ISSN 1112-5209

Journal of Electrical Systems

Volume No. 21

Issue No. 3

September - December 2025

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN 1112-5209

Journal of Electrical Systems

Managing Editor
Mr. Amit Prasad

ISSN 1112-5209

Journal of Electrical Systems

(Volume No. 21, Issue No. 3, September- December 2025)

Contents

ISSN 1112-5209

Synchronous Generator Abnormality and Fault Analysis

Lovesh B. Xaxa1,*, Sachin Kumar2, Sunil Singh3, R.K. Srivastava1, R.K. Saket1

ABSTRACT

The trouble-free operation of alternators is unavoidable to meet the rising demand for electrical energy. Any alternator failure causes overloading of the remainder of the units in a grid, posing a serious threat to network stability. In a stand-alone generation, production is seriously affected. The repairs of large capacity alternators require a trained workforce, which is not always locally available. When an alternator operates under typical fault conditions, it reduces its efficiency and shortens its lifespan. The synchronous generator's prolonged outage has an adverse impact on network reliability and impacts the economy. As a result, early detection of alternator anomalies significantly reduces fault extension, loss of supply, and maintenance costs, while also improving the alternator's life. In many cases, the early fault detection scheme for higher capacity alternators cannot be readily applied to a lower capacity one. The article discusses some practical root cause analyses of the commonly occurring faults in turbo alternators. The identification, characteristics, and analysis of multiple fault occurrences have been thoroughly addressed. This article would provide utility and protection engineers impetus in determining the urgency, selecting, and implementing the appropriate protective system for various abnormality events.

***Keywords**: Generator; condition monitoring; core burning; vibration; insulation failure*

1. Introduction

The Synchronous Generator (SG) is essential for bulk power generation and network stability. Although power generators are extremely durable and reliable, they are frequently susceptible to numerous failures usually not present in lab electrics and domestic appliances. Long-term operation in a high-stress environment and unpredictable operating conditions such as aberrant frequency, voltage, loading, leading power factor operation, local hot spot creation, slot discharge, mechanical vibrations, and insulation failure are the primary causes of generator defects. These anomalies significantly impact the generators' competence and life cycle. An early diagnosis of generator anomalies is crucial for maintaining the energy supply's sustainability while reducing equipment damage and financial losses. Several studies on anomaly detection of synchronous generators have been presented during the last few decades. Slot discharge, vibration, and sparking in large high voltage electrical machines are responsible for the life reduction of electrical machines. [1] Slot discharges are caused by loose windings, poor slot conductive coatings, and isolated slot conductive coatings. Ozone created during Partial Discharge (PD) attacks the winding insulation. In high voltage machines, severe insulation problems may arise due to this. High voltage coils are subjected to Electrodynamic forces, slot discharge, and thermo-mechanical stresses. Suitable measures are required to protect high voltage machines [2]. The asynchronous operation of the synchronous alternator under field failure causes severe damage to the machine. In the negative slip region, the mechanical power of the turbine equates with asynchronous electrical power developed [3, 4]. Rotor winding deformation leading to failure of turbo-alternator has also been well addressed. Softening of hard-drawn copper takes place at 130°C to 150°C. An increase in the normal rotor current accelerates the winding distortion troubles even in the case of properly packed end turns [5, 6]. The vibration patterns of end winding are disparate for different healthy and faulty operations of an alternator. A wide range of natural frequencies exists for the end winding structures. The stress is much lower at certain natural frequencies to cause any catastrophic failures. However, under certain other natural frequencies, a careful operation is required [7]. Unbalance magnetic conditions during single ground fault and the double ground fault may cause severe vibration enough to damage the bearing pedestal, causing the rotating field to drop physically on stator windings. It may require costly repair and a more prolonged machine outage. In the case of synchronous machinery, the AC armature and DC field breakers are operated as fast as possible, and if desired, the prime mover power may be shut off [8]. It ensures the avoidance of the induction generator operation of SG. Vibration Detection instrumentation for turbine-generator and stator end-windings is described in [9, 10]. Alleviation of torsional vibration problem has been presented in [11]. The stator interturn short circuit effect on end winding vibration has been reported in [12]. A particular requirement for force distribution in the end zone is required [13, 14].

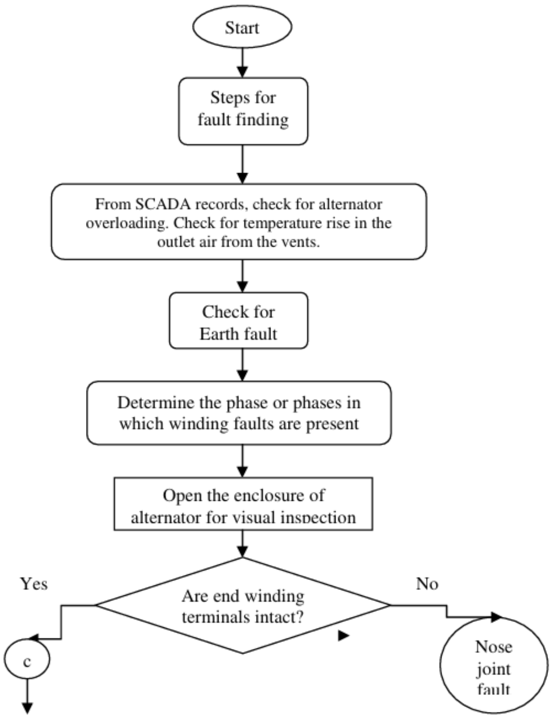
Most researchers interpret an alternator as mathematical equations and execute fault analysis based on that assumption [15, 16], neglecting any possible physical damage to the alternator caused by some defects both within and outside the alternator. Severe fault conditions cause the alternator to entirely stop functioning, necessitating costly maintenance and repair and loss of productivity. Any circuit breaker tripping due to a line fault may be quickly restored with minimal effort, while significant alternator problems might take longer to fix and use.

As a result, synchronous generator condition monitoring (CM) is necessary to protect the generators from catastrophic damage. Most of the alternators of higher capacity are fitted with the sophisticated SCADA system, which records essential input-output parameters for condition monitoring and fault analysis. Such a CM system is highly efficient in triggering the warning alert and detecting issues early on. The CM system improves machine availability, performance, and lifespan while reducing damage and maintenance expenses. The calibration of sensitive instruments measuring electrical, mechanical, and thermal parameters used in power industries is required yearly. Most faults occur due to non - compliance with annual mandatory calibration, even with SCADA. The reliability of an effective CM system depends on the calibrated measuring instruments connected to it. In insurance-related claims, it is always advisable for the owners to undergo mandatory calibration of the measuring equipment and maintain the online data before the fault. The findings, characteristics, and the consequences of several practical fault scenarios on the synchronous generator are comprehensively discussed in this article. The manufacturing and production sectors have dominated in recent decades, particularly compared to the maintenance system. According to [17], a substantial portion of maintenance money is lost due to inappropriate maintenance techniques, which is the leading cause of maintenance inefficiency.

2. Generators with abnormalities

Synchronous generators are technically relatively complicated in manufacturing standards, but they have inherent reliability and are built for a longer lifespan. Continuous operation in a high-stress environment, overloading and loss of load, and similar unpredictable operating conditions will cause the machine to fail, thereby reducing its usefulness and lifespan. The winding of any electrical machine is “the heart” of the machine where most of the faults occur. According to a CIGRE investigation of 1199 hydro-generators, insulation breakdown is responsible for around 56 percent of all anomalies. Mechanical and thermal problems are among the other significant abnormalities [18].

The flowchart for Root cause analysis for the air-cooled alternator is depicted in Fig. 1.


Start
Steps for fault finding
From SCADA records, check for alternator overloading. Check for temperature rise in the outlet air from the vents.
Check for Earth fault
Determine the phase or phases in which winding faults are present
Open the enclosure of alternator for visual inspection
Yes
Are end winding terminals intact?
No
c
Nose joint fault

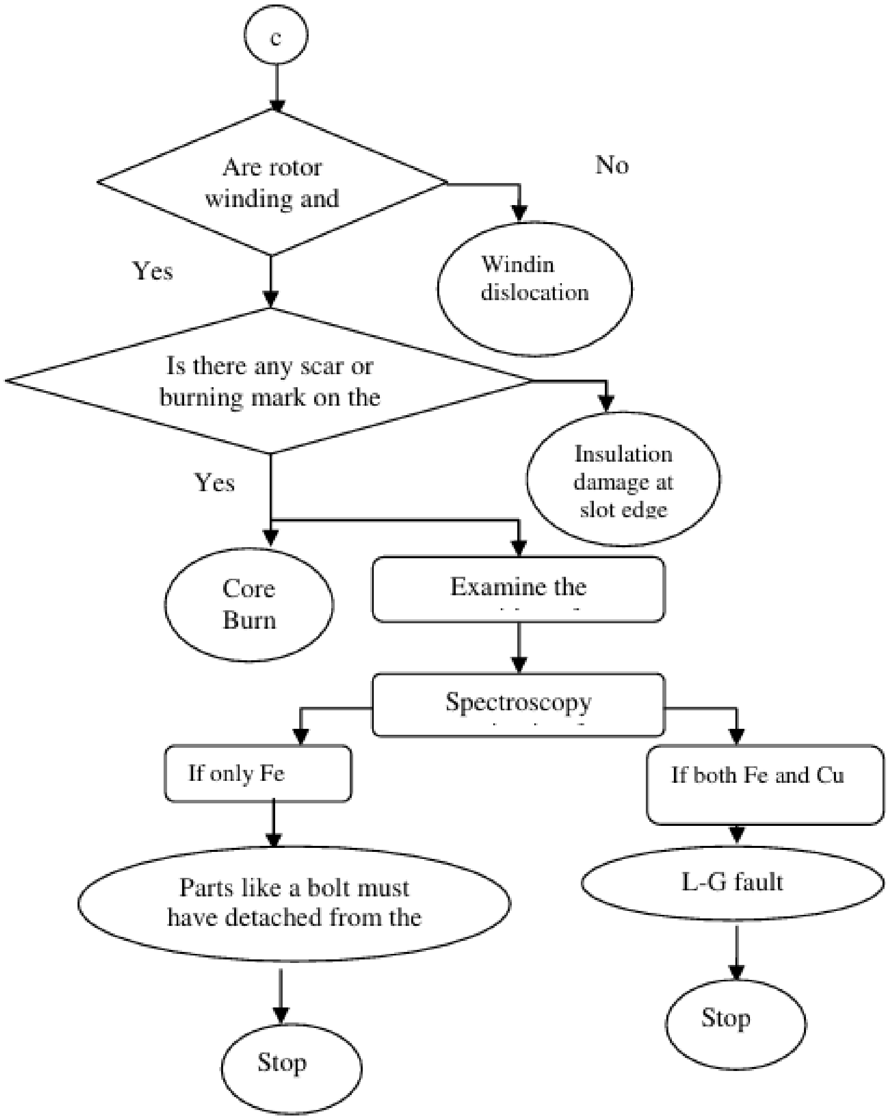


Fig. 1. A flow of the accomplished work.

3. Root cause analysis

The findings and consequences of several practical fault scenarios on the SG are discussed in this section. A fault in the coil winding like L-G, LLG, or LLLG is induced by different reasons like (i) fault in winding material, (ii) core burning, and (iii) insulation failure. Almost all are present, and it is challenging to pinpoint which fault started in the beginning, leading to catastrophic failure. The primary culprit in all the above faults is mechanical vibrations in different parts of the rotating structure.

In 150 MW alternators, the diameter of the stator bore is of the order of a few meters and is made using segmented stampings. All the insulated Silicon hot-rolled stampings form the stator stack. Several packets of stampings are assembled in such a way as to create radial ducts for cooling purposes. As per existing conventions in tropical countries, after a packet of 10 cm, a gap of 1 cm is provided while stacking. It reduces the effective iron length and increases the coil line parameters, which calls for a larger copper volume for windings. A typical packet of stampings with radial ducts, partially burnt teeth, and loosened stampings are shown in Fig. 2. A single tooth along the axial length on the stator surface is discontinuous and segmented because of the stacking of stampings in packets with spacers inserted. Each packet of a tooth has proper insulation and bindings, which protects it against vibration. These are subjected to the magneto-striction phenomenon in which each stamping in a packet of tooth dances macroscopically in a haphazard manner when subjected to alternating magnetization [19]. It causes the loosening of specific tooth stampings. Due to prolonged use, a particular tooth packet may be subjected to several stresses mentioned earlier. Loosening of stampings ensues due to wear and tear, as shown in Fig. 2, in which slot insulation degradation can be initiated. When the insulation between the stampings degrades, there are chances of more significant eddy current losses in those packets of the tooth. Due to magneto-striction, the stampings devoid of insulation regularly appear in contact with each other in cyclic magnetization resulting in a rise in local eddycurrent losses and a rise in local hot spot temperature.

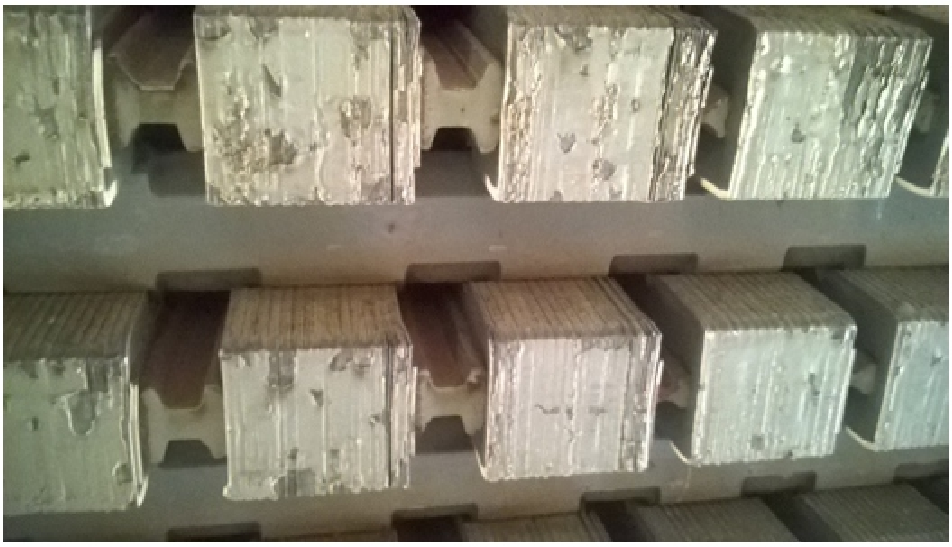


Fig. 2. Start of Loosening of Core stampings in 150 MW alternator.

The Core burning is shown in Fig. 3. The core burning appears slowly and worsens gradually. The outlet air temperature recording cannot detect the tooth insulation burning and subsequent wear and tear and loosening of packets of stampings. It results in creating a local hotspot in the heart of the core. The melting temperature of electrical grade sheet steel is around 1500 degrees Celsius, whereas the melting point of winding copper is about 1100 degrees Celsius. Due to the melting of the copper coil, insulation, and core material, just after the intense heating due to a fault, a lump of hot material protrudes, touching several teeth on the rotor, shaft, etc.

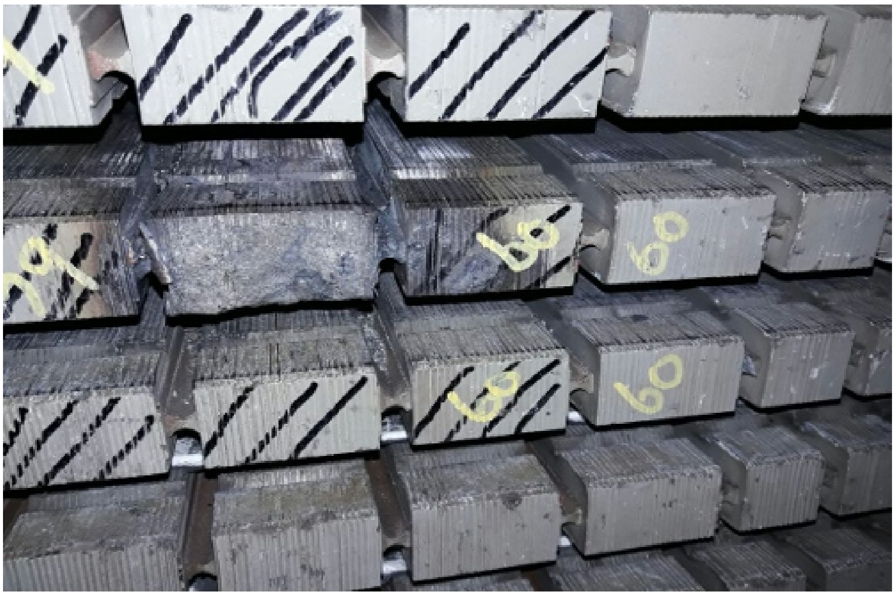


Fig. 3. Burning of packets of tooth stampings in the core.

Upon coming in contact with the teeth, the hot lump leaves a scar which eventually short circuits the stampings on the face, as shown in Fig. 4. However, when such stamping packets are used again, it leads to core burning unless properly treated with care. It calls for an online chemical analysis of outlet air, which can detect the possible faults of core burning at an early stage. However, these schemes are not available for 150 MW alternators. Core burning causes the local degradation of Class F insulation above 155° C (coil insulation) and the subsequent grounding of the coil with the core. The core burning (of a tooth) in a 150 MW alternator makes a portion of the stator core unusable. In a refurbished alternator's core, such portions of the core are removed, resulting in lowering the alternator's capacity.

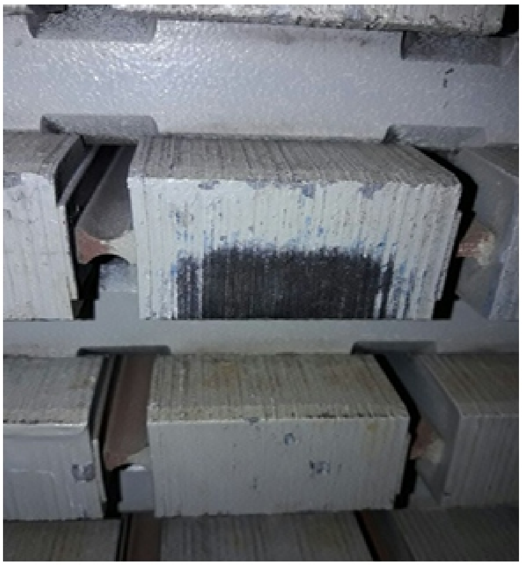


Fig. 4. Molten lump of stator winding coming in contact with slot-tooth, leaving a mark.

3.2. High Voltage Coil fault

A typical cross-section of the coil of an 11 kV, 50 Hz, 150 MW, the grid-connected air cooled alternator is shown in Fig. 5. It has two conductors per slot in single-layer windings. The preformed casted coil has several strips wrapped using Kapton tape insulation, and Class F insulation binds the coil. These strips are short-circuited on both the ends of windings to allow a large current to flow. Two conductor groups are separated by insulation.

A damaged coil showing a strip conductor is shown in Fig. 6. Due to manufacturing defects of possibly undetectable void in copper strips or possible bend or presence of foreign material during manufacturing, the creation of a hot spot surrounding the void/bend remains undetectable. The copper strip manufacturer and high voltage coil winding company should ensure void-free strips after rigorous testing of copper winding strips and the binding process. Over longer run under overloading conditions may cause a break in such defective conducting strips. The current interruption in a broken strip result in a higher current density in healthy conducting strips. It also results in partial discharge (PD) between an embedded conductor's minute gap and between the conductor and the slot. Both the ends of a broken coil are at higher potential. This sudden discharge may eventually melt the healthy strips, thermal failure of coil insulation, which results in the coil getting earthed through the grounded core, resulting in the L-G fault. A break in the continuity of any strip due to unforeseen reasons will cause the coil’s parameters to change, resulting in a slight dip in the voltage and vibration-related issues due to magnetic unbalance. The winding faults often remain undetectable when a fault is close to the neutral ground.

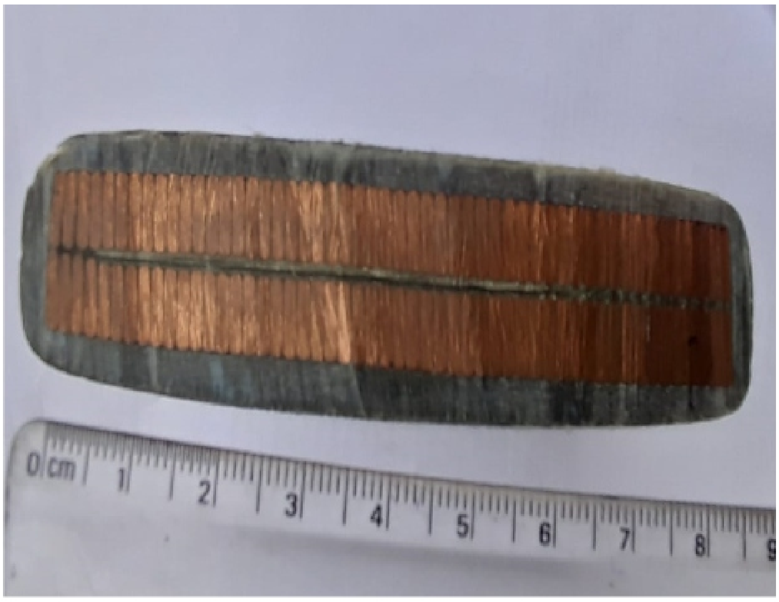


Fig. 5. Cross Section of the coil of a typical High Voltage 150 MW alternator winding.

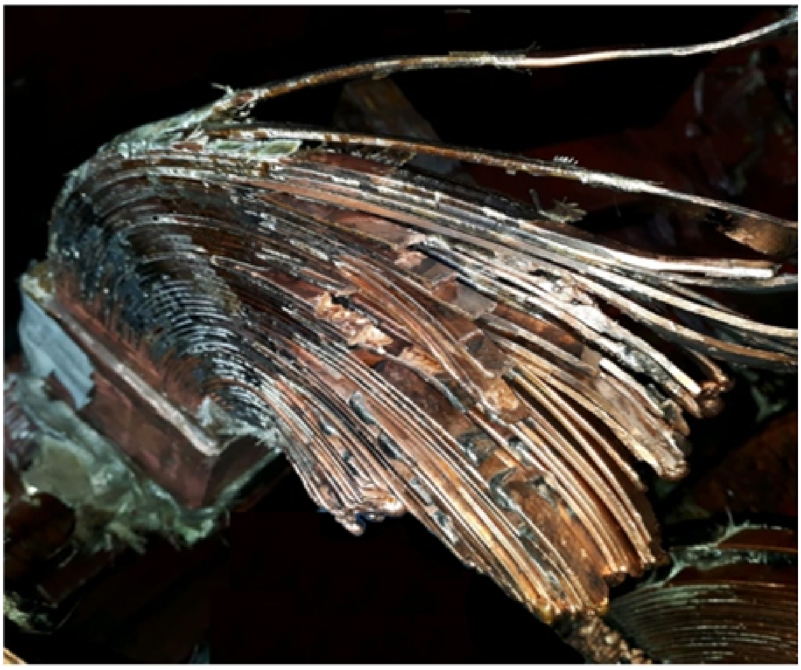


Fig. 6. A damaged coil showing burnt strip conductors in a typical high voltage alternator (Courtesy: Proclaim).

The rating of an alternator is 187.5 MVA, 150 MW, 15.75 kV, 3000RPM. Each phase had two parallel paths, and one of the R phase windings was found to be earthed 45% from neutral when it was providing 145.50 MW to the grid at 15.78 kV, 5,642.71 A, 49.62 Hz.

Due to unforeseen reasons, such pre matured faults cannot be detected in advance unless real-time chemical fume detection of outlet air technique is available for lower capacity alternators. According to IEEE SG protection rules [20], thermal protection for the SG stator core and windings may be given for (a) Generator overloading, (b) Leading Power factor operation, (c) Faulty cooling system, and (d) Localized hot spots caused by core lamination insulation failure or by localized or rapidly developing winding failures. In the present case, both the core burning and LG fault were present. There is no scheme to detect hot spot creation in 150MW alternators. It is also difficult to pinpoint which fault supported the other fault.

3.3. Dislocation of winding- slot wedge & Winding overhang

The process of L-G faults' occurrence in an alternator has been described in section (3.2). Multiple L-G faults may be present in an alternator given a complex vibration phenomenon within the turbine–alternator structure. The preformed/casted HV coils demand an open slot configuration for the alternator's higher capacity high voltage stator. Each slot opening is provided with a suitable wedge. These open slots in the stator and the alternator's rotor permit housing of larger and heavy preformed-casted coils having parallel strip conductors with insulation. Slot wedges prevent the tightly fitted coils in the slots from coming out due to electrodynamic, vibration, and thermo-mechanical forces.

The rotor overhang and stator overhang portions of windings, through properly reinforced, have their multiple natural frequencies of oscillations. Vibrations in the turbinealternator set are required to be appropriately monitored. The vibration signature varies due to different normal operating conditions, switching, changes in load, and several initial abnormal conditions that may lead to major breakdown conditions if not checked. The overhang portion of an alternator requires special reinforcement against several dynamic forces of different origins, as described earlier. The overhang portion may be subjected to mechanical resonance, which is enough to destroy the reinforcement, wedges, and slot tightening provisions. Sustained vibrations over a longer operating time may result the loosening of specific coils from the slot. Such coils may have axial movement of coil sides in a slot of a fraction of a millimeter. Due to this, the Class-F insulations that wrap the coils come out in white dust, particularly at the edges of the slots. These are detected when the alternator undergoes necessary repair and maintenance.

Such loosening of coil sides due to the macroscopic movement of coil sides remains undetected. However, with the present technological development, it is possible to visually inspect coils when the alternator is still operating. Thinning of the insulation layer causes the conductor at the slot edge to have insulation breakdown resulting in an L-G fault. The location of the L-G fault is of utmost importance. In an alternator, multiple L-G faults can be present, causing a complex winding fault that ultimately results in a complete breakdown. Depending on the position of the L-G fault in any phase winding, insulation damage due to the L-G fault may escalate into an entire L-L-L-G fault over the period of time. Under severe transients and fault conditions, the loosening of heavy stator windings in their slots was accompanied by significant gravitational and electromagnetic pressures (electrodynamic-force and thermo-mechanical stresses) in the radial downward direction. The significantly displaced windings can occasionally damage the restraining slot wedge and reinforcing bands. Under dynamic situations, this may produce a severe dislocation of the stator winding coils in the upper half in horizontal shaft machines, which may come in contact with the rotating structure in overhang regions. A typical deformation due to dislocation of the stator winding of a 15 MW, 11kV, 50 Hz, 1500 RPM, 4-pole Steam Turbo stand-alone generator supplying arc furnace has been shown in Fig. 7. A portion of the stator winding came in direct contact with the rotor overhang, thereby puncturing glass insulation on the overhang portion of the rotor, as shown in Fig. 8.

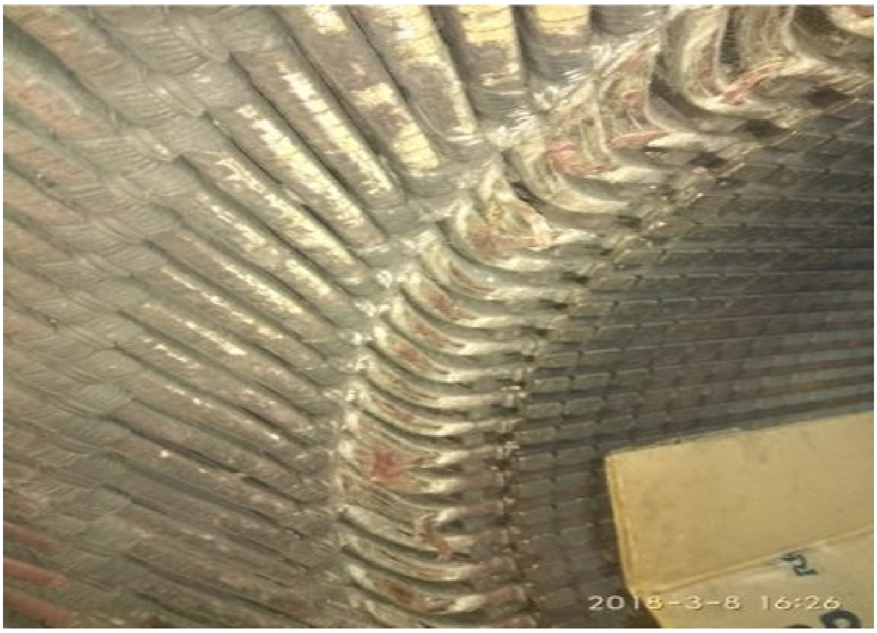


Fig. 7. Deformation of 15 MW, alternator due to dislocation.

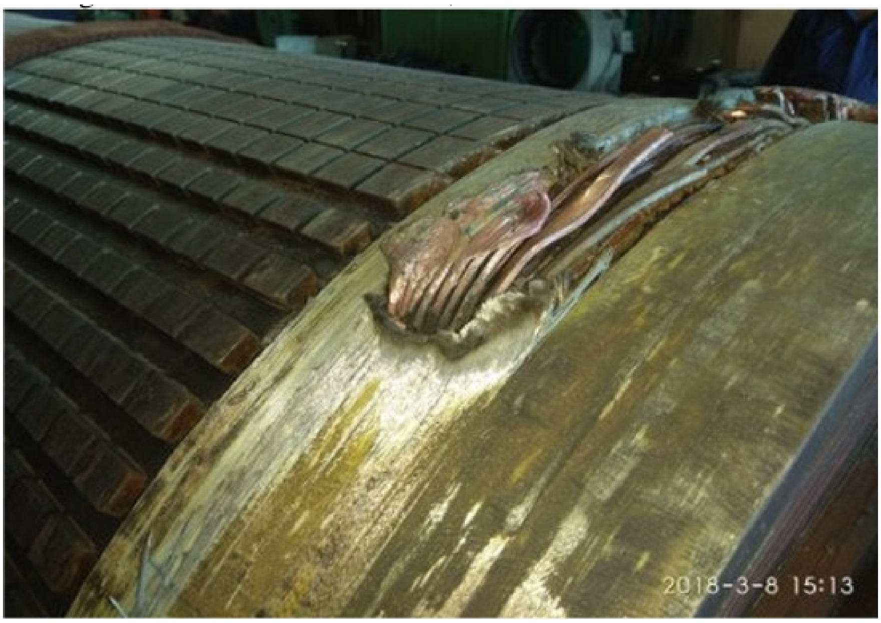


Fig. 8. Puncturing of glass insulation covering the overhang portion of the rotor due to dislocation of stator winding causing direct contact with the rotor.

It shows the dislocation of the windings and insulation rupture in the overhang region of the rotor. It may be due to excessive vibration, non-operation of the field failure relay, leading to the induction generator operation, or ruling power factor operation, ultimately breaking the restraining band that holds the overhang portion firmly. Such a type of fault is difficult to predict unless visual inspections of the alternator's rotating and stationary coil structures are recorded online, and corrective measures are taken in advance. Such instrumentation requires inexpensive digital cameras and online recording of crucial moving and static structures.

3.4. Nose joint failure

Nose joints connect the end terminals of phase windings to the bus bars connecting it to the panel. The end windings typically consist of several strip conductors which are insulated from each other, but at the end, these are short-circuited and fused with the connecting conductor to the bus bars. It is achieved by applying certain chemical compounds, which help forge the end winding terminals with the bus bars uniformly. Any flaw during the manufacturing process, formation of an air pocket or void inside the copper material increases the current density in the vicinity of the void/air pocket, causing hot spots. Over long runs, the metallurgical composition inside the copper material gets altered. Along with this and other environmental stresses such as vibrations, electrical heating due to overloading may dislodge the bus bar connecting the cable terminals with multiple ends winding conductors, causing insulation damage and disconnection of that phase.

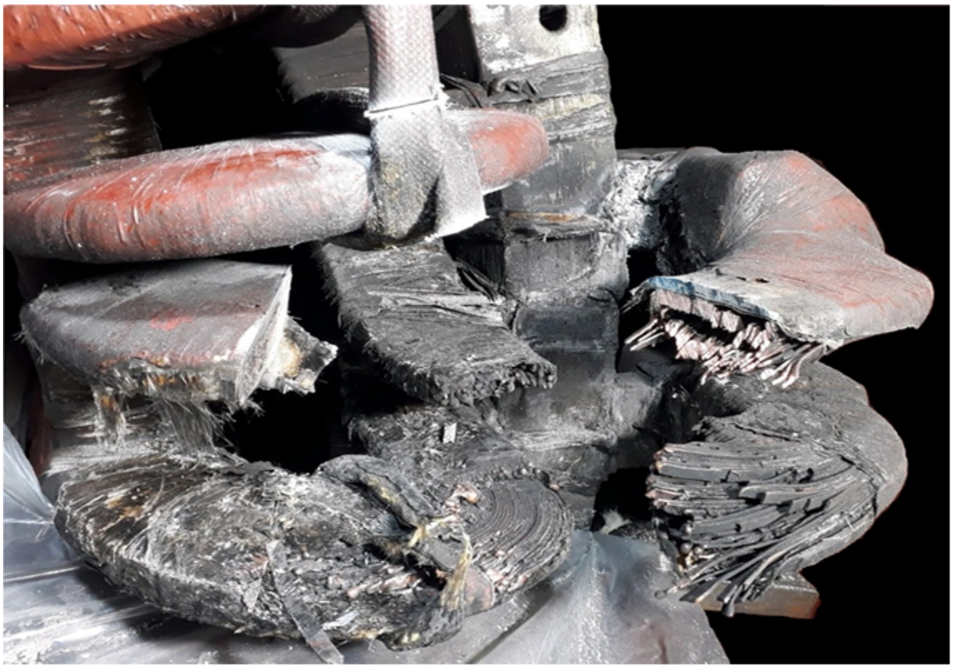


Fig. 9. Nose Joint Failure.

In an alternator with multiple parallel paths, the requirement of connecting multiple thick conductors, each having several strip conductors, to a common conductor is a more stringent manufacturing process. Fig. 9 shows a typical dislodging of the nose joint in a high voltage alternator.

4. Conclusion

Core burning causes insulation failure and destruction of the core requiring costly repair. Such faults in an alternator of smaller capacity cannot be determined in advance unless a suitable scheme is available. Chemical fume detection for sensitive elements responsible for core burning in the outlet air from vents should be developed for smaller capacity alternators. The dislocation of windings and the nose joint failure can be detected in advance if the visual recording is mounted inside the enclosure to monitor rotating and sensitive parts. Akin to these power machines, similar faults may occur in high voltage rating energy machines operating in stressful conditions such as compulsators and electromagnetic aircraft launchers.

Acknowledgment

The authors are thankful to the Indian Institute of Technology (Banaras Hindu University) Varanasi (India) for providing the necessary permission to conduct root cause analysis. They are also thankful to Sri Anil Dhingra,

References

Stone, G. C., C. V. Maughan, D. Nelson, & R. P. Schultz, Impact of slot discharges and vibration sparking on stator winding life in large generators, IEEE Electrical Insulation Magazine, 24(5), 14-21, 2008.

Vakser, Boris D. & BS. Nindra, Insulation problems in high voltage machines, IEEE Transactions on Energy Conversion, 9(1), 143-151, 1994.

Maity, Avijit, Kesab Bhattacharya, & Amar Nath Sanyal, Asynchronous operation of synchronous generators under field failure, In 2014 First IEEE Conference on Automation, Control, Energy and Systems, 1-6, 2014.

Venikov, Valentin Andreevich, Transient processes in electrical power systems, Mir Publishers, Moscow, 1977.

Noest, John G., Prevention of rotor-winding deformation on turbogenerators, Transactions of the American Institute of Electrical Engineers, 63(7), 514-519, 1944.

Juhlin, G. A., Deformation of turbo-alternator rotor windings, due to Temperature Rise, Journal of the Institution of Electrical Engineers, 85(514), 544-552, 1939.

Merkhouf, A., B. F. Boueri, & H. Karmaker, Generator end windings forces and natural frequency analysis, IEEE International Electric Machines and Drives Conference, IEMDC'03, 1, 111-114, 2003.

Webb, R. L., & C. S. Murray, Vibration protection for rotating machinery, Electrical Engineering, 63(7), 534-537, 1944.

Maughan, Clyde V., Vibration detection instrumentation for turbine-generator stator end windings, IEEE Electrical Insulation Conference, 173-177, 2009.

Letal, John, Bayu Satmoko, Nixon Manik & Greg Stone, Stator End-Winding Vibration in Two-Pole Machines: Avoiding Generator Failure, IEEE Industry Applications Magazine, 26(6), 29-39, 2020.

Ahumada, Constanza & Patrick Wheeler, Reduction of Torsional Vibrations Excited by Electromechanical Interactions in More Electric Systems, IEEE Access, 9, 95036-95045, 2021.

He, Yu-Ling, Ming-Xing Xu, Wen Zhang, Xiao-Long Wang, Peng Lu, Chris Gerada & David Gerada, Impact of stator interturn short circuit position on end winding vibration in synchronous generators, IEEE Transactions on Energy Conversion, 36(2), 713-724, 2020.

R. D. Stancheva & II Iatcheva, 3D Electromagnetic Force distribution in the end region of turbo generator, IEEE Transaction on Magnetics, 45(3), 1000-1003, 2008.

Kim, Ki-Chan, Hyung-Woo Lee, Yon-Do Chun & Ju Lee, Analysis of electromagnetic force distribution on end winding for motor reliance, IEEE Transactions on Magnetics, 41(10), 4072-4074, 2005.

Sinha, Amrita & D. N. Vishwakarma, Pattern Classification based Intelligent Numerical Protection of Salient-pole Synchronous Generator using Neural Networks, Journal of Electrical Systems, 9(1), 125-136, 2013.

Al-Kandari, A. M., B. A. Alkandari & S. A. Soliman, Modeling and Estimation of Synchronous Machine Parameters from Digitized Sudden Short-Circuit Armature Current, Journal of Electrical Systems, 11(2), 230-248, 2015.

R K Mobley, An introduction to Predictive Maintenance, 2nd Edition, Elsevier Press, 2002.

CIGRE Study Committee SC11, EG11.02, Hydrogenerator Failures– Results of the Survey, 2003.

Say, M. G, Performance and design of alternating current machines, Pitman 1958.

IEEE Guide for AC Generator Protection, IEEE Std. C37.12TM-2006 (Revision of IEEE Std. C37.102 1995).

ISSN 1112-5209

Fault Analysis of Microgrid With Grid-Connected and Islanded mode

K.V. Dhanalakshmi1, *, P.K. Panigrahi2, G.Ravi Kumar3

ABSTRACT

Now a days microgrid is one of the most widely used method in power network to reduce system losses as well as improve the reliability in the field of electrical systems. Integration of power projects typically involves adding new distributed energy sources with and without compensating devices to an existing power system network. It is essential to design new protection scheme due to changes in the topology and dynamic behavior of the system. Now fast fault detection algorithmic approaches are necessary to integrate different types of generating sources and loads under smart environment. The protection scheme must provide physical monitoring as well as parametrical with the help of new technologies. Internet-of-things(IoT) is one of the source to monitor electrical systems under various environmental conditions of the system. Wavelet (WT) basically investigates the fault transient signals of different frequency and divides the waveform into different approximate and detailed coefficient values, which provides the important knowledge about the classification and location of fault. The detection of faulty-line and the location of fault by implementation wavelet detailed coefficients of Bior1.5 mother wavelet. This proposed method provides fault analysis of IoT based protection of microgrid with Grid-connected and Islanded Mode Using Wavelet Approach under various types of faults.

Keywords: *Wavelet Transform, Distributed Generation, Fault Detection, Idle mode, Internet of things (IoT).*

1. Introduction

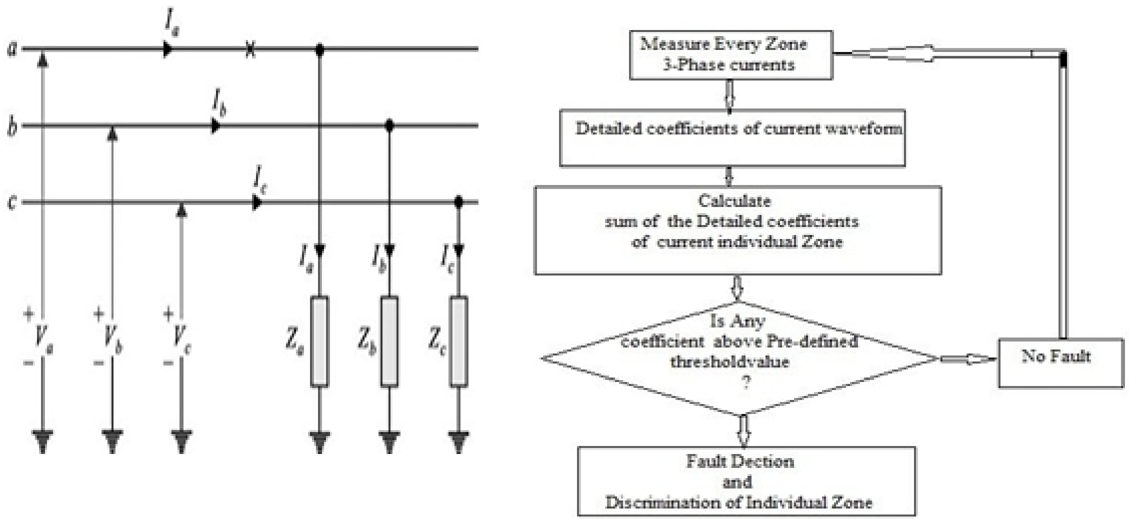
The task of the power transmission system is to transfer electric power from generating stations to load distribution centres and then consumer premises through substations and other utilities. The electrical power system should serve all its customers and inter connect partners economically and reliably. Transmission lines are transfer bulk amount of power from one location to the other location of the country. The conventional solution approach can be described as upgrading system infrastructure by erecting new lines, substations with associated equipment. Abnormal conditions are detected and prevented by protective relaying scheme and it will operate automatic switching mechanism to clear the fault by isolating faulty equipment from the existing network. The conventional line protection [1] is characterised by the ratio of two input quantities respectively proportional to the voltage and current at particular relay point. The basic measurement of impedance in comparators circuit. Now a day this type of protection may not suitable due to large detection time as well as isolation of faulty element and also it has several drawbacks [2,3] like to unwanted operation during power swings and heavy loading conditions which may leads to tripping stream and spread blackouts. Hence, it is necessary to think about alternative protection instead of distance protection scheme. In [4], now digital communication-based relays to designed for different operating condition of the system is pro- posed to detect the fault in the terminal and zones.

For the benefit of the mechanical protection Internet-of-Things (IoT) has emerged as one of the upcoming technologies for a smart grid network. As the IoT connected power network enable to develop more prominent protection scheme not only electrical as well as mechanical challenges in the existing grid network such as in design, erection commissioning, operation and maintenance [5]. Cyber security [12,13] triggers numerous problems in the system have been addressed and discussed in [6,7] about availability, integrity and confidentiality. Wired communication temporarily solves the problem but it gives problem due to interference communication channels. Few technologies related to broad band, GSM, GPRS ZigBee which cover up to the range of few kilometres due to the lack of data. If embedded IoT in the power system, can use the following communication models and protocols effectively like SCADA, DMS, GIS, CIS, OMS, etc. [8]. The applicable fast and secure communication method is Optical fibre but is very expensive [9]. since these devices are online hence making the smart grid protect to significant attacks.

A micro-grid comprises of three main components which are micro- generators, distribution and different loads. The formation of micro-grid can be Single or multi terminal with 1φ/3φ system and it is connected to low or medium-voltage for distribution of electric power, and can operate under normal and island modes [10]. Micro-grid protection has complicated challenges in design of protection scheme and which can respond main and micro-grid faults. The level of protection is depending on fault current magnitudes in the system [11,12]. The protection scheme must face the problem comparing with existing power systems is that the fault current flow is unidirectional for radial system, but in the case of micro-grid the current flow is bidirectional flow [13]. The distribute energy sources are frequently used in power sector industry. The selection of protective element is complex due to coordination required between grid side over-current protection and distance protection at transmission line discussed in [14], but these types of systems can capable to suppress challenges of electrical protection system. Considering the available information, a half cycle based moving window average technique for wind source integrated tapped transmission line .

Now a day, the system must capable to reduce transient oscillations due to frequently changing loads and protect the system from the faults. The past transmission system is unable to manage the control of load fluctuations and unwanted disturbances. The design of new method not only increase the cost as well as decrease in efficiency, but it also increases the complexity of the system. Therefore, attention is required for the stability and security of the utility grid as well as micro-grid. For the protection of existing system various approaches are investigated and found some of the alternative mechanisms are formulated such as reactive power compensation by installation of power electronics based devices to increase security of the power system. The proposed method requires faster response of power system parameters, reduce power loss and stability improvement.

The protection system can perform two major tasks mainly fault classification and forecast of fault location. Primary importance for discrimination and location of the faulted. This helps to safeguard the connected equipment as well as operating personnel and also immediate restriction of redundant power loss. Mostly unsymmetrical and symmetrical type of faults occur in transmission known as Singleline ground (SLG), Double-line-ground (DLG), Double-line (DL) and Three-phaseground (TPF) and also open-circuit(OC) faults. classification follows short circuit conditions of different phases: SLG-AG, BG and CG faults, DLG-ABG, BCG and CAG faults, DL-AB, BC and CA faults, LLL & LLLG faults are derived and discussed with figure-1 and figure-2. After getting faults in the system utmost care should be taken for restoration of system stability. The fault detection and location is major task to protect power system components for resuming normal power flow. A micro-grid protection based algorithm is described in [16] with the help of transient current wave form using wavelet detailed coefficients. The proposed research work concentrates on protection analysis of microgrid under grid connected and isolated mode with the help of Iot monitoring and wavelet based multi-Resolution-Analysis (MRA) [17] is used with the calibration of coefficients of Bior-1.5mother-wavelet. Nowadays, the digital relays are working fast as well as accurate detection and isolation of the faulty element when compared to previous methods. The following sections discuss about IoT Based protection of Microgrid with Grid-Connected and Islanded Mode Using Wavelet Approach.


a
b
c
I_a
I_b
I_c
V_a
V_b
V_c
Z_a
Z_b
Z_c
Measure Every Zone 3-Phase currents
Detailed coefficients of current waveform
Calculate sum of the Detailed coefficients of current individual Zone
Is Any coefficient above Pre-defined thresholdvalue ?
No Fault
Fault Dection and Discrimination of Individual Zone

(a) General system (b) Fault Detection Algorithm

Figure 1: General System and fault detection algorithm

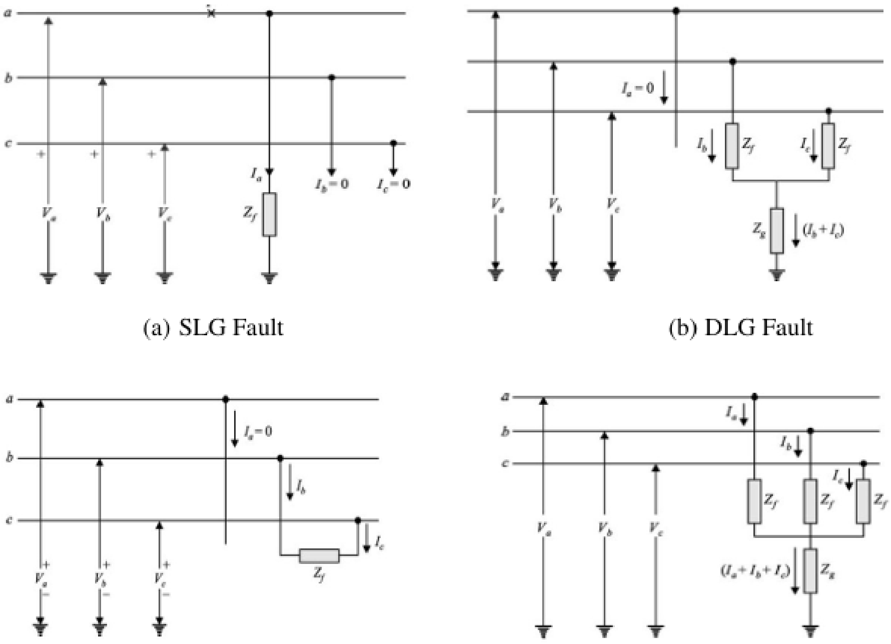
2. Fault Analysis with symmetrical components

Normally power system network may fall under one-phase, Two-Phase, Three Phase short circuit faults namely SLG (Single-Line-Ground), DLG(Double-LineGround), DL(Double-Line) and 3Phase faults categorised as unsymmetrical and symmetrical faults. The analysis of faulted network can be carried by make use of Positive, Negative and Zero sequence components and their interconnections based on the type of fault in the system. The following steps to consider for the analysis of faults.

1.Draw the single line diagram with fully labelled up to the faulty point with polarity marking and current flow directions.
2.Identify the known boundary conditions of voltage and current with respect to fault.
3.Convert voltage and current quantities from phase frame (a-b-c) system to sequence frame (1-2-0).
4.Determine the proper connection of sequence network satisfy the current and voltage relationships.
5.Interconnect sequence network according to the type of fault.

The sequential currents are represented as required phase currents are

$$\begin{bmatrix} I_0 \\ I_1 \\ I_2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix}\begin{bmatrix} I_a \\ I_b \\ I_c \end{bmatrix} \quad (1)$$



(a) SLG Fault

(b) DLG Fault

(c) DL Fault

(d) TPG Fault

Figure 2: Line diagram representation of Transmission Fault analysis

2.1 Single-Line-to-Ground-Fault

The single-line-fault with proper labelling is illustrated in figure The initial conditions assumed as follows

$$I_b = I_c = 0 \tag{2}$$

$$V_a = Z_f I_a \tag{3}$$

$$\begin{bmatrix} I_0 \\ I_1 \\ I_2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix}\begin{bmatrix} I_a \\ 0 \\ 0 \end{bmatrix} \tag{4}$$

$$I_0 = I_1 = I_2 = \frac{1}{3} I_a \tag{5}$$

$$I_0 = \frac{V_a}{Z_0+Z_1+Z_2+3Z_f} \tag{6}$$

The fault current I_a calculated as

$$I_a = 3I_0 = \frac{3V_a}{Z_0+Z_1+Z_2+3Z_f} \tag{7}$$

2.2 Line-Line-Fault

let us consider line-to-line fault is shown in figure

$I_b = -I_c$ and $I_a = 0$; $V_b - V_c = I_b Z_f$

$$\begin{bmatrix} I_0 \\ I_1 \\ I_2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix}\begin{bmatrix} 0 \\ I_b \\ -I_b \end{bmatrix} \tag{8}$$

The sequence current computed as follows

$$I_{a1} = \frac{V_a}{Z_1+Z_2+Z_f} \tag{9}$$

$$I_b = -I_c = \frac{-j\sqrt{3}V_a}{Z_1+Z_2+Z_f} \tag{10}$$

2.3 Line-Line-Ground-Fault

A double line to ground fault is shown in figure. The phase-a current is assumed as $I_a = 0$ and $V_b = V_c = (I_b + I_c)Z_f$

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix}\begin{bmatrix} V_a \\ V_b \\ V_c \end{bmatrix} \tag{11}$$

The fault current is calculated using equation-12

$$I_1 = \frac{V_a}{Z_1 + \frac{Z_2(Z_0+3Z_f)}{Z_2+Z_f+Z_0}} \tag{12}$$

2.4 Three-Phase-Ground-Fault

The three phases are short circuited known as symmetrical fault the vector sum of the fault Current is zero i.e. $I_a + I_b + I_c = 0$. As the fault is symmetrical

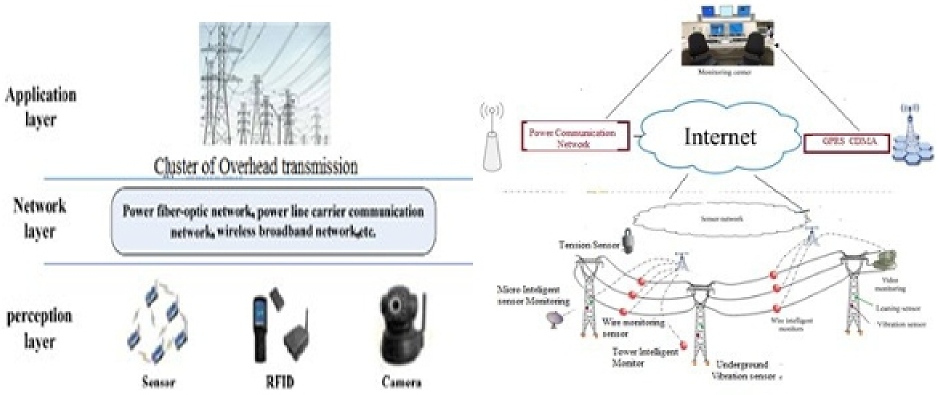
$$\begin{bmatrix} V_a \\ V_b \\ V_c \end{bmatrix} = \frac{1}{3}\begin{bmatrix} Z_f & 0 & 0 \\ 0 & Z_f & 0 \\ 0 & 0 & Z_f \end{bmatrix}\begin{bmatrix} I_a \\ I_b \\ I_c \end{bmatrix} \tag{13}$$

The fault currents are calculated as follows

$$I_a = \frac{V_a}{Z_1+Z_f}; I_b = a^2 I_1; I_c = aI_1 \tag{14}$$

3. Transmission system protection methods

At present scenario only electrical based protection schemes are not suitable for entire power network. Modern power systems require state-of-art methods to protect physically as well as electrically by the analysis of system performance. The protective system must observe natural calamities and electrical load fluctuations by make the utilisation of IoT application and fault detection algorithms [15]. Internet of Things (IoT) gives the basement for Smart City supports for instance Smart Health, Smart Transport, Smart Home, SG etc [18].


Application layer
Cluster of Overhead transmission
Network layer
Power fiber-optic network, power line carrier communication network, wireless broadband network,etc.
perception layer
Sensor
RFID
Camera
Monitoring center
Power Communication Network
Internet
GPRS CDMA
Sensor network
Tension Sensor
Micro Intelligent sensor Monitoring
Wire monitoring sensor
Tower Intelligent Monitor
Underground Vibration sensor
Wire intelligent monitors
Video monitoring
Leaning sensor
Vibration sensor

(a) IoT Architecture (b) IoT Protection

Figure 3: IoT Based Protection model

3.1 Basic IoT based Protection

The perception layer can gather required information through sensors, RFID and camera for monitoring the electrical devices which are required to send information to network layer for the protection of power transmission network [19,20]. The network layer includes fibre-optic communication channels for transmitting data from one end to other end; power line carrier communication is required for transmitting electrical data and wireless networks for remote data collection.

Application layer collect the information from various available sources and then make the protection scheme becomes real time system. IoT perform processing, integration and analysis of data, thus intelligent control services and decision making such that the protection scheme is improved.

This Iot system contains various sensors are generating premature warnings to the watching centres about physical and mechanical conditions of tower as well as conductor and also threats regarding of high voltage towers. The vibration sensors monitor underground vibrations discussed in [20]. IoT based transmission system protection incorporates mechanical and electrical safety of power lines from the problems of natural disasters, unsophisticated threats to construction, natural disaster and growing trees as illustrated in figure-3.

3.2 Wavelet based network protection

Wavelet transform (WT) is popular tool for research to detect transient faults by analysing various types of signals and separate approximate and detailed coefficients using basic mother wavelet, which gives tremendous information regarding fault classification and location [21]. A power system with microgrid protection algorithm is described in [16] Multi-resolution- Analysis (MRA) through transient current signals with mother wavelets of faulty signals with the comparison threshold value. The proposed algorithm is described in figure8.

4. Modelling and simulation of System under study

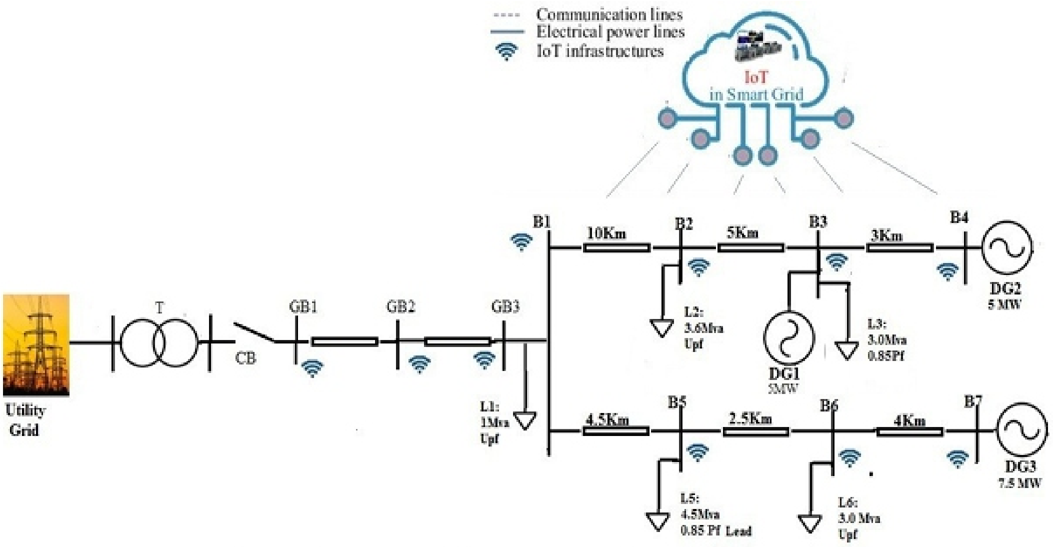


Figure 4: Proposed system model-main parameters

DG1: 7.5 MVA, 4.16 kV-DG unit at bus 3. L1:1 MVA, PF=1

DG2: 5 MVA , 4.16 kV -DG unit at bus 4 L2:=3.6 MVA, PF=1

DG3: 5 MVA , 4.16 kV DG unit at bus 7 L3:3.0 MVA, PF=0.85 lag

Line-12=10 km, Line-23=5 km, Line-34=3 km L5:4.5 MVA, PF=0.85 lead

Line-15=4.5 km, Line-56=2.5 km, Line-67=4 km L6:3.0 MVA, PF=1

$Z_{1,2} = 0.173 + j0.432\Omega/km$ $Z_0 = 0.346 + j1.800\Omega/km$

The proposed test system under study is Canadian bench mark distribution network as shown in figure-4.The system comprises of 9-bus microgrid connected system connected to grid with three synchronous DGs are connected at bus numbers 3,4 and 7.The total system divided in to eight zones as illustrated in figure-4 and system technical parameters are represented in Table-I Fig.4 shows the layout of Iot based transmission system and its main parameters are represented as follows: three phase, 34.5 kV, 60 Hz test microgrid simulated using MATLAB. The utility grid is represented by a voltage source with the short-circuit capacity of 900 MVA. This microgrid can include a combination of the following DG units: The proposed test system under study is Canadian bench mark distribution network as shown in figure. The system comprises of 9-bus microgrid connected system connected to grid with three synchronous DGs are connected at bus numbers 3,4 and 7. The total system divided in to eight zones as illustrated in figure-4 and system technical parameters are represented in Table-I.

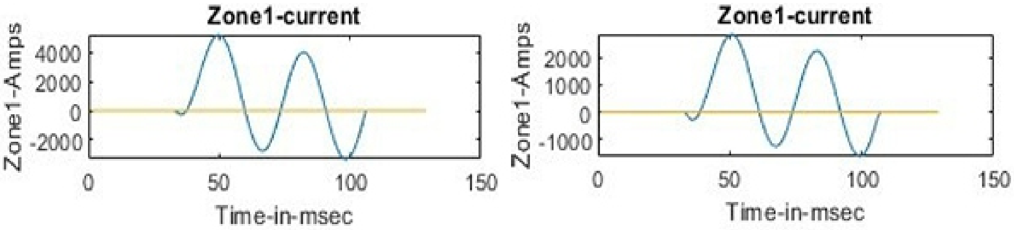
5. Simulation results

The fault cases are considered every zone of ten different types of faults. There are three main cases to Study:

1) Type of fault – SG, SLG, DLG, TLG faults

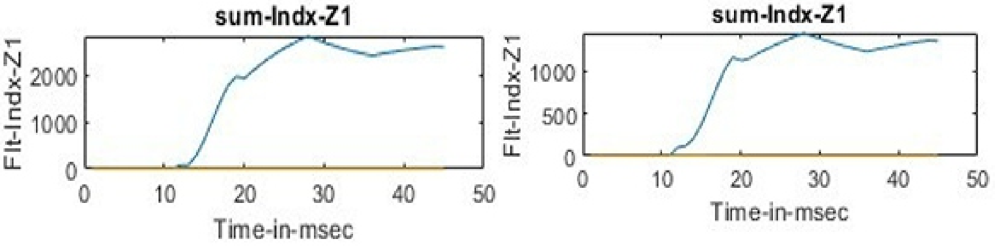
2) Total transmission divided into 8 Zones.

3) Fault inception angles (from 00 to 1800 in increment of 15 degrees



(a) Grid Connected mode (b) Grid Idle mode

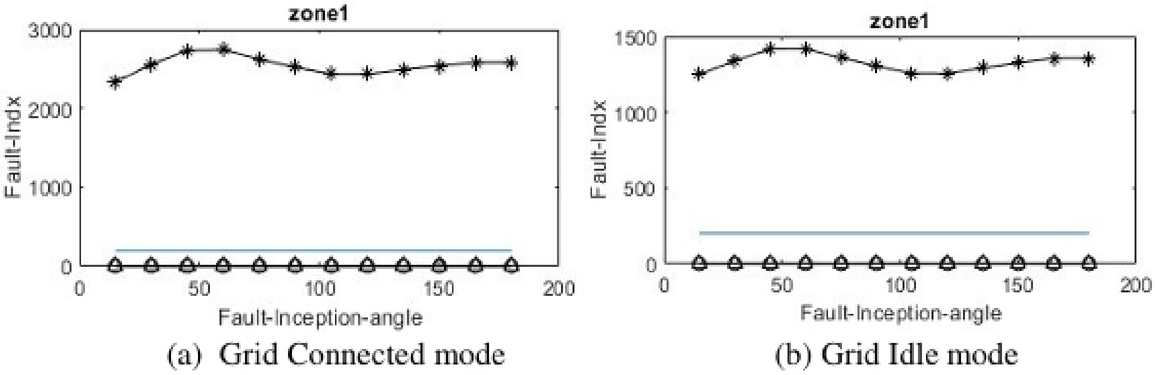
Figure 5: Current wave-forms of 9-Bus system in Zone-1 at LG-Fault



(a) Grid Connected mode (b) Grid Idle mode

Figure 6: wavelet based fault index of 9-Bus System in Zone-1 at AG-Fault

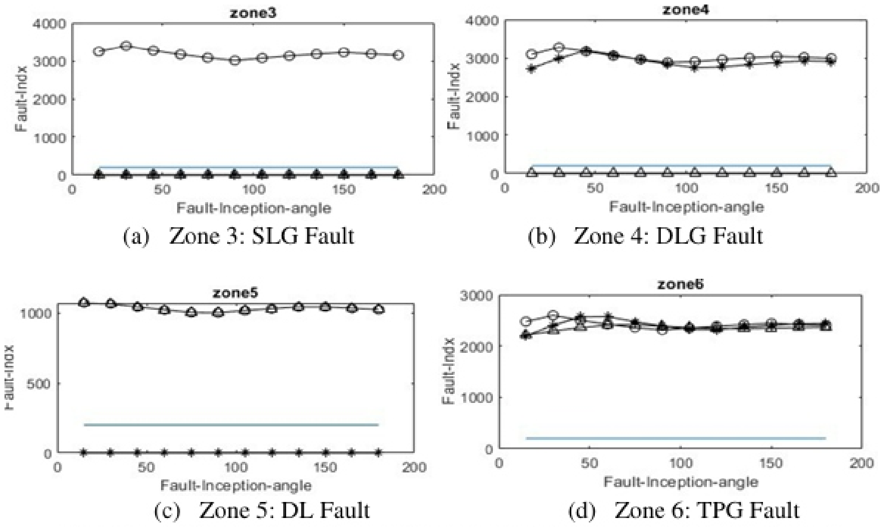
The Proposed work report detection& discrimination and location of fault in various zones by utilisation of sum-of-the-Detailed coefficients of current signal of the system. The detection of fault is observed with the analysis of fault index values. The faulty phases and healthy phases are detected with the comparison of predefined threshold value which describe the detection and discrimination of fault.



(a) Grid Connected mode (b) Grid Idle mode

Figure 7: FIA variation of fault index of 9-Bus System in Zone-1 at AG-Fault

Then the Zone current signal has sampling rate 144 kHz of Z1 to Z 8 during the fault to analyse the data after selecting bior1.5 mother wavelet. For system study total 10 types of faults in each Zone. For the differentiating grid connected and idling mode of system is described by actual current wave forms. It is observed that grid connected made has highest value when compared to idle mode and indicating that the impact of fault is higher at normal grid connected mode as shown in figure-5. The time required to find the fault is less than 12 milliseconds in the case of wavelet multi resolution with sum of the detailed coefficients algorithm where as in the case of conventional approach by observing current waveform analysis the duration to identify the fault is more than 30 milliseconds and it is found that the proposed algorithm require lesser time compared to normal conventional method which can be identified from figure-6.

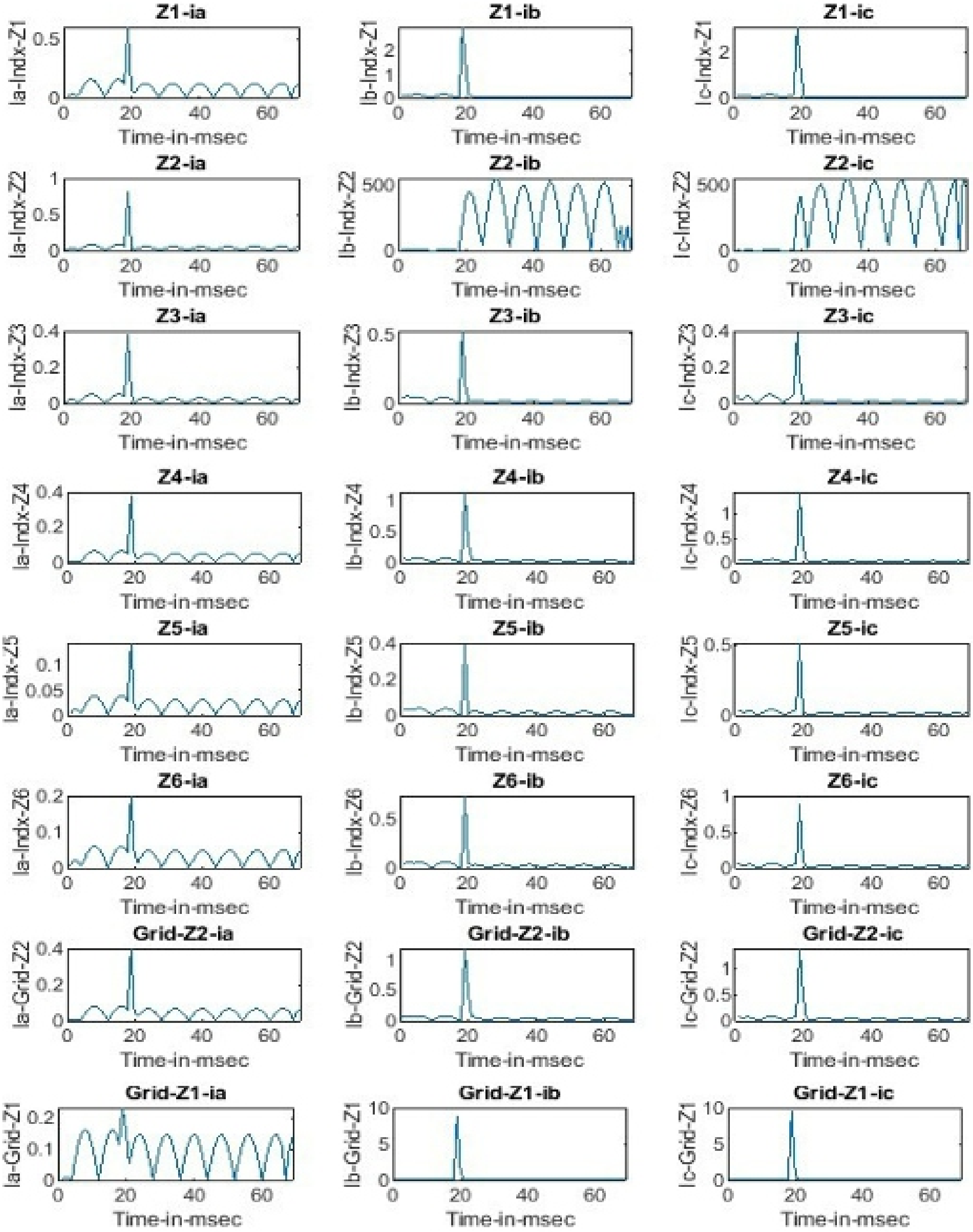


(a) Zone 3: SLG Fault (b) Zone 4: DLG Fault

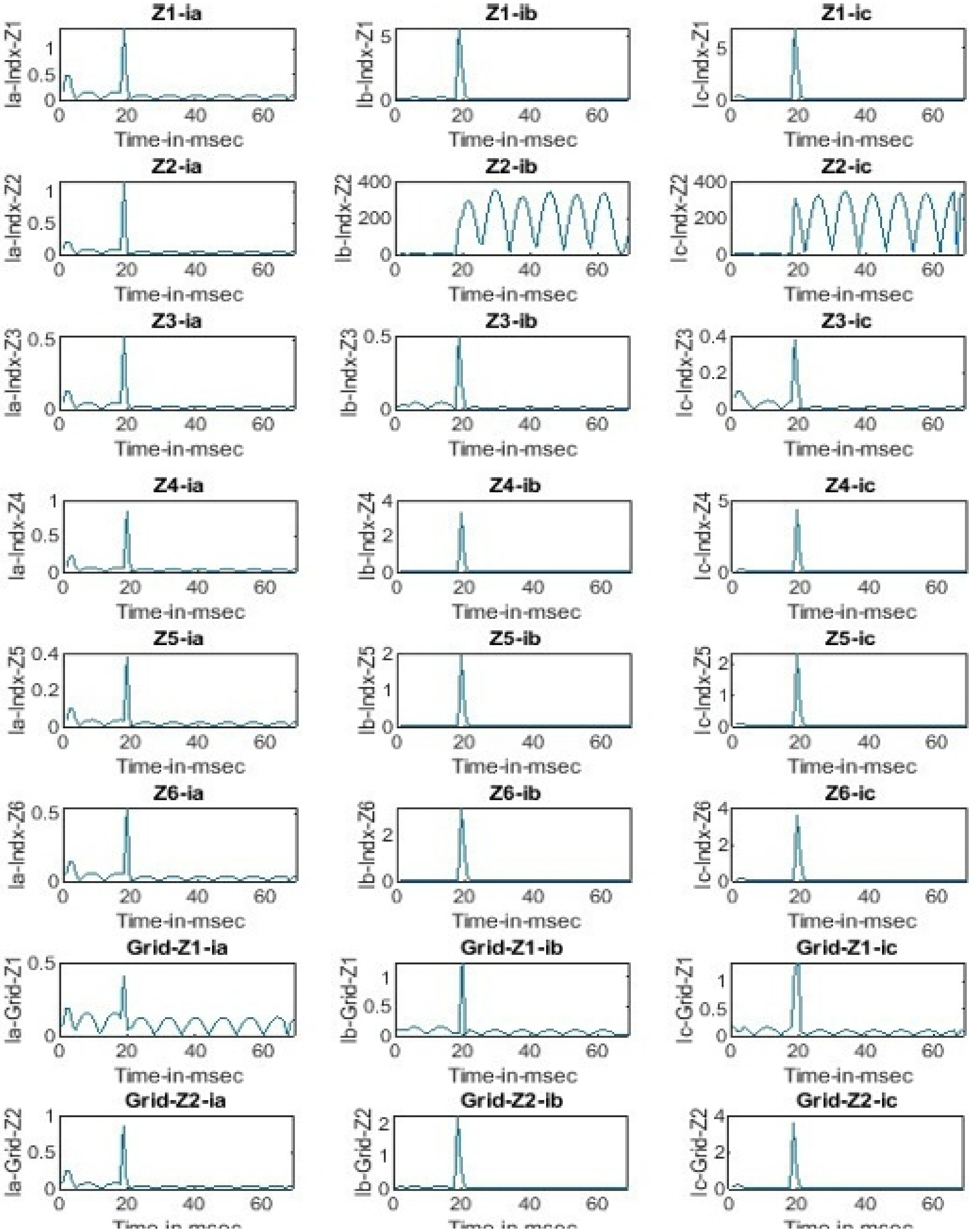
(c) Zone 5: DL Fault (d) Zone 6: TPG Fault

Figure 8: Impact of Fault Inception Angle under various Faults and Zones

The impact of fault inception angle at Zone-1 is observed from figure-7 and the system fault analysis is described in Table-I. It is observed that highest detailed coefficient values at phase-a and indicating that the phase-a to ground fault.



(a) Grid Connected mode

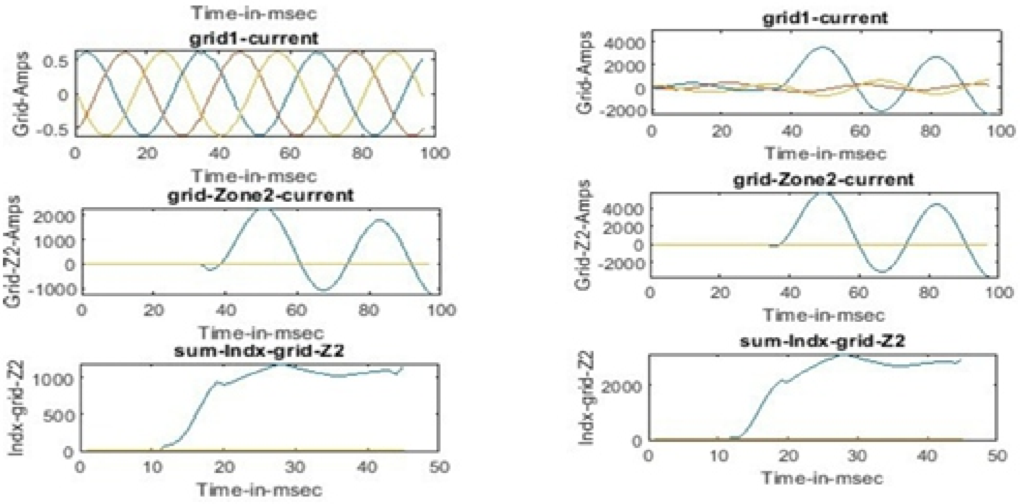


(b) Grid Idle mode

Figure 9: Detection of fault in Zone-2 at BCG-Fault

Table 1: LG-Fault at Zone-1: Analysis of fault Index at Zone-1 under grid connected and Idle mode

FIA	Fault Index at Zone-1 Grid connected			Fault Index at Zone-1 Grid Idle mode		
	I_A	I_B	I_C	I_A	I_B	I_C
15	2335.73	0.7819	0.7674	1251.59	0.7240	0.7171
30	2554.79	0.7817	0.7675	1339.77	0.7239	0.7172
45	2733.89	0.7817	0.7672	1417.64	0.7238	0.7173
60	2741.11	0.7818	0.7671	1419.77	0.7238	0.7174
75	2620.26	0.7819	0.7669	1359.03	0.7237	0.7175
90	2520.51	0.7820	0.7669	1305.38	0.7236	0.7176



(a) Grid Connected mode *(b) Grid idle mode*

Figure 10: wavelet based fault index of 9-Bus System in Zone-1 at AG-Fault

Table 2: LG-Fault at Zone-1: Analysis of fault Index at utility Grid side under grid connected and Idle mode

FIA	Fault Index at Zone-1 Grid connected			Fault Index at Zone-1 Grid Idle mode		
	I_A	I_B	I_C	I_A	I_B	I_C
15	2603.08	0.4050	0.3996	1017.07	0.3687	0.3667
30	2854.04	0.4045	0.3992	1094.62	0.3685	0.3669
45	3059.76	0.4045	0.3991	1161.92	0.3685	0.3670
60	3068.05	0.4046	0.3990	1163.98	0.3685	0.3670
75	2929.16	0.4046	0.3990	1113.27	0.3684	0.3670
90	2814.76	0.4047	0.3990	1069.23	0.3684	0.3671

The detection of fault can be identified in the entire network is illustrated in figure-9. It is observed that larger index values compared to all indices of the network which can be specified that the fault is BC-To-Ground fault in zone-2. The impact of fault inception angle can be noted for Zone-3 of BG Fault under grid idle mode, Zone-4 of ABG fault under grid connected mode and Zone-5 of CAG fault under grid connected mode illustrated in figure-8.

The analysis of wavelet-based fault analysis of idle and connected mode of grid under AG-fault in zone-1 is represented in figure-10. The fault analysis Table-II values reported that wavelet multi resolution analysis carried effectively for the detection and discrimination of faults.

6. Conclusions

This paper proposes protection scheme of Transmission system with the assistance of IoT and its applications, so that it can provide strong real protection scheme. IoT can solve real problems mechanical and physical problems with effective manner and also promoting the development of new protection algorithms. WT is one of the research tool to analyses the faults in transient signals at different frequencies by decomposing the waveform into coefficients of bior1.5 mother wavelet, which presents more prominent information regarding the class of fault and location in existing system by time and frequency domain. The Proposed algorithm has been tested for the detection of faults under various types of faults at different fault inception angles using wavelet multi resolution analysis with bios1.5 mother wavelets detailed coefficients with the help of IOT Application.

References

[1] IEEE Std C37.113-2015, "IEEE Guide for Protective Relay Applications to Transmission Lines", (2015), pp. 1–141.

[2] Patel, U., Bhatt, P., Chothani, N. (2021). Transmission Line Protection Philosophy. In: Futuristic Trends in Numerical Relaying for Transmission Line Protections. Energy Systems in Electrical Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-15-8465-7_1

[3] S.V. Unde, S.S. Dambhare, Differential protection of mutually coupled lines in modal do- main using synchronized measurements, 2016 National Power Systems Conference (NPSC), IEEE, 2016, pp. 1–5.

[4] Lien K-Y, Bui DM, Chen S-L, Zhao W-X, Chang Y-R, Lee Y-D, et al. A novel fault protection system using communication-assisted digital relays for AC microgrids having a multiple grounding system. Int J Electr Power Energy Syst 2016; 78:600–25.

[5] Amin, S.M., 2011. Smart grid: overview, issues and opportunities. Advances and challenges in sensing, modeling, simulation, optimization and control. Eur. J. Control 56, 547–567.

[6] El-Hawary, M.E., 2014. The smart grid-state-of-the-art and future trends. Electr. Power Compon. Syst. 42 (3–4), 239–250.EPRI, "EPRI Smart Grid Demonstration Initiative: Final Update".

[7] Ma, R., Chen, H.-H., Huang, Y.-R., Meng, W., 2013. Smart grid communication: challenges and opportunities. IEEE Trans. Smart Grid 4 (1).

[8] Namra Joshi, Dheeraj Nagar, Jaya Sharma "Aplication of IoT in Indian Power System", Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020) IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1

[9] Fang, X., Mishra, S., Xue, G., Yang, D., 2012. Smart grid – the new and improved power grid: a survey. IEEE Commun. Surv. Tutor. 14 (4), fourth quarter.

[10] Nikkhajoei H, Lasseter R H. Microgrid protection. In: Proceedings of IEEE power engineering society general meeting; 2007.p.1–6.

[11] Mishra M, Rout PK. Detection and classification of micro-grid faults based on HHT and machine learning techniques. IET Gener Transm Distrib 2018; 12:388–97.

[12] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "On the adaptive protection of microgrids: A review on how to mitigate cyber-attacks and communication failures," in 2017 IEEE Industry Applications Society Annual Meeting, 1-5 Oct. 2017 2017, pp. 1-8.

[13] H. J. Laaksonen, "Protection principles for future microgrids,"IEEE Transactions on Power Electronics, vol.25, no.12,pp.2910-2918, 2010.

[14] Mishra, D. P., Ray, P. (2017). Fault detection, location and classification of a transmission line. Neural Computing and Applications, 30(5), 1377-1424.

[15] G. Gantaiah Swamy, Padma Kottala , "Wavelet-ANN Based Analysis of PVIoT Integrated Two Area Power System Network Protection in presence of SVC", J. Electrical Systems 18-1 (2022): 23-38

[16] Shekar, S. C., Kumar, G., Lalitha, S. V. N. L. (2019). "A transient current based micro-grid connected power system protection scheme using wavelet approach" International Journal of Electrical and Computer Engineering, 9(1), 14.

[17] Shazia Baloch, Sunil Srivatsav, samsani, and Mannan Saeed Muhammad, "Fault Protection in Microgrid Using Wavelet Multiresolution Analysis and Data Mining, IEEE Access Volume 9, 2021, date of publication June 14, 2021, date of current version June 22, 2021.

[18] Dharmadhikari, Shweta C., Veerraju Gampala, Ch Mallikarjuna Rao, Syed Khasim, Shafali Jain, and R. Bhaskaran. "A smart grid incorporated with ML and IoT for a secure management system." Microprocessors and Microsystems 83 (2021): 103954.

[19] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems," IEEE Internet of Things Journal, vol. 5, no. 2, pp.

847–870, 2018.

[20] YasirSaleem, Noel Crespi, Mubashir Husain Rehmani, and Rebecca Copeland" Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions" IEEE Access,Page(s): 62962 – 63003.

[21] M.JayaBharata Reddy, D.Venkata Rajesh and D.K.Mohanta,"Robust Transmission Line Fault Classification Using Wavelet Multiresolution Analysis", Computers and Electrical Engineering (Elsevier publication), Vol.39, No. 4, pp. 1219-1247,May 2013.

ISSN 1112-5209

The Future of Energy: Vegetable Oils as a Viable Alternative

Dr. K. Sreenivasa Reddy1

ABSTRACT

The rising global demand for petroleum products has intensified imports, causing economic strain and environmental issues, especially for countries like India that heavily rely on imported fuels. To mitigate this, exploring alternative, renewable, and indigenous fuel sources is essential. Vegetable oils, with combustion properties close to diesel, present a viable option for compression ignition (CI) engines. However, their high viscosity and low volatility lead to poor engine performance and high smoke emissions. Methods such as blending, preheating, and transesterification have been employed to improve usability, but these still result in operational problems like filter clogging, nozzle carbon deposits, and elevated emissions. Low Heat Rejection (LHR) engines, which operate at higher in-cylinder temperatures due to insulated components, offer a promising solution. These engines enhance combustion, reduce ignition delay, and lower hydrocarbon, carbon monoxide, and smoke emissions when running on vegetable oils. Ceramic coatings on pistons, liners, and cylinder heads help reduce heat losses and potentially improve thermal efficiency. However, experimental results have been inconsistent, with some studies reporting improved fuel economy and others noting higher consumption. This study aims to modify a standard diesel engine into an LHR configuration using varying levels of ceramic insulation. Performance and emission characteristics will be evaluated using different locally available vegetable oils to identify the most suitable fuel. The research will also explore additional techniques like fuel additives to optimize engine operation. The goal is to develop a more efficient, low-emission engine compatible with renewable vegetable oils.

Keywords: *Combustion Efficiency, vegetable oils, Insulation, Limited Cooled EnginesB: Combustion*

1. Introduction

The usage of vegetable oil in an engine depends on the properties of the oil. Their properties are almost closer to diesel, particularly cetane rating and heat values. These vegetable oils are renewable and are produced easily in rural and forest areas. Their uses do not require major engine, vehicle or infrastructure modification in existing facilities. Since these oils have slightly longer ignition delay, they are most suitable to use in low heat rejection engines.

In most of the developed countries, biodiesel is produced from soybean, rapeseed, sunflower, peanut, etc., which are essentially edible in Indian context. Among the various vegetable oil sources, non-edible oils are suitable for biodiesel production. Because edible oils are already in demand and too expensive than diesel fuel.

Among the non-edible oil sources, Jatropha, karanjan, Mahua, Neems, Sal, Hemp, kusum, hemp, Nahar, Rice bran and Tumba is identified as potential biodiesel source and comparing with other sources, which has added advantages as rapid growth, higher seed productivity, suitable for tropical and subtropical regions of the world. Biodiesel is a chemically modified alternative fuel for use in diesel engines, derived from vegetable oils and animal fats. Biodiesel is produced commercially by the transesterification of vegetable oils with alcohol. These can also be produced from the biomass sources. The direct use of vegetable oil as fuel causes corrosion of various parts in the engine. The transesterification process solves this problem. The carbon cycle of vegetable oils consists of release and absorption of carbon dioxide. Combustion and respiration process release carbon dioxide and crops for their photosynthesis process absorb the carbon dioxide. Thus, the accumulation of carbon dioxide in atmosphere reduces. The carbon cycle time for fixation of CO2 and its release after combustion of biodiesel is quite small (few years) as compared to the carbon cycle time of petroleum.

FABRICATION OF INSULATED COMPONENTS

Piston

Insulated diesel engine contains a two-part piston; the top crown ,made of invar screwed to aluminum body of the piston, providing a 2mm-air gap in between the crown and the body of the piston. A nickel insert is screwed to the top portion of the liner in such a manner that an air gap of 2-mm is maintained between the insert and the liner body. The stainless steel gasket is introduced to minimize the heat loss through gasket. In the first instance, an invar crown was fitted on aluminium piston with 2.0 mm air-gap, in order to investigate the effect of air-gap alone. The total height of the standard aluminium piston was reduced by 9.0mm at the top by machining. An Invar crown of 7.0 mm thickness was turned out of Invar alloy rod of 85 mm to the shape of the standard piston crown. The hemispherical shape was turned using concave and convex turning tool. A thickness of 5mmwas maintained on the flange and bowl area of the crown. The recess for valve clearance is provided by end milling. The crown was separated by gaskets made of copper and stainless steel from the aluminium body. The stainless steel gasket is introduced to minimize the heat loss through gasket.

Cylinder Head

Ceramic coating is a simpler method of insulation for cylinder head compared with other methods. The head was insulated, by coating the area exposed to the combustion chamber with mullite. The combustion chamber area f the cylinder head was machined to a depth of 0.5 mm. The surface was then sand blasted to form innumerable pores for mullite deposition.

Valves

The bottom surfaces of the valves were machined to a depth of 0.5mm and coated with mullite material of equal thickness. With the valves assembled on the cylinder head the area of the combustion chamber was about 90-92% of the total area

Cylinder Liner

A thin mild steel sleeve was circumscribed over the cast iron liner maintaining a 2mm layer of air in the annular space between the liner and the sleeve. The joints of the sleeve were sealed to prevent seepage of cooling water into the air-gap region. Fig 2 shows the constructional details of the air gap liner. Insulation of the liner brought about considerable reduction in the heat lost to the cooling water and an increase in overall thermal efficiency of the engine.

VEGETABLE OILS

Most suitable vegetable oil can be selected from different vegetable oils by testing them in insulated engine. Their properties are almost closer to diesel, particularly cetane rating and heat values. However their viscosity values are higher but can easily be overcome by heating them. Since these oils have slightly longer ignition delay, they are most suitable to use in insulated engines. The two different vegetable oils, Hemp Oil (HO) and Kusum Oil (KO) are tried in the insulated test engine.

Hemp Oil

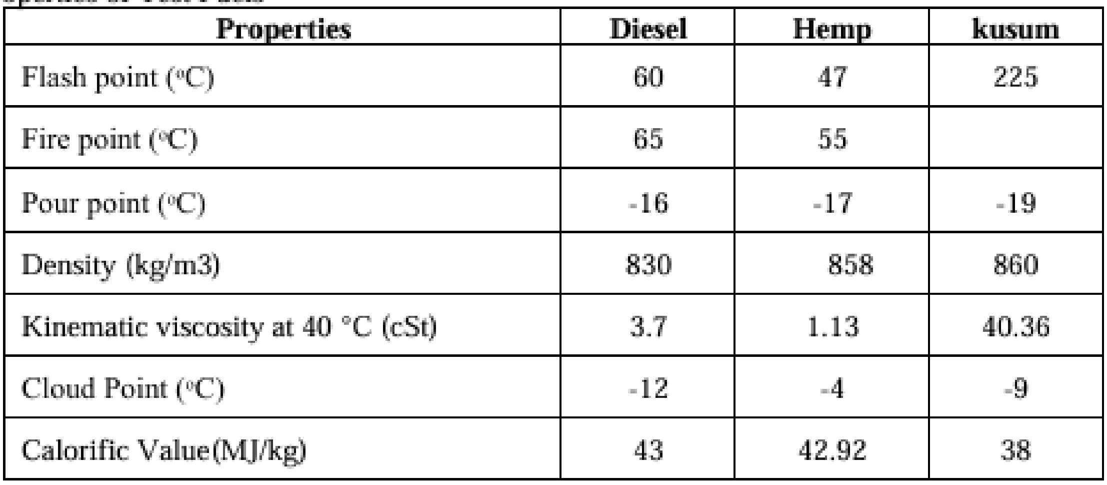
Refined hempseed oil is clear and colorless, with little flavor and lacks natural vitamins and antioxidants. Refined hempseed oil is primarily used in body care products. Industrial hempseed oil is used in lubricants, paints, inks, fuel, and plastics. Hempseed oil has found some limited use in the production of soaps, shampoos and detergents. The oil is of high nutritional value because of its 3:1 ratio of omega-6 to omega-3 essential fatty acids,which matches the balance required by the human body.It has also received attention in recent years as a possible feedstock for the large-scale production of biodiesel. There are a number of organizations that promote the production and use of hempseed oil.

Hempseed oil is manufactured from varieties of Cannabis sativa that do not contain significant amounts of tetrahydrocannabinol (THC), the psychoactive element present in the cannabis plant. This manufacturing process typically includes cleaning the seed to 99.99% before pressing the oil. There is no THC within the hempseed, although trace amounts of THC may be found in hempseed oil when plant matter adheres to the seed surface during manufacturing. The modern production of hempseed oil, particularly in Canada, has successfully lowered THC values since 1998. Regular accredited sampling of THC in Canadian hemp seed oil shows THC levels usually below detection limit of 4 ppm (parts per million, or 4 mg/kg). Legal limit for THC content in foodstuffs in Canada is 10 ppm. Some European countries have limits of 5ppm or none-detected, some EU countries do not have such limits at all.

Kusum (Schleichera oleosa)

Schleichera oleosa (Kusum) is a large deciduous (nearly evergreen) tree with a fluted comparatively short trunk and a shade spreading crown. This species occurs in the sub-Himalayan tract from Sutlej Nepal, Chhota Nagpur, Central India and the peninsula generally, apparently absent from Assam. In general, it thrives best on a light well drained gravelly or loamy soil. It is a shade bearer and frost and drought hardy, it is subject to damage by grazing. It produces root-suckers freely and its pollarding and coppicing power is good. The wood is very hard, reddish brown, used for oil and sugar mills, rice pounders, agricultural implements, and other purposes. The fruit is edible and the seeds yield an oil (Macassar oil) of some value. One of the chief uses of the tree is for the propagation of lac, the quality of which is considered better than that produced on any other tree.

Table 1: Properties of Test Fuels



Properties	Diesel	Hemp	kusum
Flash point (°C)	60	47	225
Fire point (°C)	65	55	
Pour point (°C)	-16	-17	-19
Density (kg/m3)	830	858	860
Kinematic viscosity at 40 °C (cSt)	3.7	1.13	40.36
Cloud Point (°C)	-12	-4	-9
Calorific Value(MJ/kg)	43	42.92	38

EXPERIMENTAL INVESTIGATIONS

The engine used for the experimental investigations was a Kirloskar, single cylinder, four stroke, water cooled, vertical and direct injection diesel engine. The standard engine was tested at the recommended injection timing of 270 bTDC at various loads. The engine was operated under no load for the first 20 minutes and for each load the engine was operated long enough to stabilize the condition. All the tests were conducted at the rated speed of 1500 rpm. Sets of experiments are conducted with two vegetable oils Hemp(Gongura), Kusum(Schleichera oleosa) to evaluate the performance of engine.

RESULTS & CONCLUSIONS

Experiments are conducted with Diesel and vegetable oils in an insulated engine to evaluate the performance characteristics.

Brake Thermal Efficiency

The variation of brake thermal efficiency of two vegetable oils tested in insulated engine with Brake Power output is shown in Fig. 1. All the oils have more or less equal Brake Thermal Efficiency compared to that of Diesel. The brake thermal efficiency of Hemp oil is higher throughout the load range. The thermal efficiency of Hemp oil is significantly higher compared to Kusum oil. Finally, it may be concluded that insulated is the best choice for vegetable oils from the Brake Thermal Efficiency.

Volumetric Efficiency

The variation of volumetric efficiency with power output is shown in Fig. 2. Relatively due to lower cylinder wall temperatures the volumetric efficiency is higher for Hemp oil. The volumetric efficiency is badly affected in the case of Kusum vegetable oil. The volumetric efficiency drop is more for Kusum oil and less for Hemp oil when observed for a complete power range.

Hydrocarbon Emission

Fig.3 shows the comparison of un-burnt hydrocarbon emissions of the vegetable oils with brake power output. Un-burnt hydrocarbon emissions of all vegetable oils are marginally higher than diesel oil. Poor mixing of these oils with air may be one of the reasons for this. The hydrocarbon emissions are more in the Kusum oil when observed for a complete power range.

Carbon Monoxide Emission

Carbon monoxide emission levels are also lower with Hemp oil as compared to other vegetable oils as seen in the Fig.4.

Exhaust Gas Temperature

Exhaust gas temperature variation with respect to Brake Power output for the vegetable oils are compared in the Fig.5. Exhaust temperature curves of are in close agreement with Diesel. Exhaust temperatures are Lowest for Hemp oil and highest in the case of Kusum Oil when compared with Diesel.

Frictional Loss

The variation of Frictional mean effective pressure with power output is shown in Fig. 6. From the graph, it is evident that Hemp and Kusum oils have more frictional losses when compared with Diesel.

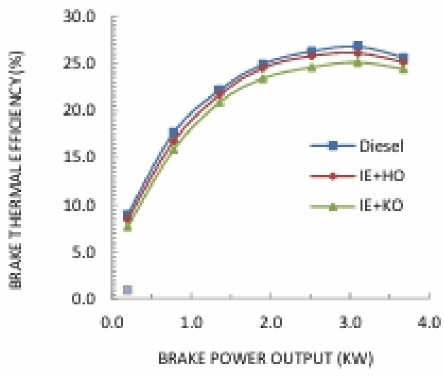


Fig.1 Comparison of brake thermal efficiency with...

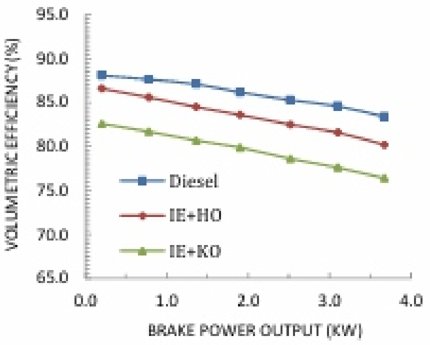


Fig. 2 Comparison of Volumetric efficiency with power...

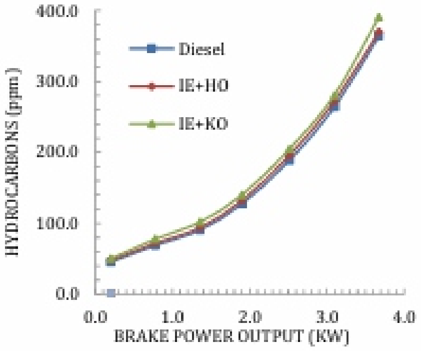


Fig 3 Comparison of Hydrocarbons with power output

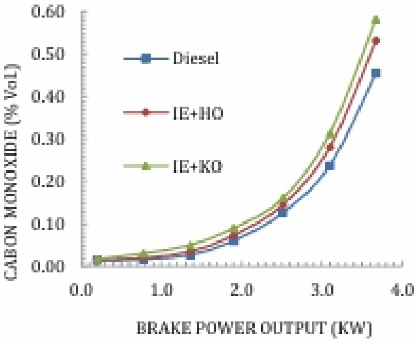


Fig. 4 Comparison of CO emission with power output

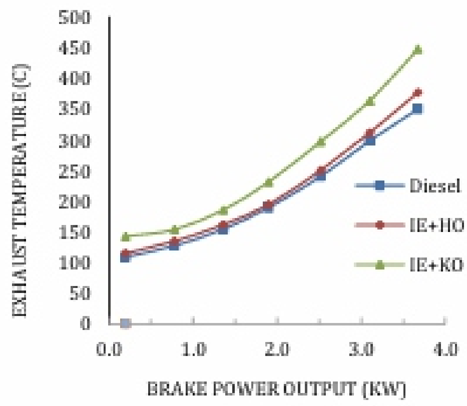


Fig.5 Comparison of Exhaust temperatureency with power output

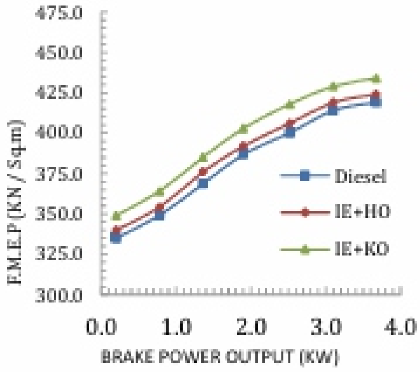


Fig.6 Comparison of Frictional mean effective...

CONCLUSIONS

Based on the experimental results the following conclusions are drawn. These conclusions are drawn based on diesel engine.

1. All the oils have more or less equal Brake Thermal Efficiency compared to that of diesel. The brake thermal efficiency of Diesel, Hemp and Kusum oils are 25.6 %, 25.2% and 24.4% at maximum load condition.
2. The Volumetric efficiency drop is observed in all the vegetable oils. The Volumetric thermal efficiency of Diesel, Hemp and Kusum oils are 83.4 %, 80.2% and 76.4% at maximum load condition.
3. There is slight increase in Hydrocarbon emissions for vegetable oils compared with normal engine. The hydrocarbon emissions of Diesel, Hemp and Kusum oils are 364, 370, 391 ppm at maximum load condition.
4. Carbon monoxide emission levels are also lower with hemp oil as compared to Kusum oil. Carbon monoxide emission of Diesel, Hemp and Kusum oils are 0.455%, 0.531% and 0.582% by volume at maximum load.
5. Among the vegetable oils tested, the exhaust temperatures are marginally higher for vegetable oils. Exhaust gas temperatures of Diesel, Hemp and Kusum oils are 3510c, 3780c and 4490c at maximum load
6. Vegetable oils have higher frictional losses than diesel .Frictional losses of Diesel, Hemp and Kusum oils are 419 KN/mm2, 424 KN/mm2 and 434 KN/mm2 at maximum load.

Insulated diesel engine with Hemp and Kusum vegetable oils performed well without any major modifications of the engine. This modified diesel engine is highly suitable for vegetable oils, due to better turbulence and elevated temperatures to overcome the problems associated with the oils, which are faced by the researchers.

REFERENCES

1. Myers P.S. and Uyehava O.A., "Efficiency, Heat transfer and pre-ignition in I.C.engines, SAE 660130, Vol 75"

2. Pradeepram, O., et al, Development and Testing of a Semi-Adiabatic Engine,8th National Conference on I.C. Engines and combustion, Trivandrum, 1983

3. Miyari, Y., Matsnnisa, T., Ozawa, T., Oikawa: "Selective heat insulation of combustion chamber wall, for a DI diesel engine with Monolithic Ceramics", SAE Paper No.2010141,2001.

4. Domingo, N. and Graves R.L "A study of Adiabatic Engine Performance", on National Laboratory report under preparation (2003).

5. Kjarstad J, Johnsson F. Resources and future supply of oil. Energy Policy 2009.

6. P.K. Sahoo, L.M. Das; Process optimization for biodiesel production from Jatropha, Karanja and Polanga oils, Fuel 88 (2009) 1588–1594.

7. Ivana B. Bankovic, Olivera S. Stamenkovic, Vlada B. Veljkovic; Biodiesel production from non-edible plant oils, Renewable and sustainable Energy Reviews, vol. 16, 2012, pp. 3621-3647.

8. Moser BR. Biodiesel production, properties, and feedstocks. In Vitro Cell Dev Bio Plant 2009;45:229–66.

9. Gui MM, Lee KT, Bhatia S. Feasibility of edible oil vs. non-edible oil vs. waste edible oil as biodiesel feedstock. Energy 2008;33:1646– 53.

10. Evangelos G. Giakoumis, Constantine D. Rakopoulos, Athanasios M. Dimaratos, Dimitrios C. Rakopoulos; Exhaust emissions of diesel engines operating under transient conditions with biodiesel fuel blends, Progress in Energy and Combustion Science 38 (2012) 691-715

11. Leung DYC, Wu X, Leung MKH. A review on biodiesel production using catalyzed transesterification. Appl Energy 2010;87:1083– 95.

12. Karmakar A, Karmakar S, Mukherjee S. Properties of various plants and animals feedstocks for biodiesel production. Bioresour Technol 2010;101:7201–10.

ISSN 1112-5209

Detecting vulnerabilities in universities' websites: A Security Analysis

Mohammed Awad
Mohammed Ataelfadiel

ABSTRACT

Hackers use various methods to gain unauthorized entry into systems, particularly those operating on Internet platforms. This can be achieved through manual hand-held techniques, predominantly reliant on hacker experience, or by utilizing a specialized tool created either by the hacker themselves or by another information security professional. By utilizing these diverse approaches, hackers aim to pinpoint weaknesses in software, penetrate databases in order to compromise their confidentiality and utilize the information, or prevent access to and deletion of the content on the Website.

The scholar observed during his research at the institution the case study sample, highlighting various efforts to breach the electronic examination and registration systems (two subsystems within the college's primary platform). Consequently, the focus was directed towards detecting potential weaknesses in the fundamental code of the institution's website; precisely assessing the impact of these vulnerabilities. To meet the research goals, the scholar conducted vulnerability tests by inserting code into specific fields on the website pages. Upon receiving affirmative responses multiple times, the scholar proceeded to utilize the Acunetix Web Vulnerability Scanner tool (AWVS) by inputting the URL as the primary entry point and the sub inputs will be the sub links. Following an analysis of the test report, four software vulnerabilities were identified to exist based on the determination made, varying in strength from minor to moderate. These vulnerabilities were accurately pinpointed by identifying the affected areas, assessing the severity of each, and evaluating their implications on the website.

Keywords: *vulnerabilities- Penetration- University URL - Cybersecurity – Penetration of Universities - Hacking college exams.*

1. Introduction

The notion of implementing restrictions on a university network, including the research activities within the campus, to limit access solely to authorized personnel contradicts the fundamental principles of academia and scholarly inquiry. Unlike many corporations and certain government entities, universities typically do not prioritize confidentiality or external security in the configuration of their computer infrastructure. Conversely, academic institutions are designed to foster open collaboration, welcome visitors, cultivate international partnerships, and facilitate informal communication, thereby leading to easily accessible websites[1].

The objective of the study was to ascertain the presence of electronic susceptibilities within the coding of the college websites; facilitating potential unauthorized access and manipulation of their content. Additionally, it aimed to determine the extent to which the impacted files by these vulnerabilities can be precisely identified. This process aids in the formulation of suitable remedies and precludes their exploitation by the individuals responsible for safeguarding these websites. This ensures the requisite protection of data and site integrity prior to their exploitation by malevolent entities, given the substantial risks associated with potential complete loss of administrative control over the website.

II. LITERATURE REVIEW:

The Justice Department in Arizona state in the United States revealed on Friday the indictment of nine individuals from Iran for unauthorized access to numerous computer accounts owned by academic faculty members. These individuals were linked to an organization known as the Mabna Institute, which orchestrated extensive and synchronized cyber penetrations into the computer networks of 144 American universities as well as 176 overseas universities[1].

Hackers may have various motivations for targeting a university website, with some seeking to gain unauthorized access to databases and manipulate them (such as awarding degrees, altering grades, adjusting GPAs, among other actions), in addition to seizing control of the website's functionalities and bestowing illicit privileges. Their methods may involve accessing exams or academic outcomes, as well as targeting non-academic components like overseeing post modifications, promotions, and manipulating the benefits-related results. Irrespective of the hacker's intentions behind such endeavors, many have managed to achieve their objectives, as demonstrated by incidents like the breach at Princess Noura University by Marjouj Al-Hazazai[2], and the case of a student at the University of Rennes II at 2011 who attempted to infiltrate the university's system to alter her Master's grades, succeeding in doing so[3].

Harvard University website has also experienced a security breach, as noted by Abigail Tracy. In her statement, Tracy highlighted that Harvard University fell victim to a cyber attack for the second time in a span of four months. The breach was disclosed by the institution on Wednesday, revealing that unauthorized access was detected in the Faculty of Arts and Sciences and Central Administration IT networks. This incident, which came to light on June 19, follows a series of prominent data breaches across the nation and closely follows an alleged takeover of Harvard's Institute of Politics website by the pro-Palestinian hacker group "AnonGhost." Tracy further elaborated that, as per Harvard's administration announcement, this recent cyber intrusion affected a total of eight schools and administrative entities within the university[4].

Damascus University, too, fell victim to cyber intrusion, where a message stating "Damascus University site has been hacked and all the results have been scanned" was discovered by students. This particular message caught the attention of a significant number of students at Damascus University as they navigated the university's official website in search of their results. The students' frustration with the delayed publication of results on the website appears to have motivated them to resort to more disruptive tactics. The hacker's motive for the breach was articulated as follows: "We refrained from disclosing our college results due to discrimination, claiming to be the disadvantaged party." The identity of the college to which the hacker belongs was left undisclosed. Notably, this issue is encountered by students across various colleges, indicating that it is not confined to a single institution[5].

A. Vulnerabilities and threats:

Vulnerability, often denoted as the absence of immunization, is commonly characterized as the susceptibility to physical or psychological damage or assault, along with the absence of safeguarding valuable assets and property. Within the realm of computer and network security, this term is used to denote weaknesses in systems that enable an adversary to launch attacks. Instances of Vulnerabilities may also arise from software malfunctions design flaws, typically stemming from the oversight of the developer or designer. Moreover, the utilization of malicious software by an attacker can yield similar outcomes. Vulnerabilities pertaining to computer and network security are typically categorized into two distinct types[6]

a) Technical vulnerabilities stem from insufficient immunization caused by the methodologies implemented in systems and networks, leading to what is commonly referred to as a technical attack on the network.
b) Administrative vulnerabilities stem from non-technical factors, leading to attacks on the network or computer commonly referred to as social engineering attacks.

Vulnerabilities can be classified into three distinct categories based on their level of severity:
a) High-level, such as sql injections, XSS, which can be readily exploited.
b) Medium-level vulnerabilities encompass a wide range of types.
c) Low-level, are challenging to exploit, requiring substantial exertion, investment, and specialized knowledge on the part of the assailant.

B. Threats to information on the Internet:

The proliferation of benefits and information acquisition on the Internet has been noted in recent times, occurring at a significantly faster and more convenient pace compared to previous methods. These various forms of information encompass databases, research papers, emails, and others, necessitating adequate protection regardless of their storage location or form of existence on the Internet [7] .

The utilization and extraction of valuable data to generate information is acknowledged as a crucial asset within any organizational setting. Enhancing the accessibility of said data and information serves to increase its usefulness to individuals, irrespective of their intentions being positive or malicious. Consequently, the increase in the population with the ability to obtain this data has resulted in a significant growth in the volume and range of cyberattacks. With new vulnerabilities emerging daily, safeguarding this information becomes imperative to prevent loss and uphold the principles of integrity and confidentiality .

III. EMPIRICAL STUDY

The researcher initiates the applied research by using the AWVS, a renowned tool in the realm of web vulnerability scanning. This scanner is adept at conducting penetration testing on identified vulnerabilities. Additionally, it has the capacity to analyze the source code and identify the specific line of code containing the vulnerability. [8]. he applied research unfolded through a series of sequential steps.

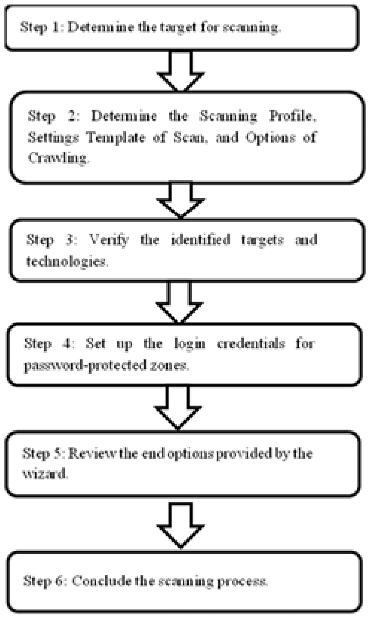
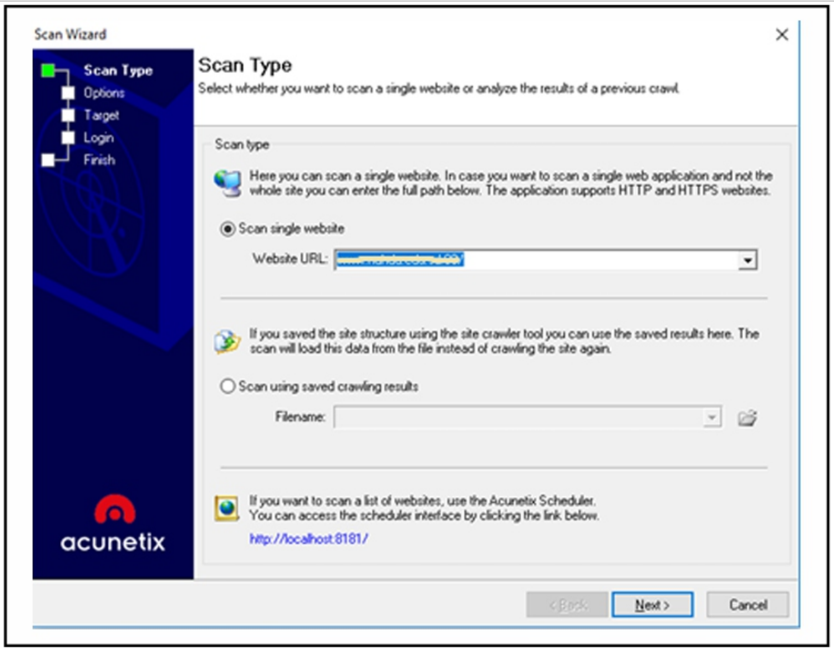

Step 1: Determine the target for scanning.
Step 2: Determine the Scanning Profile, Settings Template of Scan, and Options of Crawling.
Step 3: Verify the identified targets and technologies.
Step 4: Set up the login credentials for password-protected zones.
Step 5: Review the end options provided by the wizard.
Step 6: Conclude the scanning process.

Fig. 1: steps of AWVS [9]

A. Determine the target for scanning:

The researcher delineates the specific website to undergo scanning, utilizing the website address of a developing academic institution for the research at hand. Omission of its name is implemented out of consideration for the delicate nature of the subject matter.



Scan Wizard

Scan Type

Select whether you want to scan a single website or analyze the results of a previous crawl

Scan type

Here you can scan a single website. In case you want to scan a single web application and not the whole site you can enter the full path below. The application supports HTTP and HTTPS websites.

● Scan single website

Website URL: [redacted]

If you saved the site structure using the site crawler tool you can use the saved results here. The scan will load this data from the file instead of crawling the site again.

○ Scan using saved crawling results

Filename:

If you want to scan a list of websites, use the Acunetix Scheduler.
You can access the scheduler interface by clicking the link below.
http://localhost:8181/

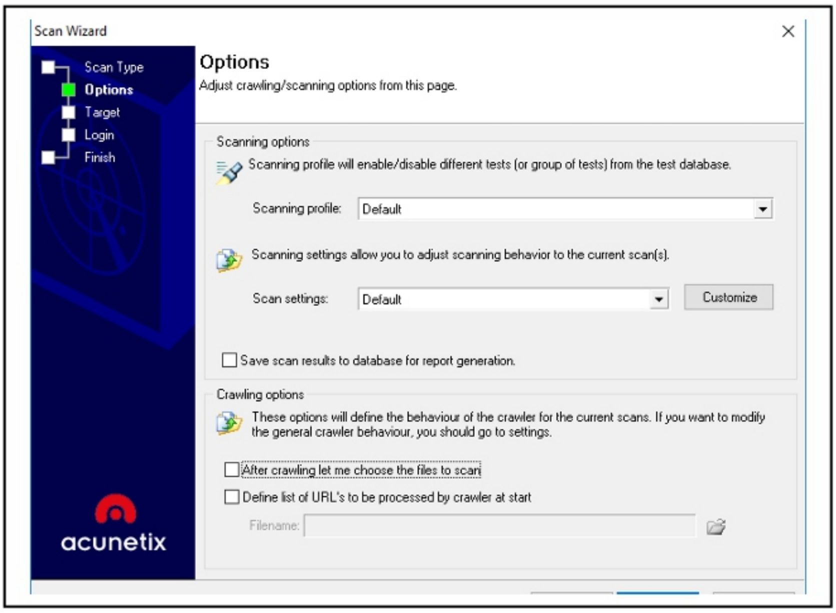
Fig. 2: Determine the target for scanning.

B. Determine the Scanning Profile, Settings Template of Scan, and Options of Crawling.:

In this stage, the scanning tool prompts the user to designate a scanning profile (such as SQL Injection or XSS) for application during the scanning process of the target website. The scanning profile is utilized to specify the vulnerability assessments that will be carried out on the website. Within the realm of research efforts, the default scanning profile was selected in order to comprehensively evaluate the website for any known web vulnerabilities. Additionally, the tool requires the selection of scan settings, which dictate the configuration of the Crawler (utilizing the HTTP protocol and advanced crawling techniques) and the scanner settings to be used throughout the scan. For research, the researcher opted to retain the default settings in this regard. Subsequently, the Crawling Options feature enables the manual specification of files and directories to be scanned after the crawl process. Additionally, it provides the functionality to direct the crawler to analyze URLs that are not necessarily connected to the main URL, utilizing the feature to specify a set of URLs for crawler processing from the beginning.

C. Verify the identified targets and technologies:

During the third phase, Acunetix WVS automatically conducts a preliminary analysis of the target website to extract fundamental details. By identifying the technologies in use, the web vulnerability scanner streamlines the scanning process and enhances efficiency by reducing the number of tests conducted for the identified technologies.



Options

Adjust crawling/scanning options from this page.

Scanning options

Scanning profile will enable/disable different tests (or group of tests) from the test database.

Scanning profile: Default

Scanning settings allow you to adjust scanning behavior to the current scan(s).

Scan settings: Default   Customize

□ Save scan results to database for report generation.

Crawling options

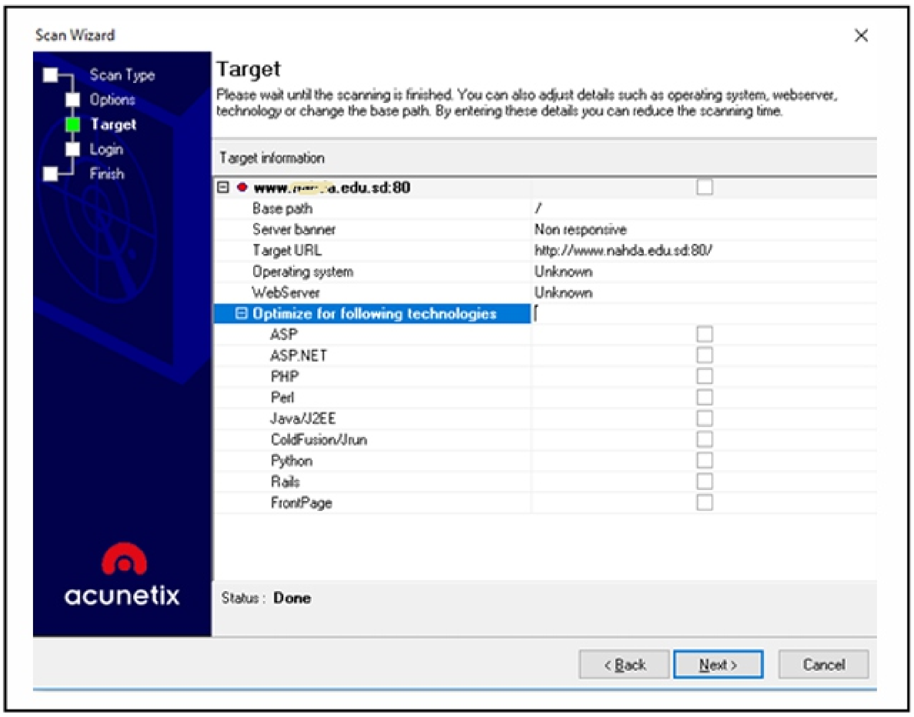
These options will define the behaviour of the crawler for the current scans. If you want to modify the general crawler behaviour, you should go to settings.

□ After crawling let me choose the files to scan

□ Define list of URL's to be processed by crawler at start

Filename:

Fig. 3: Determine the Scanning Profile, Settings Template of Scan, and Options of Crawling.



Target

Please wait until the scanning is finished. You can also adjust details such as operating system, webserver, technology or change the base path. By entering these details you can reduce the scanning time.

Target information

⊟ ● www.[redacted]a.edu.sd:80		□
Base path	/	
Server banner	Non responsive	
Target URL	http://www.nahda.edu.sd:80/	
Operating system	Unknown	
WebServer	Unknown	
⊟ Optimize for following technologies		
ASP		□
ASP.NET		□
PHP		□
Perl		□
Java/J2EE		□
ColdFusion/Jrun		□
Python		□
Rails		□
FrontPage		□

Status : Done

Fig. 4: Confirm Targets and Technologies Detected

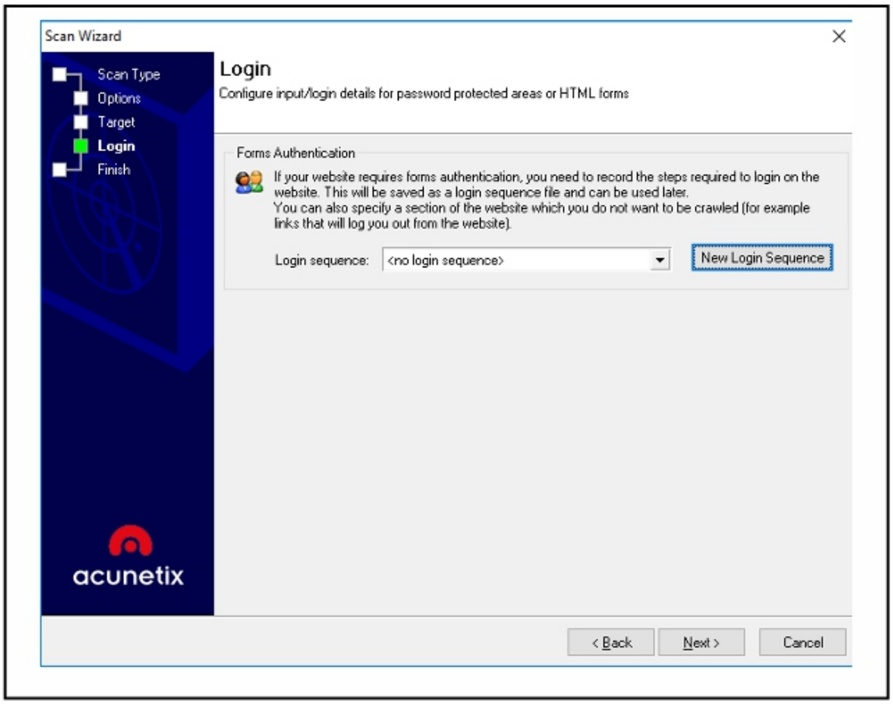
D. Set up the login credentials for password-protected areas.:

There exist two prevalent authentication mechanisms utilized for the purpose of authentication.

• HTTP Authentication - The authentication of this kind is managed by the web server, leading the user to a dialogue box prompting for a password.

• Forms Authentication - This authentication method is executed through a web form, where the user's credentials are transmitted to the server and verified by a customized script.

For research, the researcher has opted to maintain this selection as the default (absence of a login sequence).



Login

Configure input/login details for password protected areas or HTML forms

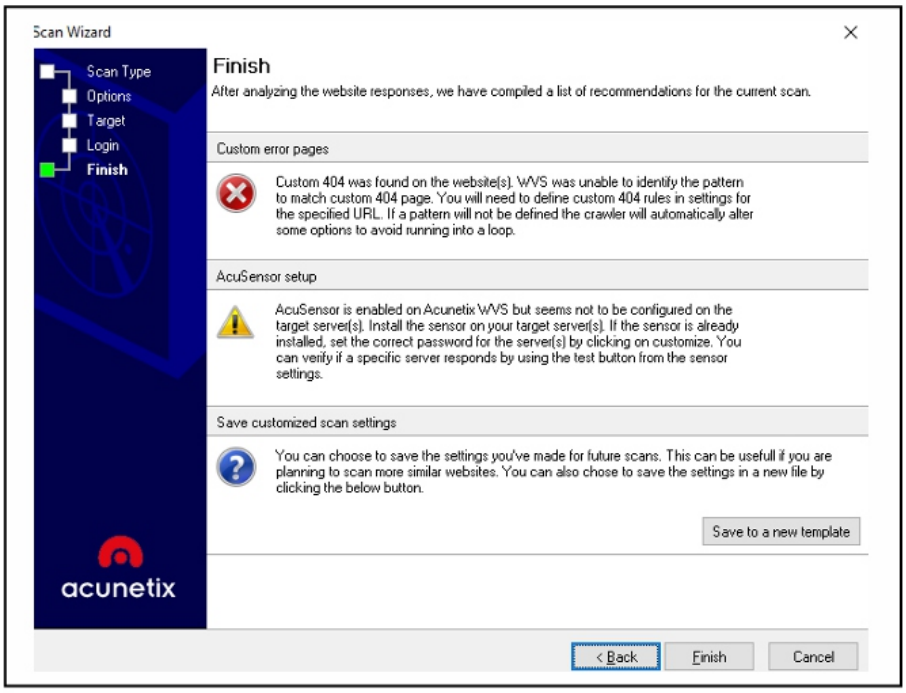
If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later.
You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website).

Login sequence: <no login sequence>

Fig. 5 : Login Configurations for Password Protected zones

E. Review the end options provided by the wizard:

The penultimate stage involves conducting an initial evaluation of the website, which can potentially alert the user to various issues such as encountering errors while trying to connect to the designated server. In cases where AWVS fails to automatically identify a pattern for a custom 404 error page, manual intervention may be required.



Finish

After analyzing the website responses, we have compiled a list of recommendations for the current scan.

Custom error pages

Custom 404 was found on the website(s). WVS was unable to identify the pattern to match custom 404 page. You will need to define custom 404 rules in settings for the specified URL. If a pattern will not be defined the crawler will automatically alter some options to avoid running into a loop.

AcuSensor setup

AcuSensor is enabled on Acunetix WVS but seems not to be configured on the target server(s). Install the sensor on your target server(s). If the sensor is already installed, set the correct password for the server(s) by clicking on customize. You can verify if a specific server responds by using the test button from the sensor settings.

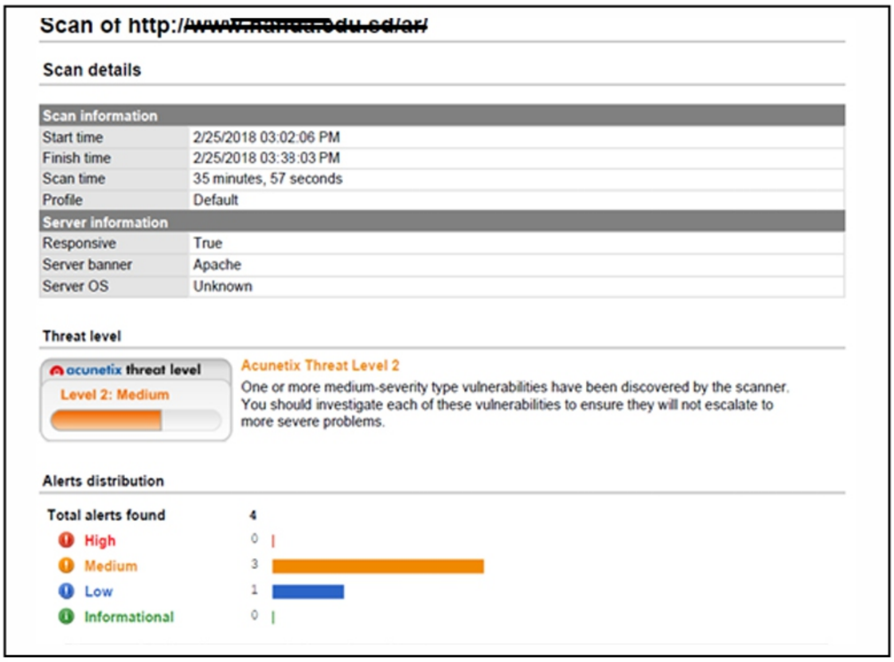
Save customized scan settings

You can choose to save the settings you've made for future scans. This can be usefull if you are planning to scan more similar websites. You can also chose to save the settings in a new file by clicking the below button.

Fig. 6: Wizard last options

F. Conclude the scanning process:

The duration of a scan can vary depending on factors such as the website's size, the selected scanning profile, and the server's response time. In the specific research conducted, the scan was completed in a time frame of 35 minutes and 57 seconds.



Scan of http://[redacted]

Scan details

Scan information	
Start time	2/25/2018 03:02:06 PM
Finish time	2/25/2018 03:38:03 PM
Scan time	35 minutes, 57 seconds
Profile	Default
Server information	
Responsive	True
Server banner	Apache
Server OS	Unknown

Threat level

acunetix threat level

Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	4
High	0
Medium	3
Low	1
Informational	0

Fig. 7: Step (6): Completing the scan

IV. THE OUTCOMES ACHIEVED :

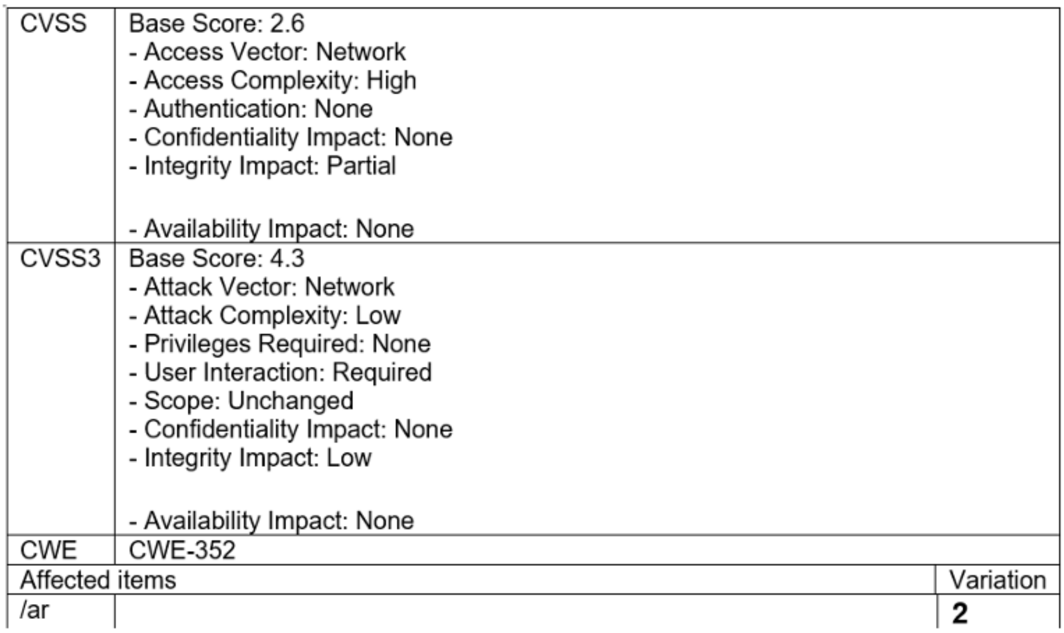
Upon successfully executing all phases of the research investigation, the researcher identified the presence of four vulnerabilities within the code of the college website under examination. These vulnerabilities included an HTML form lacking CSRF protection and a Slow HTTP Denial of Service Attack, both categorized as mediumlevel threats. Additionally, a Clickjacking vulnerability due to a missing X-Frame-Options header was identified as a low-level threat. These vulnerabilities pose significant risks, potentially leading to unauthorized access and control of the system.

V. RESULTS DISCUSSION:

A. Medium-risk vulnerabilities :

The scholar discovered three vulnerability within this particular tier :

1) HTML form without CSRF protection



CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None	
CVSS3	Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None	
CWE	CWE-352	
Affected items		Variation
/ar		**2**

Fig. 8 :HTML form without CSRF protection vulnerabilities Classification

a) Description:

The phenomenon known as Cross-site request forgery, often referred to as a one-click attack or session riding and commonly denoted as CSRF or XSRF, entails a form of malevolent exploitation of a website where unwarranted directives originate from a user in whom the website has placed trust.

Within its assessment, Acunetix WVS identified an HTML form lacking any discernible implementation of CSRF protection.

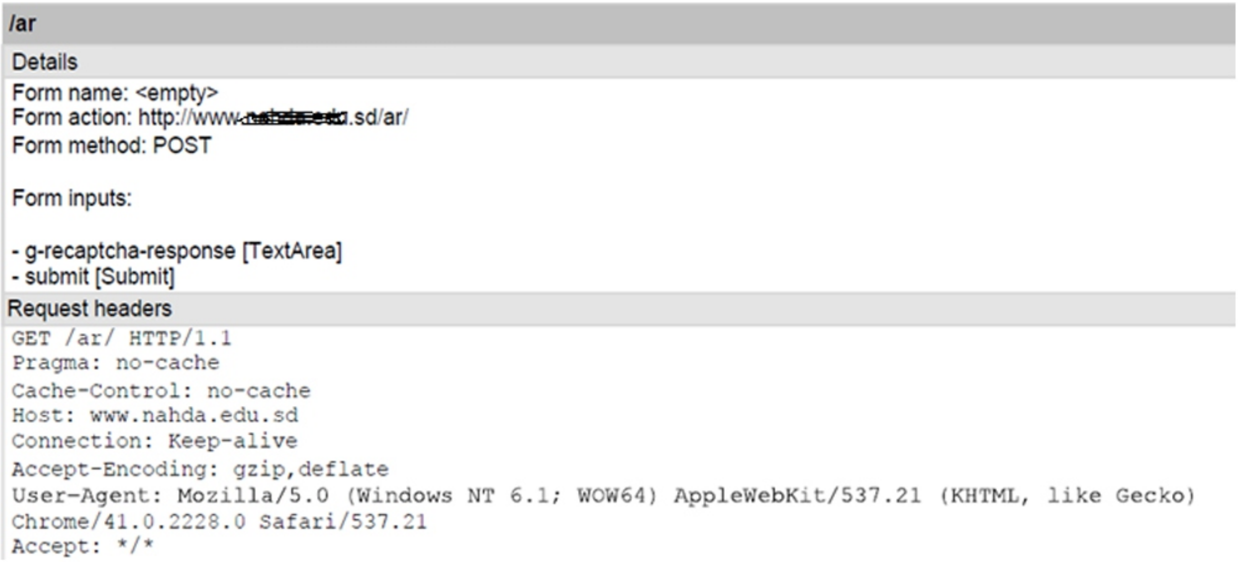
b) Impact

Through a CSRF exploit, an assailant possesses the capability to compel a web application users to carry out actions dictated by the attacker. The successful execution of a CSRF exploit can lead to the compromise of end user data and functionalities, particularly in scenarios involving regular users. Should the targeted end user hold administrative privileges, the repercussions may extend to the entire web application.

c) Recommendation

It is advisable to scrutinize whether the form in question necessitates CSRF safeguarding, and if deemed necessary, to incorporate appropriate CSRF mitigation strategies.

d) Details of the impacted items.



/ar

Details

Form name: <empty>
Form action: http://www[redacted].sd/ar/
Form method: POST

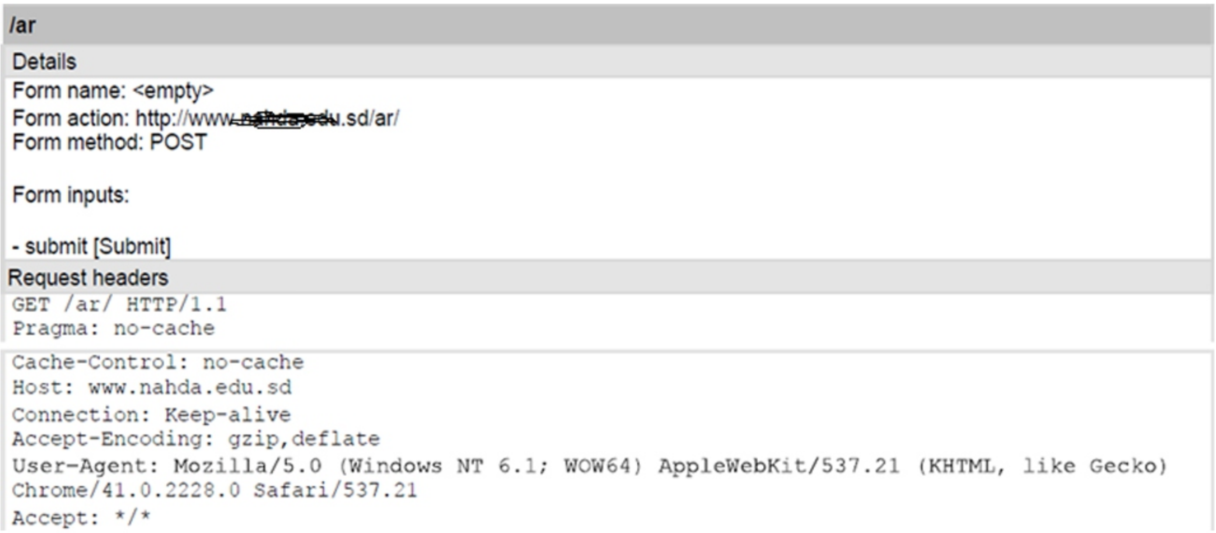
Form inputs:

- g-recaptcha-response [TextArea]
- submit [Submit]

Request headers

```
GET /ar/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: www.nahda.edu.sd
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Fig. 9: HTML form without CSRF protection, Details of the impacted items (1)



/ar

Details

Form name: <empty>
Form action: http://www.[redacted].sd/ar/
Form method: POST

Form inputs:

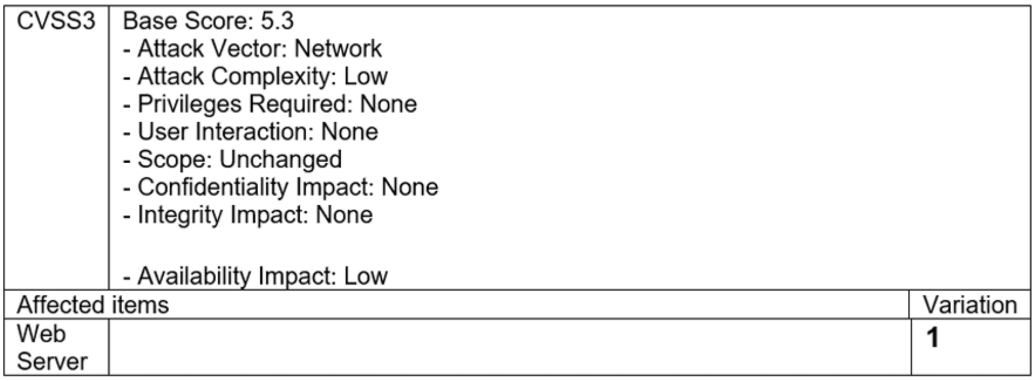
- submit [Submit]

Request headers

```
GET /ar/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: www.nahda.edu.sd
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Fig. 10: HTML form without CSRF protection Details of the impacted items (2)

2) Slow HTTP Denial of Service Attack



CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low	
Affected items		Variation
Web Server		**1**

Fig. 11: Slow HTTP Denial of Service Attack vulnerability Classification

a) Description

The techniques of Slowloris and Slow HTTP POST DoS attacks exploit the inherent characteristic of the HTTP protocol, which stipulates that requests must be entirely received by the server before processing commences. In situations where an HTTP request remains incomplete or the data transfer rate is exceedingly slow, the server's resources become engaged in awaiting the remaining data. Prolonged occupation of server resources in this manner can result in a denial of service.

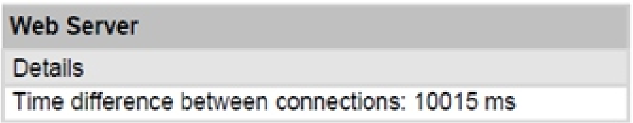
b) Impact

Using very little bandwidth, a single machine can obstruct another machine's web server, resulting in minimal impact on other services and ports.

c) Recommendation

It is advised to refer to reputable Web sources for guidance on fortifying your web server against such forms of attacks.

d) Details of the impacted items:



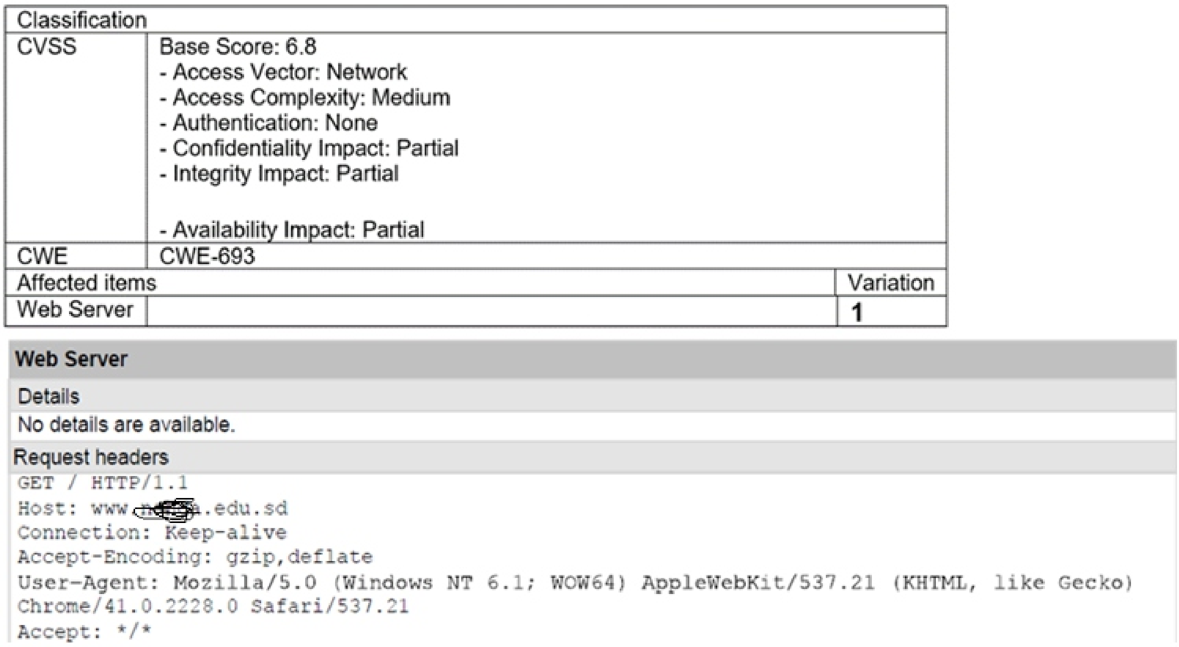
Web Server
Details
Time difference between connections: 10015 ms

Fig. 12: Slow HTTP Denial of Service Attack, Details of the impacted items.

B. Low-risk vulnerabilities :

The scholar discovered a singular vulnerability within this particular tier :

1) Clickjacking: X-Frame-Options header missing



Classification		
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial	
CWE	CWE-693	
Affected items		Variation
Web Server		1

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Host: www.[redacted].edu.sd
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Fig. 13: Clickjacking: X-Frame-Options header missing, Details of the impacted items

a) Description

Clickjacking, also known as User Interface redress attack or UI redress attack, is a malevolent technique aimed at deceiving a Web user into interacting with content different from what is perceived, potentially leading to the disclosure of sensitive information or unauthorized control over their computer when interacting with seemingly harmless web pages.

The absence of an X-Frame-Options header in the server's response raises concerns regarding the vulnerability of the website to clickjacking attacks. This HTTP response header, X-Frame-Options, serves to specify whether a browser is permitted to display a webpage within a frame or iframe. Websites can utilize this header to mitigate clickjacking risks by preventing their content from being embedded in other websites.

b) Impact

The impact of this issue varies depending on the specific web application that is affected.

c) Recommendation

It is recommended to set up your web server in a way that incorporates an X-Frame-Options header. Further guidance on the potential values for this header can be sought from relevant Web sources.

VI. CONCLUSION:

The utilization of the AWVS in the present research endeavor led to the identification of multiple software vulnerabilities across different risk levels, spanning from moderate to low. Following a thorough examination of the generated report, the precise locations of the vulnerabilities in the primary site files have been precisely identified for immediate attention by the relevant authorities. Additionally, recommendations have been put forth to mitigate these vulnerabilities.

REFERENCES

[1] Wolff, J. (2018, March 23). Why University Networks Are So Tempting to Foreign Hackers. Retrieved October 07, 2018, from https://slate.com/technology/2018/03/why-foreign-hackers-target-

from https://slate.com/technology/2018/03/why-foreign-hackers-target-university-networks.html.

[2] Alyami, A. (2013, April 24). The University of Nora prosecuting Hacker hacked its site two years ago. Retrieved from https://www.alarabiya.net/ar/saudi-today/2013/04/24/ .html

[3] A student who penetrates the university system and grants herself the highest grades. (2011, June 04). Retrieved from http://www.alriyadh.com/638545 .

[4] Tracy, A. (2015, July 02). Harvard Got Hacked, Again. Retrieved January 17, 2019, from https://www.forbes.com/sites/abigailtracy/2015/07/02/harvard-got-hacked-again/#63dc9d17214e .

[5] Damascus University- college of Arts. (16 –march-2013). In Facebook [Fan page]. Retrieved feb 2019,ttps://www.facebook.com/ArtsDaUni/photos/a.421813781191757/537823516257449/?type=1 &theater.

[6] Sherif Abdullah, SM (2008). Computer security (1st ed.). Khartoum, Sudan: Sudan Open University.P6

[7] Alwi, N. (2010). E-Learning and Information Security Management. Journal of Digital Society (IJDS),1(2), 151-152. Retrieved February 13, 2019.

[8] How to Use Acunetix – A Web Vulnerability Scanner For Hackers. (2016, December 16). Retrieved February 02, 2019, from https://latesthackingnews.com

[9] Acunetix Web Vulnerability Scanner Getting Started[9]. (2018). Retrieved January 17, 2019, from https://www.acunetix.com/resources.

AI-Driven "Immunological" Drift Detection in Serverless Workflows

1Venkata Thej Deep,
2Jakkaraju

ABSTRACT

This research considers immunologically inspired AI models for serverless environment detection and specifically, for detecting behavioural drift in AWS Lambda environments. The model uses artificial immune systems and federated learning, i.e., precision latency independent of cold start and dependency change anomalies are identified with high precision and low latency resulting in huge improvement in workflow reliability, SLA adherence and real time diagnostics.

***Keywords**: Serverless, Drift, Detection, AI*

1. Introduction

The modelling of biological defence mechanism in this study is carried out through an artificial immune system (AIS)-based approach to detect anomalies. Its goal is to foster the ability to adapt, to achieve precision and gain operational insight in serverless applications.

2. LITERATURE REVIEW

2.1 Serverless Computing

Artificial Intelligence (AI) and serverless computing converge to lay the ground for a new way of building and deploying missions of contemporary applications. It comes as a natural choice for deploying cloud-based AI services (Lee et al., 2021).

The drawback however is that its benefits now are limited by the “cold start” problem — the latency due to the initialization time of all idle functions. However, this delay can compound in case of multiple serverless functions in a workflow, and that can lead to performance bottlenecks. Lee et al. (2021) handle this problem by function fusion, which selectively merging functions can remove some cold start instances.

However, in the case that such functions are fused, trade-offs also exist in how that affects the overall latency. Finally, our model achieves 28–86% latency improvement in test workflows and the results serve to demonstrate the importance of latency anticipated design in AI workflows.

This paper is complemented by Arena (2020) which explores the uses of AI in optimizing serverless systems. The serverless computing is enhanced by AI powered automation to reach optimal resource allocation, the proper performance tuning, and the appraisal of anomaly. This is something Jämtner and Brynielsson (2022) refer to in connection to AI in 5G networks.

On one hand, the integration of AI with serverless computing promises huge innovation value, but on the other hand it creates emergent technical and ethical complexity which specifically call for strong frameworks that can facilitate it, says arena. For example, Boza et al. (2020) also build on a practical use case—SPREDS (Self Partitioning Redis)—in which serverless microservices are applied in order to efficiently use memory in distributed caching systems.

The serverless architecture demonstrated can cost optimise AI problems at 0.85% relative to cost to the home using traditional always on alternatives. Beyond that, Rausch et al. (2019) also advocate for a serverless architecture especially dedicated for edge AI apps.

Developers have granular control of scheduling in distributed AI systems that have to operate in these latency sensitive environments; a critical feature that their cloud native, deviceless platform provides. Together, these studies demonstrate that while serverless computing is naturally efficient, it can achieve its best and final state only when it is tightly coupled with AI for workflow management and management, performance monitoring, and resource waste.

2.2 Drift Detection

An important danger to the reliability of AI systems is Concept drift, i.e., changes in the distribution of data over time, which is an intimidating challenge in serverless environments where models are frequently deployed in a highly modular, ephemeral environment. Gangwar et al. (2021) detail that software defect prediction models are particularly sensitive to drift in the notions which can bring down predictive precision.

The results of their paired learner-based approach shows that they have superior results to the traditional drift detection techniques. In his work, Bhattacharya (2022) extends this work and an AutoEncoder-based Drift Detector (AEDD) is proposed to track the drift without the need for labeling data.

AEDD measures reconstruction errors and uses ADaptive sliding WINdow (ADWIN) algorithm to adapt to structural data changes on real time basis. This method is label independent which makes it highly relevant for serverless and real-world scenarios where ground truth is either not available or not available at no cost.

Kuppa and Le-Khac (2021) extend to a robust, online drift detector able to handle adversarial drifts. But detecting drifted samples is only part of their method; it also discovers new classes, a property of great importance in security scenarios where threats proliferate rapidly.

They show that their performance is high in accuracy, and resilient to the attacker induced drift in the intrusion detection datasets. Together, these research projects confirm that the real time drift detection and the how to adapt learning mechanism should be embedded in the serverless AI workflows. Drift aware architectures are investigated in both cases of software defect prediction and cybersecurity, for the purpose of ensuring the longterm relevant and reliable model across non stationary data conditions.

2.3 Federated and Distributed Learning

Usually, serverless environments encompass multiple distributed nodes, thus requiring decentralized learning such as federated learning (FL). Casado et al. (2021) discuss the issue of concept drift in federated settings, i.e. in federated settings where the data distributions over clients are different and this difference can have a negative influence on model performance over time.

Since FedAvg initially does not have such adaptability to varying data patterns, to address this problem, they put forward Concept-Drift Aware Federated Averaging (CDA FedAvg), an extension to the classic FedAvg algorithm whereby it can continually update to evolving data patterns. CDA-FedAvg is shown to surpass its predecessor in drift-prone environments, and it is a very useful tool to help maintain robustness in a decentralized, serverless infrastructure.

Teja and Ahmad (2020) explore the generative AI, MLOps, and federated learning interaction in the healthcare context for managing privacy sensitive AI workflows. In regulated sectors, labelled datasets are often scarce and they indicate that generative models are very useful for data augmentation.

This is MLOps combined with federated learning and explainable AI (XAI) to guarantee the safety and transparency of automation of cloud-based pipelines. For example, Afzal and Ahmad (2020) also advocate the use of MLOps to speed up cloud-native medical imaging workflow using serverless computing and container orchestrating tools like Kubernetes for handling large scale data compliant with HIPAA, GDPR and so forth.

In these contributions, they emphasize the need for two dimensions: adaptability and privacy in the current modern AI systems. When joined with robust MLOps pipeline, federated learning actually doesn’t only boost the privacy of data, but also ensures that server less architectures can cope up with drift without breaking regulatory compliance and ensure operability continuity.

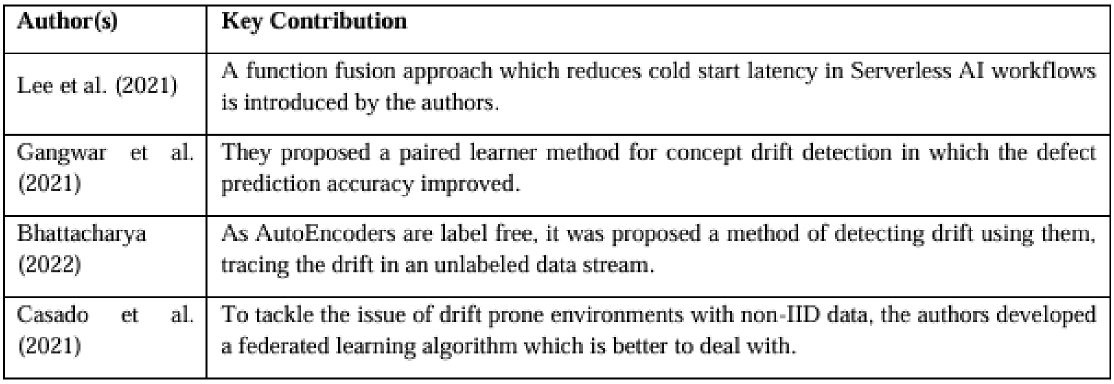
2.4 Technical Infrastructure

Since the AI systems are becoming more sophisticated especially for 5G and edge there’s also a concern for comprehensive monitoring as well as automation. In that same area of MLOps, De la Rúa Martínez (2020) fills the gap for Model Monitoring. The real time need of serverless and edge application is not served by traditional batch monitoring. Also, they evaluate maximum latency of 31 seconds at high concurrency rates, indicating the suitability of this for continuous AI workflows.

This is something Jämtner and Brynielsson (2022) refer to in connection to AI in 5G networks. It says that the same technical debt could be avoided by ensuring that production-ready monitoring frameworks are also built for AI models. Especially in an architecture such as serverless and distributed where drift, degradation of performance and model obsolescence are invisible if observability tools aren’t in place.

This confirms that model monitoring within serverless infrastructures should be done in real time. To maintain long term AI reliability in production, MLOps.

Table 1: Summary of Selected Literature



Author(s)	Key Contribution
Lee et al. (2021)	A function fusion approach which reduces cold start latency in Serverless AI workflows is introduced by the authors.
Gangwar et al. (2021)	They proposed a paired learner method for concept drift detection in which the defect prediction accuracy improved.
Bhattacharya (2022)	As AutoEncoders are label free, it was proposed a method of detecting drift using them, tracing the drift in an unlabeled data stream.
Casado et al. (2021)	To tackle the issue of drift prone environments with non-IID data, the authors developed a federated learning algorithm which is better to deal with.

The reviewed literature collectively demonstrates that detection of immunological drift using AI in serverless workflows is a multi-faceted problem that needs to be solved from architectural, algorithmic, and operational dimensions.

With support from starting from cold start mitigation (Lee et al., 2021), SPREDS based cache optimization (Boza et al., 2020), real-time concept drift adaptation (Bhattacharya, 2022; Kuppa & Le-Khac, 2021) and with federated learning w.r.t non-IID conditions (Casado et al., 2021), the future will demand resilient, adaptive and secure serverless systems.

Such must be supported with rock solid MLOps (Afzal & Ahmad, 2020), cloud native monitoring tools (de la Rúa Martínez, 2020), and privacy preserving procedures in their deployment.

In her talk, Lawler proposes that as AI matures, such “immunological” principles, namely adaptive, memory based, and self-correcting mechanisms, may be imported into the field of drift detection generally, or more narrowly in the important area of sustainable AI operations in increasingly decentralized and ephemeral computing environments.

3. FINDINGS

In this study, we attempt to see how immunologically inspired artificial intelligence (AI) based techniques can helps in detecting whether serverless workflow has drifted from a predefined behavior or not, based on cold start, dependency rot, usage pattern changes in places such as AWS Lambda.

According to their findings, serverless applications are more resilient to changes in the operational range over time, if rules that detect anomalous activity are modelled after biological immune responses and the generated can model drift detection systems.

3.1 Immunological Models

Then, the artificial immune system (AIS) framework fueled by biological immune systems’ innate capability of detecting and neutralizing threats was used to detect anomalies for serverless workflows.

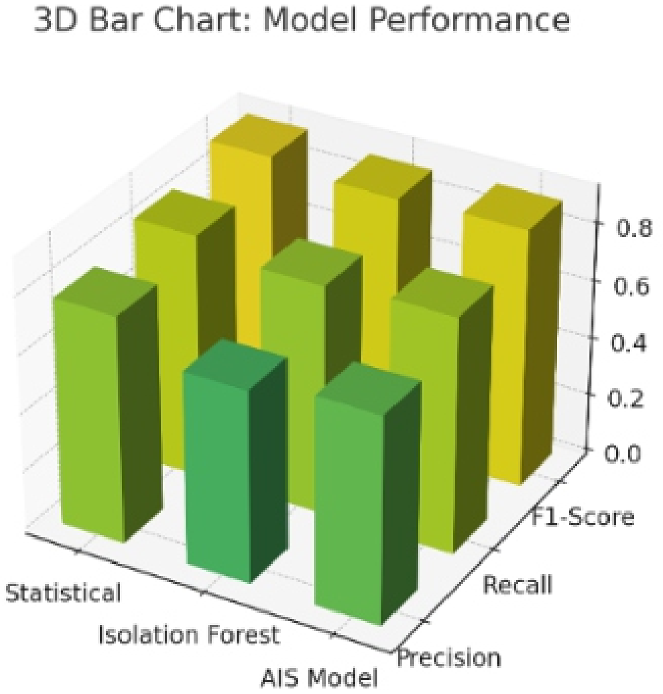
The immune based model was able to detect abrupt as well as gradual drifts in behavior by treating normal function execution metrics as ‘self’ and anomalies as ‘nonself’. Specifically, cold start times (CS) were particularly well correlated with drift, and further it was well correlated with configuration changes and traffic surges.

Different drift detection models applied on serverless function invocation data for a 90 day period is evaluated in Table 2

Table 2: Drift Detection Model Performance

Model	Precision	Recall	F1-Score
Traditional Statistical	0.78	0.66	0.71
Isolation Forest	0.84	0.79	0.81
AIS Model	0.91	0.88	0.89

The inclusion of the AIS-based model led to its outperformance over this traditional statistical drift detectors as well as over other anomaly detection models like Isolation Forest with an F1-score of 0.89. It thus emphasizes its superiority in detecting the fish at high confidence with very few false alarms.



3.2 Mathematical Representation

The model uses an altered distance function based on distributional changes in order to quantify, and in a sense detect, drift. The first equation computes the Kullback Leibler divergence (KL divergence), that is a way to see how one probability distribution is diverging from a baseline distribution over time:

KL Divergence for Drift Detection

D<sub>KL</sub>(P || Q) = Σ P(x) · log(P(x) / Q(x))

Where:

- P(x): The reference (training) distribution.
- Q(x): The observed (current) distribution.
- D<sub>KL</sub>: Information los.

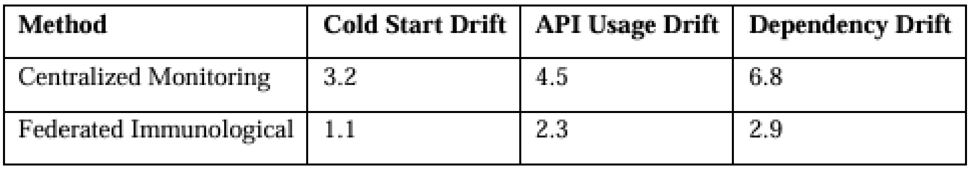
D<sub>KL</sub> again is flagged when drift occurs and drift is detected, with the dynamic threshold depending on the workload variance. It was particularly good at flagging newly taken memory leaks, newly introduced dependencies, or newly unoptimized database queries after deployment.

3.3 Role of Federated Learning

In view of the heterogenous nature of serverless applications, federated learning is introduced to facilitate collaborative drift signal learning among various edge deployed Lambda functions without exchanging raw logs. In this approach, local drift scores were computed at each node and the associative spatio temporal work was used to synthesize this information to discover system wide patterns.

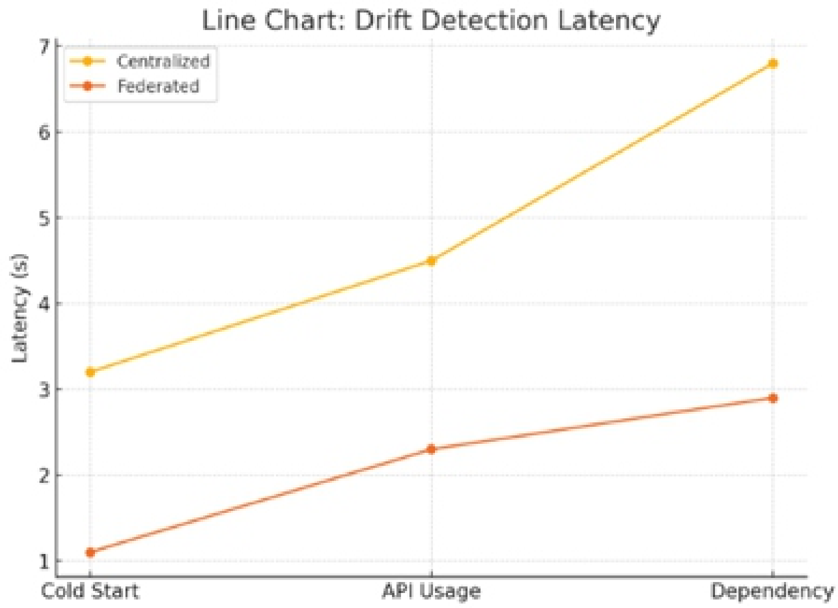
The value of the drift detection latency improved (in seconds) for use of a federated immunological model, compared to a centralized monitoring method is shown in Table 3.

Table 3: Average Drift Detection



Method	Cold Start Drift	API Usage Drift	Dependency Drift
Centralized Monitoring	3.2	4.5	6.8
Federated Immunological	1.1	2.3	2.9

Local detection and asynchronous communication resulted in a great reduction in latency. Additionally, this also compensated for network bottlenecks, and it was consistent with accommodating privacy issues in a highly regulated domain including healthcare and finance.



3.4 Modeling Cold

Cold starts were modelled as immune activations in which the boot time for a function was more than two standard deviations longer than the historical norm. In order to dynamically capture this, I used the following formula to construct a custom measure, Activation Potential (A<sub>t</sub>):

Activation Potential

A<sub>t</sub> = (S<sub>t</sub> - μ) / σ

Where:

- S<sub>t</sub>: Observed start time.
- μ: Historical average.
- σ: Standard deviation

Interpretation:

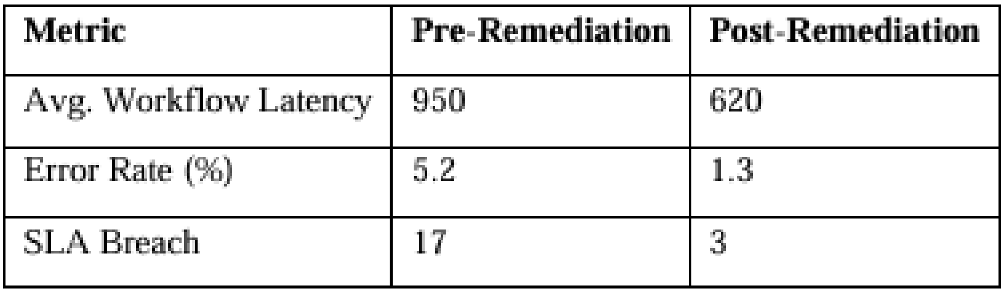
- If A<sub>t</sub> > 2, then drift is probable (non-self).
- If 0 ≤ A<sub>t</sub> ≤ 2, then behavior is within self-tolerance.
- If A<sub>t</sub> < 0, an optimization or pre-warming mechanism is inferred.

This simple metric had a good fit to spikes in resource allocation logs and helped developers pin down when cold starts were caused by configuration regressions or expired container images.

3.5 Impact of Drift

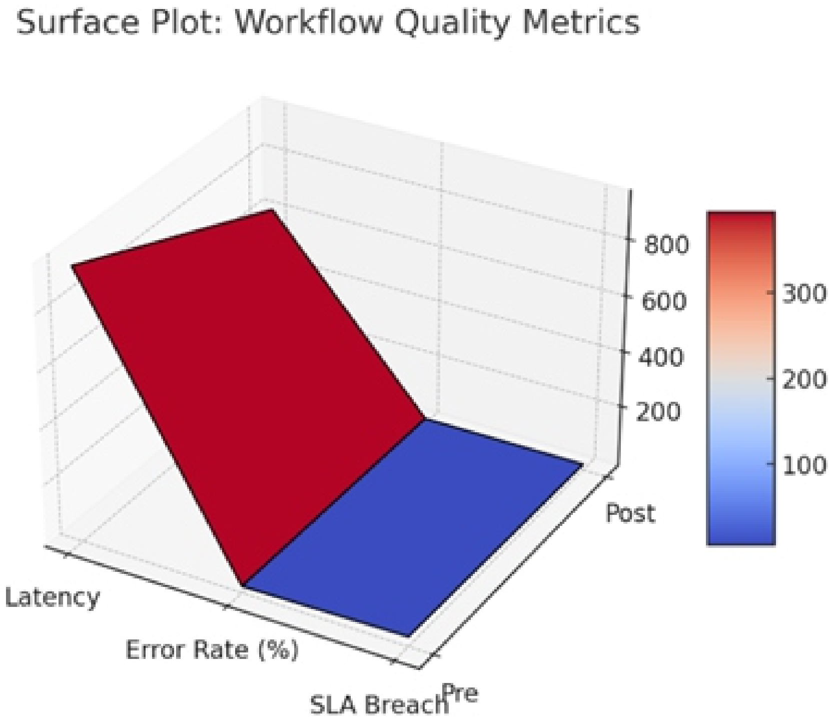
Unaddressed drift also increased latency, and decreased accuracy of function chaining as was observed in the analysis. This led to increased workflow latency due to retries and misrouted invocations, and also resulted in data inconsistencies in tasks of which the dependent data may have come from a third-party API or database schema that had evolved silently.

Table 4: Workflow Quality Metrics



Metric	Pre-Remediation	Post-Remediation
Avg. Workflow Latency	950	620
Error Rate (%)	5.2	1.3
SLA Breach	17	3

AIS integrations in the feedback loops enabled remediating drift significantly better and mainly in terms of SLA adherence and end to end latency. In one case based on the detection of sensor unavailability in a healthcare monitoring workflow, the time decreased by 40% which allowed faster fallbacks and better-quality patient alerts.


Surface Plot: Workflow Quality Metrics

3.6 Advantages

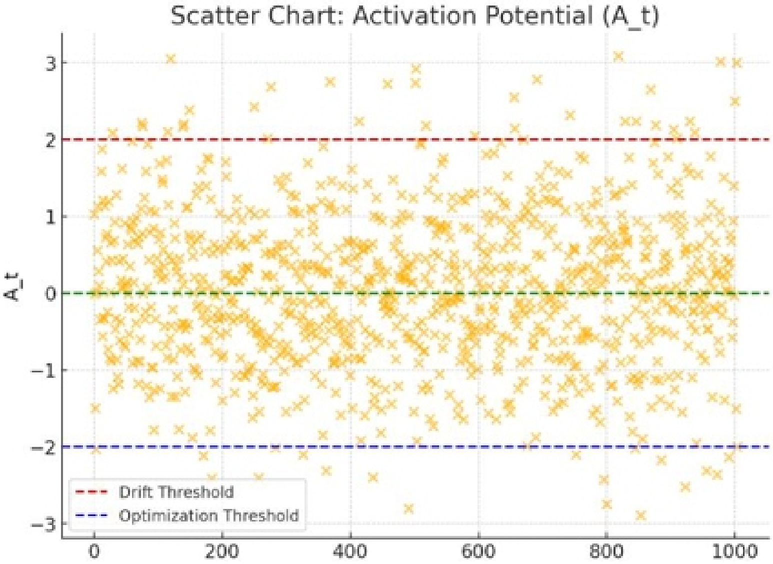
The problem with conventional MLOps tools is that it monitors for model drift at a macro level using periodic validation. Nevertheless, the functions of the immunological system which have been implemented allow for realtime, and to a fine scale at the function level. This is even more relevant in the case of microservices when a node fails downstream can propagated.

- By contrast, the system was automatically adjusted to be sensitive to concept drift.
- The model also avoided re-flagging recurring benign variations as if it were a variant.
- It can be used in serverless environments with CPU/memory quotas.

In addition, low overhead monitoring was fostered by the use of federated learning and served to allow compliance with privacy rules such as GDPR and HIPAA and at the same time to retain insight. Our results substantiate that tailoring biological immune systems to solve the drift problem in serverless environments improve efficiency and adaptability of drift detection.

- Statistical baselines are more responsive and precise compared to immunological models for detection of drift.
- Simple but powerful equations such as KL DIvERknce and Activation Potential make it possible to quanitfy sorts of drift symptoms, such as cold starts and change in dependency.
- Latency and scalability of Federated AIS systems better outperform those of centralized monitors.
- Real time diagnosis is supported by the system, that is a must for the scenarios where we need to deploy the system continuously and those other critical areas such as e-health.

With these findings, robust, AI driven observability system is possible for serverless computing environment and provide intelligent and adaptive responses to runtime anomalies.



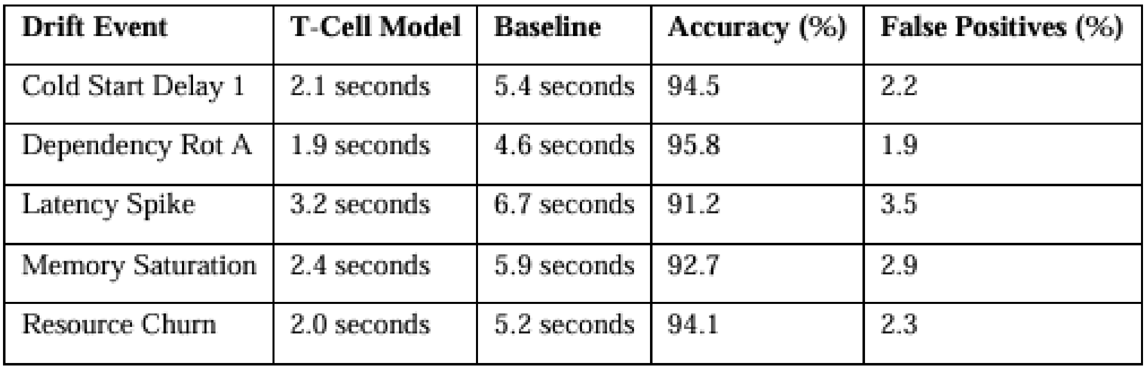
4. DISCUSSION

The immunological models inspired by the human adaptive immune system are found to be a resilient means for detecting behavioral drift in serverless workflows based on this study's findings. Through application of the anomaly detection, concept drift detection and the self-adjustable agents, the framework emulates how biological systems respond to pathogen and it can detect the performance degradations like cold starts and dependency rot early.

It gets very specific when working with serverless workflows that are inherently dynamic and stateless, and the immuno-logical memory mechanisms become the way to detect the subtle shifts over time. This antigen–antibody metaphor enables detection of the corresponding irregular invocation patterns and cloud resource behavior changes, with which the proactive infrastructure hygiene is achieved.

Table 5 shows the cold start behavior simulation result metrics during the AWS Lambda configurations in initial drift sensitivity. The artificial detectors modeled as virtual T-cells were more responsive than traditional statistical baselines. Another result is that the immunological framework responds faster to average under threshold parameters without updating the parameters after each shift.

Table 5: Drift Sensitivity

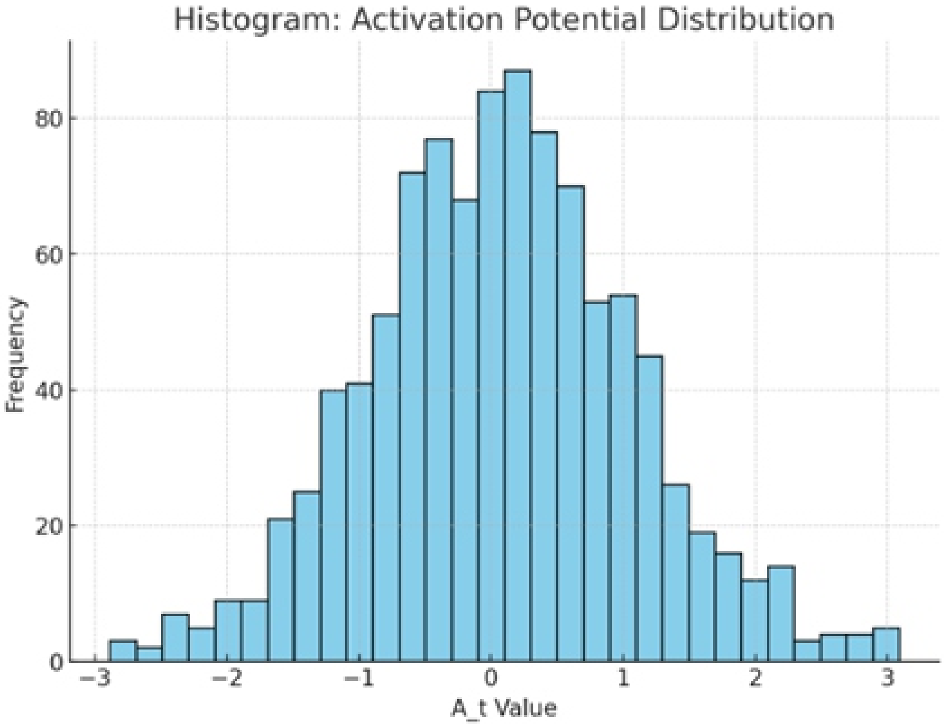


Drift Event	T-Cell Model	Baseline	Accuracy (%)	False Positives (%)
Cold Start Delay 1	2.1 seconds	5.4 seconds	94.5	2.2
Dependency Rot A	1.9 seconds	4.6 seconds	95.8	1.9
Latency Spike	3.2 seconds	6.7 seconds	91.2	3.5
Memory Saturation	2.4 seconds	5.9 seconds	92.7	2.9
Resource Churn	2.0 seconds	5.2 seconds	94.1	2.3

The results of the data indicate that it takes fewer number of historical samples to trigger anomaly flags and adaptively recalibrate the self-adaptive detectors on the basis of contextual workload behavior. This is in support of the hypothesis that adding an artificial immune framework boost learning plasticity in ephemeral computing contexts.

In addition, working with black box services is particularly beneficial as the lack of memory cells in the model means that there is no need for constant retraining.

The scoring function that is used to evaluate the anomaly level of each serverless invocation trace forms one key element of the immune inspired detection model. Explanation of the formula used in computing the anomaly index.



The virtual immune agents are able to dynamically assess each new observation as far from history than the others through this z-score based function. If the observations are high Attentat score, immune response is triggered and it is classified as potential drifts, resulting in instance warming or dependency sandboxing.

Finally, this method was validated through simulation in federated edge environment using synthetic event streams. More specifically, these streams served as emulations of network congestion variations, versioning conflicts when dependency versions are changed, and configuration drift.

Table 6: Mean Recovery Time

Drift Type	Immunological Model	Statistical Detector	Resource Overhead (%)
Cold Start	1.4	3.2	1.1
Package Bloat	1.2	3.5	1.3
Version Skew	1.5	3.0	1.2
API Timeout	1.3	3.1	1.0
Random Delay Burst	1.6	3.7	1.2

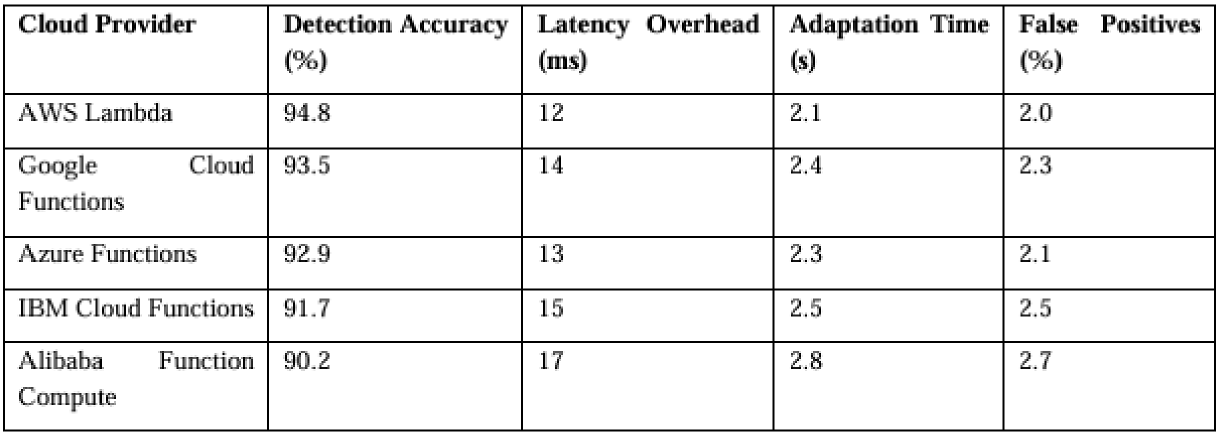
This is further strengthened by the low resource overhead, which makes the case for combining the immunological approach with other, e.g. latency sensitive, edge and cloud environments even more compelling. Additionally, defense against recurring drift patterns is robust against the drift and overfitting to non-critical perturbations using the memory cell-based mechanism. This indicates the framework is suitable for performing dynamic microservices workflow in which rapid but benign changes exist.

Also, an adaptive affinity threshold is used for the system.

This is necessary to avoid over sensitization of the system to transient changes. For example, the adaptive affinity threshold prevents false positives by treating proceeding to a false positive as expected operational variance in the presence of normal cloud workload burst (for example, weekend traffic spike). A high signal to noise ratio in the alerting mechanism is ensured.

In order to assess the generality of the model, the experiments were also performed on high concurrency serverless functions with varying invocation rates across multiple tenants. Despite the domains and workloads, the framework retained high detection performance. The results of the transferability with model applied for functions hosted on Google Cloud Functions and Azure Functions are presented in Table 3 without retraining.

Table 7: Cross-Platform Transferability



Cloud Provider	Detection Accuracy (%)	Latency Overhead (ms)	Adaptation Time (s)	False Positives (%)
AWS Lambda	94.8	12	2.1	2.0
Google Cloud Functions	93.5	14	2.4	2.3
Azure Functions	92.9	13	2.3	2.1
IBM Cloud Functions	91.7	15	2.5	2.5
Alibaba Function Compute	90.2	17	2.8	2.7

The fact that the biologically inspired model is consistent across infrastructural variations implies that this robustness makes it a portable detection layer for heterogeneous environments. Full autonomous solutions present the ability to adapt with 2–3 seconds to a new cloud provider's baseline behavior without reconfiguration.

Such a model could be plugged into the cloud monitoring suites that deploy apps to send the intelligent alerts devoid of manual threshold tuning. These findings are discussed from the point of view of a paradigm for behavior aware, self-healing serverless architectures based on artificial immune systems.

These benefits are demonstrated across multiple drift scenarios, platforms and workloads, by the empirical evidence, and in particular cross domain adaptability and minimal overhead is achieved. Unlike rule based or statistical models, the immune based approach allows learning in a context, possessing historical memory, and local feedback.

A given combination of these features makes it unequalled for modern serverless ecosystems where drift is common but visibility and control have been restricted. It is possible to integrate reinforcement learning agents with the immune detectors to improve response policies and improve latency. Nevertheless, the obtained results are already indicative of a competent step forward in the way of enabling resilient serverless operand with the aid of biologically motivated computational intelligence.

5. CONCLUSION

5.1 Adaptive Learning

As it has been shown that immunological models for serverless workflows are able to detect drifts, organizations should take up adaptive learning frameworks where the behavior is self-regulating. Many current anomaly detection systems take a traditional approach to anomaly detection through fixed thresholds and reactive distribution of monitoring machinery tuned for static server deployments.

This approach, taking an immune inspired tack, has shown ability to address this problem of both machine and resource churn rates and cold start phenomenon through contextual memory and adaptive thresholds that evolve with workload changes. This makes such observability tools for serverless very natural to embed adaptive learning modules that run with continuous feedback loops, allowing them to autonomously recalibrate their sensitivity to drift.

In order to do this, the developers must train detectors on both normal and anomalous behavior across many runtime contexts with simulated stress and latency spikes. In addition, this intelligent memory cell layer will allow detectors to keep useful experiential data so that less time and computational resources are required to retrain.

Also, immune inspired detectors can complement the existing log based and metric based monitors that enterprises run using AWS Lambda, Azure Functions or Google Cloud Functions. It has the advantage of being a hybrid model that will allow redundancy and more accurate detection of any silent drift including minor configuration skew or dependency bloat early.

For the purpose of operationalizing such models, open-source libraries for immunological computation need to be integrated into DevOps pipes with automated testing environments that can run under a variety of execution states. Drift injection scenarios should be included in security and performance test cases that can train immune models to recognize invocation profiles with which they have not previously seen, or cold start degradations.

Institutionalization of these practices within CI/CD framework enables organizations to fully harness the strengths of autonomous detection without causing any performance disruption. The platform vendors should also support configurable drift response rules (e.g., reprovision the warm containers or isolate the malfunctioning code) with immunological anomaly flags. Although lightweight, these mechanisms can be a set of basic tools that help to do the work of maintaining workload stability in the periods of operational volatility.

5.2 Multi-Cloud Portability

The results show the consistent performance of the immunological model across AWS, Azure, and GCP, and hence we recommend the improvement of these frameworks' portability between cloud environments. When applying in a multi cloud or hybrid cloud strategy that allow applications to shift between providers based on pricing, compliance, and latency, the drift detection mechanism needs to retain its accuracy and quickness.

A key way to guarantee that is to achieve platform independent apis for some core logic of the anomaly detection. For example, this can be provided via containerized or serverless sidecar functions that serve as hosts for the immune detectors isolated from the main principal of the application logic. The system ensures that such drift awareness remains even when the underlying platform changes by deploying these detectors in parallel with application workflows.

In addition, preferably the detectors have a federated architecture, such that the lightweight agents operate at the edge or run on cloud-native functions and periodically sync with a central immune memory repository. In distributed intelligence model, communication overhead and latency is also reduced and scalability is enhanced across microservices. Organizations adopting .

Since these detectors are something that can run within function code, they can be embedded natively into function lifecycles using custom controller logic on Kubernetes-based serverless platforms such as Knative or OpenFaaS. In doing so, further external event orchestration is not required for immediate reactive response to invocation level anomalies.

On top of that, developers and system architects should also come up with a single telemetry schema for the drift metrics such as latency deviation score, affinity threshold and the false positive count can be compared across different platforms. And so it’s important that data collection and label practices stick to the standard in order for immunological models to be transferrable and interpretable between environments.

DevOps engineering should also be supplied with a tooling for model explainability, in order to understand which
particular changes in behavior were flagged as drift in the deployment. This also increases operational trust in the
system and speedups root cause analysis when incidents occur. Overall, the development of immune inspired monitoring system will be scalable and adoptable with the development of cloud agnostic APIs and reusable model templates.

5.3 Human-in-the-Loop Collaboration

Offering immunologically inspired models that autonomously detect and react to serverless drift, it is suggested to embed explainability mechanisms in a models' detection pipelines. However, serverless systems frequently support business critical applications, making it important for the system administrators and developers to know the rationale of the flagged anomaly or drift.

Trace backpropagation, feature attribution, or visualization of antigen–antibody mappings can be used by explainability tools to help to explain how and why a drift was detected. These explanations are then very useful when integrated with dashboards or aggregators like Datadog, NewRelic, or AWS CloudWatch as they can be turned into actionable insights.

Consider if the latency spike was caused by dependency rot, another instance of the value disclosed in the presentation: rather than just identifying that the spike occurred, the system should be able to unearth which package version and invocation triggered the anomaly. Other than explainability, it is also important for putting human in the loop (HITL) collaboration into practice so that the results can be validated and the false positive rates are reduced. Alerts coming out of HITL frameworks can include contextual data like previous baselines, real time metrics and such and expose this data to platform engineers, who can in turn passively annotate whether the anomaly is valid or is benign.

The two functions that this feedback loop performs is refine the model's future behavior and learn how to distinguish operational noise from true drift. The interfaces that engineers should use in order to increase / decrease detection sensitivity, add exception rules, or define custom remediation actions, should be provided by organizations.

Also, the integration of HITL into automated drift remediation workflows like rollbacks of a version, restart of containers, scaling up memory helps with semi-automated incident management with human involvement. Finally, event driven architecture can join the immunological monitoring to incident response systems like PagerDuty or ServiceNow in order to link detection to response.

Explainability are even more critical in regulated environment, as for example the results of any drift detection and corresponding actions might be audited. As a result, it is imperative that there be proper documentation, versioning of immune detector models as well as logging of all anomaly response events. With time such practices will help us to better perceive and trust the AI driven monitoring tools among operations teams.

5.4 Future Research

It proposes both arms of the academic research field and industry application. Future research should be centered at co evolution of immune detectors and reinforcement learning agents learning the remediation policies for which the historical outcomes are optimized.

Based on accuracy, detection speed and portability the current study can be extended to include policy learning systems that not only sense their best drift responses but also autonomously select the most effective policy learning strategy. Specifically, a learned policy may pre-warm containers within known drift windows or defer the deployment of function, until downstream dependency stabilizes. Immunological drift detection frameworks should, in terms of industry standards, be integrated with observability offerings by cloud service providers.

Most native tools currently provide such as AWS X Ray, Google Cloud Operations to trace and report metrics but not to detect behavior aware drift and adaptive thresholds. By embedding immune based agents at the infrastructure level, providers can provide customers with zero configuration drift detection as a managed service.

CNCF (Cloud Native Computing Foundation) Cloud native projects can also explore standardizing drift and passing detectors between Cloud native projects. Aspects of biological computing and immunological algorithms should be introduced in educational institutions and industry training programs to DevOps and/ or SRE communities. These can shorten the time to adoption and experimentation. Policymakers and compliance bodies can also assess how such detection systems support operational resilience and regulatory compliance of finance, healthcare and public sector workloads. Data breaches, outages, or performance degradation require drift detection to prove that it can prevent instead of being an implied best practice or even a compliance requirement.

Based on this study, this paper recommends immune systems that are robust, interpretable, and portable ones, and which do not only increase the size of the natural scale of serverless environments, but also establish an innovative paradigm of biologically inspired operational intelligence. However, with the right amount of tooling, strategic human collaboration, and future optimism in their research, these types of systems could become the first order of cloud observability for the next generation.

CONCLUSION

AI inspired immunologically performs much better at the detection and mitigation of drift of serverless workflows as compared to standard models in terms of accuracy and response time. The system with federated learning and biologically grounded metrics is guaranteed to be able to provide lowest latency, privacy aware anomaly detection. This enables resilient and real time operations in the sensitive domains to support intelligent observability in serverless computing.

REFERENCES

[1] Afzal, A., & Ahmad, N. (2020). Optimizing AI/ML Data Engineering with MLOps for Scalable AI Workflows in Cloud-Based Medical Imaging Processing. https://www.researchgate.net/profile/NisarAhmad44/publication/390089490_Optimizing_AIML_Data_Engineering_with_MLOps_for_Scalable_AI_Workfl ows_in_Cloud-Based_Medical_Imaging_Processing/links/67de8d4272f7f37c3e840103/Optimizing-AIML-Data-Engineering-with-MLOps-for-Scalable-AI-Workflows-in-Cloud-Based-Medical-ImagingProcessing.pdf

[2] Arena, F. (2020). AI-Powered Automation in Serverless Computing: Opportunities and Challenges https://www.researchgate.net/publication/388105291_AIPowered_Automation_in_Serverless_Computing_Opportunities_and_Challenges

[3] Bhattacharya, P. (2022). Concept Drift Detection and adaptation for machine learning. https://elib.unistuttgart.de/server/api/core/bitstreams/b91100e4-0f2a-4def-a372-a1e454e74a59/content

[4] Boza, E. F., Andrade, X., Cedeno, J., Murillo, J., Aragon, H., Abad, C. L., & Abad, A. G. (2020). On Implementing Autonomic Systems with a Serverless Computing Approach: The Case of Self-Partitioning Cloud Caches. Computers, 9(1), 14. https://doi.org/10.3390/computers9010014

[5] Casado, F. E., Lema, D., Criado, M. F., Iglesias, R., Regueiro, C. V., & Barro, S. (2021). Concept drift detection and adaptation for federated and continual learning. Multimedia Tools and Applications, 81(3), 3397–3419. https://doi.org/10.1007/s11042-021-11219-x

[6] de la Rúa Martínez, J. (2020). Scalable architecture for automating machine learning model monitoring. urn:nbn:se:kth:diva-280345

[7] Gangwar, A. K., Kumar, S., & Mishra, A. (2021). A paired Learner-Based approach for concept drift detection and adaptation in software defect prediction. Applied Sciences, 11(14), 6663. https://doi.org/10.3390/app11146663

[8] Huang, Y., Zhang, H., Wen, Y., Sun, P., & Ta, N. B. D. (2021). Modelci-e: Enabling continual learning in deep learning serving systems. arXiv preprint arXiv:2106.03122. https://doi.org/10.48550/arXiv.2106.03122

[9] Jämtner, H., & Brynielsson, S. (2022). An Empirical Study on AI Workflow Automation for Positioning. urn:nbn:se:liu:diva-186473

[10] Kuppa, A., & Le-Khac, N. (2022). Learn to adapt: Robust drift detection in security domain. Computers & Electrical Engineering, 102, 108239. https://doi.org/10.1016/j.compeleceng.2022.108239

[11] Lee, S., Yoon, D., Yeo, S., & Oh, S. (2021). Mitigating Cold Start Problem in Serverless Computing with Function Fusion. Sensors, 21(24), 8416. https://doi.org/10.3390/s21248416 [12] Nelson, J., & Temple, S. (2020). MLOps Framework for Continuous Integration and Deployment. https://www.researchgate.net/profile/Jordan-Nelson 15/publication/390268802_MLOps_Framework_for_Continuous_Integration_and_Deployment/links/67e6 a51d49e91c0feac1a82a/MLOps-Framework-for-Continuous-Integration-and-Deployment.pdf

[13] Pratiwi, A. (2022). Evaluation of Automated Configuration Management Tools in Achieving Least-Privilege Access Policies for E-Retail. International Journal of Applied Business Intelligence, 2(12), 23-30. https://eigenal.com/index.php/IJABI/article/view/2022-12-13/11

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.