prof. Dr. Burhan DUMAN Applied Sciences University of Isparta - TURKEY
Dr. Merve VAROL ARISOY Mehmet Akif Ersoy University - TURKEY

Advisory Board

Prof. Dr. Kamaruzzaman Seman Universiti Sains Islam Malaysia University- MALAYSIAN
Prof. Dr. David HUI University of New Orleans- USA
Prof. Dr. Vladimir Jotsov University of Library Studies and IT - BULGARIA
Assoc. Prof Dr. Madiah MOHD SAUDI Universiti Sains Islam Malaysia - MALAYSIA
Assoc. Prof Dr. Azni Haslizan Ab Halim Universiti Sains Islam Malaysia - MALAYSIA
Asst. Prof. Dr. Ali Dinç American University of Middle East - KUWAIT
Dr. Fotis Kokkoras Technological Educational Inst. of Thessaly – GREECE

Reviewers for this issue

R AFOLABI
Ömer ÇOKAKLI
Remzi GÜRFİDAN
Ahmet Serdar GÜLDİBİ
Volkan EVRİN
Maher AL-MAGHALSEH
Özlem ÇALIŞKAN

Temitope OGUNKUNLE
İlker ERCAN
Özlem ALPU
Mehmet Ali ŞİMŞEK
Erhan KAHYA
Sameer KHADER
Kanat Burak BOZDOĞAN

International Journal of Engineering and Innovative Research (IJEIR)

Year: 2021

Volume: 3

Issue: 2

CONTENTS

PAGE

Research Articles

DESIGN AND IMPLEMENTATION OF A SOLAR PV MICROGRID: A CASE STUDY OF PALESTINE

Fouad Zaro , Ibrahim Kiriakos.....89-100

CORRELATIONS FOR ESTIMATING CHANGE IN RESIDUAL OIL SATURATION DURING LOW SALINITY WATER FLOODING

David Alaigba, Onaiwu Oduwa , Olalekan Olafuyi.....101-114

2k FACTORIAL EXPERIMENTS IN RELIABILITY ANALYSIS FOR WEIBULL AND LOG-NORMAL DISTRIBUTIONS

Berna Yazıcı , Beldine Omondi.....115-120

INTERNET SPEED ISSUE OF TURKEY

Hüseyin CEYLAN , Gizem DEMİR , Ziya ELRİ.....121-132

INVESTIGATION OF HOLE SHAPE EFFECT ON STATIC ANALYSIS OF PERFORATED PLATES WITH STAGGERED HOLES

Mustafa Halûk Saraçoğlu , Fethullah Uslu , Uğur Albayrak.....133-144

Review

SECURITY CONTROLS AGAINST MOBILE APPLICATION THREATS OF ANDROID DEVICES

Ahmet Efe, Şerife Özdamarlar.....145-162

A STUDY OF BLOCKCHAIN IN IOT ARCHITECTURE

Mehmet Ali Şimşek.....163-174



Research Article

DESIGN AND IMPLEMENTATION OF A SOLAR PV MICROGRID: A CASE STUDY OF PALESTINE

Authors: Fouad Zaro , Ibrahim Kiriakos 

To cite to this article: Zaro, F., Kiriakos, I., (2021). Design and Implementation of A Solar PV Microgrid: A Case Study Of Palestine, International Journal of Engineering and Innovative Research, 3(2), p 89-100.

DOI: 10.47933/ijeir.858179

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



International Journal of Engineering and Innovative Research

<http://dergipark.gov.tr/ijeir>

DESIGN AND IMPLEMENTATION OF A SOLAR PV MICROGRID: A CASE STUDY OF PALESTINE

Fouad Zaro^{1*}, Ibrahim Kiriakos¹

¹Palestine Polytechnic University, College of Engineering, Electrical Engineering Department, Hebron, Palestine.

*Corresponding Author: fzaro@ppu.edu
(Received: 11.01.2021; Accepted: 10.03.2021)

<https://doi.org/10.47933/ijeir.858179>

ABSTRACT: Microgrid is a power subsystem consist of small generators, storages and local loads. The attention to renewable resources and local generation is increasing for three important reasons: economics benefits, environmental matters and limits of fossil fuels. However, development of renewable resources in electrical power systems has been grown rapidly. Microgrid has the ability to support high power quality and sustainability with elimination of load shedding. This paper presents design and implementation of a real microgrid as per the recommended microgrid topology and dispatch methodology real Photovoltaic (PV) station with a local load using real data collected using different monitoring systems, the suggested microgrid is implemented and tested using MATLAB simulation tool, assuring power quality and sustainability, electrical and financial results are reported supporting this design. This study showed that implementing this sort of project can provide clean, economical, and continuous electricity production in countries with daily blackouts.

Keywords: Microgrid, PV System, Power quality, load shedding.

1. INTRODUCTION

Energy demand worldwide is increasing dramatically. CO₂ emissions is increasing with the electricity generation causing serious impact on environment. Intergovernmental panel on climate change (IPCC) and international energy agency (IEA) had put regulations to decrease CO₂ emissions, and the penetration of renewable resources start to increase annually [1].

Stability of power system requires the supply equals the demand, in conventional power system the supply can be controlled, while renewable energy cannot be controlled because it depends on climate changes and other aspects. At higher renewable penetration levels, the supply may exceed the demand, in this case the excess energy can be stored by using energy storage system (ESS), this energy can be used during on-peak times or as an emergency when the main grid is off [2].

Microgrid system which is a cluster of interconnected distributed generators (DG), loads and ESS that co-operate with each other to be collectively treated by the grid as a controllable load or generator. The Microgrid can operate in the islanded mode or the grid-connected mode. The microgrid system in the grid-connected mode either supply energy to the main grid or consume energy from it. The microgrid system must be able to separate or island itself from the main grid and supply the local load effectively when the power from the main grid is off or when the power quality of the main power source is poor. Many countries in the world encourage

applying the microgrid systems by assigning certain policies and in corporation with research institutes, universities and private sectors. However, there are two main standards for microgrids issues: IEC 61850-7-420 titled by "communications standard for distributed energy resources", and IEEE Std 1547.4™-2011 which is titled by " IEEE guide for design, operation, and integration of distributed resource island systems with electric power systems" [3-6].

The microgrid system of the university of California-San Diego (UcsD) is one of the famous practical experience implantations has a 42MW microgrid that self-generates 92% of its annual electricity load and 95% of its heating and cooling load, saves more than \$800,000 (USD) per month by using the generation on its microgrid comparing with being a direct consumer from the grid. Furthermore, it has the ability to supply the loads during the shading time with the aid of battery containers and microgrid controllers [7]. The new energy and industrial technology development organization (NEDO) in Japan had developed many microgrid projects connected with the national grid, to solve the effect of high penetration of renewable resources and to increase power quality [8].

Researchers and developers that are interested in microgrid systems focus their researches in the following fields:

- *Control strategies* is the main part of microgrid system, it controls the operation of microgrid components based on measurements. It classified according to the capacity of microgrid, load sharing, dynamic response, and grid complexity. Many methodologies implemented in this field from SCADA systems connected to local controller to one control unit for small scale microgrid (nano-grid) [9].
- *Effective energy storage systems* play an important role in restoring balance between supply and demand, has very fast dynamic response and encountered rapid developments. There are many types of storage systems which can be used in accordance with the scale of microgrid and operation response such as pumped hydropower storage, compressed air energy storage (CAES), flywheel, electrochemical batteries (lead-acid, NaS, Liion and Ni-Cd), flow batteries (vanadium –redox), superconducting magnetic energy storage, super capacitors, and hydro energy storage (power gas technologies) [10].
- *Power conversion* due to the fast development of semiconductor materials and decreasing of its cost with increasing its efficiency, power conversion has encountered rapid development [11].
- *Power quality and integration with the grid*: microgrid can improve power quality of the loads especially commercial industrial loads and maximize the profit of these loads [12].
- *DC microgrid systems* are more efficient comparing to AC systems, because there are no conversion losses, and less thermal losses comparing to AC microgrid [13].
- *Economic dispatch*: electricity prices are expensive because it depends on many factors such as running cost of generators and grid and other economic aspects, so supply the load with own generated power will be more feasible [14].

This paper presents a real case study for designing a real microgrid system based on real collected data for a part of Jerusalem District Electricity Company (JDECO) system, the details of the presented case study are as follow: JDECO has a PV station consists of 13 inverters of 60kW each, with 2360 panels occupied with 10000m² land, tilt angle of 15°, Latitude 32 1'17.83" N, Longitude 35° 26' 26.23" E. The station is connected to the 33kV medium voltage grid. The main objective of this study is converting the established PV station with the interconnected critical load part to a microgrid system with minimum cost, sustainability and good power quality as well.

The organization of the rest of the paper is as follows: section 2 provides the methods, adopted scenarios, data, the assessments of the proposed scenarios, cases of work strategies, and how the data have been collected. In section 3, the simulation results and discussion of different scenarios are presented. The economic dispatch of the proposed system is explained in section 4. Finally, the conclusions are depicted in section 5.

2. METHODS AND DATA

This paper proposed a real microgrid system for the residential load of a transformer 250kVA allocated about 5km from the PV station through the medium voltage line, and this paper studies the PV energy profile as well. Figure 1 presents the general scheme of the interconnection between PV station and the selected distribution transformer that will be the load of the proposed microgrid.

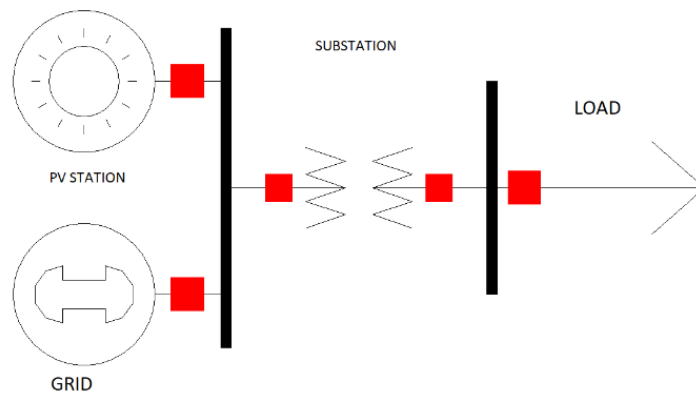


Figure 1. Interconnection between PV station and distribution transformer.

Three different feasible scenarios have been proposed to modify the PV station from on grid station to a microgrid station supplying the target load 24 hours 365 days and the optimum scenario will be implemented, in all scenarios the controller will connect and discount circuit breakers managing the operation of PV and ESS and LOAD and GRID as shown in Figure 2.

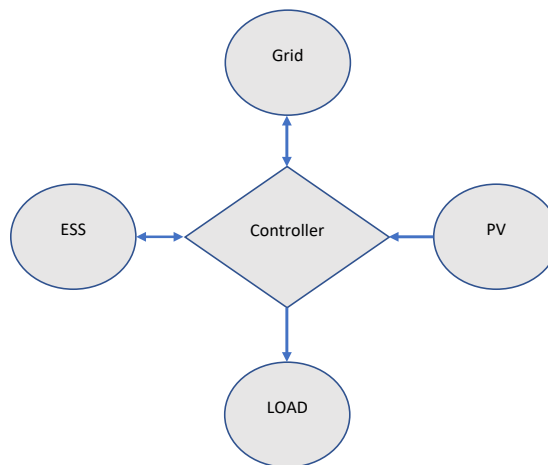


Figure 2. Block Diagram of the Proposed Microgrid System.

The presented three scenarios:

- **Scenario 1**

Dividing the existing PV station into two stations; ON grid station and OFF grid station with same panels ,by adding ESS working with main controller connected to MV Circuit breakers and adding OFF Grid inverters with power of 300kW peak to the existing PV station , and DC circuit breakers connected to the strings , when the power is on the station will work as ON grid station , when the power is off the controller will disconnect the MV circuit breakers and DC circuit breakers connected to On grid inverters ,after that will connect the DC circuit breakers connected to OFF grid inverters and the station will work as OFF Grid station, the ESS system in this case is the main supply of power , the topology of the system is shown in Figure 3.

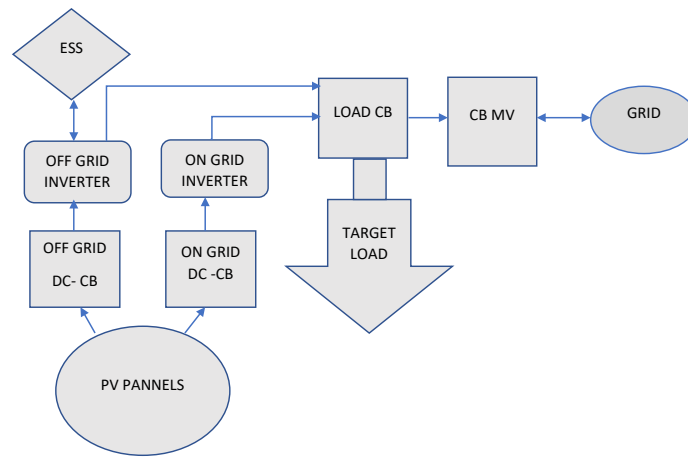


Figure 3. Scenario 1.

• Scenario 2

Dividing the existing PV station into two station; ON grid station and Microgrid station with same panels by adding ESS working with main controller connected to MV Circuit breakers and adding Microgrid inverters with power of 300kW peak to the existing PV station, and DC circuit breakers connected to the strings , when the power is on the station will work as ON grid station, when the power is off the controller will disconnect the MV circuit breakers and DC circuit breakers connected to on grid inverters ,after that will connect the DC circuit breakers connected to Microgrid inverters, ESS will share the supply of power with PV, the topology of the system is shown in Figure 4.

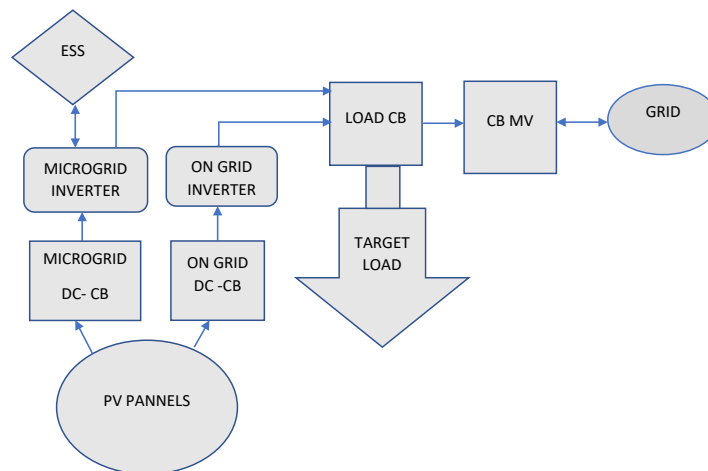


Figure 4. Scenario 2.

• Scenario 3

Modifying the existing PV station into two station , On grid station and Microgrid station with same panels, by adding ESS System working with main controller connected to MV Circuit breakers and changing 5 On-Grid inverters to Microgrid inverters , when the power is On the station will work as On grid station, when the grid is off the controller will disconnect the circuit breakers connected to MV circuit breakers and AC circuit breaker connected to the inverters that already exist in the station , the topology of the system is shown in Figure 5.

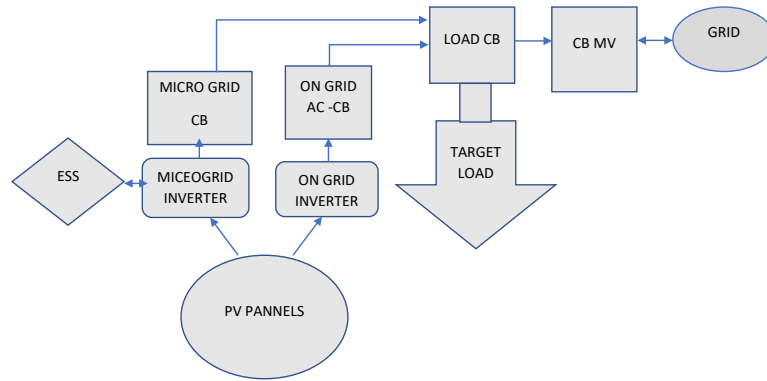


Figure 5. scenario 3.

The storage system has the major cost, it is not economically feasible to use ESS as the main supply to the load. It is more desirable to supply the load from PV system and the shortage covered from ESS system or to cover the whole load during emergency time, thus the scenarios 1 and 2 are not economically feasible. On the other hand, the scenario 3 is economically feasible and applicable just by changing 5 inverters with 300 kW peak and controlling the ac circuit breakers only.

Data are collected using POWERCOM monitoring system for demand and GREENPOWER monitoring system for PV station, these data were not organized on hourly basis, effort were done to reorganize this data on hourly basis for 24 hours and 365 days.

The maximum recorded load for the selected transformer is 200 kW for 1 hour, while the average load is around 100 kW, for the proposed microgrid system no need to use all the battery power, in worst case with no sunshine and no grid a 300 kW battery power is efficient and safe, the depth of discharge in worst case is 67% with average load and 34% with maximum load.

There are 3 variable inputs: demand, PV power and grid power; the demand is dynamically changing over the day, while PV power changes based on weather conditions and the amount of dust over PV panels and temperature and radiation, however, sometimes the grid power is off because of the faults that occur suddenly on the grid or scheduled maintenance of medium voltage stations and lines.

There are 4 calculated outputs which are as follow:

1. Calculating the amount of energy bought from IEC

- If Demand + Bat charge > PV power and the Grid is ON, the amount of electricity bought = demand -PV + Bat charge (This statement give priority to charge the batteries from PV).
- If Demand < PV power and the Grid is ON, the amount of electricity bought = ZERO
- If Demand < PV power OR Demand > PV power and the Grid is OFF, the amount of electricity bought = ZERO

2. Calculating the amount of energy sold to consumers
 - If Demand > PV power and the Grid is ON, the amount of electricity sold = ZERO
 - If Demand+ Bat charge < PV power and the Grid is ON, the amount of electricity sold = PV -demand – Bat charge (This statement give priority to charge the batteries from PV).
 - If Demand < PV power OR Demand > PV power and the Grid is OFF, the amount of electricity sold= ZERO
3. Battery discharging
 - If the Grid is Off and PV < Demand, the amount of discharged power = demand -PV
 - If the Grid is Off and PV > Demand, the amount of discharged power = Zero
 - If the Grid is ON and PV > Demand, PV < Demand, the amount of discharged power = Zero
4. Battery charging
 - If battery is discharged and the Grid is ON, Battery charging = Battery discharging

The logic statement chart is shown in Figure 6.

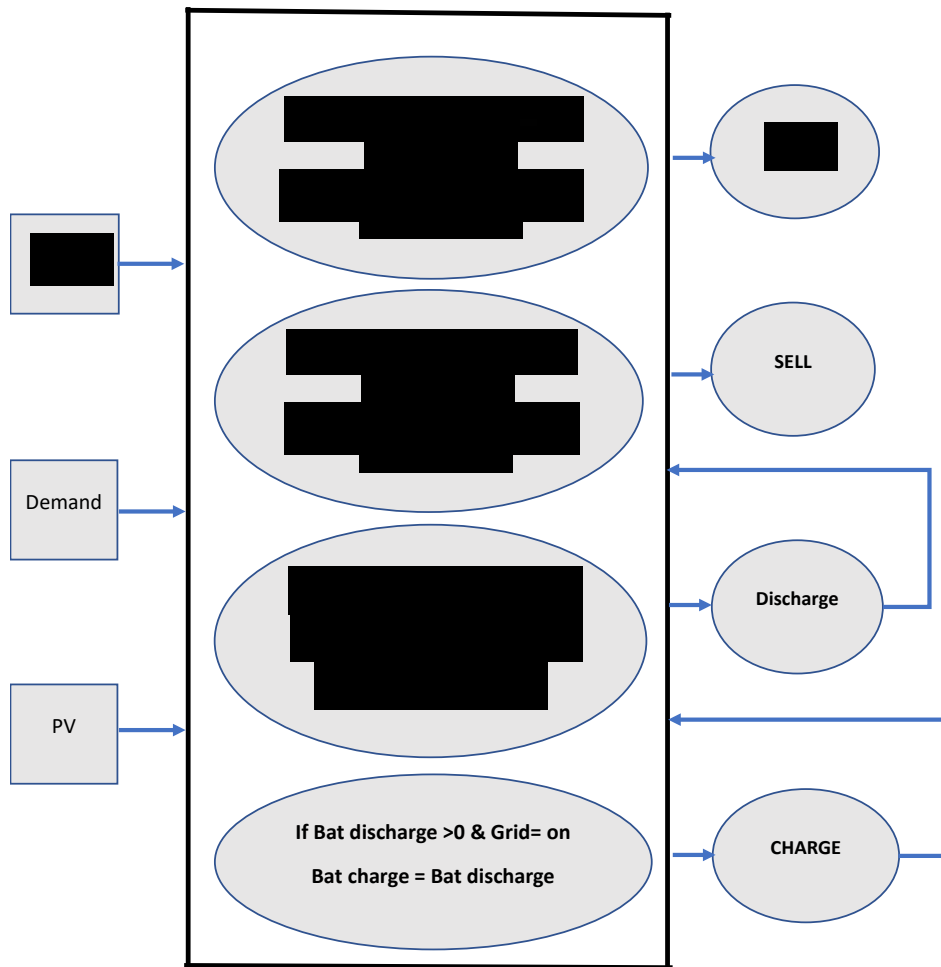


Figure 6. Logic statement chart.

There are three different cases for the proposed system as follows:

- Case 1:** If the Demand equal 50kW and PV energy equal 100kW and the grid is On,
- Energy sold =50 kWh

- Energy bought = ZERO
- Battery discharged = ZERO
- Battery charged = ZERO

Case 2: If the Demand equal 50kW and PV energy equal 100kW and the grid is Off

- Energy sold =ZERO
- Energy bought = ZERO
- Battery discharged = ZERO
- Battery charged = ZERO

The load is totally supplied by PV energy

Case 3: If the Demand equal 50kW and PV energy equal 40kW and the grid is Off

- Energy sold =ZERO
- Energy bought = ZERO
- Battery discharged = 10kWh
- Battery charged = ZERO

The load is supplied by PV energy and batteries

3. SIMULATION RESULTS

The main block diagram of the proposed model is shown in Figure 7, the PV system is divided into two systems PV microgrid system connected to CB-MG (circuit breaker microgrid) and PV On Grid system connected to CB-OG (circuit breaker on grid), CB1 (circuit breaker 1) is used to island the target load from the grid.

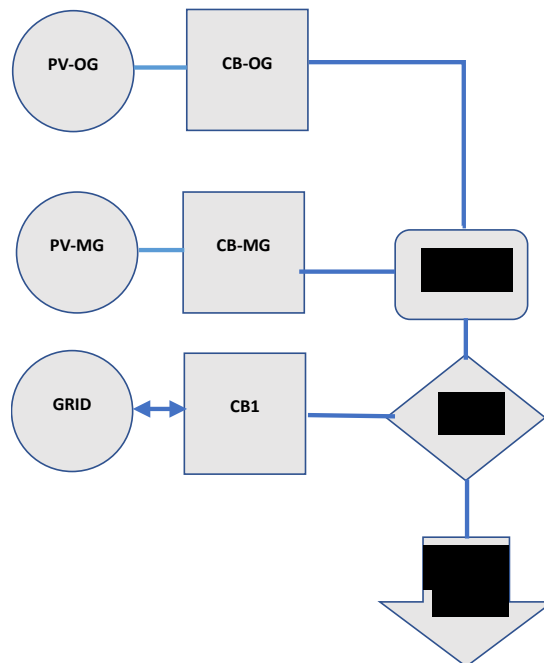


Figure 7. Main block diagram of the proposed model.

This microgrid has two operation modes, depending upon the measurement of RMS current and THD, the added controller has input from measurement unit and based on this measurement the controller will operate according to the flowchart shown in Figure 8.

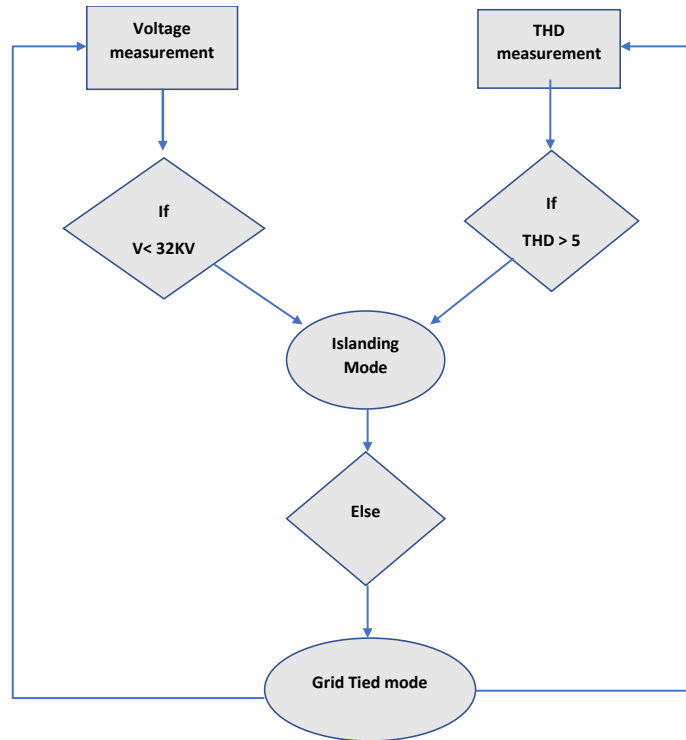


Figure 8. Controller operation flow chart.

The modes of operation are described as follow:

- **Grid tied mode:** In this mode, the controller is just monitoring the grid and THD of the target load, all the circuit breakers are on.
- **Islanding mode:** The microgrid will go to islanding mode when the grid is off or when THD larger than 5%.
- **Islanding mode, grid off:** when the grid is off, the controller will open CB1 and CB-OG which are shown in figure 7, then supplying the power to the target load using the microgrid. The current from the grid is shown in Figure 9 over 10 seconds of simulation time, the target load voltage before improving the system is shown in Figure 10, after improving the system the target load is shown in Figure 11.

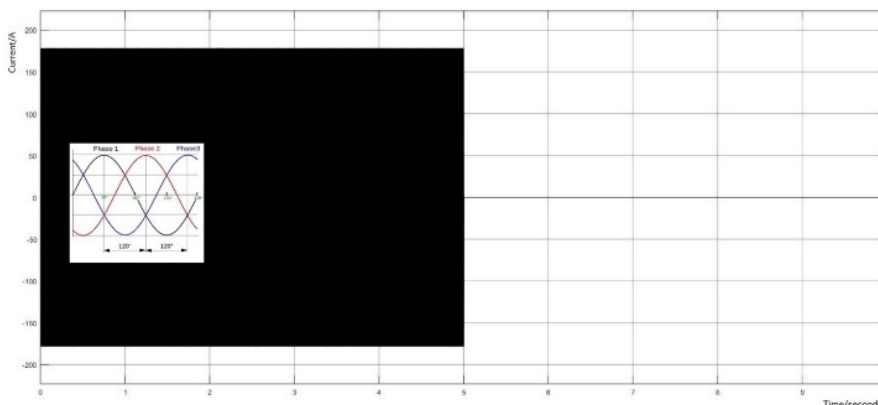


Figure 9. The current of the main grid.

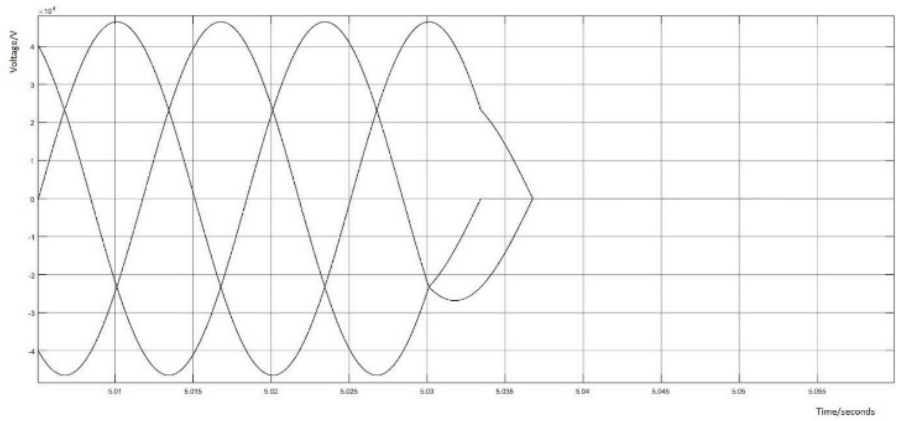


Figure 10. Load voltage without microgrid operation.

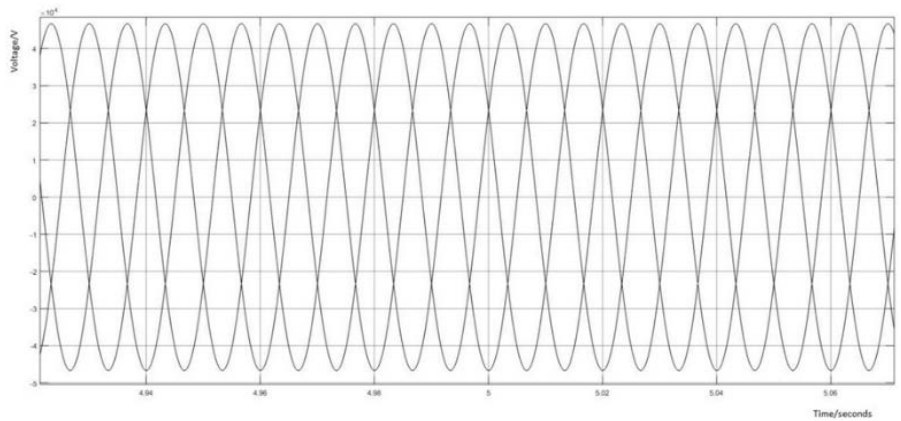


Figure 11. Load voltage with microgrid operation.

As shown in Figure 9 the grid is off after 5 seconds, without operating the system, the load also will be off as shown in Figure 10, operating microgrid system will keep supplying the load with energy as shown in Figure 11.

- Islanding mode improving THD:** In this mode if the THD is greater than 5% the controller will open CB1 and CB-OG which are shown in figure 7, thus supplying the target load using microgrid system, where the THD of the grid is shown in Figure12, and the THD of the load is shown in Figure 13.

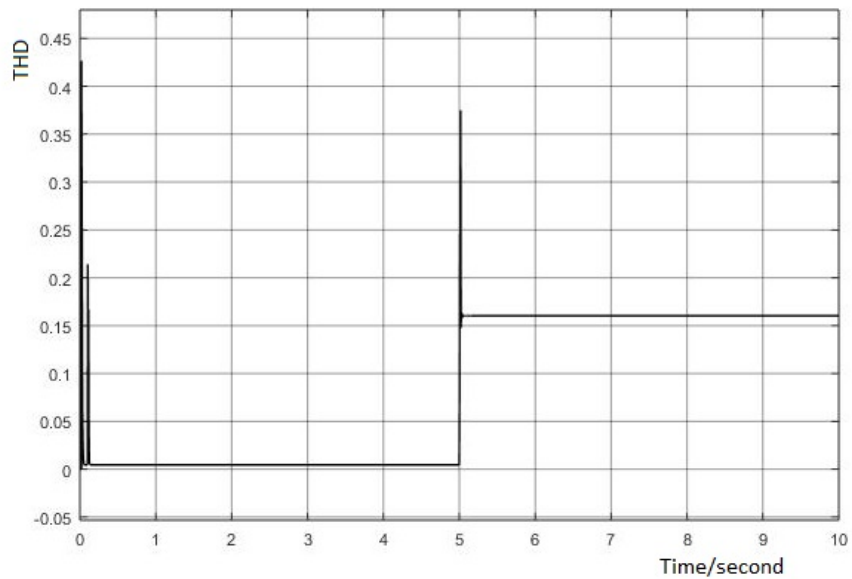


Figure 12. THD of the Grid.

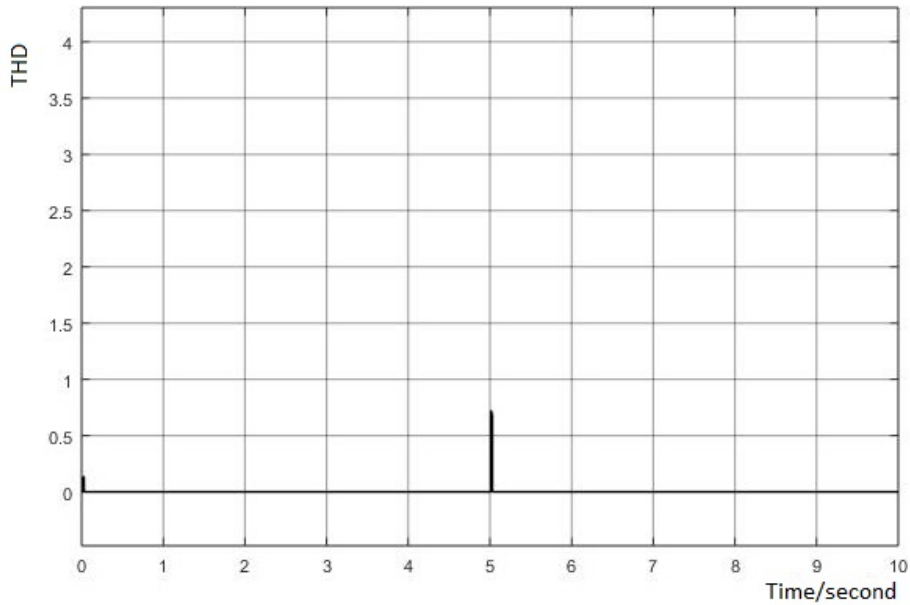


Figure 13. THD of the target load.

Usually, the THD is variable and depends on other loads connected to the grid, Figure 12 shows at 5 seconds some undesirable loads enter the grid, disconnecting the grid and operating in islanding mode will be good solution to improve the THD as shown in Figure 13.

4. ECONOMIC DISPATCH

After running the system, the total amount of energy bought and sold, using microgrid operation for every month is shown in Figure 14.

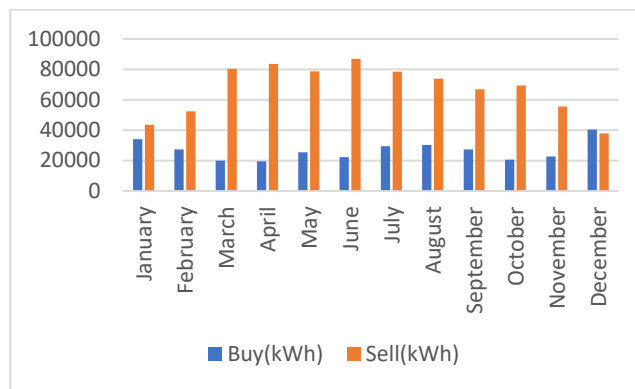


Figure 14. Energy bought and sold in 2018.

Microgrid system supply the target load 365 days 24 hours, and the excess energy is sold to the grid, which increases the revenue, the expenses depend on the amount of energy bought from IEC, the buying tariff from IEC in 2018 is 0.371 NIS, and the selling tariff is 0.5448 NIS, Figure 15 shows the expenses vs revenue monthly, they are calculated using the following formulas.

$$Expenses = amount\ of\ energy\ bought * buying\ tariff$$

$$Revenue = (amount\ of\ energy\ sold\ to\ the\ grid + demand) * selling\ tariff$$

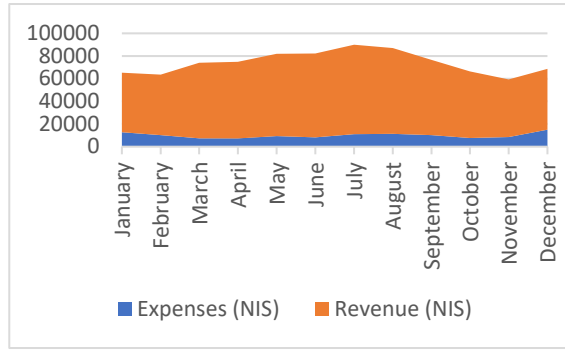


Figure 15. Expenses vs revenue.

The monthly profit with microgrid implementation equals revenue minus expenses minus battery usage factor which is 6562NIS/month based on practical experience, profit without microgrid implementation equals demand multiplied by the difference between selling and buying tariff, if the grid is on. Figure 16 shows the profit comparison between microgrid operation and supplying the load without using microgrid.

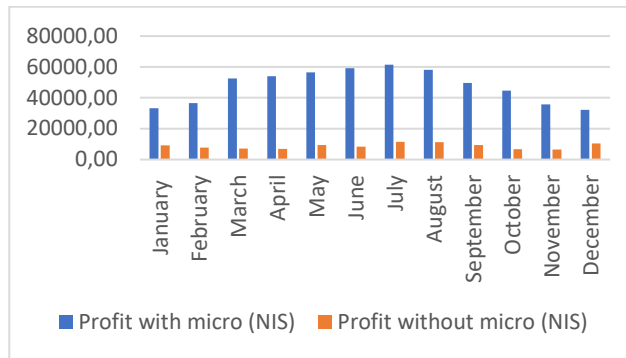


Figure 16. Profit comparison.

The cost of the station contains the fixed cost and running cost and modification cost, it is shown in Table 1.

Table 1. Total cost.

Item	Cost US \$
Old station	700,000
Inverters	45,000
Controller and accessories	20,000
Running cost for 5 years	35,000
Sum	800,000

With a degradation factor the profit will be minimized for every year, Table 2 shows the profit for 5 years with degradation factor of 1%.

Table 2. Five years' economic dispatch.

Year	Profit (US \$)
1	164,045
2	162,405
3	160,781
4	159,173
5	157,581
Total	803,985

Based on the above data, the payback period is within 5 years with overall station cost of \$800,000 USD and degradation factor of 1%.

5. CONCLUSIONS

Design and implementation of a real microgrid based on real data and as per the recommended microgrid topology and dispatch methodology is proposed in this paper. The proposed microgrid achieved good power quality and sustainability by eliminating load shedding for the selected load as well as economic benefits with a payback period of fewer than five years and increasing the reliability of the system. This study aimed to analyze the techno-economic and environmental feasibility of a solar PV microgrid system that is able to supply the load during both grid availability and outage periods and showed that implementing this sort of project can provide clean, economical, and continuous electricity production in countries with daily blackouts. A section of household in Jericho was selected as a case study.

REFERENCES

- [1] Hatziargyriou N, Asano H, Iravani R, Marnay C, (2007). Microgrids, *IEEE Power Energy Magazine*, 5 (4) 78–94.
- [2] Svetec E, Nađ L, Pašičko R, Pavlin B, (2019). Blockchain application in renewable energy microgrids: an overview of existing technology towards creating climate-resilient and energy independent communities. *16th International Conference on the European Energy Market (EEM)*, pp. 1-7.
- [3] Neto P, Barros T, Silveira J, Filho E, Vasquez J and Guerrero J, (2020). Power Management Strategy Based on Virtual Inertia for DC Microgrids. in *IEEE Transactions on Power Electronics*, vol. 35, no. 11, pp. 12472-12485, Nov. 2020, doi: 10.1109/TPEL.2020.2986283.
- [4] Kroposki B, Basso T, DeBlasio R, (2008). Microgrid standards and technologies. *Proceedings of IEEE Power & Energy Society 2008 General Meeting: Conversion & Delivery of Electrical Energy in the 21st Century*.
- [5] Martin-Martínez F, Sánchez-Miralles A, Rivier M, (2016). A literature review of microgrids: a functional layer-based classification. *Renewable Sustainable Energy Rev*, 62:11, 33–53.
- [6] Meng L, Sanseverino E, Luna A, Dragicevic T, Vasquez J, Guerrero J, (2016). Microgrid supervisory controllers and energy management systems: a literature review. *Renewable Sustainable Energy Rev*, 60:12, 63–73.
- [7] Washom B, Dilliot J, Weil D, Kleissl J, Balac N, Torre W, and Richter C, (2013). Ivory tower of power: microgrid implementation at the University of California, San Diego. *IEEE Power and Energy Magazine*, vol. 11, no. 4, pp. 28-32.
- [8] Morozumi S, (2007). Micro-grid demonstration projects in Japan. in *Proceeding 4th Power Conversion Conference*, Japan, 635–642.
- [9] Rocabert J, Luna A, Blaabjerg F, and Rodriguez P, (2012). Control of power converters in AC microgrids. *IEEE Transactin. Power Electronics*, vol.27,no. 11, pp. 4734–4749.
- [10] Farrokhhabadi M, Koenig S, Canizares C, Bhattacharya K, and Leibfried T, (2018). Battery energy storage system model for microgrid stability analysis and dynamic simulation. *IEEE Transaction. Power Systems*, Vol. 33, No. 2, pp.2301-2312.
- [11] Dong X, Li X. and Cheng S, (2020). Energy Management Optimization of Microgrid Cluster Based on Multi-Agent-System and Hierarchical Stackelberg Game Theory. in *IEEE Access*, vol. 8, pp. 206183-206197,doi: 10.1109/ACCESS.2020.3037676.
- [12] Alqam S, Zaro F, (2019). Power Quality Detection and Classification Using S-Transform and Rule-Based Decision Tree. *International Journal of Electrical and Electronic Engineering & Telecommunications* Vol. 8, No. 1, 45-50.
- [13] Nasir M, Khan H, Hussain A, Mateen L, and Zaffar N, (2018). Solar PV-Based Scalable DC Microgrid for Rural Electrification in Developing Regions. *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 390-399.
- [14] Palma-Behnke R, Benavides C, Lanás F, Severino B, Reyes L, Llanos J, et al., (2013). A microgrid energy management system based on the rolling horizon strategy,” *IEEE Transaction Smart Grid*, vol. 4, no. 2, pp. 996–1006.



Research Article

CORRELATIONS FOR ESTIMATING CHANGE IN RESIDUAL OIL SATURATION DURING LOW SALINITY WATER FLOODING

Authors: David Alaigba*, Onaiwu Oduwa , Olalekan Olafuyi 

To cite to this article: Alaigba, D., Oduwa, O., Olafuyi, O., (2021). Correlations for Estimating Change in Residual Oil Saturation During Low Salinity Water Flooding, *International Journal of Engineering and Innovative Research*, 3(2), p 101-114.

DOI: 10.47933/ijeir.838245

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



CORRELATIONS FOR ESTIMATING CHANGE IN RESIDUAL OIL SATURATION DURING LOW SALINITY WATER FLOODING

David Alaigba^{1*}, Onaiwu Oduwa¹, Olalekan Olafuyi¹

¹University of Benin, Faculty of Engineering, Petroleum Engineering, Benin-City, Nigeria.

*Corresponding Author: david.alaigba@gmail.com

(Received: 09.12.2020; Accepted: 17.02.2021)

<https://doi.org/10.47933/ijeir.838245>

ABSTRACT: Prior to embarking on a laboratory and subsequently pilot test for a potential improved oil recovery scheme in a green or brown field, it is important to have a sense of potential gains from the available options. This is usually done using correlations. Whereas there had been existing models for use in making these approximations, this work has developed a robust correlation for use in estimating the potential reduction in residual oil saturation post Optimized Salinity Water flooding (OPTSWF) (and consequently additional recovery) as a function of change in Interfacial tension (IFT), change in salinity, porosity, permeability, start residual oil saturation, and API gravity of the crude oil. This was done for a field in the Niger Delta. The model was tested against available data and showed good correlation with a correlation coefficient ranging from 99.36% to 99.89%. Also, the performance of the model was tested alongside that proposed by Tripathy et. al and in all cases, the model developed by this work performed better with lower RMS errors.

Keywords: Improved Oil Recovery, Optimized Salinity Water flooding, Niger Delta, Modeling.

1. INTRODUCTION

Water flooding is a secondary recovery scheme employed for optimal development of oilfields. This practice dates as far as the 1800s [1] Owing to its relative abundance, seawater with some treatment (for compatibility and to prevent formation damage) is one of the fluids employed for the injection.

The process typically entails the injection of water using dedicated injection wells for the following benefits:

- Voidage replacement leading to reservoir pressure maintenance
- Better volumetric sweep efficiencies
- Improved reserves, recoveries and project economics
- Effective management of produced water
- Energy security for coming generations
- Improved geomechanics or prevention of subsidence resulting from formation compaction (In cases where formations have high compressibilities)

Water flooding is a secondary recovery scheme which involves the injection of water into the reservoir to supplement the primary reservoir energy lost due to production by maintaining the reservoir pressure and also sweeping more oil towards the production wells. This has resulted

in improving recoveries up to 40-60% of the original oil in place [2]. Figure 1 depicts a typical water flooding scheme with surface and Sub-Surface processes.

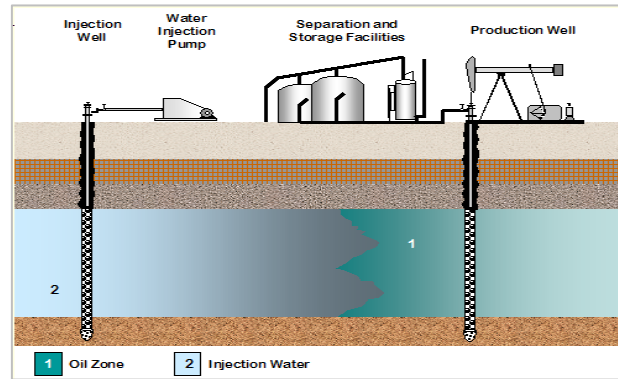


Figure 1. Waterflooding Schematic.

Low Salinity Waterflooding (LSWF), entails the use of diluted/Low Salinity Water (LSW) (500ppm-5000ppm of total dissolved solids) for injection instead of conventional sea water (35000ppm) or reservoir brine. Other names for LSWF in literature include; Smart Waterflooding, LoSal, Advanced Ion Management or Ion Tuning [3]. The author prefers to refer to the process as **Optimized Salinity Water Flooding (OPTSWF)**.

Among many attempts which have been made to model the effects of LSWF, the one proposed by Jerauld et al. [4] stands out. Their model which is based on the results of several core flood studies involving varying salinities of injection and connate brine. They observed that above and below a certain High Salinity (HS) and Low Salinity (LS) threshold, the injection brine salinity had no effect on oil recovery. The model assumes a linear dependence of relative permeability and capillary pressure on salinity between the thresholds. Equations 1 to 4 spell out the relationships. These equations have been successfully applied to history match LSWF experiments and field observations, [4, 5].

$$k_{rw} = \theta k_{rw}^{HS}(S^*) + (1 - \theta)k_{rw}^{LS}(S^*) \quad (1)$$

$$k_{row} = \theta k_{row}^{HS}(S^*) + (1 - \theta)k_{row}^{LS}(S^*) \quad (2)$$

$$P_{cow} = \theta P_{cow}^{HS}(S^*) + (1 - \theta)P_{cow}^{LS}(S^*) \quad (3)$$

$$\theta = \frac{S_{orw} - S_{orw}^{LS}}{S_{orw}^{HS} - S_{orw}^{LS}} \quad (4)$$

$$S^* = \frac{S_o - S_{orw}}{1 - S_{wr} - S_{orw}} \quad (5)$$

Tripathi and Mohanty, [6] in their attempt to model the LSWF process also adopted a linear dependence of relative permeability's, residual oil saturation and Corey's oil exponent on salt concentration. They then validated their model by using experimental data.

$$S_{or}(X_c) = S_{or}^{LS} + \frac{X_c - X_c^{LS}}{X_c^{LS} - X_c^{HS}} (S_{or}^{LS} - S_{or}^{HS}) \quad (6)$$

$$k_{rw}(X_c) = k_{rw}^{LS} + \frac{X_c - X_c^{LS}}{X_c^{LS} - X_c^{HS}} (k_{rw}^{LS} - k_{rw}^{HS}) \quad (7)$$

$$n_o(X_c) = n_o^{LS} + \frac{X_c - X_c^{LS}}{X_c^{LS} - X_c^{HS}} (n_o^{LS} - n_o^{HS}) \quad (8)$$

In applying the above models, Tripathi et al., [6] used Corey's equation [7] to model relative permeability and that of Skjaeveland [8] to generate capillary pressure curves. Relative permeabilities can also be derived using the Johnson-Bossler-Naumann (JBN) method or and the Jones and Roszelle (JR) technique from unsteady state flow experiments like core flooding, [9].

$$k_{rw} = k_{rw}^o (S_w^*)^{n_w} \quad (9)$$

$$k_{ro} = k_{ro}^o (1 - S_w^*)^{n_o} \quad (10)$$

$$S_w^* = \frac{S_w - S_{wr}}{1 - S_{wr} - S_{or}} \quad (11)$$

$$P_c = \frac{c_w}{\left(\frac{S_w - S_{wi}}{1 - S_{wi}}\right)^{a_w}} - \frac{c_o}{\left(\frac{1 - S_w - S_{or}}{1 - S_{or}}\right)^{a_o}} \quad (12)$$

Whereas many authors have attributed the observed LSE to an interplay of forces within the COBR system, both models do not account for the crude oil properties, pore structure parameters (porosity and permeability) and crude-brine interfacial tension, IFT.

More so, the current modeling approach of LSWF in literature is based on a linear dependence of rock and fluid properties on salinity, [6, 4]. The adoption of a linear relationship while easy to implement can lead to over simplification. It would be interesting to explore alternative and improved models and compare the obtained results with that currently in use.

Also, Al-Shalabi and Sepehrnoori [10] stressed that in modeling LSWF, emphasis should be placed on the oil composition so as to take into account possible reactions that could impact on the outcome of the LSWF scheme.

The objective of this research work is to develop robust correlations which incorporates parameters linked with the crude oil, water and rock properties for use in estimating the performance of OPSWF at the core scale. These correlations can then be used to screen potential OPSWF candidate fields before embarking on the expensive and time consuming laboratory experiments and pilot tests.

2. METHODOLOGY

This research adopted a mathematical modelling framework for use in obtaining robust correlations.

As emphasized by [11] the following parameters have been identified as impactful to the observed LSE effect in Niger Delta system;

- i. Change in IFT, ΔIFT

- ii. Change in Salinity, ΔSAL
- iii. PV of injected brine, PV_{inj}
- iv. Porosity of core, ϕ
- v. Core Permeability, K
- vi. Oil Saturation at start of OPTSWF S_{os} and
- vii. API gravity of crude oil. API

The formulation of the proposed equation is presented as:

$$\Delta S_{or} = C_0 + C_1(\Delta SAL)(\Delta IFT) + C_2 PV_{inj} + C_3 K^\phi + C_4 API^{S_{os}} \quad (13)$$

Where C_0, C_1, C_2, C_3 and C_4 are empirical constants derived from regressing OPTSWF experimental data.

$$\Delta S_{or} = C_0 + C_1 X_1 + C_2 X_2 + C_3 X_3 + C_4 X_4 \quad (14)$$

Where $X_1 = (\Delta SAL)(\Delta IFT), X_2 = PV_{inj}, X_3 = K^\phi, X_4 = API^{S_{os}}$

Discretizing,

$$\Delta S_{ori} = C_0 X_{0i} + C_1 X_{1i} + C_2 X_{2i} + C_3 X_{3i} + C_4 X_{4i} \quad (15)$$

For a data set of $i = 1$ to n , we have an n by 5 matrix for ΔS_{ori} .

Let X equal to the $n \times 5$ matrix containing X_{01} to X_{4n} .

$$X = \begin{bmatrix} X_{01} & X_{11} & X_{12} & X_{13} & X_{14} \\ X_{02} & X_{21} & X_{22} & X_{23} & X_{24} \\ X_{03} & X_{31} & X_{32} & X_{33} & X_{34} \\ \dots & \dots & \dots & \dots & \dots \\ X_{0n} & X_{n1} & X_{n2} & X_{n3} & X_{n4} \end{bmatrix}$$

Let C be equal to a vector containing C_0, C_1, C_2, C_3 and C_4

$$C = \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix}$$

Let y be the vector of experimental observations of ΔS_{ori} ($i = 1$ to n).

$$y = \begin{bmatrix} \Delta S_{or1} \\ \Delta S_{or2} \\ \Delta S_{or3} \\ \dots \\ \Delta S_{orn} \end{bmatrix}$$

To solve for the constants C_0, C_1, C_2, C_3 and C_4 , we can make use of the normal equation [12] as follows;

$$C = (X^T X)^{-1} \cdot (X^T y) \quad (16)$$

2.1. Data for Study

The data for study were sourced from [11] and is presented in Table 1 and **Error! Reference source not found..** It can be observed that $n = 16$.

Table 1. Raw Experimental Data.

S/NO	SALT	ΔIFT	ΔSAL	PVINJ	K	PHI	API	SOS	ΔSOR	DRF
1	NACL	62.60	5000.00	1.00	298.10	0.20	26.25	0.51	0.08	0.09
2	NACL	60.50	2500.00	0.50	298.10	0.20	26.25	0.51	0.02	0.03
3	NACL	58.50	1000.00	0.50	298.10	0.20	26.25	0.51	0.04	0.04
4	NACL	55.30	625.00	0.38	298.10	0.20	26.25	0.51	0.01	0.01
5	K2SO4	55.30	5000.00	1.65	274.00	0.23	26.25	0.63	0.10	0.10
6	K2SO4	54.60	2500.00	1.05	274.00	0.23	26.25	0.63	0.04	0.04
7	K2SO4	54.50	1000.00	0.60	274.00	0.23	26.25	0.63	0.01	0.01
8	K2SO4	52.60	625.00	0.45	274.00	0.23	26.25	0.63	0.01	0.01
9	CACL2	51.90	5000.00	1.77	268.00	0.22	26.25	0.62	0.19	0.21
10	CACL2	46.50	2500.00	1.13	268.00	0.22	26.25	0.62	0.04	0.05
11	CACL2	44.80	1000.00	0.65	268.00	0.22	26.25	0.62	0.03	0.03
12	CACL2	43.60	625.00	0.48	268.00	0.22	26.25	0.62	0.01	0.02
13	MGSO4	55.50	5000.00	0.95	293.00	0.20	26.25	0.70	0.18	0.19
14	MGSO4	53.20	2500.00	1.07	293.00	0.20	26.25	0.70	0.10	0.10
15	MGSO4	51.90	1000.00	0.71	293.00	0.20	26.25	0.70	0.02	0.02
16	MGSO4	48.90	625.00	0.12	293.00	0.20	26.25	0.70	0.00	0.00

Table 2. Refined experimental data ready for modeling.

i	X0	X1=DIFT*DSAL/100000	X2=PVINJ	X3=K^PHI	X4=API^SOS	Y=DSOR_EXP
1	1	3.13	1.00	3.13	5.25	0.08
2	1	1.51	0.50	3.13	5.25	0.02
3	1	0.59	0.50	3.13	5.25	0.04
4	1	0.35	0.38	3.13	5.25	0.01
5	1	2.77	1.65	3.64	7.78	0.10
6	1	1.37	1.05	3.64	7.78	0.04
7	1	0.55	0.60	3.64	7.78	0.01
8	1	0.33	0.45	3.64	7.78	0.01
9	1	2.60	1.77	3.42	7.68	0.19
10	1	1.16	1.13	3.42	7.68	0.04
11	1	0.45	0.65	3.42	7.68	0.03
12	1	0.27	0.48	3.42	7.68	0.01
13	1	2.78	0.95	3.11	9.80	0.18
14	1	1.33	1.07	3.11	9.80	0.10
15	1	0.52	0.71	3.11	9.80	0.02
16	1	0.31	0.12	3.11	9.80	0.00

3. RESULTS/ DISCUSSIONS

3.1. Correlation for Four Brines - NACL, K2SO4, CACL2, MGSO4

The normal equation 16 was applied to the data set presented in Table 2 to obtain the correlation coefficients in **Error! Reference source not found**. Equation 17 is obtained by substituting these parameters in equation 13. Figure 2 shows a comparison of the model calculated and experimentally derived change in oil saturation and the match is very good with the trend closely followed. The error margin is 0.64%.

Table 3. Correlation Parameters for All Salts.

DSOR_ALL	
c0	0.110045
c1	0.027029
c2	0.061203
c3	-0.05858
c4	0.007361

$$\Delta S_{orALL} = 0.110045 + 0.027029(\Delta SAL)(\Delta IFT) + 0.061203PV_{inj} - 0.05858K^{\phi} + 0.007361API^{S_{os}} \tag{17}$$

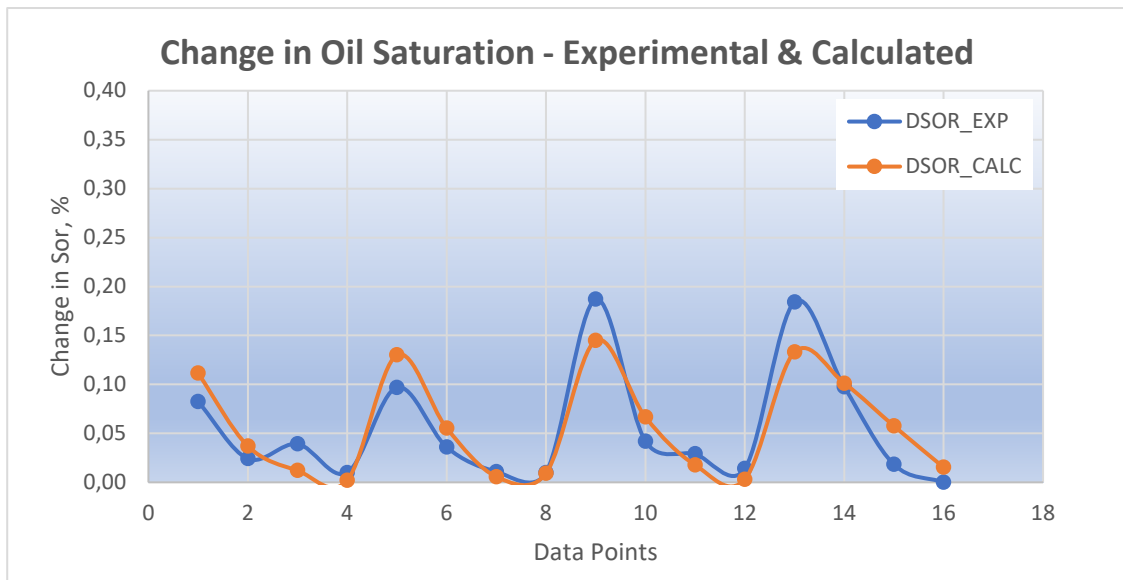


Figure 2. Experimental DSOR vs Model DSOR – All Salts.

3.2. Correlation for NACL

The normal equation 16 was applied to the data set presented in Table 4 to obtain the correlation coefficients in Table 5. Equation 18 is obtained by substituting these parameters in equation 13. Figure 3 and Table 6 show a comparison of the model calculated and experimentally derived change in oil saturation and the match is very good with the trend closely followed. The error margin is 0.25%.

Table 4. NACL Experimental Data.

SAL, PPM	X0	X1=DIFT*DSAL/100000	X2=PVINJ	X3=K^PHI	X4=API^SOS	Y = DSOR_EXP
5000	1	3.13	1.00	3.13	5.25	8%
2500	1	1.51	0.50	3.13	5.25	2%
1250	1	0.59	0.50	3.13	5.25	4%
625	1	0.35	0.38	3.13	5.25	1%

Table 5: Correlation Parameters for NaCl.

DSOR_NACL	
c0	-0.00127
c1	-0.01869
c2	0.188801
c3	-0.00398
c4	-0.00667

$$\Delta S_{orNACL} = -0.00127 - 0.01869(\Delta SAL)(\Delta IFT) + 0.188801PV_{inj} - 0.00398K^{\phi} - 0.00667API^{S_{os}} \tag{18}$$

Table 6. Experimental Vs Model Calculated DSOR – NACL

DSAL	DSOR_EXP	DSOR_CALC
5000	8%	8%
2500	2%	2%
1000	4%	3%
625	1%	2%

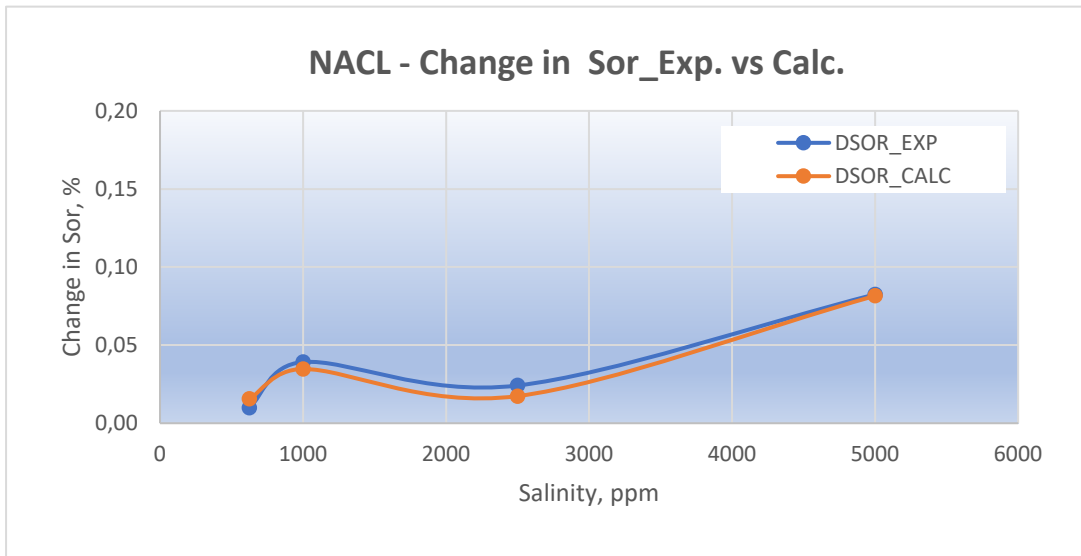


Figure 3. Experimental DSOR Vs Model DSOR – NACL.

3.3. Correlation for K2SO4

The normal equation 16 was applied to the data set presented in Table 7 to obtain the correlation coefficients in Table 8. Equation 19 is obtained by substituting these parameters in equation 13. Figure 4 and Table 9 show a comparison of the model calculated and experimentally derived change in oil saturation and the match is very good with the trend closely followed. The error margin is 0.11%.

TABLE 7. K2SO4 Experimental Data.

S/NO	X0	X1=DIFT*DSAL/100000	X2=PVINJ	X3=K^PHI	X4=API^SOS	Y = DSOR_EXP
5000	1	2.77	1.65	3.64	7.78	10%
2500	1	1.37	1.05	3.64	7.78	4%
1250	1	0.55	0.60	3.64	7.78	1%
625	1	0.33	0.45	3.64	7.78	1%

Table 8. Correlation Parameters for K2SO4.

DSOR_K2SO4	
c0	0.000326
c1	0.086268
c2	-0.09883
c3	0.001187
c4	0.002537

$$\Delta S_{orK_2SO_4} = 0.000326 - 0.086268(\Delta SAL)(\Delta IFT) - 0.09883PV_{inj} + 0.001187K^\phi + 0.02537API^{S_{os}} \tag{19}$$

Table 9. Experimental Vs Model Calculated DSOR – K2SO4.

DSAL	DSOR_EXP	DSOR_CALC
5000	10%	10%
2500	4%	4%
1000	1%	1%
625	1%	1%

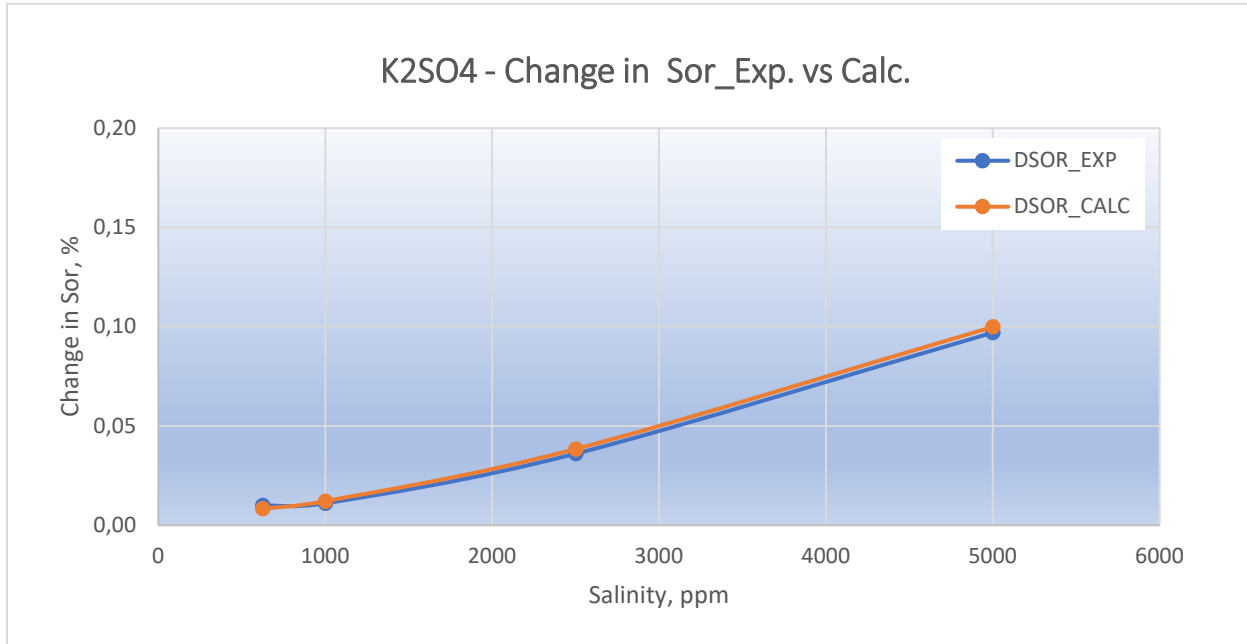


Figure 4. Experimental DSOR vs Model DSOR – K2SO4.

3.4. Correlation for CACL2

The normal equation 16 was applied to the data set presented in Table 10 to obtain the correlation coefficients in Table 11. Equation 20 is obtained by substituting these parameters in equation 13. Figure 5 and Table 12 show a comparison of the model calculated and

experimentally derived change in oil saturation and the match is very good with the trend closely followed. The error margin is 0.37%.

Table 10. CACL2 Experimental Data.

S/NO	X0	X1=DIFT*DSAL/100000	X2=PVINJ	X3=K^PHI	X4=API^SOS	Y = DSOR_EXP
5000	1	2.60	1.77	3.42	7.68	19%
2500	1	1.16	1.13	3.42	7.68	4%
1250	1	0.45	0.65	3.42	7.68	3%
625	1	0.27	0.48	3.42	7.68	1%

Table 11. Correlation Parameters for CACL2

DSOR_CACL2	
c0	0.001097
c1	0.204884
c2	-0.23879
c3	0.003751
c4	0.008423

$$\Delta S_{orCACL_2} = 0.001097 + 0.204884(\Delta SAL)(\Delta IFT) - 0.23879PV_{inj} + 0.003751K^\phi + 0.008423API^{S_{os}} \tag{20}$$

Table 12. Experimental vs Model Calculated DSOR – CACL2.

DSAL	DSOR_EXP	DSOR_CALC
5000	19%	19%
2500	4%	5%
1000	3%	2%
625	1%	2%

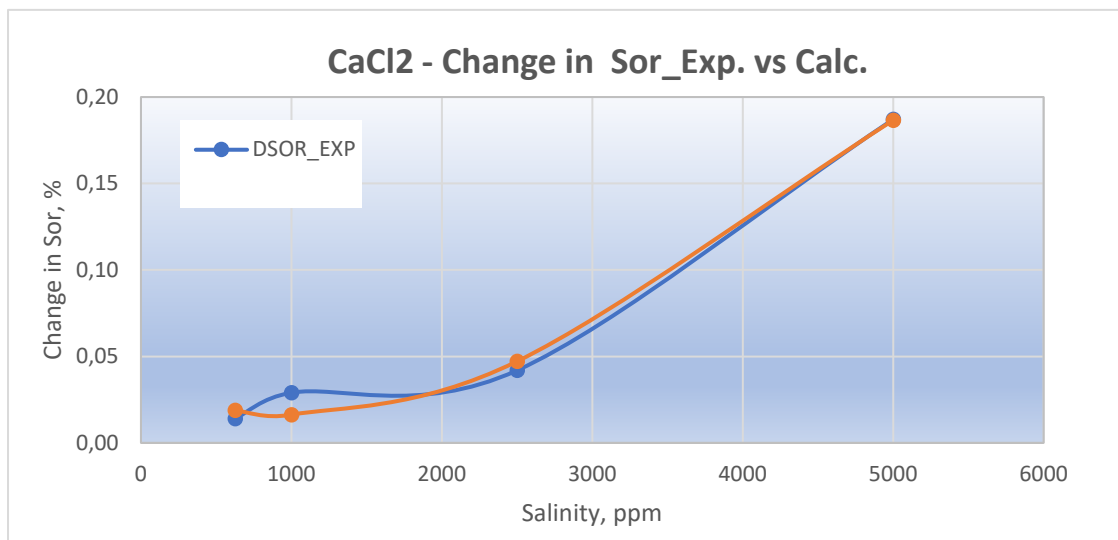


Figure 5: Experimental DSOR vs Model DSOR – CACL2.

3.5. Correlation for MGSO4

The normal equation 16 was applied to the data set presented in Table 13 to obtain the correlation coefficients in Table 14. Equation 21 is obtained by substituting these parameters in equation 13. Figure 6 and Table 15 show a comparison of the model calculated and experimentally derived change in oil saturation and the match is very good with the trend closely followed. The error margin is 0.37%.

Table 13. MGSO4 Experimental Data.

S/NO	X0	X1=DIFT*DSAL/100000	X2=PVINJ	X3=K^PHI	X4=API^SOS	Y = DSOR_EXP
5000	1	2.78	0.95	3.11	9.80	18%
2500	1	1.33	1.07	3.11	9.80	10%
1250	1	0.52	0.71	3.11	9.80	2%
625	1	0.31	0.12	3.11	9.80	0%

Table 14. Correlation Parameters for MGSO4.

DSOR_MGSO4	
c0	-0.00026
c1	0.064583
c2	0.031848
c3	-0.0008
c4	-0.00252

$$S_{orMGSO4} = -0.00026 + 0.064583(\Delta SAL)(\Delta IFT) + 0.031848PV_{inj} - 0.0008K^{\phi} - 0.00252API^{S_{os}} \tag{21}$$

Table 15. Experimental vs Model Calculated DSOR – MGSO4.

DSAL	DSOR_EXP	DSOR_CALC
5000	18%	18%
2500	10%	9%
1000	2%	3%
625	0%	0%

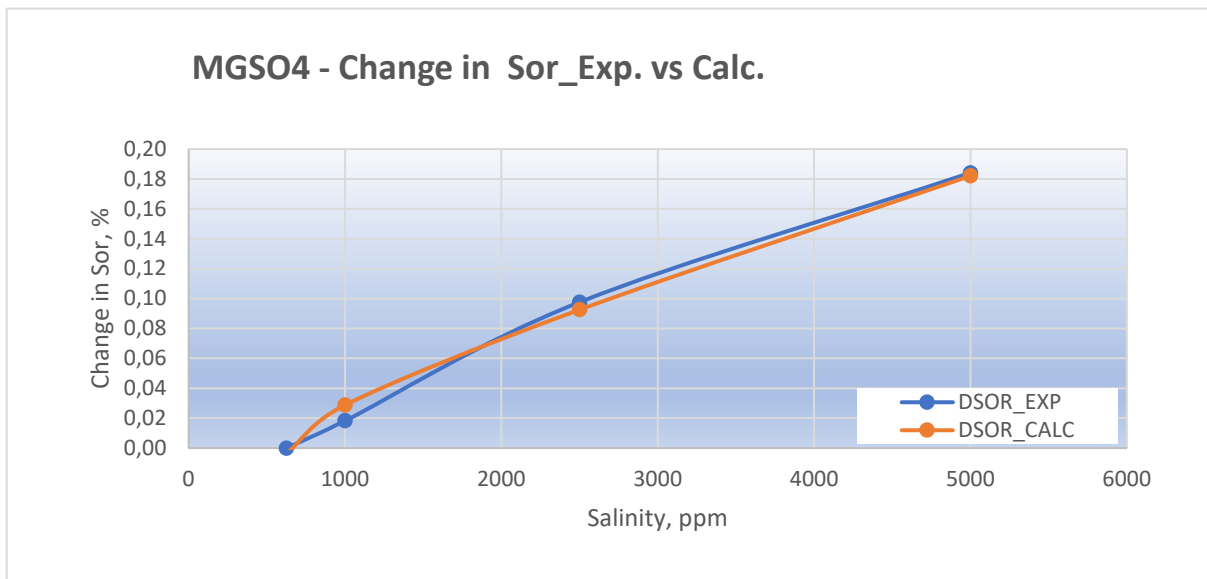


Figure 6. Experimental DSOR vs Model DSOR – MGSO4.

3.6. Derived Model vs Tripathy and Mohanty's Model

The derived model for the four salts was compared with an existing one [6] and the results for the four salts are presented in Figure 7, Figure 8, Figure 9 and Figure 10. It is to be noted that the model derived by this work shows consistently better match with the observed experimental results. Table 16 summarizes the error comparison between the model from this work and that from [6].

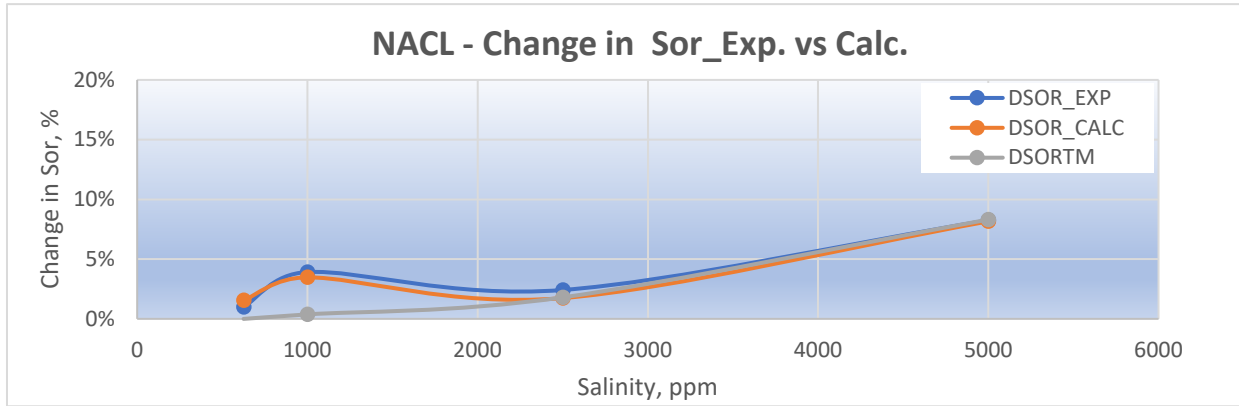


Figure 7. Comparison between Derived Model and Tripathy and Mohanty's – NaCl.

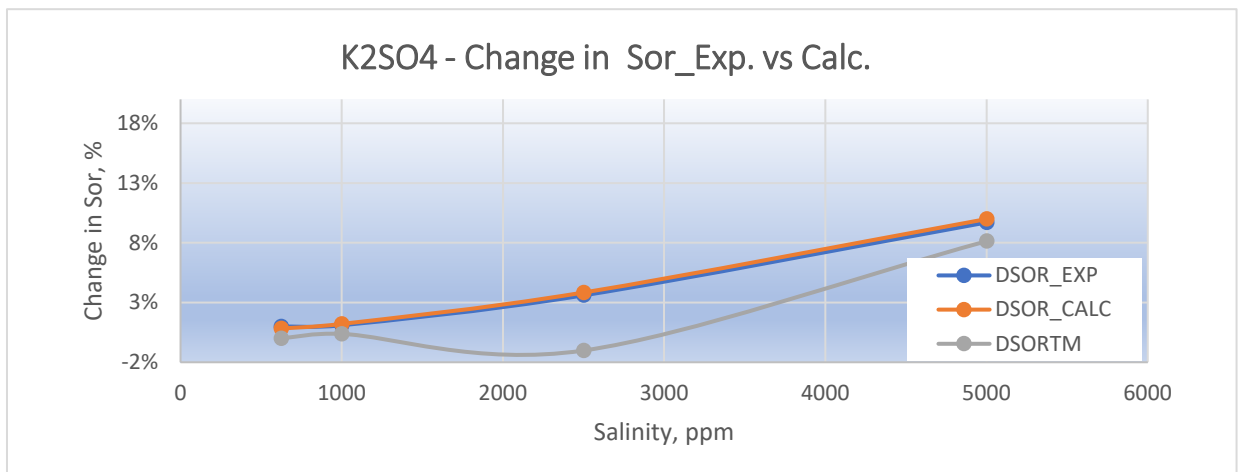


Figure 8. Comparison between Derived Model and Tripathy and Mohanty's – K2SO4.

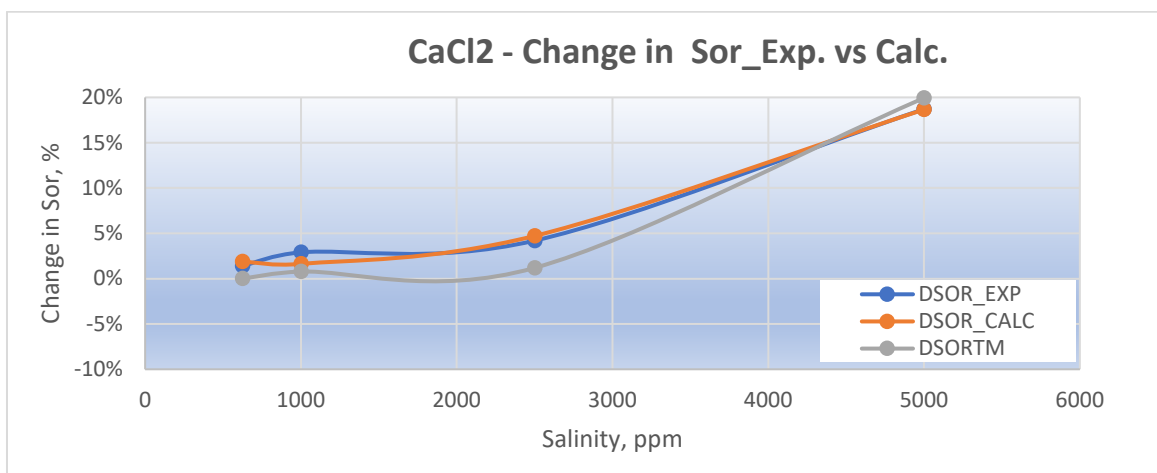


Figure 9. Comparison Between Derived Model and Tripathy and Mohanty's – CaCl2.

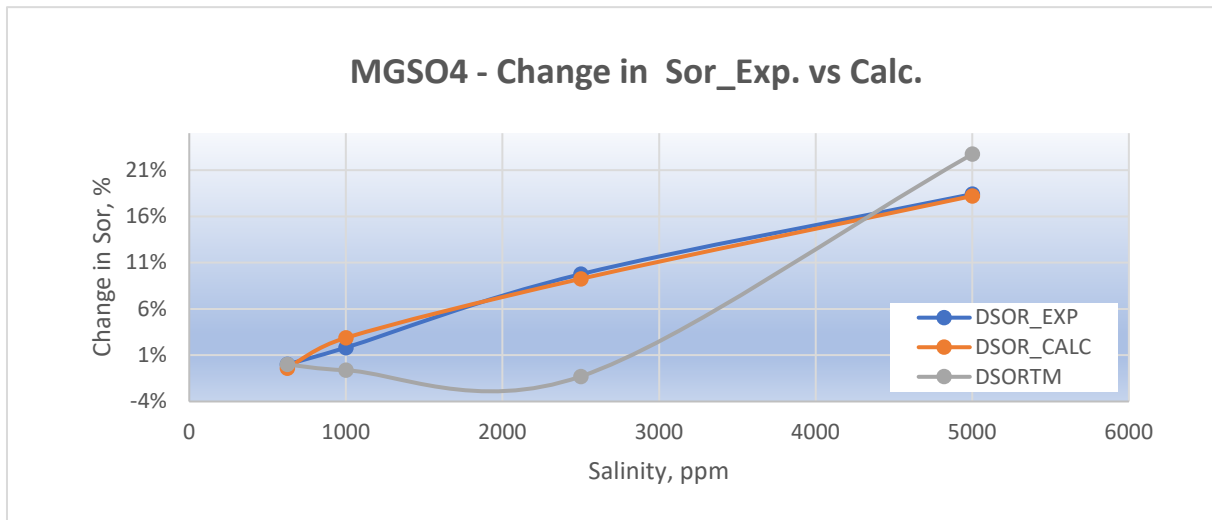


Figure 10. Comparison between Derived Model and Tripathi and Mohanty's – MGSO4.

Table 16: Error Comparison between This Model and Tripathi and Mahanty's Model.

BRINE	ERROR_THIS MODEL	ERROR_T&M
NACL	0.25%	0.93%
K2SO4	0.11%	5.23%
CACL2	0.37%	1.03%
MGSO4	0.31%	3.03%

4. CONCLUSION and RECOMMENDATIONS

In conclusion, robust models which have integrated both rock and fluid properties have been developed for the estimation of potential reduction in residual oil saturation post-OPSWF for four salts and these have been tested with very good matches with laboratory data. The performance of the models were also compared with a previously existing model and in all cases, the models developed in this work produced better results with lower error margins when compared with the previously existing model. Areas of applications would include screening of IOR candidates to estimate potential gains by implementing the OPSWF scheme and benchmarking laboratory results. In contrast to existing models, the models developed in this work takes into account the brine, rock and crude oil properties.

The following areas can be taken up for further studies

1. Integrate additional experiments and update model
2. Test developed model on data from other authors across globe

ACKNOWLEDGEMENTS

The authors would like to appreciate the Department of Petroleum Resources and Platform Petroleum Nigeria Limited for providing the research materials used in this study. The authors would also like to thank the Petroleum Engineering Laboratories at: University of Benin, University of Ibadan and Covenant University, Ota.

REFERENCES

- [1] I. G. B. J. Satter A, Practical Enhanced reservoir Engineering, Tulsa: PennWell, 2008.
- [2] BP, "Statistical Review of World Energy," London, 2020.
- [3] H. M. S. B. S. H. W.-B. Bartels, "Literature review of low salinity waterflooding from a length and time scale perspective," Fuel, vol. 236, no. 236, pp. 338-353, 2019.
- [4] Gary R. Jerauld, C.Y. Lin, Kevin J. Webb and Jim C. Seccombe, "Modeling Low-Salinity Waterflooding. SPE-102239-PA," in 2006 SPE Annual Technical Conference and Exhibition, an Antonio, Texas, 2008.
- [5] Mohammad-Javad Shojaei, Mohammad Hossein Ghazanfari and Moshen Masihi, "Relative Permeability and Capillary Pressure Curves for Low Salinity Waterflooding in Sandstone Rocks," Journal of Natural Gas Science and Engineering, vol. 25, pp. 30-38, 2015.
- [6] Tripathi, I., Mohanty, K., "Instability due to wettability alteration in displacements through porous media," Chem. Eng. Sci., vol. 63, pp. 5366-5374, 2008.
- [7] Delshad, M., Pope, G.A., "Comparison of the three-phase oil relative permeability models," Transp. Porous Media, vol. 4, pp. 59-83, 1989.
- [8] Skjaeveland, S., Siqveland, L., Kjosavik, A., Hammervold, W., Virnovsky, G., "Capillary pressure correlation for mixed-wet reservoirs," SPE Journal Paper, vol. 3, no. 01, 2000.
- [9] Richard L. Christiansen, James S. Kalbus, Susan M. Howarth, "Evaluation of Methods for Measuring Relative Permeability of Anhydrite from the Salado Formation: Sensitivity Analysis and Data Reduction," Sandia National Laboratories, Albuquerque, New Mexico, 1997.
- [10] Emad W. Al-Shalabi, Kamy Sepehrnoori, "A comprehensive review of low salinity/engineered water injections," Journal of Petroleum Science and Engineering, vol. 139, p. 137–161, 2015.
- [11] Alaigba David, Oduwa Onaiwu, Ohenhen Ikponmwosa, Olafuyi Olalekan, "Optimized Salinity Water Flooding as an Improved Oil Recovery IOR Scheme in the Niger Delta," in SPE Nigeria Annual International Conference and Exhibition, 11-13 August, Virtual, Lagos, Nigeria, 2020.
- [12] N. Springer New York, "Normal Equations In: The Concise Encyclopedia of Statistics Springer, New York, NY.," New York, 2008.
- [13] C. Myers, Intelligent Buildings: A Guide for Facility Managers, Newyork: Upword Publishing, 1996.
- [14] K. G. Shankar , "Control of Boiler Operation using PLC – SCADA," in Proceedings of the International MultiConference of Engineers and Computer Scientists 2008, Hong Kong, 2008.
- [15] J. Figueiredo and J. da Costab, "A SCADA system for energy management in intelligent buildings," Energy and Buildings, pp. 85-98, 2012.
- [16] Z. Zheng and A. N. Reddy, "Towards Improving Data Validity of Cyber-Physical Systems through Path Redundancy," in CPSS '17 Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Abu Dhabi, 2017.
- [17] R. Bayındır, O. Kaplan, C. Bayyığıt, Y. Sarıkaya and M. Hallaçlıoğlu, "PLC ve SCADA kullanılarak bir endüstriyel sistemin otomasyonu," Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, pp. 107-115, 2011.
- [18] İ. Kırık and N. Özdemir, "PLC kontrollü sürekli tahrikli sürtünme kaynak makinesinin tasarım ve imalatı," in International Conference on Welding Technologies and Exhibition , Ankara, 2012.

NOMENCLATURE

θ -	Interpolation Parameter
r -	Pore Radius
q -	Flow Rate of Injection
k -	Absolute Permeability
PV_{inj} -	PV Brine Injected
API -	API Gravity of Crude Oil
SWCTT -	Single Well Chemical Tracer Test
PV -	Pore Volume
PPM -	Parts per Million
OPTSWF -	Optimized Salinity Water flooding
NPV -	Net Present Value
LSWF -	Low Salinity Water Flooding

IRR -	Internal Rate of Return
IFT -	Interfacial Tension
COBR -	Crude Oil-Brine-Rock
CBRS -	Crude Oil-Brine-Rock System
CBR -	Crude-Brine-Rock
ΔSAL -	Change in Salinity
ΔIFT -	Change in IFT
\emptyset -	Porosity
σ_{ow} -	Oil-Water Interfacial Tension, IFT
μ_w -	Water viscosity
μ_o -	Oil Viscosity
n_w -	Corey's oil Parameter
n_o^{LS} -	Corey's oil Parameter at LS Condition
n_o^{HS} -	Corey's oil Parameter at HS Condition
$n_o(X_c)$ -	Corey's Oil Parameter
n_o -	Corey's oil Parameter
k_{rw}^{LS} -	Relative Permeability to Water at LS Condition
k_{rw}^{HS} -	Relative Permeability to Water at HS Condition
$k_{rw}(X_c)$ -	Relative Permeability to Water as a Function of Salinity
k_{rw} -	Relative Permeability to Water
k_{ro} -	Relative Permeability to Oil
c_w -	Water Compressibility
c_o -	Oil Compressibility
X_c^{LS} -	Brine Salinity at LS Condition
X_c^{HS} -	Brine Salinity at HS Condition
X_c -	Brine Salinity
S_{wr} -	Residual water saturation
S_{wi} -	Initial Water Saturation
S_w^* -	Average water saturation
S_{os} -	Oil saturation at start of OPTSWF
S_{or}^{LS} -	Residual Oil Saturation Post-LS Flooding
S_{or}^{HS} -	Residual Oil Saturation Post-HS Flooding
$S_{or}(X_c)$ -	Oil Saturation as a Function of Salinity
S_{or} -	Residual Oil Saturation
S_o -	Oil Saturation
P_c -	Capillary Pressure



Research Article

2k FACTORIAL EXPERIMENTS IN RELIABILITY ANALYSIS FOR WEIBULL AND LOG-NORMAL DISTRIBUTIONS

Authors: Berna Yazıcı* , Beldine Omondi 

*Corresponding Author: bbaloglu@eskisehir.edu.tr



To cite to this article: Yazıcı, B., Omondi, B., (2021). 2k Factorial Experiments in Reliability Analysis for Weibull And Log-Normal Distributions, *International Journal of Engineering and Innovative Research*, 3(2), p 115-120.

DOI: 10.47933/ijeir.826795

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



2^k FACTORIAL EXPERIMENTS IN RELIABILITY ANALYSIS FOR WEIBULL AND LOG-NORMAL DISTRIBUTIONS

Berna Yazıcı^{1*} , Beldine Omondi² 

¹ Eskisehir Technical University, Science Faculty, Department of Statistics, Eskisehir, Turkey.

² Anadolu University, Science Faculty, Department of Statistics, Eskisehir, Turkey.

*Corresponding Author: bbaloglu@eskisehir.edu.tr

(Received: 18.02.2021; Accepted: 10.04.2021)

<https://doi.org/10.47933/ijeir.826795>

ABSTRACT: The life times of the components of a product are often analysed in quality control processes. Design of Experiment is mainly used to achieve quality but its' application to life times are less common. Life times always associate with Reliability. This study integrates experimental design specifically a two-level factorial experimental design and simulation models to determine the important the stress factors subjected to different conditions which significantly effects the life times of a product. The main purpose is to optimize the response by extending the lifetimes of a product. The Factors considered are temperature and voltage and their magnitude of the power are set at two levels. Simulation design of Weibull and log-normal distributions are used to generate failure times and maximum likelihood (ML) applied in the estimation of parameters.

Keywords: Reliability; Simulation; Weibull distribution; Log-normal distribution; Factorial design.

1. INTRODUCTION

Technology advancement, budget constrain and restrictive testing time has translated to high reliability of products [1]. Hence, manufactures strive to remain competitive and completely relevant to the global market by meeting consumer's demands in terms of quality expectations. Likewise, the product lifetime is equally an increasing important characteristic [2] and manufactures need to understand the expected life times of their product under various operating conditions. As a result, manufacturing companies target new products to reduce the initial failures, minimize random failures and to increase product reliability. Lifetime of a product is not only a common concern to engineers but also to statisticians and is a key characteristic of product quality and reliability. It characterizes the time-span during which a product can be expected to operate safely under certain conditions and meet specified standards of performance.

A lot of efforts have been made by researchers to develop new reliability models [3]. Yu and Chen, 2014 developed reliability model of a complicated product with multiple failure modes under different stress conditions [4], Huairou 2008 [5] and Hu, Zhen and Du, Xiaoping, 2014 [6] developed a new lifetime cost optimization model to predict product lifetime and Beaudry, 1978 studied measures to reflect interaction between the reliability and performance characteristics of a product. In the review article it was described that, the distribution of lifetimes and how lifetimes depend on set experimental (predictor) variables among others [7].

According to Khan & Islam, 2012 [8] reliability is the percentage measure of degree to which product/system is in an operable and committable state at the point in time when it is needed. That is, the availability of a product or a system. Reliability is very important in that product and brand reputations are made or destroyed by their product reliability performance. Poor reliability (unreliability) causes adverse consequences and therefore a number of products or systems are serious threat. Unreliability may have implications for: Safety, reputation, good will, delays, profit margins, cost of repair and maintenance and competitiveness. Work to minimize failures, improve maintenance effectiveness, shorten repair times and meet customer and organization expectation has numerous benefits. Reliability has broad and important impact across the product life cycle. Therefore, the cost of unreliability can damage a company's image. Many manufactures have adopted reliability testing to meet and exceed the demands of customers [9]. Considering the reliability definition by Crowder, 2002 [10] as "probability of performing without failure a specified function under given conditions for a specified period of time." Therefore, reliability testing usually involves simulation of conditions under which the item will be used during its lifespan. Reliability does not compare the product to some predetermined specifications, such as the case with quality assurance, but rather investigates the performance over a predetermined period of time.

Traditionally, the lifetime of a product can be demonstrated by three different patterns of failures over time. These patterns are combined to produce a bathtub curve as shown in Fig. 1. The curves not only represent reliability performance of components or non-repaired items, but also observes the reliability performance of a large sample of homogeneous items entering the field at some start time (usually zero). If we observe the items over their lifetime without replacement then we can observe three distinct patterns or shapes. The three distinct patterns or periods are mathematically categorized as; a decreasing rate of failure, a constant rate of failure and an increasing rate of failure which in practice are known as infant mortality, useful life and wear out as shown in Fig. 1. During the infant mortality phase, the weaker components are removed during manufacturing process, pre-delivery testing or when an item comes into service. At the useful phase, new component has an equal probability of failure as the old component. Finally, the wear out failure which has increasing failure rate caused by weariness, fatigue and degradation [11]. As reliability (or part) of a product improves, cases of failed parts become less frequent in the field [12]. When a new product is introduced, the company ensures that initial failure is minimized, random failures are reduced during the expected working period of a product and finally to extend the product's lifetime.

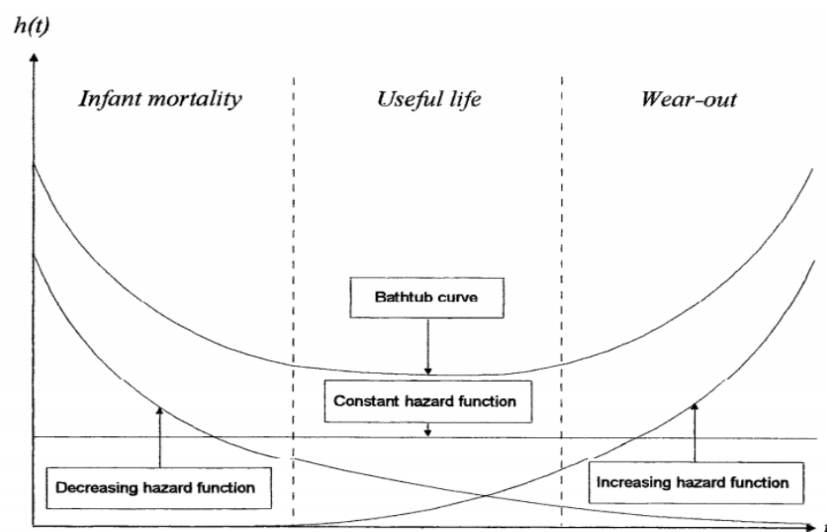


Figure 1. The Bathtub curve.

When design of experiment (DOE) is used for life testing, the response is life or failure time. Failure time distribution is the most widely used measure for reliability of a product. The distribution is constructed based on failure time data of a product. The failure time or lifetime of a product is described as a continuous random variable T . Its probability distribution function is characterized by cumulative density function, probability density function, reliability function or hazard function. The reliability function gives the probability of a product surviving up to time t while the hazard function also known as the failure rate function describes the probability of failure at the smallest interval $(t, \delta + t)$, given survival up to.

In this article we are concerned with finding factors that affect the lifetimes of a product and also increasing the lifetimes by conducting simulation with right censoring both for Weibull and log-normal distribution. Simulation model is developed based on these factor levels. Maximum likelihood method is used to estimate the parameters of both Weibull distribution and log-normal distribution. Finally, we find that combination of input-factor values that optimizes the response.

1.1. Maximum Likelihood Estimation (MLE)

Maximum likelihood estimate (MLE) can be described as follows: Given the model and its parameters, the MLE function is the probability (density) of a sample data seen as a function of the model parameters. Estimates of the model parameters are obtained by maximizing logarithm of the likelihood. Estimates are the values that maximizes probability of the sample data. Its main aim is to find combination of parameters β and η that maximize the probability of a given data. MLE estimates tend to predict long life with small samples.

The PDF of a log normal distribution is given by:

$$f(t/\mu, \sigma^2) = \frac{1}{\sigma t \sqrt{2\pi}} \exp\left(-\frac{(\log t - \mu)^2}{2\sigma^2}\right), \quad t > 0 \quad (1)$$

Where σ is the shape parameter and $\mu = T_{50}$, median (scale) parameter.

While the PDF of Weibull distribution is:

$$f\left(\frac{t}{\eta}, \beta\right) = \frac{\beta}{\eta} \left(\frac{t}{\eta}\right)^{\beta-1} \exp\left(-\left(\frac{t}{\eta}\right)^\beta\right), \quad t > 0 \quad (2)$$

η is the scale parameter and β is the shape parameter.

2. MATERIAL AND METHOD

A complete factorial design can become large even at two levels of each factors. An experiment with eight factors would require $2^5 = 32$ runs. In the case of reliability experiment, each run may be measured as in hours, days, months etc and may take several thousand hours, which would be practically infeasible to conduct 32 runs. Thus, more efficient methods of conducting experiments are needed. Fractional factorial designs can reduce the number of runs by choosing a subset or fraction of the complete factorial design. A 2^{5-2} factorial design would reduce the

number of runs by using a quarter fractional factorial experiment, $(1/4 (2^{5-2}))$ to eight runs. Although this provides an advantage of reducing the number of runs, the disadvantage is that many of the effects are hidden or confounded by the main effect factors that the experimenter deems the most important.

This assumes that many of the confounded effects are not significant and have very minimal effect or do not affect the response at all. Fractional factorial designs are particularly useful if it can be estimated which main effects and interactions are significant so that the remaining effects can be confounded [13].

The parameters are chosen to determine their corresponding influence on the lifetimes, which are:

- Voltage (V)
- Temperature (C)

These factors are to be studied in levels of high and low.

Table 1. Factors and factor levels used in the design.

Factor	Low(-)	High(+)
Temperature	38	43
Voltage	105	120

2.1. Simulation Test

A simulation of two factors temperature and voltage were investigated to determine the reliability of a product. A simulation of a 2^2 design with no interaction was conducted for Weibull distribution and log-normal distribution. The main objective is to identify the significant factors that affect the lifetimes of a product. Table 2 gives the layout of the design matrix.

Table 2. Layout of 2^2 design matrix.

Run	I	A	B	AB	Response
1	1	+	-	-	R ₁
2	1	-	+	-	R ₂
3	1	+	+	+	R ₃
4	1	-	-	+	R ₄

$$ln(\eta) = \alpha_0 + \alpha_1 T \text{ emperature} + \alpha_2 V \text{ oltage} + \alpha_{12}(T \text{ emperature})(V \text{ oltage}) \tag{3}$$

2.2. Simulation Results

The simulation results are summarized for Weibull distribution and given in Table 3. Similarly, the results for Log-normal distribution are summarized and given in Table 4.

Table 3. Weibull distribution analysis results.

Likelihood ratio test-table				
Model	Effect	DF	Ln(LKV)	P Value
Reduced	Temperature	1	-1378.3	<0.0001
	Voltage	1	-1281	0.0007
Full	-	4	-1377	-

Estimates of Parameters			
Predictor	Coef.	S.d Error	P Value
Intercept	4.8139	1.647	0.068
Temperature	0.0304	0.013	1.15E-02
Voltage	-0.0466	0.257	7.17E-03

Table 4. Log-normal distribution analysis results.

Likelihood ratio test - table				
Model	Effect	DF	Ln(LKV)	P Value
Reduced	Temperature	1	-1425	0.0001
	Voltage	1	-1654	0.0200
Full	-	4	-2144	-

Estimates of Parameters			
Predictor	Coef.	S.d Error	P Value
Intercept	5.0753	0.0432	0.0067
Temperature	0.0998	0.077	0.0231
Voltage	-0.1006	0.0266	0.0002

The layout of table 3 and table 4 are similar to the ANOVA table. This makes it easy to read for those who are familiar with ANOVA. From the P value column, temperature and voltage are important to the product life. The estimated relationship is:

$$\ln(\eta) = \alpha_0 + \alpha_1 T \text{ emperature} + \alpha_2 V \text{ oltage}$$

for weibull distribution and for log-normal distribution. The estimated shape parameter for the weibull distribution is 1.85.

3. CONCLUSION

Instant results and sequentially make agricultural experiments different from industrial experiments. For most industrial experiments results are always available instantly (days, hours e.t.c) and the results from each group can be acted upon to be used in the next experiments while in agricultural experiments, processes are always restricted during growing seasons. In addition, normal distribution which characterizes most experimental designs is not a logical distribution for lifetimes due to censoring. Due to censoring, analysis of variance (ANOVA) and least square method (LSM) cannot be used to improve reliability [14]. In this case, ANOVA method can only be applicable if suspensions are treated as failures and midpoint of interval data used as failure times.

This approximation gives wrong results and lead to wrong conclusions. Consequently, the use of ANOVA method on lifetimes data violates the normal distribution assumption among others. In addition, the commonly used ML estimate approach is considered to have an “estimability” problem. Testing for important effects in the model cannot be done by comparing the ML estimates with their corresponding standard errors because the ML estimates may be infinite. One factor with two levels experiment with censored observation and failure time data is given according to the factor levels. In this example it is observed that as the parameter tends toward infinity the likelihood function increase to the maximum and therefore concluded that ML estimate for the main effect tends to be infinite when the true factor effect is large [15].

The study aims at increasing the lifetimes of a product by simulation. The important factors are identified through the screening process and a second order (quadratic) response surface

methodology used to determine the optimal values. Weibull and lognormal models with an assumed scale parameter was used in the model simulation and maximum likelihood estimation for the parameter estimation. Temperature and voltage were found to be significant effects and therefore they play an important role in the lifetimes of a component.

REFERENCES

- [1] Zhang, C. W., Zhang, T., Xu, D., and Xie, M. (2013). Analyzing highly censored reliability data without exact failure times: an efficient tool for practitioners. *Quality Engineering*, 25(4), 392–400. <http://doi.org/10.1080/08982112.2013.783598>.
- [2] Kesler, J. L. K., Freeman, L. J., and Vining, G. G. (2014). A Practitioner's guide to analyzing reliability experiments with random and subsampling. *Quality Engineering*, 26(3), 359–369. <http://doi.org/10.1080/08982112.2014.887101>.
- [3] Beaudry, M. (1978). Performance-reliability measures for computing systems. *IEEE Transactions on Computing*, Vol. 27.
- [4] Yu, Z., Ren, Z., Tao, J., and Chen, X. (2014). Accelerated testing with multiple failure modes under several temperature conditions, *Mathematical Problems in Engineering*, Vol.1 <http://doi.org/10.1155/2014/839042>.
- [5] Huairou, A. M. (2008). Reliability assessment using a likelihood ratio test. *International Journal of Performance Engineering*, 4, 196-198. <http://doi.org/10.23940/ijpe.08.p196.mag>.
- [6] Hu, Z. and Du, Xiaoping D. (2013). Lifetime cost optimization with time-dependent reliability, *Journal of Engineering Optimization*, Vol. 46, Issue 10, p.1389-1410. <http://doi.org/10.1080/0305215X.2013.841905>.
- [7] Rigdon, S. E., Englert, B. R., Lawson, I. A., Borrer, C. M., Montgomery, D. C. and Pan, R. (2012). Experiments for reliability achievement. *Quality Engineering*, 25(1), 54-72. <http://doi.org/10.1080/08982112.2013.733611>.
- [8] Khan, M. A. and Islam, H. M. (2012). Bayesian analysis of system availability with half-normal life time. *Quality Technology and Quantitative Management*, 9(2), 203-209. <http://doi.org/10.1080/16843703.2012.11673286>.
- [9] Lwo, B. J., Frank, Lin, M. S., Huang, K. H. (2014). TSV reliability model under various stress tests. *IEEE 64th Electronic Components and Technology Conference (ECTC)*, <http://doi.org/10.1109/ECTE.2014.6897350>.
- [10] Crowder, M. a. (2002). *Statistical concepts in reliability*. (Vol. 50). Springer.
- [11] Tobias, P. A. and Trindade, D. (2012). *Applied reliability*. New York: CRC Press.
- [12] Woo, S., and Neal, D. L. O. (2018). Improving the reliability of a domestic refrigerator compressor subjected to repetitive loading, *International Compressor Engineering Conference*.
- [13] Wu, C. F. J. and Hamada, M. S. (2009). *Experiments: Planning, Analysis, and Optimization*, 2nd Edition, John Wiley and Sons.
- [14] Wang, G. a. (2017). Bootstrap analysis of designed experiments for reliability improvement with a non-constant scale parameter. *Reliability Engineering & System Safety*, 160, p.114-121, <http://dx.doi.org/10.1016/j.ress.2016.12.006>.
- [15] Silvapulle, M. J. (1986). Existence of maximum likelihood estimates in regression models for grouped and ungrouped data. *Journal of the Royal Statistical Society*, Vol. 48. No.1, p. 100-106.



Research Article

INTERNET SPEED ISSUE OF TURKEY

Authors: Hüseyin CEYLAN*^{iD}, Gizem DEMİR^{iD}, Ziya ELRİ^{iD}

*Corresponding Author: huseyinceylan@kku.edu.tr

To cite to this article: Ceylan, H., Demir, G., Eri, Z., (2021). Internet Speed Issue of Turkey, International Journal of Engineering and Innovative Research, 3(2), p 121-132.

DOI: 10.47933/ijeir.902060




To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



International Journal of Engineering and Innovative Research

<http://dergipark.gov.tr/ijeir>

INTERNET SPEED ISSUE OF TURKEY

Hüseyin CEYLAN^{1*}, Gizem DEMİR², Ziya ELRİ³

¹Kırıkkale University, Kırıkkale Vocational School, Kırıkkale, Turkey.

²Ericsson, IT Test Engineer, Ankara, Turkey.

³Kırıkkale University, Institute of Science, Defense Technologies Department, Kırıkkale, Turkey.

*Corresponding Author: huseyinceylan@kku.edu.tr

(Received: 23.03.2021; Accepted: 20.04.2021)

<https://doi.org/10.47933/ijeir.902060>

ABSTRACT: The internet, used by a large population around the world, has become a part of daily life. The internet is used in scientific research, education, commerce, health, communication, banking, tourism, transportation and many similar fields. The need for internet increases in parallel with digitalization and becomes more and more important day by day. Especially during the covid-19 epidemic, providing education over the internet and doing some work from home over the internet has more increased dependence on the internet. Turkey has one of the 20 largest economies in the world by economy size. It is an important country with a population of approximately 84 million. According to the Turkey Statistical Institute (TurkStat) data, in 2020, 90.7% of house in Turkey have access to the internet and the proportion of individuals using the internet is 79.0%. In Turkey, which is one of the important countries of the world and where the use of the internet is widespread, the internet is not at the desired speed. According to the latest report of Speedtest, founded by Ookla in 2006, which measures internet speed most accurately and regularly publishes the "Speedtest Global Index", Turkey is ranked 103 out of 175 countries with Fixed Broadband Internet Speed. Moreover, the 30.51 Mbps download speed is far below the global average of 96.98 Mbps. It is remarkable that the internet speeds of countries that are incomparable to Turkey in terms of economic size and some of which can be called island states are higher than Turkey. These countries are Andorra, Macau (SAR), Liechtenstein, San Marino, Barbados, Trinidad and Tobago, Grenada, Southern Cyprus Greek Region, Armenia, Montenegro, Kosovo, The Bahamas, Saint Lucia, Guyana, Laos, Madagascar, Belize, Dominica, North Macedonia, Côte d'Ivoire, Saint Kitts and Nevis. Turkey has passed to 4,5 G as of April 1, 2016 to increase the speed of the internet. Despite this, Turkey's internet speed is relatively slow and this is an important ergonomic problem. Low connection speeds negatively affect both education and all sectors where the internet is used during the global epidemic. In this study, the reasons for the slow internet speed in Turkey are examined and various solutions to the problem are proposed.

Keywords: Internet, Speed, Fiber, Turkey, Ergonomics, User-Friendly Systems, SpeedTest.

1. INTRODUCTION

The Internet is described by many as the greatest technological breakthrough of our time, sometimes of all time. With the rapid development of technology in recent years, the internet has become a part of our daily life. In the time we lived in, internet technologies have begun to take place in our lives so much and made our lives easier that it has become almost impossible to imagine a life without the internet. The internet, which was developed by the US Department of Defense in the 1970s to connect remote points and to provide information exchange between these points, brought with it many innovations and facilities. It is now possible to access anywhere in the world and accesses all kinds of information via the Internet. Thanks to the internet, which is the basis of communication today, people can easily

access everything they see away. This access is not limited to information only. With the introduction of social networks in our lives, communication and interaction between people has also increased. In addition to increasing the accessibility of the Internet, another reason why it has become so important in human life is that it makes many works in daily life easier. Especially recently, some innovations such as digital banking, online shopping applications, online education tools have become indispensable for the internet. People can perform transactions they want to do via the internet without going to banks and stores. The benefits of the internet in education are also undeniable. Previously, students spent time going to libraries and learning the right information from the right books. Nowadays, this confusion has been eliminated with the internet to reach information and students can access the information they want by using search engines. In addition, many educational institutions provide their education on the internet. People can easily receive training from experts or even teachers elsewhere in the world in accordance with their interests. The fact that the internet is a part of daily life causes technological developments to increase gradually. While people used to access the Internet from their mobile phones, tablets and computers, lately they can also access the Internet through other household items. With this technology developed as the "Internet of Things (IoT)", it is aimed for household items to communicate with each other using the internet and to make daily work easier.

For many people, accessing the internet is very important, even at low speed. However, high-speed internet also has quite high importance in accessing information. Everything from browsing browsers to downloading apps becomes more convenient and easier with high-speed internet. Today, even photo galleries are kept and stored in internet-based applications known as the cloud [1]. High speed internet makes it easy to access these storages. Although people prefer to access the internet for little money due to the low fees paid to internet service providers for low-speed internet, this solution will not be enough in the long run. In today's digital world where online trainings, conferences and live broadcasts are held, reaching the fast internet has become the goal, not the reaching internet. Thanks to the fast internet, the working time of people is shortened and thus both time and money are saved.

It can still be experienced major Internet outages in Turkey in 2021 Turkey ranks 103rd among 170 countries in the Hard Broad-Band Internet Speed and in the mobile Internet, speed ranks 57th among 140 countries [2]. This is not acceptable for a country that is one of the 20 largest economies in the world and aims to be in the top 10. In this study, the reasons for Turkey's internet speed problem are discussed and proposals are made to solve this problem which is vital for the Turkish economy.

2. INTERNET AND TECHNICAL FEATURES

The birth of the Internet started with the increase in the importance of communication. As a result of the experiments carried out in the laboratory for the US military to communicate, it was possible to transfer information from one computer to another with various communication protocols [3]. This adventure, which started with data transfer between two computers, has turned into a network system that is effective worldwide today, that is, the internet.

The Internet can be defined as a global computer network that supports packet-switched data transmission between computer systems with completely different operating systems controlled by the TCP/IP protocol suite, where connections between each other are provided by a telecommunications infrastructure [4]. It is clear that the future is in digital and electronic

environment. The Internet is one of the keys to the future. Internet engineering departments can also be opened at universities [5]. Nowadays, Internet has become a mandatory need. If the people of a country cannot access the Internet in ideal conditions, it will be very difficult for them to access information and keep up with the age. Today, internet usage rates and especially broadband internet services penetration are important in terms of showing the competitiveness of countries [6].

There is no owner of the internet in the world [3]. A person, an institution, or a state does not have any rights over it. However, there are Internet Service Providers (ISP) that allow a user to easily access a huge computer network for a fee. These companies allow the user to access the internet via fiber optic cable infrastructure or wireless network (cellular, GSM, 3G, 4G, 4.5 G, 5G, etc.).

2.1. What is Cellular Network?

A cellular network is a type of wireless network created using several radio cells (also called "cells" for short) [7]. Base stations serve each cell. Popular examples today are GSM, DECT or Wi-fi.

Cellular networks have many advantages according to the regular networks [7]:

- ✓ Higher capacity
- ✓ Less power consumption
- ✓ Better scope

Cellular networks, which form the basis of internet technologies, have shown a great development until today. 1G networks, known as 1st Generation Networks, came into our lives in the 1980s and were designed only for analog voice transmission [8]. After that, 2nd Generation Networks have been developed. 2G technology, the technical name of which is Global System for Mobile Communications (GSM), is a mobile phone communication protocol and unlike 1G, it is completely digital [8]. Because it supports GPRS technologies for text message (SMS), video message (MMS) and internet access, it has made it inevitable to increase the number of mobile devices immeasurably, strengthen the infrastructure and improve the quality of Service. Especially with the introduction of smart phones in the market, mobile internet access has gained importance.

2.2. What is 3G?

After 2G, 3G technology (3rd Generation Networks) that includes more data, video calls and mobile internet, emerged. 3G or 3rd Generation networks are a family of standards defined by the International Telecommunication Union and covering GSM EDGE, UMTS, CDMA2000, DECT and WiMAX technologies [9]. 3G (3rd Generation) technology, which replaced GPRS, EDGE and MMS technologies, made it possible to transfer voice, data and images at high speed due to its infrastructure. Although it is around Gigabit in terms of bandwidth, it has been observed that users have reached data transfer speeds of around 20 Mbps. The data rate in 3G networks, which can be described as slow in current conditions, reaches 2Mbps in fixed or stationary devices and up to 384 Kbps in roaming devices [9]. In this way, it has been possible to access sites and transfer data through IP and packet switching technologies over all devices that can connect to the internet, including mobile devices. This is how it started to stand next to companies that provide internet over cable infrastructure.

2.3. What are 4G and 4.5G?

4th generation wireless communication networks are generally called 4G. 4G (LTE) and 4.5G (LTE-Advanced) networks are used today. Due to the fact that a more advanced version of 4G will be used in Turkey, the 4.5G (LTE Advanced) concept is used instead of 4G. This technology is a mobile communication technology that provides higher speed, lower latency and high capacity mobile internet [7]. Cellular networks that are approximately 500 times faster than 3G; support high-definition mobile TV, video conferencing and much more. In LTE networks, the base station defines a bandwidth of 1.4-20 MHz for each mobile phone or device [9]. The delay of 100-500 milliseconds observed in 3G networks has dropped to 20-30 milliseconds with 4.5G [10]. Due to the decrease in latency and the increase in defined bandwidth, LTE networks allow us to connect to the internet more quickly today.

High-speed broadband offers internet service with a completely IP-based network structure. It is considered as a continuation of WiMAX technology. Turkey has started to use 4.5G as of April 1, 2016.

2.4. Differences between 3G and 4.5 G [11]:

- ✓ 4.5G is faster than 3G in terms of speed.
- ✓ The frequency amount of mobile network operators increased from 183.8 MHz to 549.2 MHz. Therefore, users will have the opportunity to receive faster service on broadband.
- ✓ While downloading an 8GB high resolution movie takes approximately 27 minutes on 3G, it takes 67 seconds on 4.5G.
- ✓ In 2022, it is estimated that an average of 4 family members in OECD countries, including Turkey, will have 50 devices connected to the internet. Internet traffic generated by these devices will be able to be transported easily over fast networks such as 4.5G. (IPv6)

2.5. Internet Speed

Internet speed is an important factor. The size of today's internet pages is increasing, and the need for high bandwidth in the data transfers that are now needed cannot be ignored.

In order to provide a healthy broadband high-speed internet, first of all forward and backward direction signals (from subscriber to circuit, from transfer to subscriber) must be transmitted without loss. In addition, it is an important factor that any point in the infrastructure is not affected by noise (electrical signal distortion).

The ping values, which are the time to reach the target of the data, should be low and the devices between the customer and the network should have bandwidth that can accommodate intensive data use [12]. The importance of this was experienced especially during the pandemic period, and it was observed that many internet companies entered the bottleneck due to the intensive use of internet lines during the quarantine period.

Internet slowness can be experienced even if there is no problem in the infrastructure. The most important reason for this is the Wi-Fi connection between the computer and the modem. The factors that kill Wi-Fi signals need to be eliminated. First of all, the modem must be kept away from noise that may disturb wireless signals (wireless phone, microwave oven,

television) [13]. If the receiver and the transmitter are in different rooms, the type of walls can affect. (It can significantly reduce the low signal strength.) Another possible problem with wireless modems is due to the occupancy rate of the wireless frequency channels. If more than one wireless device in the environment provides a connection from the same channel, this channel enters the bottleneck and the data transfer rate decreases [14]. Channel setting can be selected automatically in today's modems. Despite all this, if there is still slowness, providing a device called an Access point to strengthen the signal and placing it in an appropriate point will greatly solve the problem.

3. TURKEY'S BUILT-IN SPEED INTERNET INFRASTRUCTURE

The internet has become an indispensable technology to develop, grow and capture the age in every subject. A world without internet is unthinkable today. The Internet provides instant access to the most up-to-date information wherever it is in the world. By accelerating the flow of data, the Internet removes the limits of communication. Approximately 4 billion IPv4 addresses, which determine the limit of devices that can be connected to the Internet, have been exhausted and various solutions such as IPv6 have been developed [12]. Considering that the world population is approximately 7.8 billion, it can be said that the importance of the internet is accepted by the whole world.

Turkey has an important place as geographic location. It is one of the 20 largest economies in the world and a member of the G20. It is a country that aims to be among the developed countries with its 83 million young populations and wants to have a say in the world in different sectors. In this case, it is not an acceptable situation to remain behind many developing countries and even in some of the island statelet in terms of internet speed and internet infrastructure. According to the latest reports published by Speedtest, Turkey's ranking among countries in Mobile and fixed broadband internet speeds is seen in Table 1 and Table 2. [2]

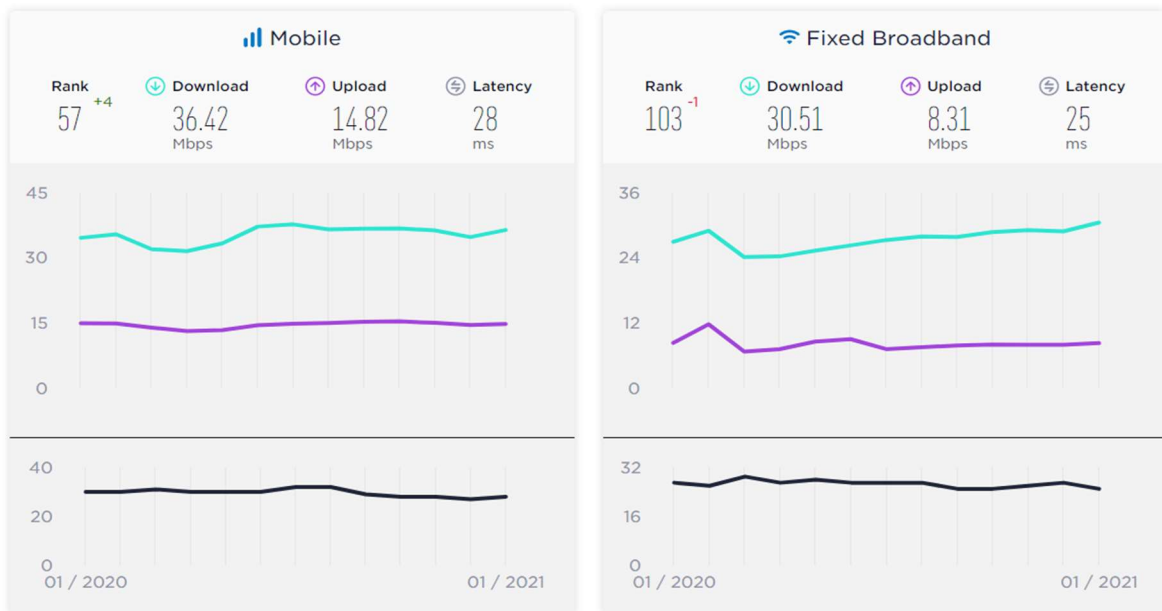
Table 1. Fixed Broadband Internet Speed Ranking of Countries (January 2021)-Speedtest Global Index.

Rank	Country	Download Speed (Mbps)
4	Romania	198.01
7	Monaco	187.88
16	Chile	171.02
21	Luxembourg	147.60
24	Malta	141.29
40	Moldova	97.36
58	Ukraine	63.81
62	Ghana	58.25
69	Grenada	52.23
87	Saint Vincent and the Grenadine	39.93
90	Belize	37.85
97	Côte d'Ivoire	33.45
102	Saint Kitts and Nevis	32.02
103	Turkey	30.51

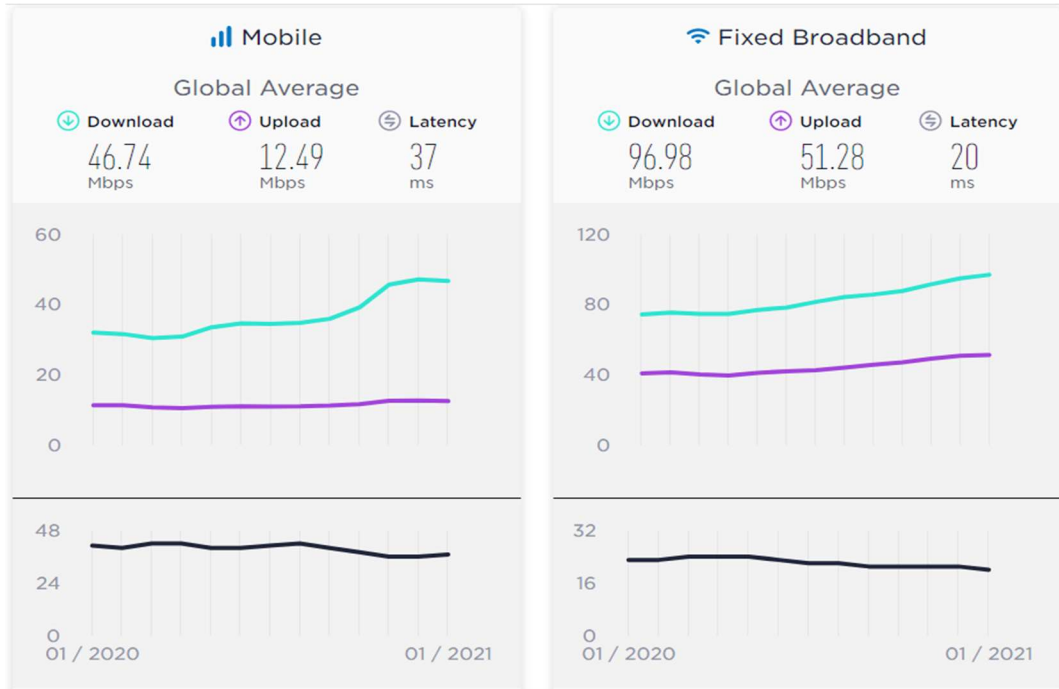
Table 2. Mobile Internet Speed Ranking of Countries (January 2021)-Speedtest Global Index.

Rank	Country	Download Speed (Mbps)
12	Luxembourg	82.87
18	Bahrain	70.45
21	Croatia	66.71
29	Greece	56.39
33	North Macedonia	51.49
35	Albania	50.15
38	Romania	47.69
45	Maldives	44.30
47	Malta	44.07
55	Georgia	36.86
56	Brunei	36.75
57	Turkey	36.42

Table 1 summarizes some of the country's fixed broadband internet speeds and Turkey's order is given as according to these countries. Looking at download speeds, Turkey ranks 103 out of 175 countries [2]. This shows that the internet download speed in Turkey is much lower than in other countries. With a download speed of 30.51 Mbps, it stayed behind even smaller countries in economic and social terms. Likewise, when we look at the countries in Table 2 mobile download speeds Turkey ranks 57 among 140 countries [2]. It stayed behind countries such as Albania, North Macedonia and Malta. Unfortunately, this situation showed that we are not at the desired level. The main reasons why Turkey gets behind other countries in terms of internet speed can be shown as insufficient infrastructure and less investment by internet service providers.



Graph 1. Mobile and Fixed Broadband Connection Speeds of Turkey.



Graph 2. Mobile and Fixed Broadband Connection Speeds (Global Average).

According to Speedtest's measurements, Turkey's mobile and fixed broadband internet speeds are given in Graph-1, and the world average is given in Graph-2 [2]. When the graphic-1 is viewed Turkey's mobile internet download speed is around 36 Mbps and upload speeds of 15 Mbps. Likewise, it has 31 Mbps download and 8 Mbps upload speeds on fixed broadband internet. When we compare these data with world averages, it seems that Turkey is very, very slow from the world in terms of constant broadband internet speed, both download and download speeds. World average fixed broadband internet has approximately 97 Mbps download speed and 51 Mbps upload speed. The world average fixed broadband internet speed is 2 times more than Turkey's download speed and 6 times more than Turkey's upload speed. The mobile internet with the world average of 47 Mbps download speed is still faster than Turkey. Just upload speed mobile internet in Turkey is approximately 12 Mbps, which is slightly better than the world average.

It would be wrong to treat this situation only as internet speed data. In the simplest way, the difference between loading speeds reveals the development and speed of development of a country. Because it is an issue that directly affects content production. On the other hand, download speed, access to information and the importance of communication is an issue that cannot be ignored. Given these data, it shows that there are serious problems with the internet infrastructure and speed in Turkey.

TURKSTAT has published its "Household Information Technologies (IT) Usage Survey" on August 25, 2020. According to this study, it has been determined that:

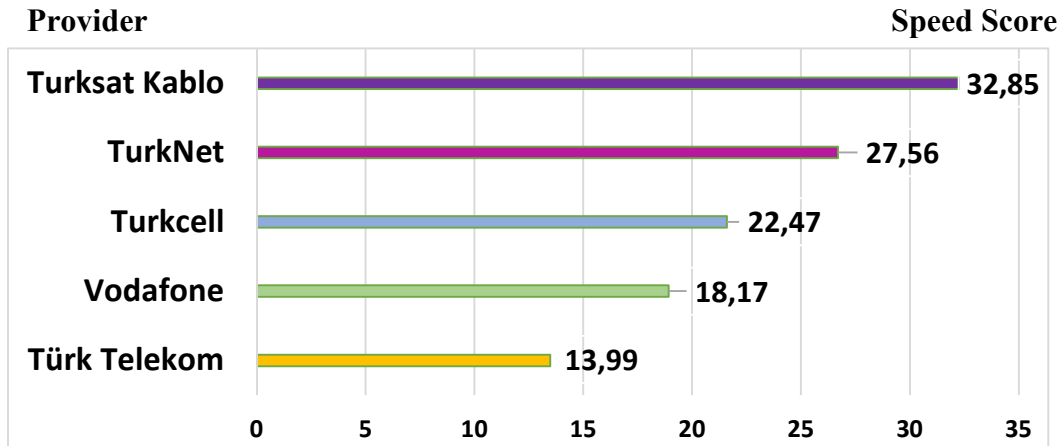
- ✓ The rate of individuals using the Internet is 79%,
- ✓ 90.7% of households have access to the Internet from home,
- ✓ 89.9% of households have access to broadband Internet,

In Turkey in 2020. The same study shows that in Turkey the use of internet increased compared to the previous year [15]. The number of individuals using the internet, which has increased in recent years, the opportunity to access the internet from home, the activity on social platforms, and the spread of e-government services reveals the importance of the

internet for Turkey. It is a serious problem that the speed of the internet, whose importance and use is increasing day by day in Turkey, is very slow compared to the world.

4. INTERNET SERVIS PROVIDERS IN TURKEY

In the report published by Speedtest on Turkey's internet speed in the 4th quarter of 2020, data on operators providing internet services are given in Graph-3. When these data are taken into consideration, "Turksat Kablo" is the operator providing the fastest internet service and "Türk Telekom" is in the last place [2].



Graph 3. Speed sequence of operators that provide Internet services in Turkey.

This situation is not only experienced at internet speed, but it is also seen in Table 3 where latency times of operators providing internet service are given and Table 4 where "Consistency Scores" are given. In addition to Turksat Cable, which is in the first place with 15 ms in delay time and second in consistency score, it is quite remarkable that Turk Telekom, which is the leader in this market, is in the last place [2].

Table 3. Ranking of Internet latency speed Internet service providers in Turkey.

Provider	Mean Latency
Turksat Kablo	15 ms
TurkNet	23 ms
Turkcell	27 ms
Türk Telekom	28 ms
Vodafone	38 ms

Table 4. Consistency scores of internet service providers in Turkey.

Provider	Consistency Score™
TurkNet	57.0%
Turksat Kablo	53.2%
Turkcell	40.8%
Vodafone	33.6%
Türk Telekom	21.7%

The fact that Turk Telekom, which has its own infrastructure, except for municipalities throughout the country, leases it to other internet service operators and is a leader in the sector, is at this level is a fact that brings down the entire sector.

Table 5. Number of subscribers by internet service providers in Turkey.

Provider	Number of subscribers (%)
TTNet	65,75
Superonline	14,73
Vodafone Net	7,58
D-Smart	3,87
Turknet	3,05
Millenicom	1,68
Others	3,34

Table 5 gives the number of subscribers of internet service providers in the last quarter of 2020. Considering these data, the three businesses with the highest share are Türk Telekom (TTNet), Turkcell (Superonline) and Vodafone Net. Türk Telekom ranks first with a ratio of approximately 65%. [16]

Internet service also has an economic dimension. It can be seen in the data shared above that internet use in Turkey has reached serious levels. In spite of this, it is shown in Table 6 that the average cost per Mbps has decreased worldwide in certain periods of 2019 and 2020 [17]. However, the average cost per Mbps for Turkey is much higher than these values. This situation is shown in Table 7. [18]

Table 6. Average Internet Prices for Certain Regions of the World.

Region	Average Cost per Mbps (Q2 2019)	Average Cost per Mbps (Q4 2019)	Average Cost per Mbps (Q2 2020)
Asia-Pacific	\$0.14	\$0.14	\$0.10
Eastern Europe	\$0.41	\$0.36	\$0.33
Latin America	\$1.52	\$1.51	\$1.19
Middle East and Africa	\$2.22	\$2.75	\$2.63
North America	\$ 0.31	\$ 0.28	\$ 0.26
South and East Asia	\$ 0.32	\$ 0.31	\$ 0.25
Western Europe	\$0.23	\$0.22	\$0.20

Table 7. According to Turk Telekom's unlimited internet data prices in Turkey (Converted to dollars at the exchange rates is dated January 29, 2020).

Internet Speed	Price	Average Cost per Mbps (TL)	Average Cost per Mbps (\$)
For 100 Mbps	330 TL	3,3 TL	0,57 \$
For 50 Mbps	310 TL	6,2 TL	1,10 \$
For 35 Mbps	290 TL	8,3 TL	1,44 \$
For 24 Mbps	270 TL	11,25 TL	1,95 \$
For 16 Mbps	255 TL	16 TL	2,77 \$.
For 8 Mbps	155 TL	19,4 TL	3,37 \$
For 100 Mbps	330 TL	3,3 TL	0,57 \$

According to these data, there is a slow internet service with insufficient infrastructure in Turkey and this service is given much more expensive than the world market. As mentioned before, this is a serious problem and there are important reasons for this problem to occur.

There are two factors that provide internet infrastructure service throughout Turkey. These are Turk Telekom and municipalities. Other operators providing internet services use the infrastructure of these two. Due to this situation, the quality of the service they provide cannot go beyond the borders set by Turk Telekom and the municipalities. A simple example of this situation can be seen in Table 8. This table shows the top 5 cities with the fastest internet in Turkey according to the report published by the Speedtest. Ankara is the first in this ranking, but it can be easily seen that there is no big difference between the internet speeds provided. 5 cities given in Table 8 is Turkey's large cities and it shows that provided internet speeds are kept quality within certain limits. This situation also shows that there is no competitive environment between the operators providing internet service or that this competitive environment prevents the formation [2].

Table 8. Cities with the fastest internet in Turkey

Rank	City	Average Download Speed (Mbps)	Average Upload Speed (Mbps)	Average Latency (ms)
1	Ankara	32.83	7.38	22
2	Istanbul	31.48	9.65	24
3	Izmir	29.72	8.61	28
4	Adana	26.59	7.24	30
5	Bursa	24.18	5.73	27

Considering the progress of the process, there are two options that an operator who wants to provide internet service can choose. These options offer their own strict rules and terms. It is impossible to exclude Turk Telekom from this equation due to its infrastructure found throughout the country. Being aware of this situation, Turk Telekom has brought the dimension of the business to the point of being a monopoly. In this way, it has become a leader in the market and attained the support to maintain this position. But the biggest reason behind this problem is municipalities. Operators who want to work with municipalities are faced with higher than expected rental rates at this time. While on one side there are high usage costs and strict rules, on the other side there are astronomical rental prices. In this case, it prevents the competitive environment desired to be created in the sector and the aimed progress. On the contrary, the desired competitive environment moves away from its purpose and turns into a track where municipalities and Turk Telekom compete with each other. The customer who cannot get their money's worth is most affected by this situation. But since no steps have been taken to resolve this situation, it has been going on for a long time.

5. CONCLUSION, DISCUSSION AND SUGGESTIONS

The internet, which has become an important requirement even in the most remote corner of the world and is an integral part of life, unfortunately cannot see the importance and value it deserves in Turkey. Also the internet, which is one of the most important weapons for accessing information in developing countries like us, plays a key role not only in this, but also in social life, technology and government affairs. While developing countries take the necessary steps to have this key in the best way, Turkey remains a spectator.

In Turkey, while only Turk Telekom and municipalities are in the field, others on the edge of the field as a spectator in this sector. That's why; this sector is breaking away from the world and dropping behind every day. This service, which slows down day by day compared to the world and on the contrary increases in price, is the greatest proof of this situation. The attitude of municipalities established to serve the public and working with public taxes and Turk Telekom, which has existed for many years and has reached a monopoly position in the sector are the two main reasons behind this situation. The fact that this sector is deprived of legal regulations prevents the operators providing internet service, except for these two institutions, from entering the sector. As a result, there is no competition and the desired progress cannot be achieved.

One of the most important steps to be taken in order to prevent this situation is to make legal regulations regarding the sector. In this way, Turk Telekom's power over the sector can be broken and the attitudes of the municipalities can be changed. If the attitudes of the municipalities are changed, other operators providing internet service can participate in the race. As a result of this situation, a healthy competitive environment is created and a service that will satisfy internet users is provided. Breaking the power of Turk Telekom will lead to breaking and changing the rules, and in this way the sector will become more balanced and more open to investment. In addition, the infrastructure problem in the country must be solved and investments in this area must be increased. Factors such as the quality of the equipment used, the higher quality and safer line used for transmission, the higher bandwidth used by the Internet Service Provider companies directly affect the internet speed. Looking at developed countries where Internet speed is high, the infrastructure usually used is fiber and performs faster transmission, but this increases the cost. If we want to be among the developed countries in the future, technology, therefore, the internet is an important step for this and it is very important to increase investments in this field.

It is great importance not only for us but also for our future generations that Turkey, which has great goals, can use the internet, which is one of the most powerful weapons in this process. Internet is one of the most important colors in the palette that will paint the future.

REFERENCES

- [1] Tahta, M., Comparison of Classic and Cloud Domain Name System for Internet Service Providers. <https://ab.org.tr/ab17/bildiri/78.pdf>, Access Date: 18.11.2020.
- [2] Speedtest CLI, 2021, Speedtest Global Index, <https://www.speedtest.net/global-index>, Access Date: 10.02.2021
- [3] Pastor-Satorras, R., & Vespignani, A. (2007). Evolution and structure of the Internet: A statistical physics approach. Cambridge University Press.
- [4] Güngör, M., & Evren, G. (2002). Internet Sector and Turkey Reviews. Telecommunications Authority Tariffs Department, Ankara. <http://tacs.eu/>. Access Date: 18.11.2020. <http://tacs.eu/tr/pdf/internet.pdf>.
- [5] Parlak, A., & Balık, H. (2005). Internet and Internet Development in Turkey. Firat University, Faculty of Engineering, Department of Electrical and Electronics, Elazığ. Access Date: 18.11.2020. <http://www.hasanbalik.com/Projeler/Bitirme/39.Pdf>.
- [6] Güngör, M., & Tözer, A. (2008). Broadband Internet Services: Current Situation Assessment and Recommendations in Turkey. http://inet-tr.org.tr/inetconf13/kitap/gungor_tozer_inet08.pdf. Access Date: 18.11.2020
- [7] Sezgin, E., & Kasalak, T. F. A Study on Turkey's Internet and Broadband Data. Access Date: 18.11.2020. <https://ab.org.tr/ab12/bildiri/8.pdf>
- [8] Rives, A. W., & Galitski, T. (2003). Modular organization of cellular networks. Proceedings of the national Academy of sciences, 100(3), 1128-1133.

- [9] Yavuz, B., & Soydaş, H. (2010). Mobile Broadband Development and Evaluation of 4th Generation (4G) Mobile Communication System LTE. Article ID, 83, 10-12. <https://www.academia.edu/>. Access Date: 18.11.2020.
- [10] Liu, Y. H., Prince, J., & Wallsten, S. (2018). Distinguishing bandwidth and latency in households' willingness-to-pay for broadband internet speed. *Information Economics and Policy*, 45, 1-15.
- [11] Kumaravel, K. (2011). Comparative study of 3G and 4G in mobile technology. *International Journal of Computer Science Issues (IJCSI)*, 8(5), 256.
- [12] Schrewe, B. (2021). Connected from coast to coast to coast: Toward equitable high-speed Internet access for all. *Paediatrics & Child Health*. <https://academic.oup.com>, Access Date: 08.02.2021. <https://academic.oup.com/pch/advance-article-abstract/doi/10.1093/pch/pxaa129/6096381>.
- [13] Özcerit, A., & Altunay, H. (2014). Performance Analysis of Turkey's Internet Network Infrastructure. *Sakarya University Journal of Science and Technology*, 18(3), 167-170. <https://www.researchgate.net/>. Access Date: 18.11.2020.
- [14] Steimer, H. (2020). Firm responses to high-speed internet (No. 258). Discussion Paper. <https://www.econstor.eu/handle/10419/225266>, Access Date: 08.02.2021.
- [15] TUIK, 2020, "Household Information Technologies (IT) Usage Survey", [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2020-33679](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2020-33679), Access Date: 13.02.2021
- [16] BTK Market Data, 2020, <https://www.btk.gov.tr/pazar-verileri>, 2020-Q4 Access Date: 29.03.2021
- [17] POINT TOPIC, 2020, "Fixed broadband tariffs in Q2 2020", <http://point-topic.com/free-analysis/fixed-broadband-tariffs-in-q2-2020/>, Access Date: 15.02.2021
- [18] Elif Akgül, 2020, "Slow Internet and Expensive Being in Turkey Is it a preference?" 29.01.2020, <https://www.freewebsiteurkey.com/turkiyede-internetin-yavas-ve-pahali-olmasi-bir-tercih-mi/> Access Date: 18.02.2021



Research Article

INVESTIGATION OF HOLE SHAPE EFFECT ON STATIC ANALYSIS OF PERFORATED PLATES WITH STAGGERED HOLES

Authors: Mustafa Halûk Saraçoğlu* , Fethullah Uslu , Uğur Albayrak 

***Corresponding Author:** mhaluk.saracoglu@dpu.edu.tr

To cite to this article: Saraçoğlu, M., H., Uslu, F., Albayrak, U., (2021). Investigation of Hole Shape Effect on Static Analysis of Perforated Plates with Staggered Holes, International Journal of Engineering and Innovative Research, 3(2), p 133-144.

DOI: 10.47933/ijeir.883510

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



INVESTIGATION OF HOLE SHAPE EFFECT ON STATIC ANALYSIS OF PERFORATED PLATES WITH STAGGERED HOLES

Mustafa Halûk Saraçoğlu^{1*}, Fethullah Uslu¹, Uğur Albayrak²

¹Kütahya Dumlupınar University, Faculty of Engineering, Department of Civil Engineering, Kütahya, Turkey.

²Eskişehir Osmangazi University, Faculty of Engineering, Department of civil engineering, Eskişehir, Turkey.

*Corresponding Author: mhaluk.saracoglu@dpu.edu.tr

(Received: 19.02.2021; Accepted: 10.04.2021)

<https://doi.org/10.47933/ijeir.883510>

ABSTRACT: In this paper, a series of analysis with finite element method was carried out with varying hole shapes of perforation as well as plate dimensions. Eight different models about holes that number of edges at the hole is four to infinite namely circular holes was presented. Then the analyze results of these models with different boundary conditions as fixed supported and simply supported at four edges were compared. In this study it has shown that when the number of edges for a hole is infinite, in other words when the perforation of the plate is circular, mid-point deflection is decreasing according to the other perforation styles. And also analyze results of eight different models of perforated plates are given in tables and comparative graphs.

Keywords: Ansys, Noncircular hole, 60° staggered perforated, Square thin plate, Mid-point deflection, Equivalent (von Mises) stress.

1. INTRODUCTION

The square thin plates made of steel are structural elements that are largely used in civil and mechanical engineering. In some cases they are also used as perforated plates by composing holes on the plates. The perforated plates have some advantages over non-perforated plates. These elements have many different usage areas in the automotive and air industries as vehicles and aircrafts manufacturing, and also furniture manufacturing, construction industry, distilling, food refining, mining and plenty of more uses.

Perforated steel plates have technical advantages over expanded metal, welded wire, woven wires, which can be used as an alternative to these perforated elements. The functional capacity of perforated plates compared to these other materials is distinguished when considering filtration, ventilation, radiation protections, sound absorption, and others. One of the advantage of perforated plates is its variability in allowing a variation of combinations of open areas in a single sheet.

There are many studies about analysis of perforated plates in literature. In the studies generally experimental and numerical methods have been used. Numerical methods that are using finite element method is the most preferred one among the solutions [1-5]. Perforated plates with in-plane loading are also interested with some researchers [6], [7].

Bailey and Hicks is developed a theoretical method for determining the elastic behaviour of end-loaded plates completely perforated with closely spaced circular holes forming a square or diagonal pattern [8].

For perforated plates which have many holes, the shape of the holes will affect the value and location of the maximum stresses. In this subject Jafari and Jafari investigated the stress distribution around holes with different shapes in an infinite composite plate under uniform heat flux. In their study, the effect of various parameters on stress distributions around a different hole in an infinite composite plate was separately investigated [9].

Pascu et.al, describe the method of calculating the forces which appear at the bending of perforated plates with holes of different shapes and placed in different patterns in their study [10].

Konieczny et.al., presents an analysis of an isotropic circular axisymmetric perforated plate loaded with concentrated force applied in the geometric center of the plate using finite element software ANSYS [11], [12].

Kalita and Halder, investigated the deflection and stresses for isotropic and orthotropic plates with central circular and square cutout under transverse loading by using finite element package ANSYS [13].

Atanasiu and Sorohan, studied the stress distribution in a circular plate of Plexiglas with a diameter of 300 mm and thickness of 10 mm, perforated by 96 circular holes of diameter 12 mm, arranged in a grid of squares of 24 mm by using the finite element analysis (FEA) and experimentally. Load is acting through a central concentrated load and distributed load and considered as simply supported on its exterior margin. And also they studied a non-perforated plate of the same supports, the same material and the same load condition to make a comparisons between the behaviour of the two types of plates [14].

Andh et. Al., investigated the stress analysis of finite plate with special shaped cut out for stress distribution and Stress Concentration Factors (SCF) by using the finite element method and photoelasticity. And also an experimental investigation is taken to study for the stress analysis of plates with special shaped cut outs [4].

Rayhan performed a finite element analysis on the buckling behavior of a simply supported quasi-isotropic symmetric composite panel with central circular cutouts, reinforced with stiffeners on both sides of the cutouts under uniaxial, biaxial and combined loading conditions by using popular commercial software code Ansys [19].

Jafari et al., investigated the optimal values of effective parameters on the stress distribution around a circular/elliptical/quasi-square cutout in the perforated orthotropic plate under in-plane loadings. They use the PSO algorithm in their study to determine the optimal design variables to increase the strength of the perforated plates. And also finite element method (FEM) was employed to examine the results of the present analytical solution [20].

Lorenzini et. al., studied the influence of the type and shape of the hole in the behavior of buckling perforated steel plates numerically [15].

Helbig et. al., investigated the influence of the shape, size and type of the opening in the buckling behavior of a thin steel plate by developing some computational models using ANSYS software [16].

There are not much works about various shaped holes for perforations in perforated plates, justifying the present research. However, here only the perforated thin square plate bending behavior is studied, for investigating about various hole type effect that were not much performed previously. The present work employs the computational modeling for the study of fixed supported and simply supported thin steel perforated square plates subjected to the uniformly distributed load and its self-weight.

2. METHODS

The Plates are solid bodies bounded by two parallel planes and the thickness of the plate which is the separation between these two parallel planes is small compared with the lateral dimensions (Figure 3). They are solid bodies but it is often not necessary to model plates using three-dimensional elasticity theory. Stress and strain analysis of three dimensional plates under plane stress or plane strain can be treated as two dimensional problems [17].

Compatibility equations and boundary conditions must be provided together in the solution of equilibrium equations of two dimensional problems. By neglecting the components of body force per unit volume, the equation of equilibrium for forces in the x- direction and y-direction is follows respectively:

$$\frac{\partial \sigma_x}{\partial x} + \frac{\partial \sigma_{xy}}{\partial y} = 0 \quad (1)$$

$$\frac{\partial \sigma_y}{\partial y} + \frac{\partial \sigma_{xy}}{\partial x} = 0 \quad (2)$$

The compatibility equation in terms of stress components is as follows:

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right) (\sigma_x + \sigma_y) = 0 \quad (3)$$

Substituting the stress components in equation 1, 2 and 3 by displacements u and v is as follows:

$$\frac{\partial^2 u}{\partial x^2} + \frac{(1-\nu)}{2} \left(\frac{\partial^2 u}{\partial y^2} \right) + \frac{(1+\nu)}{2} \left(\frac{\partial^2 v}{\partial x \partial y} \right) = 0 \quad (4)$$

$$\frac{\partial^2 v}{\partial y^2} + \frac{(1-\nu)}{2} \left(\frac{\partial^2 v}{\partial x^2} \right) + \frac{(1+\nu)}{2} \left(\frac{\partial^2 u}{\partial x \partial y} \right) = 0 \quad (5)$$

In this equations ν is the Poisson's ratio of the material. By reducing the problem to a single function $\phi(x,y)$ which can take place of the two displacement functions u and v and satisfies the equations 4 and 5, solution can be defined as serial solutions. This displacement function $\phi(x,y)$ can be defined as follows:

$$u = \frac{\partial^2 \phi}{\partial x \partial y} \tag{6}$$

$$v = - \left[(1-\nu) \left(\frac{\partial^2 \phi}{\partial y^2} \right) + 2 \left(\frac{\partial^2 \phi}{\partial x^2} \right) \right] / (1-\nu) \tag{7}$$

In this way, a series of solutions are obtained for equilibrium equations. The exact solution of the problem is also the solution that provides the compatibility equations. Thus, if the body force of the plate is neglected, the solution of a two-dimensional problem is reduced to finding the solution that provides the boundary condition of equation (8).

$$\frac{\partial^4 \phi}{\partial x^4} + 2 \left(\frac{\partial^4 \phi}{\partial x^2 \partial y^2} \right) + \frac{\partial^4 \phi}{\partial y^4} = 0 \tag{8}$$

By using a combination of the kinematic, constitutive, force resultant, and equilibrium equations, the classical plate equation of Kirschhoff can be derived as in equation (9).

$$\frac{\partial^4 w}{\partial x^4} + 2 \left(\frac{\partial^4 w}{\partial x^2 \partial y^2} \right) + \frac{\partial^4 w}{\partial y^4} = \frac{q}{D} \tag{9}$$

In this equation w is the small transverse (out-of-plane) displacement of a thin plate, q is the distributed load acting transversely on the plate as shown in figure 3 and D is the flexural rigidity of the plate defined as in equation [10].

$$D = \frac{E h^3}{12(1-\nu^2)} \tag{10}$$

E is the Young's modulus, h is the thickness of the plate and ν is the Poisson's ratio of the plate material.

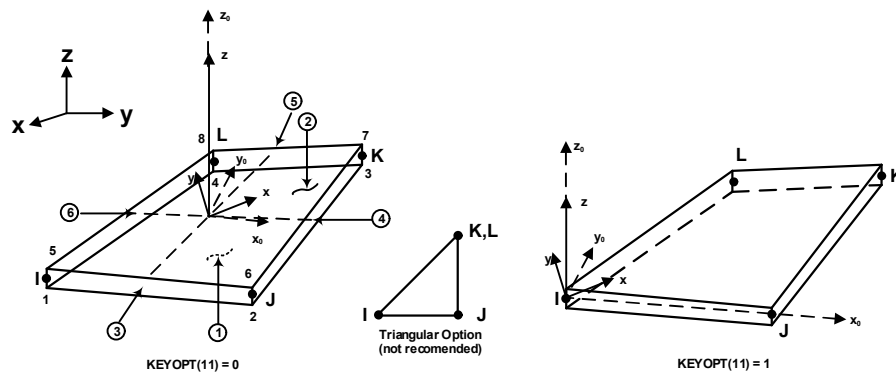


Figure 1. Geometry of SHELL181 finite element in ANSYS [18].

The ANSYS finite element software is also used in the modeling of plates. For this purpose, firstly, the material properties and the geometric properties of the element are defined and then plate is divided into finite elements. SHELL 181 element which is a 4-Node Structural Shell is selected from ANSYS library.

“Shell181” is a 4-node structural finite element in the program element library as shown in Figure 1. The element has six degrees of freedom at each node: translations in the nodal x , y and z directions and rotations about the nodal x , y and z -axes.

Firstly, the geometry of the problem is defined in the program and a model is created. Then material properties and elements are defined. For the calculations the definition of static analysis is made. Fixed supported and simply supported boundary conditions of the perforated square plates are defined separately. A load of uniformly distributed $q=1 \text{ kN/m}^2$ load to the plate surface and its own weight is applied at the $-Z$ direction. After these processes were completed, static analysis was performed and the results of deformation were obtained from the program.

Stress output for SHELL181 element is as follows:

σ_x is normal stress due to X axis (SX)

σ_y is normal stress due to Y axis (SY)

σ_{xy} is shear stress (SXY)

3. NUMERICAL EXAMPLES

Three different dimensioned square thin perforated plates have analyzed. One dimension of square plate is taken as 300 mm, 450 mm and 600 mm. In all of these three sets of plate examples, thickness to length ratio was taken constant as 1/150 in all examples to provide thin plate assumptions. So that thickness of the plates are 2 mm, 3 mm and 4 mm respectively (Table 2).

The plate models are assumed made of steel material. The material parameters of the steel plates are shown in Table 1.

Table 1. Material properties

Property	Value
Young's modulus, E (GPa)	200
Poisson's ratio, ν	0.3
Mass density, ρ (kg/m ³)	7850

Every set of plates has the same open area percentage in itself as shown in Table 3 but different hole shapes. Area of a one hole is defined as $A = \frac{1}{4} n k^2 \cot\left(\frac{\pi}{n}\right)$. In this equation n is the number of edges and k is the length of a one edge in the polygon.

Table 2. Parameters of perforated square plates

Length a (mm)	Thickness h (mm)	Number of holes	Open area percentage (%)
300	2	264	33.18
450	3	634	35.41
600	4	1166	36.63

For each set of plate example, eight different models and a non-perforated plate have been arranged as shown in Table 3. In the models number of edges increases from four to infinite. When the number of edges are four, there are square holes at the perforated plate. When the number of edges are infinite, there are circular holes at the perforated plate (Figure 2).

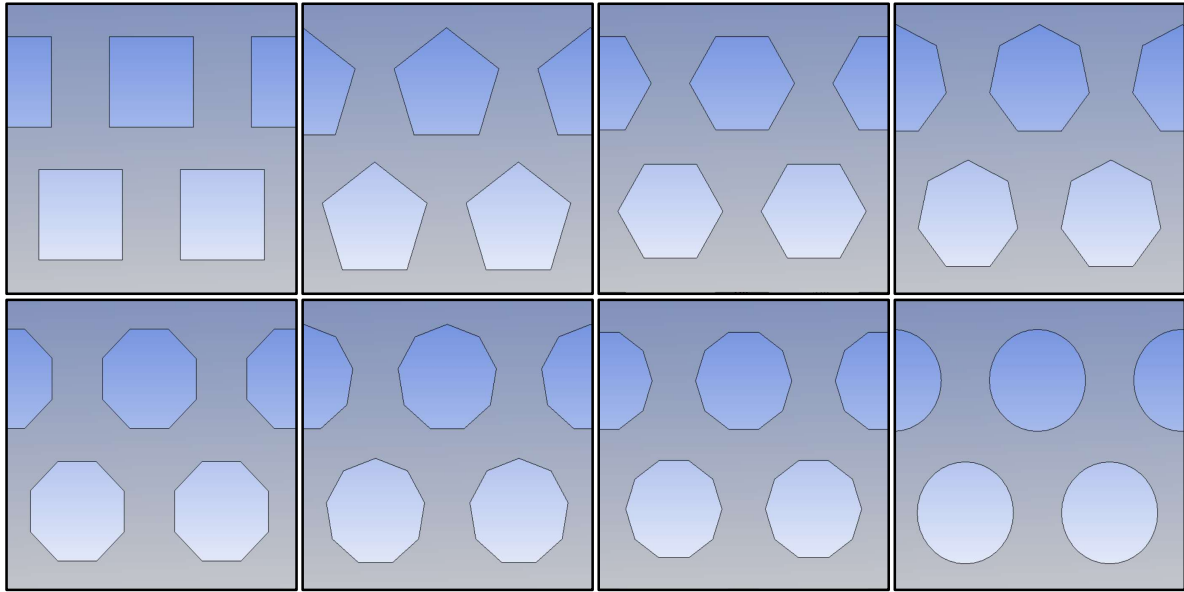


Figure 2. Perforated plate models.

Coordinates, loads and perforation schema for investigated plate models is shown in Figure 3. As shown in figure loads are applied at the $-Z$ direction and magnitude of uniformly distributed load is $q=1 \text{ kN/m}^2$. Perforated square plate’s own weight is also considered.

This study investigates which the hole geometry has the minimum displacements and stresses. For this purpose 600 staggered pattern distribution which is one of the most popular shape in the perforated metal industry has been used.

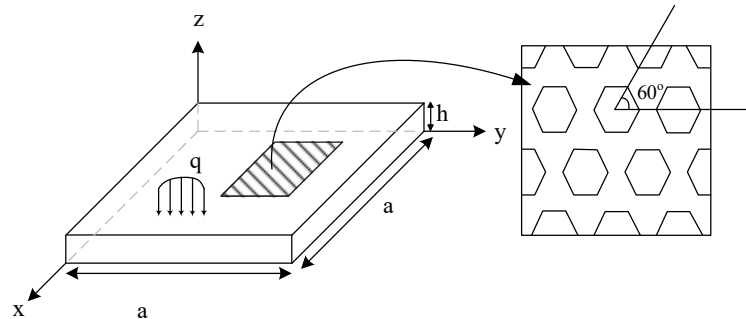


Figure 3. Coordinates, loads and perforation schema for plate models.

Stress and displacement analysis of perforated square plates are investigated. Midpoint deflections and critical stresses are calculated. Two different boundary conditions as simply supported and fixed supported are considered. Hole information for perforated plates is shown in Table 3. Since the number of holes is constant in all models, the percentage of open hole areas in the plates are also constant.

Table 3. Information for perforated plate models.

Model no	Model name	Number of edges on hole	Length of edge on hole (mm)
1	Square	4	10.634723
2	Pentagon	5	8.107775
3	Hexagon	6	6.597817
4	Heptagon	7	5.578776

5	Octagon	8	4.839755
6	Nonagon	9	4.277282
7	Decagon	10	3.833930
8	Circle	∞	0.000000
9	Non-perforated	-	-

4. RESULTS AND DISCUSSION

The bending behavior of various perforated plates were numerically simulated by means of the ANSYS software, which is based on the finite element method. Three sets of perforated square plates and eight different models for each set together with non-perforated plate are investigated.

Table 4. Mid-point deflections of perforated square plates (mm).

a(mm) edges	Fixed Supported			Simply Supported		
	300	450	600	300	450	600
4	-0.10652	-0.18747	-0.28346	-0.37807	-0.64420	-0.96540
5	-0.10240	-0.17872	-0.26827	-0.36466	-0.61354	-0.90736
6	-0.10127	-0.17645	-0.26437	-0.36083	-0.60614	-0.89488
7	-0.09985	-0.17335	-0.25930	-0.35587	-0.59588	-0.87818
8	-0.09941	-0.17248	-0.25767	-0.35429	-0.59276	-0.87257
9	-0.09915	-0.17187	-0.25669	-0.35340	-0.59089	-0.86950
10	-0.09899	-0.17153	-0.25611	-0.35285	-0.58972	-0.86755
∞	-0.09856	-0.17064	-0.25468	-0.35130	-0.58676	-0.86284
0	-0.08079	-0.12927	-0.18314	-0.26054	-0.41701	-0.59085

Mid-point deflections of all sets and models of perforated square plates are shown in Table 4. Calculations indicate that the maximum deflection of the perforated square plate under distributed load acting perpendicular to the plate surface is at the mid-point of it. From the table one can see that mid-point deflections of perforated plates are greater than non-perforated ones. And also when the number of edges increases mid-point deflections are decreases. The difference of mid-point deflections between the models are decreases when the number of hole edge increases and this ratio is the biggest between non-perforated and perforated ones. This behavior is similar for fixed supported and simply supported boundary conditions but the difference between non-perforated plates is much bigger for simply supported models.

As an example mid-point deflections of perforated square plates for a=300 mm and h=2 mm is shown in the Figure 4.

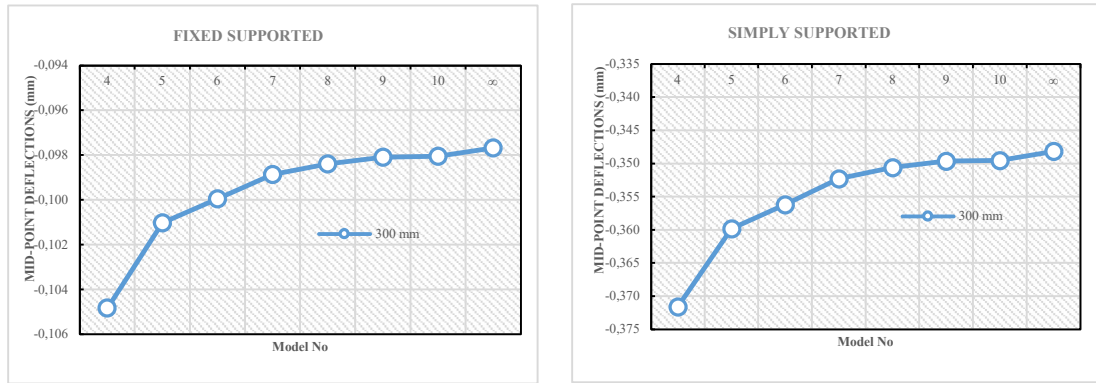


Figure 4. Mid-point deflections of perforated square plates for a=300 mm.

The values in the figure are for perforated square plates with fixed supported and simply supported at four edges. And the mid-point deflections for perforated square plates with eight different shaped hole models are also shown at the figure.

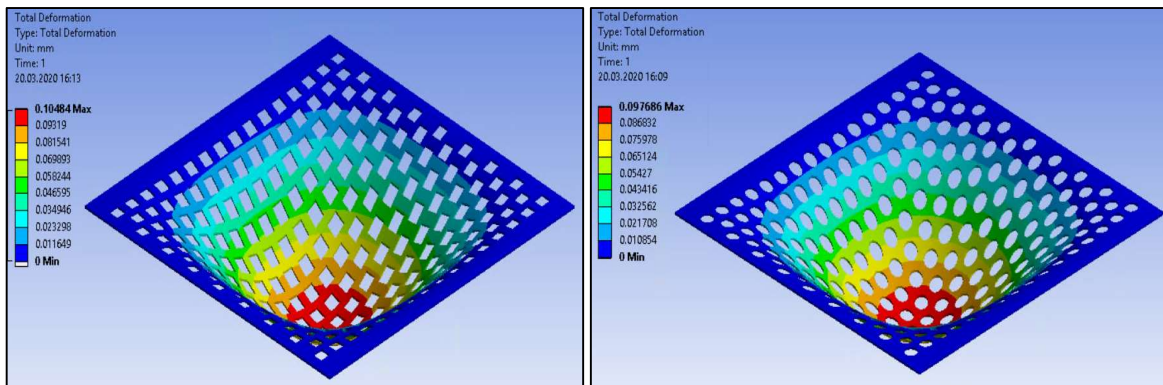


Figure 5. Mid-point deflections of perforated plates for square and circular models.

Mid-point deflections of perforated square plates which have square holes and circular holes are depicted in Figure 5. In the figure square plates have 300 mm length in one edge and have fixed supported boundary conditions at the four edges.

Table 5. Critical stresses of the plates subjected to a uniformly distributed load (MPa).

Model no	Fixed Supported				Simply Supported			
	S _y	S _x	S _{xy}	Von-Mises	S _y	S _x	S _{xy}	Von-Mises
1	10.5749	12.3315	4.0274	12.1918	13.1865	15.0102	8.7468	19.1774
2	12.4436	12.1358	3.8199	11.9058	16.8273	15.9662	8.4672	17.7789
3	12.6162	10.5776	3.6768	11.9822	18.2594	14.0572	8.1429	17.0617
4	10.6838	9.9117	3.3514	10.3062	14.8732	14.9453	7.5134	15.4733
5	9.5229	9.7359	3.5400	10.0716	13.0527	13.4008	7.1670	14.9605
6	10.3149	10.1714	3.5512	9.9939	14.5713	13.5096	7.0957	14.4206
7	9.6228	9.5203	3.3497	9.7380	13.0294	13.5271	7.0863	14.3009
8	8.7277	8.2747	2.9016	8.6012	12.3388	11.3666	7.0542	12.4904

As an example, maximum stresses of square plates with eight different shaped hole models for $a=300$ mm and $h=2$ mm is given in the Table 5. The values in the table are for perforated square plates with fixed supported and simply supported at four edges.

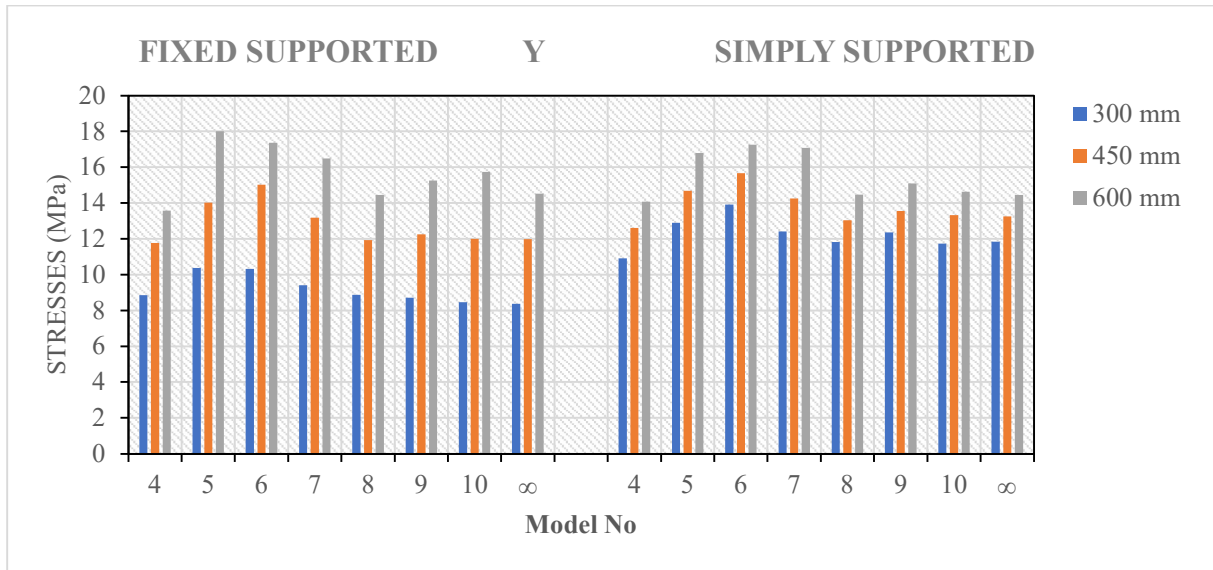


Figure 6. Absolute maximum SY stresses.

Absolute maximum SY stress values for three different sizes of square perforated plates are shown in the Figure 6. The values in the figure are for perforated square plates with fixed supported and simply supported at four edges.

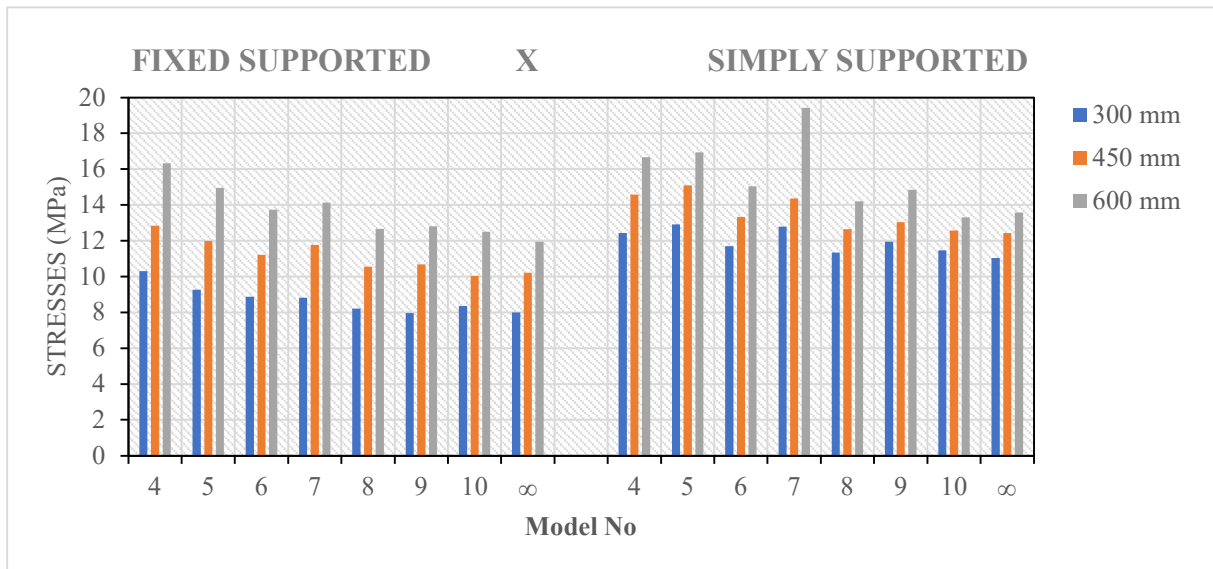


Figure 7. Absolute maximum SX stresses.

Absolute maximum SX stress values for three different sizes of square perforated plates are shown in the Figure 7. The values in the figure are for perforated square plates with fixed supported and simply supported at four edges.

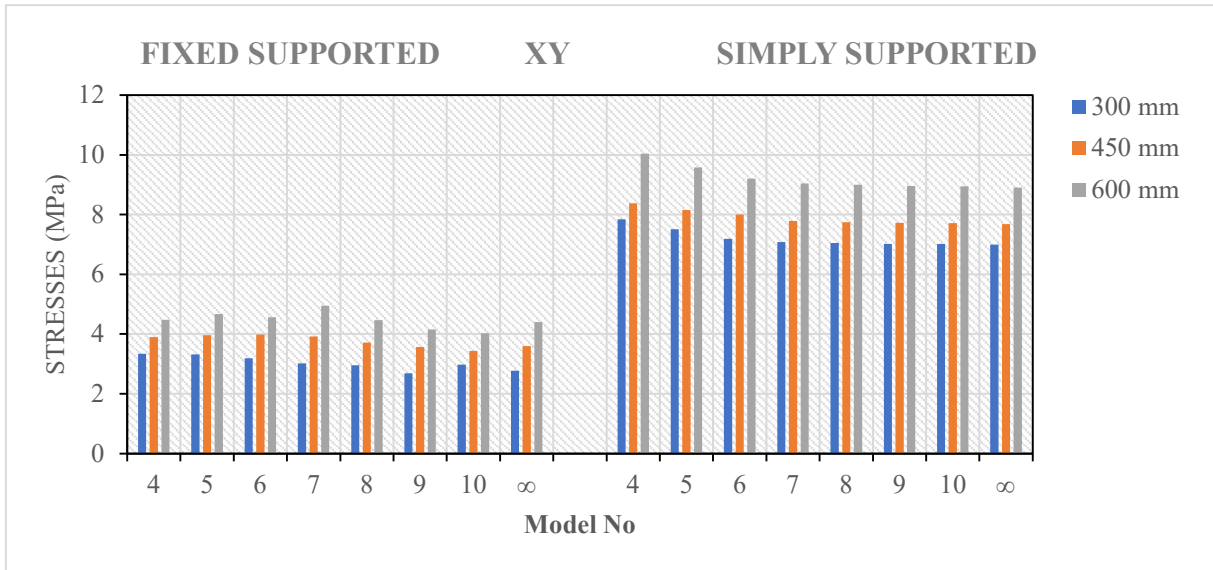


Figure 8. Absolute maximum SXY stresses.

Absolute maximum SXY stress values for three different sizes of square perforated plates are shown in the Figure 8. The values in the figure are for perforated square plates with fixed supported and simply supported at four edges.

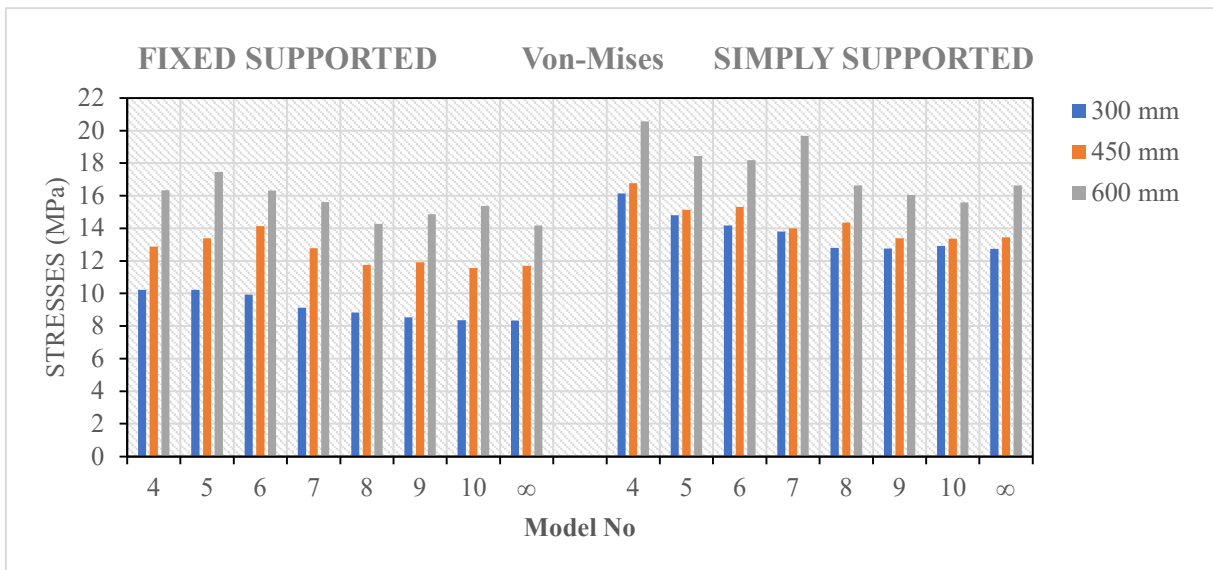


Figure 9. Absolute maximum equivalent Von-Mises stresses.

Absolute maximum equivalent Von-Mises stress values for three different sizes of square perforated plates are shown in the Figure 9. The values in the figure are for perforated square plates with fixed supported and simply supported at four edges.

5. CONCLUSIONS

Bending of perforated square thin plates made of steel with three different thickness 2mm, 3mm and 4mm are investigated under self-weight and 1kN/m² uniformly distributed loads. Thickness to length ratio is constant as 1/150. The results that were obtained with numerical calculations by using ANSYS software have been compared. Every perforated plate example has the same open area percentage in itself but different hole shapes. For perforated plate

examples eight different models that has different number of hole edges from four to infinite have been arranged and also a non-perforated plate example examined to understand the effect of perforation. The aim of the study is investigating the hole geometry which makes the minimum displacements and stresses on perforated plate. For examined problems the most commonly used pattern distribution 600 staggered has been used.

It is important to highlight that the present work has shown that when the number of edges is infinite, in other words when the perforation of the plate is circular, it has more advantage than the other perforation styles. This investigation is made with defining several geometrical configurations and the total material volume of the perforated plate sets for all models were keeping constant. And also, a performance comparison among the defined hole geometries of perforated plate has been carried out.

Therefore, based on the obtained results, the importance of the geometrical evaluation in structural engineering, as well as the effectiveness of the constructional design method application in the mechanics of material problems, is evident.

The bending analysis about the effect of number of hole edges over the geometric configurations of the perforated square plates, as well as the graphical representation of the stress distribution for all plate models, can be found in this study.

REFERENCES

- [1] M. H. Saraçoğlu and U. Albayrak, "Linear static analysis of perforated plates with round and staggered holes under their self-weights," *Res. Eng. Struct. Mater.*, vol. 2, no. 1, pp. 39–47, 2016.
- [2] U. Albayrak and M. H. Saraçoğlu, "Analysis of Regular Perforated Metal Ceiling Tiles," *Int. J. Eng. Technol.*, vol. 10, no. 6, pp. 440–446, 2018.
- [3] S. Singh, K. Kulkarni, R. Pandey, and H. Singh, "Buckling analysis of thin rectangular plates with cutouts subjected to partial edge compression using FEM," *J. Eng. Des. Technol.*, vol. 10, no. 1, pp. 128–142, Mar. 2012.
- [4] U. B. Andh, S. M. Chavan, S. G. Kulkarni, and S. N. Khurd, "Stress analysis of perforated plates under uniaxial compression using FEA and photoelasticity," *Int. Res. J. Eng. Technol.*, 2016.
- [5] J. Rezaeepazhand and M. Jafari, "Stress analysis of perforated composite plates," *Compos. Struct.*, vol. 71, no. 3–4, pp. 463–468, Dec. 2005.
- [6] A. M. Sayed, "Numerical analysis of the perforated steel sheets under uni-axial tensile force," *Metals (Basel)*, vol. 9, no. 6, pp. 1–16, 2019.
- [7] M. Diany, "Effects of the Position and the Inclination of the Hole in Thin Plate on the Stress Concentration Factor," vol. 2, no. 12, pp. 8–12, 2013.
- [8] R. H. R. Bailey, "Behaviour of perforated plates under plane stress," *J. Mech. Eng. Sci.*, vol. 2, no. 2, pp. 143–165, 1960.
- [9] M. Jafari and M. Jafari, "Effect of hole geometry on the thermal stress analysis of perforated composite plate under uniform heat flux," *J. Compos. Mater.*, vol. 53, no. 8, pp. 1079–1095, 2019.
- [10] E. Pascu, A., Oleksik, M., Avrigean, "Experimental method for determining forces at bending of perforated plates," *Acta Universitatis Cibiniensis – Tech. Ser.*, vol. 69, no. 1, pp. 52–58, 2017.
- [11] H. Achtelik, G. Gasiak, and J. Grzelak, "Strength tests of axially symmetric perforated plates for chemical reactors: Part 2-Experiments," *Int. J. Press. Vessel. Pip.*, vol. 85, no. 4, pp. 257–264, 2008.
- [12] M. M. Konieczny, H. Achtelik, and G. Gasiak, "Finite element analysis (FEA) and experimental stress analysis in circular perforated plates loaded with concentrated force," *Frat. ed Integrita Strutt.*, vol. 14, no. 51, pp. 164–173, 2020.
- [13] K. Kalita and S. Halder, "Static analysis of transversely loaded isotropic and orthotropic plates with central cutout," *J. Inst. Eng. India Ser. C*, vol. 95, no. 4, 2014.
- [14] C. Atanasiu and S. Sorohan, "Displacements and stresses in bending of circular perforated plate," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 147, no. 1, 2016.
- [15] G. Lorenzini et al., "Numerical evaluation of the effect of type and shape of perforations on the buckling of thin steel plates by means of the constructional design method," *Int. J. Heat Technol.*, vol. 34, no. S1, pp. S9–S20, Jan. 2016.

- [16] D. Helbig, C. C. C. Da Silva, M. de V. Real, E. D. dos Santos, L. A. Isoldi, and L. A. O. Rocha, “Study about buckling phenomenon in perforated thin steel plates employing computational modeling and constructal design method,” *Lat. Am. J. Solids Struct.*, vol. 13, no. 10, pp. 1912–1936, 2016.
- [17] Timoshenko, S, Goodier, J. N., *Theory of Elasticity*. McGraw-Hill, Newyork, USA, 1951.
- [18] A. Swanson Analysis System Inc., “ANSYS User’s manual.” 2005.
- [19] S.B. Rayhan, “Elastic buckling response of a composite panel stiffened around cutouts,” *International Journal of Engineering, Transactions A: Basics*, vol. 34, no. 1, 2021.
- [20] M. Jafari, S. A. Mahmodzade Hoseyni, H. Altenbach, E. Craciun, “Optimum design of infinite perforated orthotropic and isotropic plates,” *Mathematics*, vol. 8, no. 4, 2020.



Review Article

SECURITY CONTROLS AGAINST MOBILE APPLICATION THREATS OF ANDROID DEVICES

Authors: Ahmet Efe , Şerife Özdamarlar 

To cite to this article: Efe, A., Özdamarlar, Ş., (2021). Security Controls Against Mobile Application Threats of Android Devices, International Journal of Engineering and Innovative Research, 3(2), p 145-162.

DOI: 10.47933/ijeir.838873

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



SECURITY CONTROLS AGAINST MOBILE APPLICATION THREATS OF ANDROID DEVICES

Ahmet Efe^{1*}, Şerife Özdamarlar²

¹ Dr., CISA, CRISC, PMP, Ankara Development Agency, TURKEY.

² Department of Computer Engineering, Yıldırım Beyazıt University, TURKEY.

*Corresponding Author: aefer@ankaraka.org.tr

(Received: 10.12.2020; Accepted: 03.02.2021)

<https://doi.org/10.47933/ijeir.838873>

ABSTRACT: In the ever developing world of technology, mobile applications are increasing day by day alongside with mobile cyber threats as the new cutting edge technology makes continuous advances. This fact is valid as a result of shifts from e-government to m-government and classical e-business to m-business solutions as a requirement of user friendly and secure mobile technology and applications. The main threat is to the critical and sensitive personal data and information that can be captured by malicious codes and hence dangerous results can be faced. In this paper, malicious software and security techniques of the android mobile applications are analyzed in addition to protection systems from user, developer aspects and even Google Play. The main issue of this paper is providing a current picture of the security concerns of the mobile applications and some sets of counter controls for covering the risks and vulnerabilities of mobile applications in the Android platforms.

Keywords: Cyber security, Android application security, malicious software, mobile security.

1. INTRODUCTION

Mobile device usage is increasing and applications are developed day by day. Mobile device generally is tablet computer and cell phone which is like a small computer instead of only cell phone functionality such as SMS and voice-calls. Banking operations, social interactions, shopping, reading and editing can be examples of these small computers. Privacy analysis or phishing can be made with the data generate through mobile applications. Application permissions are an important problem that threats privacy and business-critical information elements. Some applications request all permissions whether necessary or not and usually majority of users tend to give what they want. There are a little percentage of users who have knowledge about the permission if required and safe or not. Users' personal data which are identity information, photographs, affiliation, location information and messages can be captured with these permissions and attacker can use this information. Because of the fact that android is an open source and it's the top system which are mostly being used by developers and vendors, there are lots of attacks for Android operating system. So the security risk is emerging in the mobile applications and many are not aware of it as is shown in the figure 1.

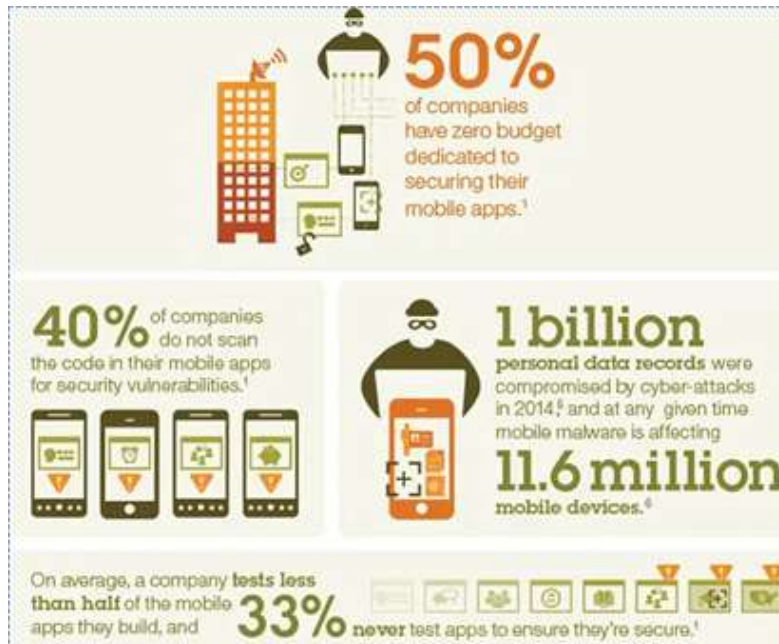


Figure 1. Impact of Weak Mobile App Security [IBM].

Like personal computers, mobile devices run on operating systems with their own vulnerabilities and security issues. Therefore, the increase in mobile device usage has led security experts to improve mobile application security processes while hackers improve their sophistication. Since the secure configuration of mobile devices as hardware is not commercially preferred, data must be protected by certain software on mobile devices and user awareness play a very crucial role here.

Mobile cloud computing is also one of the most important problems of mobile application security that needs to be discussed. Cloud computing on mobile platforms triggers a new wave of evolution as well as new security risks and vulnerabilities in the rapidly developing mobile world. While a few striking studies have been done on the computing counterparts of mobile technology, the cloud computing space for the mobile world seems largely unexplored. The research conducted by Swarnpreet et al. Introduced the Mobile Cloud Computing (MCC) concept, its internal processes and various applicable architectures related to MCC. Cloud computing is computing that provides virtualized IT resources as a remote service using Internet technology. In cloud computing, the user lends and uses IT resources such as software, storage, server, network and security as required, receives real-time scalability support according to the service load, and payments are made accordingly. In particular, the cloud computing environment distributes IT resources and allocates them according to the user's wishes, so some work should be done on the technology that manages these resources and deals with them effectively [1]

The problem faced by software products supporting mobile applications is insurmountable cyber security issues. Specifically, there are three main problems that are most cited:

- A hostile host can send code to another host with undesirable behavior. Currently, there seems to be no way to ensure that a hostile host cannot inject unsafe code into the mobile application system.
- A mobile application cannot be easily protected from a hostile host. Specifically, when a mobile app arrives at a host and starts execution programs, this mobile app is still in the host's compassionate hands. In other words, there is no guarantee that the host will

execute computer instructions accurately and securely. There is not even any guarantee that the host computer will run any particular software; and

- The mobile application cannot be sent or received securely to a host other than a group of trusted computers known as the Trusted Computing Base (TCB).

All these security problems related to mobile applications need to be overcome for mobile applications to be accepted as an alternative to traditional computing systems. Therefore, it is desirable to provide a mobile application security system and method that overcomes the above problems and limitations with conventional mobile application systems. For this purpose, the present technological invention has been directed to use mobile applications in most financial, commercial, administrative and military computer systems [2].

The top ten mobile application risks that are defined by OWASP are as demonstrated in the Fig.2. OWASP is an open source Mobile Security Project and a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications [3].



Figure 1. Top 10 Mobile Risks in 2014 [3].

However in 2016 the top ten risks have been completely changed. This shows the degree of new technology and the characteristic of concomitant threats that are being renewed by time rapidly. The new ratings are as follows.

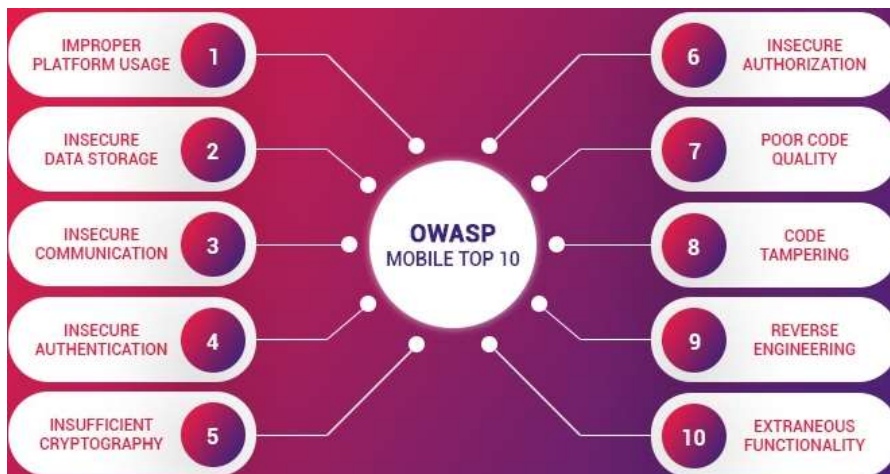


Figure 2. Figure 1. Top 10 Mobile Risks in 2016 [3].

Therefore, M1: Improper Platform Usage¹, M2: Insecure Data Storage², M3: Insecure Communication³, M4: Insecure Authentication⁴, M5: Insufficient Cryptography⁵, M6: Insecure Authorization⁶, M7: Poor Code Quality⁷, M8: Code Tampering⁸, M9: Reverse Engineering⁹ and M10: Extraneous Functionality¹⁰ are considered as the most dangerous threats of mobile applications. However, according to the latest reports, these risks have been completely changed due to new attack vectors that make the most of the newest technology advantages. Here is the new listing:

OWASP Top 10 Vulnerabilities in 2021 are:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring¹¹

Unlike web and desktop applications where system information leaks from outside in more applications than other types of vulnerabilities, more mobile applications contain more system information leaks than any other vulnerability. Internal system holes contain information disclosed to other mobile apps installed on the same system, a much greater concern in the mobile world. When paired with the previous year, several types of vulnerabilities created a Cameo, including Weak Encryption, Insecure Storage: Insecure Deployment: Incomplete Jailbreak Protection and Weak Cryptographic Hash replacing SQL Injection [4].

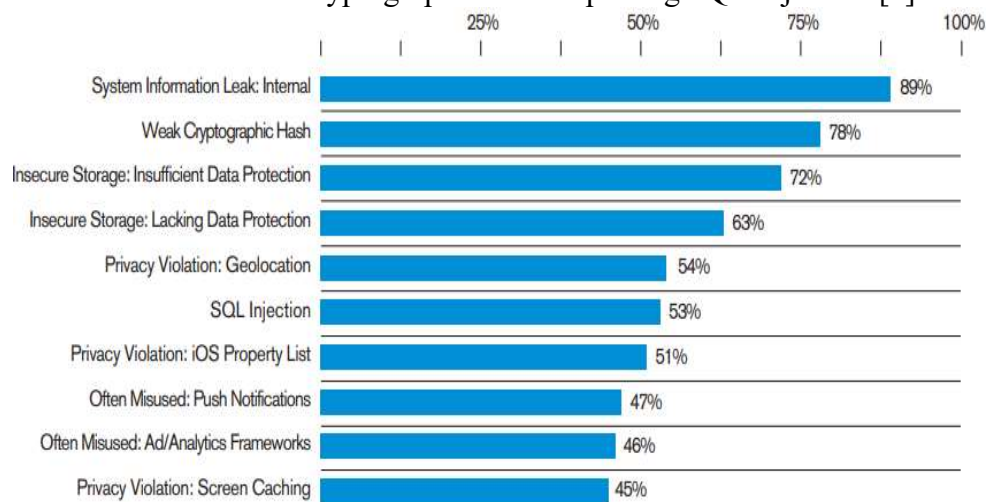


Figure 3. The 10 most commonly occurring vulnerabilities in the mobile applications dataset (Percentage of vulnerable mobile apps) [4].

¹ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M1-Improper_Platform_Usage

² For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M2-Insecure_Data_Storage

³ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M3-Insecure_Communication

⁴ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M4-Insecure_Authentication

⁵ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M5-Insufficient_Cryptography

⁶ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M6-Insecure_Authorization

⁷ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M7-Poor_Code_Quality

⁸ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M8-Code_Tampering

⁹ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M9-Reverse_Engineering

¹⁰ For details see: https://www.owasp.org/index.php/Mobile_Top_10_2016-M10-Extraneous_Functionality

¹¹ For the details of the data for the 2021 year see: <https://www.immuniweb.com/resources/owasp-top-ten/>

In this paper, brief information will be given about risks of cyber-attacks on mobile applications. For this reason, detection and protection of mobile malicious software will be analyzed. Also, the claim which is Android platform is not secure will be refuted with some relevant data from security reports. In addition, some suggestions will be given to application users and developers.

2. RELATED WORKS

The rate of upgrading traditional mobile phones to smartphones is tremendous nowadays, due to the extremely high leap in functionality. One of the most attractive features of smartphones is actually the availability of numerous apps that users can download and install with user-friendly use. However, it also means that hackers can easily distribute malware to smartphones and launch various attacks via social media. This issue can be analyzed with both preventive approaches and effective detection techniques of the latest technology. A study by Daojing He, Sammy Chan, and Mohsen Guizani discusses why smartphones are so easily vulnerable to security attacks. They then presented the malicious behavior and threats of some malware, and then reviewed the existing malware prevention and detection techniques. They point out the efforts of app developers, app store administrators, and users to defend against this type of malware [5].

Sagiroglu and friends represented approaches in the literature and mentioned most important five mobile threats [13]. Also, mobile threats are assessed and some detection and protection methods are represented [6]. Another research about mobile application security is mobile malware detection and protection systems [7]. These approaches bring light to understand detection and protection methods for android. Another approach is cyber security issues in mobile life [8]. Another paper mentions about android based mobile application development and its security. It represents static and dynamic analysis of android applications [7]. This paper also tries to explain android security framework. To understand android security framework is significant to find the causes of security vulnerabilities. Butler represents android phone market growth, android application software, applications and developer, and its security framework [6]. In addition to these approaches, there are mobile security reports. The important report is Android Security Report 2016 which is published by the Google [9].

This report has been published annually. Android security report provides to increase the security of Android. The other report is MacAfee mobile threat report published in 2019. This report handles new threats which affect Android OS. Those who use Android phones that were released before 2012 need to be particularly concerned, as these devices have lacked the security enhancements Google posted and are vulnerable amongst many others to the following 3 the most dangerous vulnerabilities.

1. BlueFrag: A critical vulnerability that could allow the device to be compromised to steal data and spread malware. This malicious code can be sent via the Bluetooth MAC address and users' data can be stolen. According to the security company statement, this BlueFrag vulnerability does not work on Android 10. In other words, there is no security risk from BlueFrag for users using Android 10.
2. Stagefright: first discovered in 2015, this vulnerability is used to infect malware via MMS message. As it can be understood, with this vulnerability, the attackers can obtain all personal information by running the malicious codes they want on their Android devices with the MMS they send. The most important issue caused by the vulnerability in question is that these malicious codes can delete themselves from your Android

device, making you not even aware. In addition, hackers can delete this MMS message when requested, and with this vulnerability, they can access the device's hardware, including the camera and SD card.

3. Joker: A vulnerability that appears as an official app on the Google Play store, but allows unauthorized access to the address book on devices when downloaded and used. The android malware called "Joker" was detected in 24 android applications in the Google Play Store and it was stated that these applications were downloaded more than 472,000 in total. The malware discovered by security researcher Aleksejs Kuprins enables users to spend their money on premium subscription services they use. Applications that host this malware secretly click an ad in the background and register on the site to which it is directed.

3. MOBILE ATTACKS

3.1. Cyber Attacks

Cyber-attacks are increasing with developing technology day by day. We can classify cyber-attacks into five groups. First is denial of service attacks and distributed denial of service attacks. Second group is malicious software which are viruses, worms, Trojan horses, key logger, ad words and spyware. Another cyber-attack is phishing. Fourthly, spam is a cyber-attack. At last but not least cyber-attack is listening traffic.

3.2. Mobile Attacks

Malicious software is divided into three groups which are malware, spyware and grayware. Malware can access to device to collect personal data or damage to device. When this software installed to the device, user personal data can be caught by attacker. Also, attacker can have unauthorized access. Another type is spyware. This software collects information which is messages, stored data and location. Spyware can be installed via physical access and personal data stored in this software. Last type is grayware. Grayware is defined as any unwanted software that can cause moderate to severe discomfort for users, including unwanted and unexpected behavior. Unlike a virus, it may not potentially harm the computer. The term grayware can refer to the fine line between a virus and legitimate software. This collects data which is about user. These data are used to marketing and statistical information about users.

4. MOBILE MALWARE

Mobile application area is developing day by day. Because android is an open source and widely used platform; it becomes a usual the target for attackers. In the figure 5 shows rate of using android platform.

The aim of the mobile malware is hacking the device, collecting personal data about user and earning income. Mobile malware has ability which is accessing user phonebook, sending message, remote access and locking the device. \$12,000 money was earned without user knowledge according to a report which is published in 2013. There are lots of different mobile threats which are adware, Trojan-SMS, Trojan-banker and Trojan.

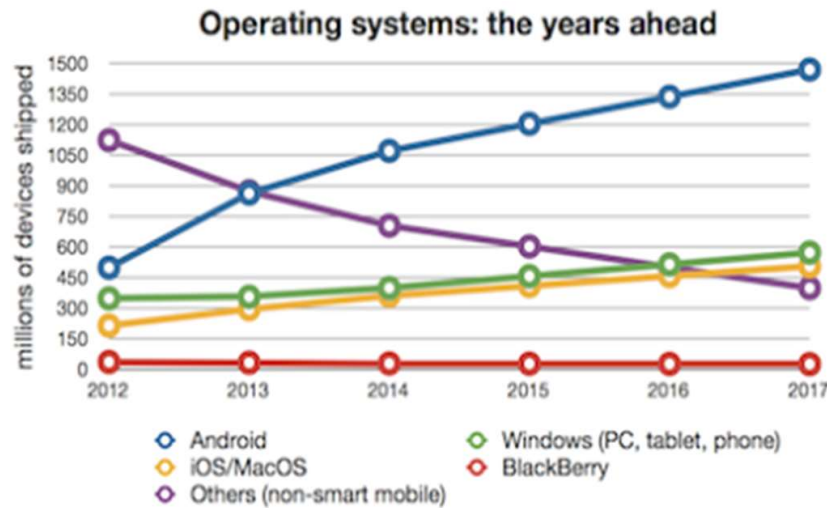


Figure 5. Market share by operating systems [10].

4.1. Adware

Adware is software which gives information about visiting websites, shopping preferences. If this collecting data is occurred without user's knowledge, this software will be malware. In this way, attacker can have information about victim and cheat them using this information.

4.2. Trojan-SMS

Trojan-SMS is the fastest and simple applications in the malicious software. Because SMS feature is placed from classic phones to smart phones, this way gives good solutions for attacker. Also, they earn lots of money via Trojan-SMS. This malware cause spending money via sending message from user phones to paid phone numbers.

Serious security vulnerabilities have been detected in Go SMS Pro, the messaging application widely used. In the vulnerability disclosed by TrustWave researchers, it is stated that the images that users have sent each other are collected by the company on a single server and that this server is configured to be accessed by third parties. It is known that Go SMS Pro, which is offered free of charge on Google PlayStore, has 100 million users worldwide. Go SMS Pro creates a special URL after uploading the files to an online server where everyone can access the images that the people using the application send to each other. Users can see images sent to each other via this URL. The checks made by the researchers also determined that these URL addresses are accessible to everyone and reported that the users' private data may have been disclosed.

4.3. Trojan-Banker

Trojan - Banker is a Trojan horse application to capture information in the online banking process. These applications can be seen harmless and useful by the user but they are prepared to perform illegal operations. Trojan horses use user to multiplication because they have not ability to multiplication. Zeus is the common Trojan - Banker application which can collect data without user knowledge. Trojan - Banker gather information with different ways. The first common way is that mobile device screen is saved when user access to the online banking application. Personal data of the user which are password and customer number with this way. The other way is environment listening via Trojan. While using phone banking, card information can be saved thanks to device microphone and attacker can use this information.

4.4. Trojan

Trojan is containing harmful applications and installing program and it works secretly inside any program. Trojan software is placed to system document of the popular applications. Since their capacities are very little, they take a small space in system documents. Trojan horses have not ability to self-processing. Because of this reason, they need user process. They are used with two different ways in the mobile devices. The first one is like keylogger. They save key motion and keep secret information like password. The second one is capturing session which is user session is captured and e-mail confirmation step can be passed easily while any attack are making.

5. ZERO-DAY EXPLOITS OF MOBILE APPLICATIONS

The cybercrime world is characterized by the rapid discovery and exploitation of any vulnerabilities or problems that may be found in a system or a machine. So-called "Zero Day" attacks are one of the most feared and dangerous security incidents, in addition, around 80% of large-scale attacks that occur are due to Zero Day vulnerabilities detected on hardware or software devices. Considering ever increasing wide range of usage of mobile applications, these types of attacks affect both home users and corporate environments. These attacks have the ability to exploit these identified vulnerabilities and malware variants to exploit for a specific malign purpose.

Vulnerabilities declared on the mobile platforms are available in the Exploit-DB¹² database. For an android application security, the zero-day is a free vulnerability in the Android kernel that could allow a privileged attacker or an application to elevate its privileges to gain root access to a vulnerable device and potentially take full control of the device. These are not only related with Android but also IOS. The most important measure that highlights what someone can (and should) do is to protect mobile device according to latest security tools and mechanisms. However, just installing an antivirus or a complete security solution isn't enough. To get the most out of these tools and to ensure protection, it is important that we know how to deal with the basic risks or at least the most important ones. Another important precaution to be implemented is to keep the software up to date. Both the operating system and the different programs used need security patches against vulnerabilities and discovered for zero-day attacks. Many people have been victims of attacks due to not keeping programs up to date. The complexity of Zero-Day attacks is very high. This is the importance that in addition to people working in technology, all users in general should be alert and take proactive measures. It may not be possible to reduce any type of cyberattacks 100%, but equally, reaching a significant and reasonable level of assurance against them can make a difference.

The table 1 below gives detailed information for a set of declared vulnerabilities of which details can be studied in the hyperlinks for each row.

Table 1. Vulnerabilities on EXPLOIT-DB for Android Applications in Hyperlinks.

<i>Date</i>	<i>Title</i>
2020-02-24	Android Binder - Use-After-Free (Metasploit)
2020-01-14	Android - ashmem Readonly Bypasses via remap_file_pages() and ASHMEM_UNPIN
2019-11-08	Android Janus - APK Signature Bypass (Metasploit)
2019-10-04	Android - Binder Driver Use-After-Free
2019-05-29	Qualcomm Android - Kernel Use-After-Free via Incorrect set_page_dirty() in KGSL

¹² For detailed information see: <https://www.exploit-db.com/>

2019-03-06	Android - getpidcon() Usage in Hardware binder ServiceManager Permits ACL Bypass
2019-03-06	Android - binder Use-After-Free via racy Initialization of ->allow_user_free
2019-02-20	Android Kernel < 4.8 - ptrace seccomp Filter Bypass
2019-02-12	Android - binder Use-After-Free of VMA via race Between reclaim and munmap
2019-02-12	Android - binder Use-After-Free via fdget() Optimization
2018-10-08	Android - sdcardfs Changes current->fs Without Proper Locking
2018-09-11	Android - 'zygote->init;' Chain from USB Privilege Escalation
2018-08-13	Android - Directory Traversal over USB via Injection in blkid Output
2018-02-07	Android - 'getpidcon' Permission Bypass in KeyStore Service
2018-01-11	Android - Hardware Service Manager Arbitrary Service Replacement due to getpidcon
2018-01-08	Android - Inter-Process munmap due to Race Condition in ashmem
2017-12-18	Outlook for Android - Attachment Download Directory Traversal
2017-11-28	Android Gmail < 7.11.5.176568039 - Directory Traversal in Attachment Download
2012-12-21	Google Android 4.2 Browser and WebView - 'addJavascriptInterface' Code Execution
2017-02-14	Google Android - android.util.MemoryIntArray Ashmem Race Conditions
2017-02-14	Google Android - Inter-process munmap in android.util.MemoryIntArray
2017-02-02	Google Android - 'rkp_set_init_page_ro' RKP Memory Corruption
2017-02-01	Google Android - RKP Information Disclosure via s2-remapping Physical Ranges
2017-02-01	Google Android - RKP EL1 Code Loading Bypass
2017-02-01	Google Android - Unprotected MSRs in EL1 RKP Privilege Escalation
2017-02-01	Google Android - 'cfp_rop_new_key_reene'/'cfp_rop_new_key' RKP Memory Corruption
2017-01-26	Google Android - 'pm_qos' KASLR Bypass
2017-01-19	Google Android TSP sysfs - 'cmd_store' Multiple Overflows
2017-01-06	Google Android max86902 Driver - 'sysfs' Interfaces Race Condition
2016-12-29	Google Android - get_user/put_user (Metasploit)
2016-12-20	Google Android - WifiNative::setHotlist Stack Overflow
2016-12-06	Google Android - 'IOMXNodeInstance::enableNativeBuffers' Unchecked Index
2016-12-06	Google Android - Inter-Process munmap with User-Controlled Size in android.graphics.Bitmap
2016-10-12	Google Android - Binder Generic ASLR Leak
2016-10-11	Google Android - 'gpsOneXtra' Data Files Denial of Service
2016-10-03	Google Android - Insufficient Binder Message Verification Pointer Leak
2016-09-27	Google Android 5.0 < 5.1.1 - 'Stagefright' .MP4 tx3g Integer Overflow (Metasploit)
2016-09-14	Google Android - getpidcon Usage binder Service Replacement Race Condition
2016-09-08	Google Android - libutils UTF16 to UTF8 Conversion Heap Buffer Overflow
2016-07-06	Samsung Android JACK - Local Privilege Escalation
2016-06-10	Google Android - '/system/bin/sdcard' Stack Buffer Overflow (PoC)
2016-04-11	Google Android - IMemory Native Interface is Insecure for IPC Use
2016-04-11	Google Android - IOMX 'getConfig'/'getParameter' Information Disclosure
2016-04-01	Google Android - 'ih264d_process_intra_mb' Memory Corruption
2016-03-28	Android One - mt_wifi IOCTL_GET_STRUCT Privilege Escalation
2016-02-08	Samsung Galaxy S6 - 'android.media.process' Face Recognition Memory Corruption
2016-01-26	Google Android ADB Debug Server - Remote Payload Execution (Metasploit)
2014-01-23	GoToMeeting for Android - Multiple Local Information Disclosure Vulnerabilities
2013-11-04	Google Android - Signature Verification Security Bypass
2013-07-03	Google Android - 'APK' code Remote Security Bypass
2015-11-03	Samsung Galaxy S6 - android.media.process Face Recognition Memory Corruption
2013-06-15	TaxiMonger for Android - 'name' HTML Injection
2011-11-03	Google Android 2.3.5 - PowerVR SGX Driver Information Disclosure
2015-09-17	Google Android - libstagefright Integer Overflow Remote Code Execution
2013-01-07	Facebook for Android - 'LoginActivity' Information Disclosure
2015-09-09	Google Android - 'Stagefright' Remote Code Execution
2012-09-12	Google Chrome for Android - Same-origin Policy Bypass Local Symlink
2012-09-12	Google Chrome for Android - Local Application Handling Cookie Theft
2012-09-12	Google Chrome for Android - Multiple 'file:.' URL Handler Content Disclosure Vulnerabilities
2012-09-12	Google Chrome for Android - com.android.browser.application Extra Data Cross-Site Scripting
2011-08-02	Open Handset Alliance Android 2.3.4/3.1 - Browser Sandbox Security Bypass
2015-01-26	Android WiFi-Direct - Denial of Service
2014-12-28	WhatsApp 2.11.476 (Android) - Remote Reboot/Crash App (Denial of Service)
2014-11-18	Samsung Galaxy KNOX Android Browser - Remote Code Execution (Metasploit)
2014-06-17	Adobe Reader for Android < 11.2.0 - 'addJavascriptInterface' Local Overflow (Metasploit)

2014-04-15	Adobe Reader for Android 11.1.3 - Arbitrary JavaScript Execution
2014-02-07	Android Browser and WebView addJavascriptInterface - Code Execution (Metasploit)
2008-03-04	Google Android Web Browser - '.BMP' File Integer Overflow
2008-03-04	Google Android Web Browser - '.GIF' File Heap Buffer Overflow
2012-12-09	Google Android Kernel 2.6 - Local Denial of Service Crash (PoC)
2011-03-14	Google Android 2.0/2.1/2.1.1 - WebKit Use-After-Free
2011-02-02	Google Android 1.x/2.x - Local Privilege Escalation
2011-02-02	Android 1.x/2.x HTC Wildfire - Local Privilege Escalation
2010-11-15	Google Android 2.0/2.1 - Use-After-Free Remote Code Execution on Webkit
2009-08-18	Linux Kernel 2.x (Android) - 'sock_sendpage()' Local Privilege Escalation

Source: exploit-db.com

6. ANDROID MALICIOUS SOFTWARE DETECTION AND PROTECTION SYSTEMS

According to InfoWorld, there are three basic security elements in all smartphones. Your first important task as a mobile device user is to be aware of these layers and enable them on your devices:

Device Protection: Allowing remote "wiping" of data in case your device is lost or stolen.

Data Protection: Preventing corporate data from being transferred to personal applications running on the same device or personal network.

Application Management Security: To protect in-application information against interception.

Smartphone security is based on Mobile Device Management (MDM) technology that is installed not only on phones but also on company servers and controls and manages device security. Both have to work together to offer good security [26].

Android malicious software detection and protection systems are developing to get rid of attacks. We can analyze detection and protection system into four groups which are static analysis approach, dynamic analysis approach, signature-based analysis approach and cryptographic data transmission.

6.1. Static Analysis Approach

Static analysis approach provides a control mechanism with data of applications. This control mechanism detects malware and protect device before application installed to the device. Thanks to static analysis, malware detection is provided in the application before installation. We can observe some applications which are developed with static analysis approach for detection and protection. First one is DroidMat. This tool provides detection via API calling for manifest files and related permissions [14]. Secondly, Drebin detects malware with combining static analysis approach and machine learning approach. This tool uses source codes and manifest files of the application. Thus, it capture some data which are permissions which is need by application, API calling and network addressing. Drebin creates a vector with these data and detect malicious software [15]. The final system is Stowaway. This system provides detection of permission which is requested by the application unnecessarily. Stow-away consists of two parts which are determining API calling and matching permissions to APIs and detection permissions which are needed for API calling.

6.2. Dynamic Analysis Approach

Dynamic analysis approach works in runtime differently from static analysis approach [11]. In this approach, we will analyze some applications which are Crowdroid, RiskRanker, DroidMOSS and Paranoid Android. Crowdroid detects abnormal behavior on the Android applications. It classifies Android applications as harmless and malicious. While making this, it uses Strace command which is based on Linux in Android Kernel. Then, Crowdroid compile system callings and classifies the applications. RiskRanker [12] analyses application whether making some dangerous behavior or not. These dangerous behaviors are sending SMS in background and taking high level permission. DroidMOSSSS purposes to detect repackaging applications with malicious software in Play Store. Repackaging process is adding malicious software to application in the market. This process can be harmful for user because some popular applications can be dangerous. ParanoidAndroid makes security scanning for android Applications [16].. While making this, it creates a copy for device on the virtual environment.

6.3. Signature Based Analyze and Protection

Applications are kept on the signature database. In this approach, there are server and signature databases. While central server is assigned to analyze and protect processes, database server keeps finding analyses and provides reusing in the next analyses. Some systems were developed in this system. The first one is TractorBeam. System images are created in the central server with TractorBeam and they are analyzed. Analysis application consists of detectors and loggers. Detectors contain malicious software techniques. On the other hand, loggers save activities potential malicious software. Secondly, MADAM is complex detection tool. It detects malicious software in the Kernel and application level. The final but not least system is DroidRanger. It detects new malicious software examples with using schema behavior which is based on permission [17].

PHA category	2016 share in PHA Category	2015-2016 change in PHA installs	2016 percent of total installs	2015-2016 percentage point change of total installs
trojan	77.8%	31.3%	2.58579%	-0.23835
backdoor	8.8%	229.8%	0.29347%	+0.16592
hostile downloaders	3.9%	-94.7%	0.12925%	-3.34500
privilege escalations	3.0%	66.4%	0.09873%	+0.01365
sms fraud	2.9%	108.6%	0.09730%	+0.03043
spyware	1.8%	272.7%	0.06078%	+0.03740
call fraud	0.5%	-61.8%	0.01536%	-0.04227
rooting malware	0.4%	-43.5%	0.01282%	-0.01969
phishing	0.4%	-46.2%	0.01262%	-0.02098
toll fraud	0.3%	-79.7%	0.00893%	-0.05418

Figure 6. Methods to defend against reverse engineering [6].

6.4. Cryptographic Data Transmission

The aim of the cryptographic data transmission is security data transferring and preventing security gaps. Pocatilu maintained an approach. In this approach, uses SMS information, e-mails, files are saved in the database. If saved data is needed by another application, data is taken from database and is decrypted and is transmitted to the application[18]. Android programming application contains javax.crypto package. This package provides symmetric encryption (AES, DES), public key cryptography and message digest classes. In the play store, apk files of the applications are taken and are modified with malicious software. Then, modified application presents with different names on the play store or web pages. There are some tools for modification processes. These are APKTool, smali, dex2jar and JD-GUI [19].

7. FINDINGS AND RESULTS

Android security threat should be analyzed into two groups which are client-side and developer side. There are some security gaps for clients. First security gap is some used applications can access other applications and realize operations on behalf of the user. Secondly, malicious software has ability to install some application without user knowledge. Finally, any application which requests unnecessary permission can be classified as malicious software. Lots of users have not knowledge about permissions and they confirm all permissions which requested from application. They cannot be aware whether these permissions are required or not. In this issue, user should be careful. The second aspect is developer side. While developers are implementing any application, some situations should be considered. First of all, application source code should be kept for security attack because malicious software which is placed into source code can be exposed to attack. The other is using wrong permission request. Another is that deprecated permissions should be removed. Then, using signature and system permission should not be used. In addition, some reviews should not be forgotten while testing process. The final and important problem is that copy-paste code should not be used because some unnecessary permission can be placed.

Protection steps can be classified into two groups like android security threat. First group is user protection steps to avoid installation of potential harmful application. First of all, user should turn off MMS auto retrieval. If you suspect under the threat of Stagefright malware, you should turn off MMS auto retrieval to protect from Stagefright. This malware infected from MMS and it take control of user personal data, camera and microphone. Another is updating your device regularly. Lots of update contains security fixes to previously unknown vulnerabilities on your device. Another important protection method is that user should not open messages from suspicious resource because lots of malware infect via message. SMiShing continue to improve phishing. If user is careful to open SMS and clicking on the link, the danger of SMiShing can be decreased dramatically. The final and the most important thing is that user should use comprehensive security software to protect device from cybercriminals. The other protection perspective is developer protection systems. First of all, developer must store sensitive data with encrypted. Developer can use javax.crypto class for encryption of sensitive data. The other is sensitive data should not be stored in the system log. In addition, application backup should be disabled because attacker can access data which stored from application thanks to backup. Another developer protection system is to use secure channel (HTTPS) for external communication. The most important thing is to protect against reverse engineering. Reverse engineering methods can cause a popular application to be embedded malware from

malicious people. In Figure 6, developer should use methods to defend against reverse engineering [20].

Besides the user and developer preventions I mentioned, there are protection methods that offered by Google. Google says there are over 6 billion app installs per day, and each of them is scanned for malware. According to report of Google Android Security 2016 Year in Review, Verify Apps, an app that helps to verify Android's apps, says that the Google Play Store apps have dropped harmful activity from record level to 2015-2016 [21, 22]. In Figure 7 and 8 show decreasing rate effects of applications.

Technique	Defend Against	Description
Control Flow Obfuscation	Reverse Engineering	Make code flow difficult to follow
Symbol Stripping/Renaming	Reverse Engineering	Remove program symbols from application binaries and rename all human-understandable symbols
String Encryption	Reverse Engineering	Hide clear text strings through encryption
Anti-Debug	Reverse Engineering	Logic detects if debuggers is attached
Checksum	Tampering	Logic detects code/data changes
Self-Repair	Tampering	Logic erases attack changes
White-Box Cryptography	Cryptographic Key Theft	Implement cryptographic algorithms such that keys remain secure even when the code is subjected to white-box analysis
Class/asset/resource Encryption	Tampering/Reverse Engineering	Encrypt assets, resources or classes of the application

Figure 7. Malware effects of applications source from Google Play [9].

Android and Mac OS apps have become an essential element of the busy and daily lives of mobile device users, which is translating into a surge in mobile apps. Now even a new daily user can access a large number of applications through different platforms such as the play store, apple store. Due to certain vulnerabilities of mobile platforms, hackers develop mobile malware which is a threat and therefore the system can be subject to remote control and data privacy loss. Therefore, it is necessary to detect the threat level of a specific application installed on mobile devices and implement the necessary controls [27].

Before an app is available on Google Play, it passes an app review process to confirm that it complies with Google Play policies. Google analyze applications according to developed tools whether potential harmful or not. If an application is marked suspicious, it is sent to security analyst for manual review. After these processes, application is available on Google Play for user.

Google Play

PHA category	2016 share in PHA Category	2015-2016 change in PHA installs	2016 percent of total installs	2015-2016 percentage point change of total installs
trojan	54.2%	-51.5%	0.01623%	-0.01725
hostile downloaders	12.7%	-54.6%	0.00380%	-0.00458
backdoor	11.7%	-30.5%	0.00351%	-0.00154
sms fraud	9.9%	282.2%	0.00296%	+0.00219
phishing	6.2%	-73.0%	0.00185%	-0.00501
privilege escalations	2.5%	-77.6%	0.00076%	-0.00263
toll fraud	2.0%	592.8%	0.00060%	0.00051
commercial spyware	0.4%	-45.3%	0.00012%	+0.00004
call fraud	0.3%	-50.4%	0.00008%	-0.00008
ransomware	0.002%	-92.9%	0.000001%	-0.000009

Figure 8. Malware effects of applications source from outside of Google Play [9].

8. CONCLUSIONS

Businesses tend to rely on mobile devices for critical business operations, collaboration, and access to private data and information. Google continues to invest in innovative technology and artificial intelligence-based resources to further strengthen the security of the Android platform. Android's approach to open-source development seems to be an important part of its security. Developers, device manufacturers, security researchers, SoC vendors, academics, and the wider Android community are trying to create a collective level of competence for the entire ecosystem that finds and mitigates vulnerabilities. With Android, multiple layers of security can enable a variety of users to utilize states of an open platform, while also enabling adequate security to protect user and corporate data. In addition, Android platform security can keep devices, data, and applications safe through tools such as application sandboxing, exploit mitigation, and device encryption. A wide variety of management APIs can provide IT departments with tools to help prevent data leakage and ensure compliance in a variety of mobile usage risk scenarios. Work profiles allow organizations to create a separate, secure profile on user devices where mobile applications and important company data are kept secure and separate from personal information. "Google Play Protect", the world's most widely used

mobile threat protection service, can be provided with built-in protections on every android device. Supported by "Google machine learning", "Play Protect" tends to scan the device to catch, block and eradicate any PHA or malware. "Google Safe Browsing in Chrome" attempts to protect corporate users as they browse the web by warning of potentially harmful sites.

According to the latest statistics, the usage of mobile internet is one of the top trends which is acceding over % 90 of the total internet users. This is an indication that cyber risks and threats will also increase in the mobile world targeting social media and privacy.

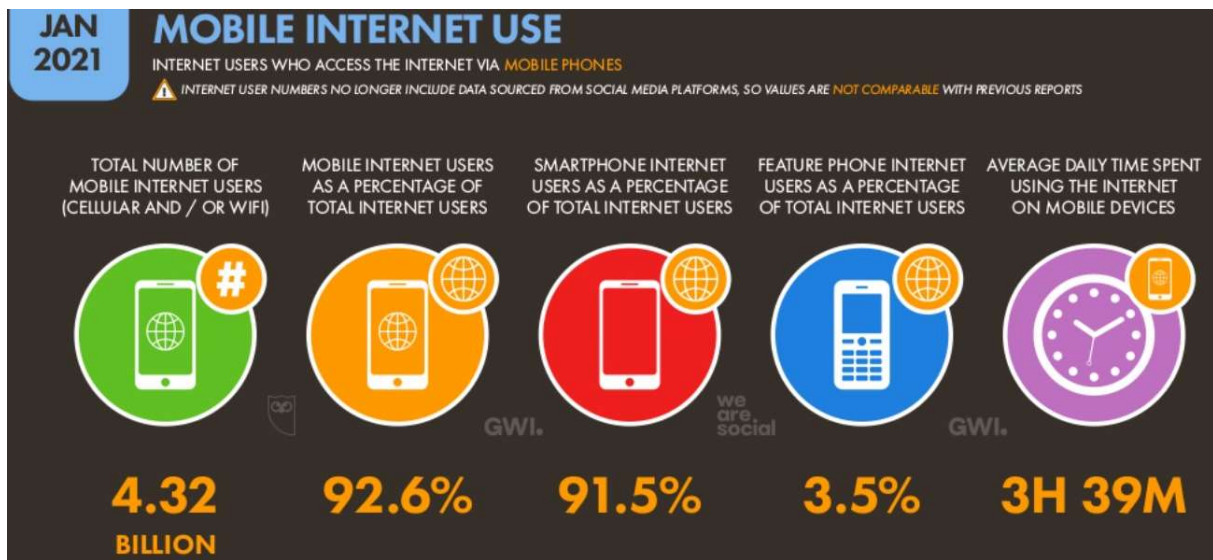


Figure 9. Latest statistics for mobile internet and mobile devices [25].

Like personal computers, mobile devices run on operating systems with their own vulnerabilities and security issues. The increase in the use of mobile devices has led security experts to improve mobile application security processes. Since the secure configuration of mobile devices in hardware is not commercially preferred, data must be protected by certain software and awareness of risk within mobile devices. In software measures, the key can be estimated from the runtime memory preview or the information in the application. Insufficient security measures can lead to situations such as data failure, privacy breach, credit card payment standards violation, identity theft and fraud.

An android application requires certain permissions from the user to access system resources and perform the necessary functions the user wants. Recently, the android market has been showing an exponential growth performance leading to an increase in malware applications. These applications are developed by hackers purposefully to gain access to users' private data and negatively affect the usability of the application through their malicious use. Appropriate tools are urgently needed to detect malware on Android systems, as malware can damage the user's system and data. Since both malware and cleanup security applications require similar types of permissions, distinguishing between them from the user's point of view becomes a very difficult task. A new algorithm should be developed to identify malware-based applications by investigating permission patterns [28]. Since mobile applications make people's lives easier, there are many mobile applications in the markets that are customized and ready to use for people's needs. While app markets provide a platform for people to download apps, it is also a platform that malware developers can use to distribute their malicious apps. Permissions on Android are used to prevent users from installing apps that may violate their privacy by providing warnings to increase their awareness. From the point of view of privacy and security,

it can be well understood if the functionality of applications in Android systems is given in sufficient detail in the descriptions, if the requested permissions are required. This is defined in the literature as permit compliance by definition [29].

If you are a mobile application manufacturer, your competitors' insufficient sensitivity to security measures will play a positive role in your preference with the security measures you increase in your applications. Although it is a reasonable justification for other application developers to prioritize performance in the operation of the process as well as time, and to consider that the usage performance of the application will decrease when the security measures are increased, it is a fact that your applications will remain on the smartphones of the users you are addressing for a long time and their use will be continuous if they like it. If the user is too involved with the application; It will increase the risk of encountering security problems. So, getting your mobile app to get the attention it deserves will not only be a positive improvement, but also bring some risks. Considering that there are too many Android applications on a subject, any security problem faced by users will lead your user to choose the product of the rival application developer from your application.

As a result, android platform is still getting safer and more secure. Although android platform is known as unsafe, Google improve safety level day by day. According to Google Android Report, android application has decreased malware proportion especially within one year. Because increasing of android application safety, android platform can be used mind at peace. Security is an important problem both user and developer. Both of them should be consider security steps to protect personal data.

9. RECOMMENDATIONS

It is recommended to take the following security measures in order to gain a good place in the application market where you will take a place for a long time with the "mobile application security" that you will prioritize:

Protecting Application Integrity against Attacks: The installation files of applications should be prevented from being published in different markets by assuming that attackers can change them. The way to do this is to make application files controllable on the server.

Correcting the Use of Authorization: It is recommended to only include the necessary authorizations while developing an "Android Application".

Overlooked Errors in Description Lines: One of the most common mobile application mistakes is that the notes taken by the application developer in the description lines and the passwords they use are easily visible later. Therefore, this issue is also among the things that need attention.

Considering Data Storage Sensitivity: No matter if "iOS" and "Android" applications, the data needed to be kept should be encrypted and stored in a suitable folder. It is extremely inconvenient to save sensitive and critical information on any mobile device while the application is in use without any security measure. When it is necessary to keep it, using the password and locked-folder methods effectively will allow you to avoid an important security problem.

Considering Privacy and Personal Data Leak Risks: Confirmation of access to a lot of information such as personal information, phone records, address books and locations of the

users through the mobile application in the first stage of obtaining the product is a widely used data collection method. But there is an overlooked risk factor, which is that personal data accumulated in mobile applications is the target of malicious third parties. Data leakage risks are one of the most common security problems that can be encountered and are a matter of extreme concern.

On the other hand, using broken crypto algorithms, providing data entry from unreliable sources, and keeping the controls performed on the weak server side also constitute important security problems of your application. Effective measures against security problems will play an important role in gaining the trust of users who prefer products in both iOS application and Android applications in mobile market.

ACKNOWLEDGEMENTS

We acknowledge significant contributions of Mr. Volkan Evrin, (CISA, CRISC, CEHv9, CDPSE, COBIT 2019F, ISO 20000-22301-27001 LA) Enterprise Applications and Information Security Manager at KAREL; Part-time instructor at Bilkent University Information Systems and Technologies (CTIS).

REFERENCES

- [1]. Swarnpreet Singh Saini, R. B. (2012). Architecture of Mobile application, Security issues and Services involved in Mobile Cloud Computing Environment. IJCER.
- [2]. Rygaard, C. A. (2006). Patent No. Mobile application peer-to-peer security system and method. US 7046995 B2.
- [3]. OWASP, https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_10_Mobile_Risks
- [4]. White Paper of 2017 Application Security Research <http://files.asset.microfocus.com/9395/en/9395.pdf>
- [5]. He, D., Chan, S., & Guizani, M. (2015). Mobile application security: malware threats and defenses. IEEE Wireless Communications.
- [6]. Butler, M. (2011). Android: Changing the Mobile Landscape. IEEE Pervasive Computing, 10(1), pp.4-7.
- [7]. Holla, S. and Katti, M. (2012). Android Based Mobile Application Development and its Security. International Journal of Computer Trends and Technology, 3(3), pp.486-490. <http://ijcttjournal.org/Volume3/issue-3/IJCTT-V3I3P130.pdf>
- [8]. Gokce, K., Sahinaslan, E. and Dincel, S. (2014). Cyber Security Approach in Mobile Life. 7th International Conference on Information Security and Cryptology.
- [9]. Google. (March, 2017). Android Security 2016 Year In Review.
- [10]. Intel Security. (2016). Mobile Threat Report Whats on the Horizon for 2016.
- [11]. OWASP, https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Secure_M-Development
- [12]. <https://mbatraveller.wordpress.com/>
- [13]. Kabakus, A., Dogru, I. and Cetin, A. (2015). Android Malware Detection and Protection System. Erciyes University Journal of the Institute of Science and Technology, 31(1), pp.9-16.
- [14]. M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, RiskRanker: Scalable and Accurate Zero-day Android Malware Detection, in Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys 12, 2012, pp. 281294.
- [15]. Arslan, B., Gunduz, M. and Sagiroglu, (2014). Current Mobile Threats and Precautions to Be Taken.
- [16]. T. Vidas, N. Christin, and L. F. Cranor, Curbing Android Permission Creep, in In Proceedings of the 2011 Web 2.0 Security and Privacy Workshop (W2SP 2011), 2011.
- [17]. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, Android permissions demystified, in Proceedings of the 18th ACM conference on Computer and communications security - CCS 11, 2011, p. 627.
- [18]. Dynamic Analysis vs. Static Analysis, Intel, 2013. [Web]. Retrieved from: <https://software.intel.com/sites/products/documentati on/doclib/>
- [19]. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, Crowdroid: behavior-based malware detection system for Android, Science (80-.), pp. 1525, 2011
- [20]. G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, Paranoid Android: Versatile Protection for Smartphones, in Annual Computer Security Applications Conference (ACSAC), 2010, pp. 347 356.

- [21]. M. Guido, J. Ondricek, J. Grover, D. Wilburn, T. Nguyen, and A. Hunt, Automated identification of installed malicious Android applications, *Digit. Investig.*, vol. 10, pp. 96104, 2013.
- [22]. G. Dini, F. Martinelli, A. Saracino, and D. Sgandurra, MADAM: A Multi-level Anomaly Detector for Android Malware, in *Computer Network Security*, vol. 7531, I. Kottenko and V. Skormin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 240-253.
- [23]. Barrera, P. C. Van Oorschot, and A. Somayaji, A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android Categories and Subject Descriptors, in *Proceedings of 17th ACM Conference on Computer and Communications Security*, 2010, pp. 7384.
- [24]. D.-J. Wu, C.-H. Mao, T.-E. Wei, H.-M. Lee, and K.P. Wu, DroidMat: Android Malware Detection through Manifest and API Calls Tracing, in *2012 Seventh Asia Joint Conference on Information Security*, 2012, pp. 6269.
- [25]. Dataportal, (2021) Digital 2021 Global Overview Report (January 2021) v01, <https://www.slideshare.net/DataReportal/digital-2021-global-overview-report-january-2021-v01>
- [26]. Gruman, Garen (2015) Mobile security: iOS vs. Android vs. BlackBerry vs. Windows Phone <https://www.infoworld.com/article/2987635/mobile-security-ios-vs-android-vs-blackberry-vs-windows-phone.html>
- [27]. Deepa D., Jena S., Ganesh Y., Roobini M.S., Ponraj A. (2021) Threat Level Detection in Android Platform Using Machine Learning Algorithms. In: Mallick P.K., Bhoi A.K., Chae GS., Kalita K. (eds) *Advances in Electronics, Communication and Computing. Lecture Notes in Electrical Engineering*, vol 709. Springer, Singapore. https://doi.org/10.1007/978-981-15-8752-8_55
- [28]. Shrivastava G. Kumar P. (2019) Android application behavioural analysis for data leakage, *Wiley Online Library*, <https://doi.org/10.1111/exsy.12468>
- [29]. Alecakir, H., Can, B. & Sen, S. (2021). Attention: there is an inconsistency between android permissions and application metadata!. *Int. J. Inf. Secur.* <https://doi.org/10.1007/s10207-020-00536-1>



Review Article

A STUDY OF BLOCKCHAIN IN IOT ARCHITECTURE

Authors: Mehmet Ali Şimşek 

*Corresponding Author: masimsek@nku.edu.tr


To cite to this article: Şimşek, M.A., (2021). A Study of Blockchain In IOT Architecture, International Journal of Engineering and Innovative Research, 3(2), p 163-174.

DOI: 10.47933/ijeir.851109

To link to this article: <https://dergipark.org.tr/tr/pub/ijeir/archive>



A STUDY OF BLOCKCHAIN IN IOT ARCHITECTURE

Mehmet Ali ŞİMŞEK^{1*} 

¹Tekirdağ Namik Kemal University TBMYO, Department of Computer Technologies, Tekirdağ, TURKEY.

*Corresponding Author: masimsek@nku.edu.tr
(Received: 31.12.2020; Accepted: 15.02.2021)

<https://doi.org/10.47933/ijeir.851109>

ABSTRACT: Industry 4.0 includes that components such as artificial intelligence, big data, autonomous systems, human-robot interaction, and the internet of things. Because of these components; some benefits are aimed, such as minimizing human impact, reducing costs, and increasing business volume. It is seen that the most fundamental problem of Internet of Things (IoT) technology, which is one of the basic concepts of Industry 4.0, is security. In recent years, blockchain architectures have been trying to find a solution to this problem. This study focuses on blockchain architectures used in the IoT ecosystem.

Keywords: IOT, Blockchain, Industry 4.0, IoT.

1. INTRODUCTION

IoT, which is one of the basic concepts of Industry 4.0, facilitates communication between different types of devices due to the development of the internet and hardware in recent years. These developments, where billions of devices access the Internet, have enabled the development of the Internet of Things concept. The goal of IoT is to develop a smarter environment and a simplified lifestyle by saving time, energy, and money [1-2].

IoT is the network of all kinds of things embedded with sensors, electronics, software, etc. connected to the internet according to the Global Standards Initiative of the International Telecommunication Union. Gartner predicted that by the end of 2015, 4.9 billion linked objects will be used, reaching 25 billion by 2020 [3]. In recent years, it has been observed that the devices connected to the internet have increased exponentially all over the world. These devices are expected to grow at a higher rate in the future. It is estimated that IoT will be able to connect 500 billion devices by 2030 [4]. It is seen that IoT is used in different areas as a result of the increasing use and importance.

IoT devices and applications appear in many areas such as smart cities and smart grids, education, finance, banking, communication, control, health, and defense. Such a trend, it is also called Internet of Things (IoT), Internet of Medical Things (IOMT), Internet of Battlefield Things (IOBT), Blockchain-Based Internet of Vehicles (IOV). In short, it also calls the internet the Internet of everything that includes the internet [5]. IoT technology is getting bigger and more complex. It is seen as an innovation that we can communicate with and manage with every object in our life.

It seems that the IoT ecosystem is growing steadily. Accordingly, the increase in the volume of data it carries causes security weakness. This raises the public and industry stakeholders to worry about being exposed to security breaches.

As IoT devices proliferate, these devices often lack the necessary authentication standards to keep user data safe. Hackers' wide variety of attacks enters the device is damaged critical infrastructure is to know. It needs to be widely adopted to ensure trust, authentication, and standardization among all elements of IoT [6]. It is important not to experience both financial and data loss in such attacks. Although there are some technologies to ensure security in data communication between IoT objects, the most prominent is the blockchain.

Blockchain provides a decentralized data storage service with a break-proof ledger made up of blocks serially chained in distributed networks. It can record and secure transactions or transaction events using encryption. The first blockchain was proposed by Satoshi Nakamoto in 2008. Cryptocurrency in 2009 - Bitcoin apply for the activation technique is MIS [7-8].

Although blockchain was originally designed for cryptocurrencies, thanks to its effective success, it is used in many areas today. Interestingly, blockchain is implemented in many industries beyond cryptocurrencies because of its unique and attractive features such as transactional privacy, security, data immutability, auditability, integrity, authorization, system transparency, and fault tolerance. This a la those some identity management, intelligent transportation, supply chain management, mobile crowdsensing, agriculture, industry 4.0, energy internet (IOA), and security in mission-critical systems emerge as [9].

Security of IoT devices; It can be divided into 3 main sections as authentication, connection, and operation. Efforts to prevent problems in identity verification, data communication, and processing have recently gained importance. Recently, blockchain applications have been used to ensure the physical and hardware security of IoT. With blockchain, it provides the reduction of danger, the creation of data privacy, and protection from third parties in data transfer. Thus, it also makes the end-to-end (P2P) communication safe. For all these reasons, it is said to play an important role in IoT security.

Although blockchain architecture was first used in cryptocurrencies in 2008, it was introduced in 1991. The first use of blockchain architecture with IoT was in 2015. When the relevant literature is scanned with the keywords "Blockchain", "IoT", "Internet of Things", it is seen that thousands of publications are made. It is seen that the usability of the existing two technologies together increases as time passes. Within the scope of this research study, researches, original articles, and conference papers that have been published in good journals and have a high number of citations will be scanned.

In the studies examined so far, it is seen that the data set cannot be kept on IoT devices due to security problems, but this can now be made possible with the help of blockchain technology. Different IoT architectures are also proposed where the data can be stored distributed without being collected in a center.

Authentication in IoT devices and sending information to other devices in the ecosystem are seen as another problem in terms of security. It is seen that the blockchain architecture can be used for end-to-end messaging transactions and for data security.

The structure of blockchain, its areas of use, why blockchain is important for IoT, the future of blockchain in IoT technologies, difficulties in its use, and the difficulties of using blockchain in today's IoT technologies constitute the scope of this study. In addition, examples of blockchain architectures used in IoT technologies are given in Section 3.2.

2. Blockchain and Uses

Although blockchain architecture was first introduced in cryptocurrencies in 2008, it was introduced in 1991. The first use of Blockchain architecture in conjunction with IoT was in 2015.

Blockchain can be thought of as blocks chained together. Since the advent of a new type of cryptocurrency (such as Bitcoin), they are also publicly referred to as digital notebooks. Blockchain is a comprehensively distributed architecture that emphasizes features such as data consistency, transparency, user privacy, resistance to backward changes, and so on. Unlike other centralized systems, blockchain-based systems often use a peer-to-peer (P2P) network to deploy data processing tasks to different nodes. Using a mechanism called compromise, information stored on each node and the data generated can be synchronized [10].

Generally, a blockchain is a distributed ledger with timestamps built on a P2P network using a consensus mechanism between nodes. Blockchain has neutralization, anonymity, traceability, transparency, and tamper-proof features. The blockchain is built on the P2P network and is located on every node in the P2P network. The P2P network implemented on the blockchain is a peer-to-peer, decentralized, and distributed network of computers. In a P2P network, the state and functions of all nodes are equal. Shared resources set up by nodes such as compute resources, storage resources, and network resources can be shared by other nodes. The more nodes added to this network, the more resources are shared, and the better the service quality of the whole system. The decentralized nature of the P2P network brings scalability and robustness to it, which is the basis for the success of the blockchain. The P2P network structure is shown in Figure 1 [11].

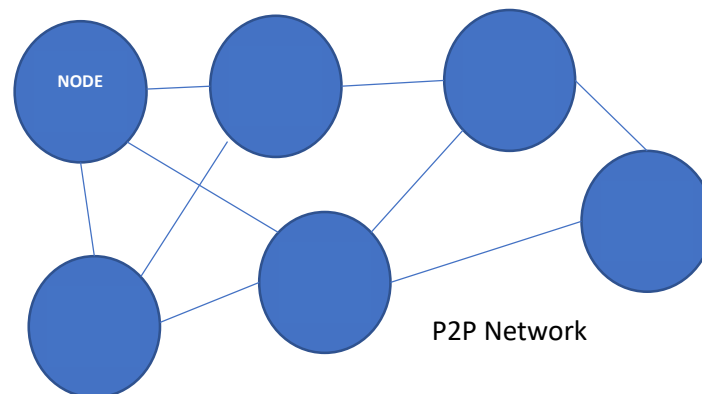


Figure 1. Blockchain P2P network structure.

A block in Blockchain architecture is a collective dataset that can be defined using a cipher function of each block. The created block contains a summary of the previous block. In this way, all data can be linked through a connected chain structure. Each block points to the immediately preceding block via a reference, which is the hash value of the previous block called the top block. Figure 2 shows a blockchain architecture. Each block; consists of two

parts, the head, and the body. Title part; the block version contains structures such as the password of the ancestor block, the time stated the current password format. The first block of a blockchain is called the genesis block, which has no main block [9, 12]. Figure 3 shows the general structure of a block.

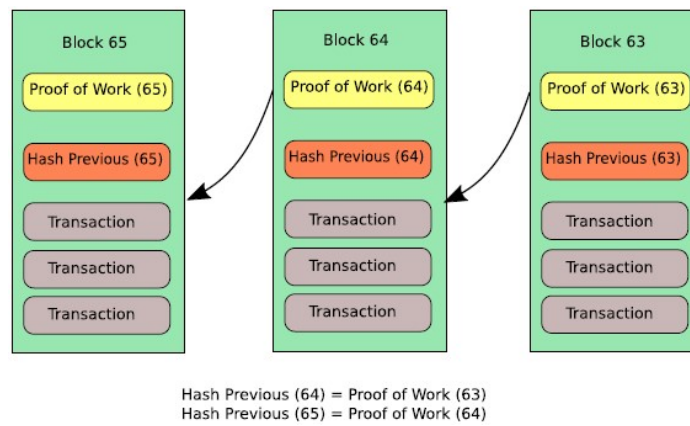


Figure 2. Architecture of Blockchain [9].

Block version	02000000
Parent Block Hash	b5ff0b1b1680a2862a30ca44d346d9e8 910d334beb48ca0c000000000000000
Merkle Tree Root	9d10aa52ee949386ca9385695f04ede2 70dda20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30e31b18
Nonce	fe9f0864

Transaction Counter

TX 1 TX 2 ... TX n

Figure 3. A block structure for blockchain [12].

Blockchain networks generally; the public blockchain is divided into three different categories: the private blockchain federal / consortium (Federated or Consortium) blockchain. The public blockchain provides access to everyone, nobody has access restrictions. Anyone can read and write data on this network. Private blockchain is based on permission. Nobody can access it unless the blockchain administrator has been given permission. Consortium or federated blockchain networks show similarities in permissions to private blockchain networks. Consortium blockchain is a specific blockchain that has authorized nodes to protect distributed data [13, 14].

Blockchain applications; many IoT applications now appear to be using blockchain for various purposes. Generally, it is seen that it is mostly used in digital payment, smart contract service, digital signature and data storage areas [10].

Digital payment: it is the first and most used area for blockchain. While initially operating on a distributed network supported by high-performance machines, now proprietary optimization supported by large blockchains such as Bitcoin and Ethereum is used for devices with insignificant computing power such as smartphones and pocket computers. Rather than being assigned large computational jobs, low-end devices often operate as lightweight nodes that do not keep the entire chain in their local repositories or participate in the most power-hungry

processes such as mining. These features have made mobile payment with the technical blockchain much more accessible than before [10].

Smart contract: a part of "crypto economically secure code execution" running on the basis of blockchain. Without any assistance from third parties, the smart contract automatically executes the relevant contract term after the defined condition is triggered. In addition, it provides real-time auditing as all actions are recorded and verified as transactions in a decentralized blockchain ledger. These operations are traceable and undeniable, thus increasing machine execution security. It converts various assets such as smart contracts, IoT devices, and digital assets into virtual identities on the blockchain and enables them to interact with other assets. The smart contract is attractive as an efficient and secure method to replace normal contracts. With the smart contract, the Blockchain is used to replace the Intelligent Transport Structure (ITS) and perform reliable software updates of IoT devices [7].

Digital signature: Each user has a pair of private keys and public keys. The private key is used to sign transactions. Digitally signed transactions are spread over the entire network and can then be accessed by public keys that are visible to everyone on the network [12].

Data Storage: It has shown that it can be used as a database for distributed and secure storage of data sets in blockchain data storage applications. The given chain can be used for data privacy. It can be used to group data such as health, financial and education.

3. BLOCKCHAIN FOR IOT

IoT and blockchain are customized and optimized blockchain systems to enable IoT applications. IoT applications have been developed and applied in many areas. However, most of these apps are prone to issues like data loss and systematic malfunction. To mitigate these problematic effects, blockchain has been used to provide higher security and stability for traditional IoT applications [10].

Blockchain was originally used to record financial transactions where transactions are encoded and held by all participants (Bitcoins and other cryptocurrencies etc.). Thus, all transactions have become transparent and any changes can be easily tracked and detected [5]. Blockchain offers actionable reality to increase IoT security. In this section, views on the importance of using blockchain for IoT security, architectural examples, usage challenges and future are given.

3.1 Importance of Blockchain Technology for IoT

Blockchain technology has been envisioned by the industry and the redial community as a stunning technology that is ready to play an important role in managing, controlling, and most importantly, securing IoT devices [15]. It is powerful enough to be a technology that provides an important opportunity to provide viable security solutions to blockchain's tough IoT security problems today.

Blockchain for IoT devices is what devices have done in the past; It allows it to be kept under a registry without being changed. These devices provide verification without being connected to third party devices. In addition, it provides the opportunity to securely provide device-to-device (P2P) messaging and data transmission. Blockchain brings new approaches to Internet of Things technology in privacy and security issues.

Figure 4 shows a typical blockchain transaction. When a transaction is made, a block is created. The block is broadcast to all nodes in the network. One of the nodes verifies the block (called mining in bitcoin) and streams it back to the network. If the block is validated and the block references the previous block correctly, the nodes add the block to their blockchain [5].

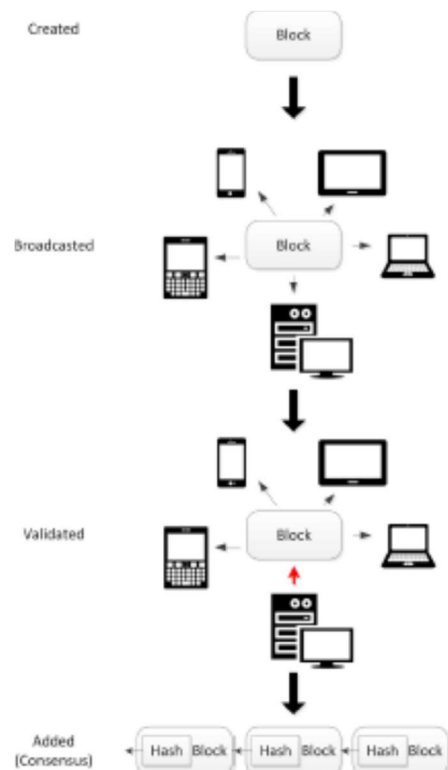


Figure 4. A typical blockchain workflow [5].

3.2. Samples of Blockchain Architectures Used in IoT Technologies

Blockchain technology is seen as one of the solution suggestions for the IoT ecosystem due to the increasing importance of concepts such as security, privacy, and confidentiality. Based on this approach, some architectures that include IoT and blockchain technology have been developed. OSCAR, ACE, BPIIoT architectures are one of them. Under this section, the architectures that have offered solutions from 2018 to the present are examined.

3.2.1. IoTChain

IoTChain, a program that combines the OSCAR and ACE authorization framework to provide an E2E solution for secure authorized access to IoT resources, Alphand (2018) et al [16]. Suggested by. Under the ACE framework, clients must create an encrypted and authenticated channel with a secure authorization server that requires the use of certificates or unlimited secret sharing. In addition, rogue authorization servers can freely issue access tokens for each protected resource. It replaces the only trusted authorization server in the ACE framework with a trusted authorization blockchain. The authorization block chain enhances the ACE authorization model by keeping resource access control robust, flexible and possibly confidential. The blockchain consensus protocol requires an attacker to control at least 51% of the blockchain before obtaining illegitimate tokens. In IoTChain, the resource owner discloses access rights in a smart contract, which automatically generates access tokens for the customer when certain conditions are met. Unlike ACE, the access token is not transmitted to the client, but the smart contract is stored securely in internal storage. The smart contract can then be

interrogated by other organizations to check the validity of the token [16]. In this architecture, the IoT device is responsible for data generation. The data owner is responsible for uploading the data to the blockchain. The OSCAR architecture and ACE authorization framework are responsible for ensuring the security of user data [10].

Figure 5 shows the main elements of the architecture and shows the sequence of operations leading to authorized access to IoT resources. The terminology specified by the IETF has been followed to avoid confusion regarding nomenclature and the roles of different organizations.

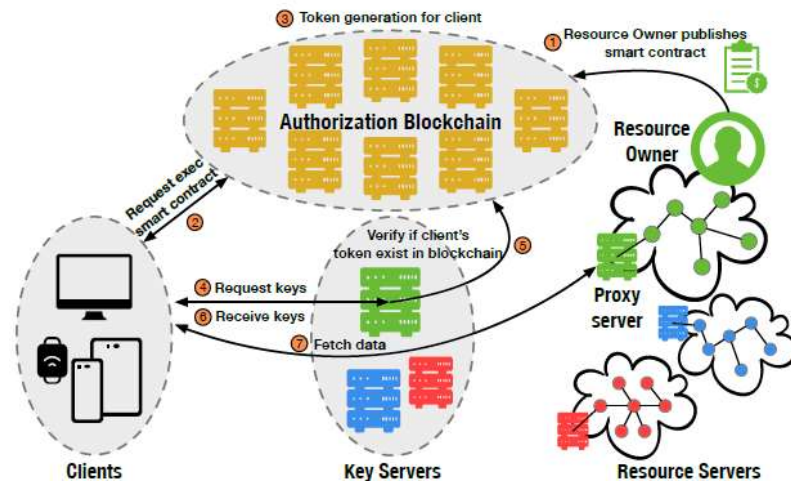


Figure 5. IoTChain architecture [16].

Source Servers (Resource Servers) creates and stores protected resources.

Resource owners (Resource Owners) are the legal owners of the resources that the source server and create them.

Clients are third parties seeking access to protected resources.

Proxy Servers (Proxy Servers) source server resources in a manner substantially restricted when stores encrypted.

Key Servers (Key Servers) to encrypt resources and create the necessary keys to decrypt.

Access tokens, (Access tokens) describes a particular client and the access rights of a particular resource.

Authorization Servers (Authorization Servers) creates access tokens.

3.2.2. Distributed access control system in IOT

Distributed access control system in IoT is proposed by Novo (2018) [17]. It is a new decentralized access management system in which access control information is stored and distributed using blockchain technology. All assets will be part of blockchain technology except IoT devices and headquarters nodes. Nodes in a blockchain network must contain a copy of the blockchain. The size of the blockchain can be quite large and will continue to increase over time. Most IoT devices will not be able to store blockchain information due to their constraints. As a result, the proposed architecture does not include IoT devices in the blockchain and

alternatively defines a new node called the management center that requests access control information from the blockchain on behalf of IoT devices.

In addition, the solution includes a single smart contract that defines all allowed operations in the access control system. This contract is unique and cannot be deleted from the system. Entities called administrators can interact with the smart contract to define the access control policy of the system [17]. Distributed access control system architecture in IOT is given in Figure 6. The architecture consists of 6 different structures: wireless sensor networks, administrators, agent node, smart contract, blockchain network, and management centers.

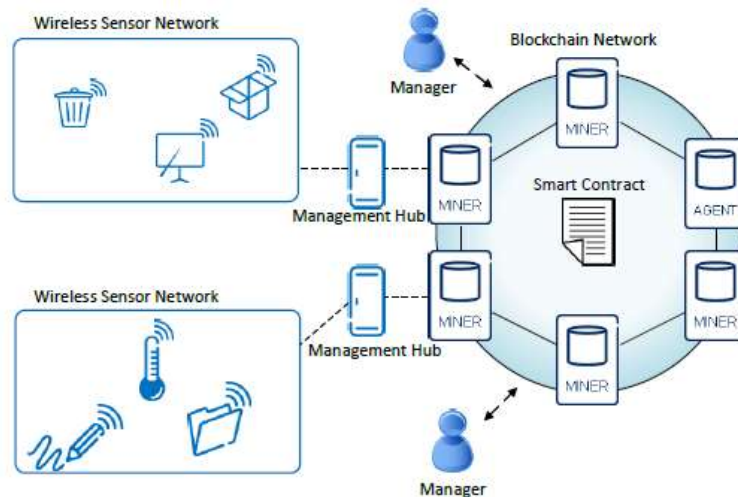


Figure 6. Distributed access control system architecture in IoT [17].

3.2.3. IIOT recommended for mild hybrid based blockchain's architecture

The lightweight hybrid-based blockchain architecture proposed for IIoT was proposed by Seok and Park (2019) [16]. Industry IoT (IIoT) includes many heterogeneous devices with limited resources. If we apply existing blockchain technology, it could affect the availability of the network. In order to increase the efficiency of IIoT, computational resources should be calculated and scalable, removing lag times.

Recommended block chain net "cell node" and "storage node" from the formed and the area between the layer and the control layer operates. Purdue model was used to design the proposed architecture. The architect area layer corresponds to level 0 and level 1 in the Purdue model. The proposed architectural control layer corresponds to level 2 in the Purdue model. To cover many heterogeneous devices in a large area, its area is divided into a small area called "Cell" and almost all IIoT devices connected to the located cell node. The cell node creates a block from data collected by connected devices and broadcasts to other nodes in the blockchain for block validation after block mining. After the block validation process, all the node participating in the block validation sends the return message to the storage node for the result validation notification, and then the block update is processed. Storage nodes, block and update records book ni is responsible for managing. In the block update process, the storage node adds the approved block. All of the processed transactions can be checked from the distributed ledger on the storage node [18]. Figure 7 shows our proposed architecture.

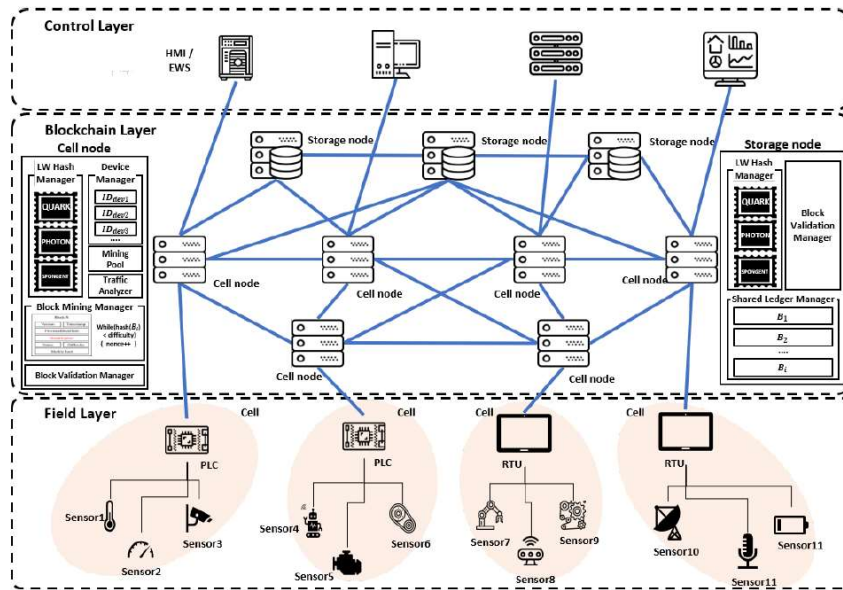


Figure 7. IIOT proposed for a lightweight composite based blockchain the architecture [18].

3.2.4. Health care monitoring architecture

The model proposed by Attia (2019) et al [19] focuses on a remote healthcare monitoring scenario of out-of-hospital patients. For this purpose, information on the health status (blood pressure and oxygen saturation, heart rate, body temperature, etc.) of each patient and a person is obtained. Other sensors can be installed in the patient's home to monitor the patient's immediate environment and allow detection of a person's activity and events such as falls. Data broadcast by these wearables and other sensors in the home are permanently uploaded to a remote database system. At this stage, a live monitoring system steps in to analyze this data to detect abnormalities and alerts clinicians who can take some action remotely if necessary. These data are also stored to keep track of all occurring events and can serve physicians following the evolution of patients' health status. All transactions between different parts of our scenario are carried out on very sensitive personal data. It is clear that these medical reports must be confidential and have limited access in a global system that ensures they are not objectionable. To meet all these requirements, an architecture based on blockchain technology has been proposed to remotely monitor patient status [19]. The architecture shown in Figure 8 basically consists of two blockchains, a monitoring system and medical devices.

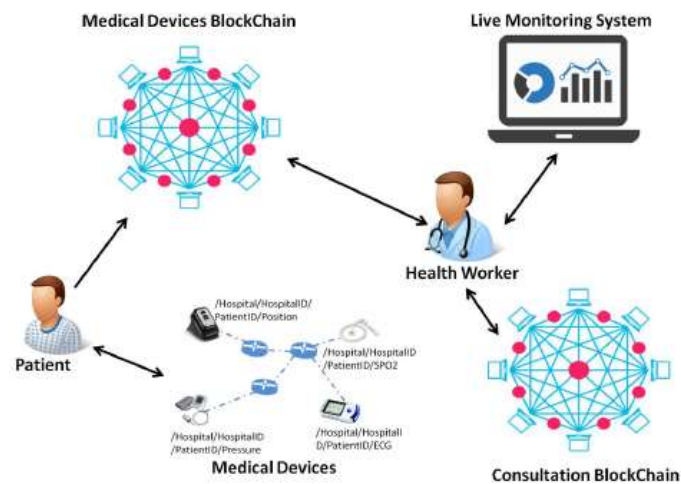


Figure 8. Healthcare monitoring architecture [19].

3.3. Challenges in Using Blockchain in IoT Technologies

Despite the benefit that blockchain brings to traditional IoT applications, there are still many hurdles in its implementation. The biggest problems arise from the limitations of IoT devices. Issues such as task distribution, power consumption, and computing capability need to be considered for blockchain to be effectively implemented in most IoT applications. To overcome these problems, there have been many attempts to adopt blockchain in IoT applications in recent years [10]. It is hoped that in the future, IoT devices will be able to work fully integrated with blockchain and gain more capabilities in the field of application.

A recent study found that the processing power and associated energy costs required for public blockchain networks are challenging for enterprise scenarios. In other words, the Bitcoin network consumes enough energy to power over 1.3 million US households [4]. Considering that many devices will join the IoT world day by day, energy consumption is seen as a huge problem. It emerges that studies on power consumption should be carried out among future studies.

Blockchain technology can be applied effectively in almost all areas of IoT. Considering the number of nodes and block size involved in the encryption process for such systems, it appears to affect power usage, network propagation, and network congestion [9]. In some cases, it may not be necessary to use a blockchain. It can be determined whether the system created will use blockchain or not and a choice can be made accordingly.

When too many verification requests are made, the prolongation of the time required for the processing of transactions is another problem. Stronger hardware structures are required in order to perform these processes in a shorter time.

It is known that data sets obtained from IoT devices are collected in a central device. Thanks to Blockchain technology, these data; In other words, membership information is recorded and shared by all members, including the center. In other words, membership information is recorded and shared by all members, including the center. But the lifetime of these data subjects is another problem that needs attention. Owners of datasets may not want to share them permanently. However, once any transaction is recorded by the blockchain, it cannot be changed or deleted. While this is a strong security property, if any record needs to be removed it may not be suitable for sharing. As a solution to this situation, the blockchain structure named Reference Integrity Metrics (RIM) has been proposed by Banerjee (2018) et al [5].

The industrial IoT ecosystem consists of many heterogeneous devices with constrained resources (Sensors, Actuators and Programmable Logic Controllers (PLC) etc.) and network availability should preferably be considered. Therefore, there are difficulties in implementing existing blockchain technology [18].

3.4. Blockchain Future in the IoT Ecosystem

IoT technology will play an increasingly important role in our society or in the foreseeable future in both civilian and military (hostile) contexts, including the internet of drones, the internet of battlefields, and the internet of military things [5]. Therefore, it is obvious that the security of all IoT devices used, especially in the defense industry, will be the most important issue. It is most desirable to protect data security and privacy in end-to-end communication of devices, whether in individual use or in industrial use, and that data is not

passed on to third parties. When all these situations are considered together, it is seen that the biggest issue in IoT devices is security.

Blockchain appears to be the most optimal solution to security for IoT devices. It is seen that blockchain-based solutions are recommended and used for the IoT ecosystem, increasingly since 2015. Although it is accepted that there are some problems experienced with the use of blockchain in the IoT ecosystem, it should not be ignored that the problems in the past have been solved. It is known that new studies are carried out to overcome the problems of the IoT ecosystem with the blockchain, which further increases the security by offering a distributed security system. Each step taken to solve the difficulties mentioned in Section 3.3 will serve to create a more optimal IoT ecosystem.

4. CONCLUSION

This study looks at the use of blockchain technology in the IoT ecosystem. In accordance with this purpose; It has been sought to answer the suggestions such as why blockchain is important for IoT, what is the future of blockchain in IoT technologies, what are the difficulties in its use and the difficulties of using blockchain in today's IoT technologies. In the literature studies, the use of IoT-blockchain, which has been increasing since 2015, is seen. Examples of architectures encountered in the literature are also included.

In every aspect of modern life, the existence of IoT devices and the existence of security problems of these devices are now seen. Although IoT-blockchain technologies appear to be used, IoT-blockchain applications are still in their infancy. However, the integration of IoT and blockchain is evolving and growing rapidly.

It is thought that the difficulties in using blockchain in IoT technologies specified in Section 3.3 will be solved and developed one by one in the near future. It is obvious that IoT-blockchain applications will develop rapidly in these days when it is important to ensure the security of communication, information and data.

Considering that the number of IoT-blockchain applications is increasing every year, it is believed that new consensus mechanisms to improve the performance of IoT devices in blockchain networking will be well in the coming years. Also, solutions to solve the problem of scalability, processing power or storage of the IoT device in the blockchain network are interesting issues.

REFERENCES

- [1].Mahdavinejad, M. S., Rezvan, M., Barekataan, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018, August 1). Machine learning for internet of things data analysis: a survey. *Digital Communications and Networks*, Vol. 4, pp. 161–175. <https://doi.org/10.1016/j.dcan.2017.10.002>.
- [2].Ahmet Ali Sützen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem", *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.12, No.1, pp.1-12, 2020. DOI: 10.5815/ijenis.2020.01.01
- [3].Charmonman, S., Mongkhonvanit, P., Ngoc Dieu, V., & van der Linden, N. (n.d.). Applications of Internet of Things in E-Learning. In *International Journal of the Computer, the Internet and Management* (Vol. 23). Retrieved from www.charm.SiamTechU.net.
- [4].Mouri, N. J. (2019). Nusrath Jahan Mouri IOT Protocols and Security Faculty of Computing and Electrical Engineering. (July).
- [5].Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, 4(3), 149–160. <https://doi.org/10.1016/j.dcan.2017.10.006>.

- [6]. Shaik, K. (2018). Why blockchain and IoT are best friends - Blockchain Pulse: IBM Blockchain Blog. Retrieved April 25, 2020, from IBM website: <https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/>.
- [7]. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, 136(August 2018), 10–29. <https://doi.org/10.1016/j.comcom.2019.01.006>.
- [8]. Gürfidan, R., Akçay, Z. (2020). Blok Zincir Temelli Güvenli Elektronik Oylama Modeli. *International Journal of Engineering and Innovative Research*, 2 (3), 148-155. DOI: 10.47933/ijeir.746235
- [9]. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2), 2188–2204. <https://doi.org/10.1109/JIOT.2018.2882794>.
- [10]. Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Computing Surveys*, 53(1). <https://doi.org/10.1145/3372136>.
- [11]. Ren, Y., Zhu, F., Sharma, P. K., Wang, T., Wang, J., Alfarraj, O., & Tolba, A. (2020). Data query mechanism based on hash computing power of blockchain in internet of things. *Sensors (Switzerland)*, 20(1). <https://doi.org/10.3390/s20010207>.
- [12]. Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4), 352. <https://doi.org/10.1504/ijwgs.2018.10016848>.
- [13]. Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., & Alam, T. M. (2019). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. 2019 International Conference on Innovative Computing (ICIC). Retrieved from <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8966700>.
- [14]. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8), 3690–3700. <https://doi.org/10.1109/TII.2017.2786307>.
- [15]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411. <https://doi.org/10.1016/j.future.2017.11.022>.
- [16]. Alphand, O., Amoretti, M., Claeys, T., Dall’Asta, S., Duda, A., Ferrari, G., ... Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. *IEEE Wireless Communications and Networking Conference, WCNC, 2018-April*, 1–6. <https://doi.org/10.1109/WCNC.2018.8377385>.
- [17]. Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195. <https://doi.org/10.1109/JIOT.2018.2812239>.
- [18]. Seok, B., Park, J., & Park, J. H. (2019). A lightweight hash-based blockchain architecture for industrial IoT. *Applied Sciences (Switzerland)*, 9(18). <https://doi.org/10.3390/app9183740>.
- [19]. Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019). An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application. 2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop, 1–5. <https://doi.org/10.1109/NTMS.2019.8763849>.