ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse49912020.pdf
https://doi.org/10.30534/ijatcse/2020/49912020

Disruptive emerging technologies: Change in service operating model

Subramaniam Radhakrishnan [1], Dr. Prashobhan Palakkeel [2], Dr. Raja Sreedharan. V [3]
[1] Ph.D. Scholar, Amrita Vishwa Vidyapeetham, Coimbatore, India, salemradha@gmail.com / 30+ years of IT industry experience (currently in Singapore Telecommunication Group, Singapore)
[2]Assistant Professor, Amrita Vishwa Vidyapeetham, School of Business, Bengaluru, India, p_palakkeel@blr.amrita.edu
[3]Assistant Professor, Rabat Business School, Université Internationale de Rabat, Morocco, rajasreedharan1@gmail.com

ABSTRACT

The service operation is quite important to run a business and deliver customer service up to the expectation. This paper is looking at IT services and the use of artificial intelligence (AI) with machine learning (ML). The authors figured out that the service operation model is disturbed by the use of AI and ML. This paper was looking at the possible extent of disruption in specific to IT service but it is quite relevant to other service industries as well. The service operating model getting changed by disruptive technology (AI and ML) which replace the human drastically. The service operating model will be changed to an AI-led human supervised model. IT services and even service platforms will be changed by embedding AI and ML in the platform. IT capital replaces humans to mitigate skill demand in developed economies. Our study cautioning service providers and even enterprises to get prepared for this drastic disruption to gain early competitiveness in the marketplace. AI and ML together with an automation engine or platform is the future for the service industry and industry to get prepared for this mainstream alignment quickly.

Key words: service operation, artificial intelligence, machine learning, operating model.

1. INTRODUCTION

The business requires IT alignment which is managed by Information Technology service management (ITSM) [1] since managing complex IT infrastructures and applications with agility. It is not only for business alignment as the cost of providing service must be economic and cutting costs [2] is pressure for service providers and even organizations. It is important to have a framework for end-to-end service management so as to optimize processes, people and technology and this is facilitated by Information Technology and Infrastructure Library (ITIL) [3]-[4] and Ahmad et al. 2013). ITSM covers five main areas of service strategy, service design, service delivery, service operations and continuous service improvement (CSI). ITIL framework is having well-defined processes [5]. It has been predicted that 82 percent of ITSM professionals [6] feel that the job is going to be more challenging and even though only 16 percent had identified the role of AI in ITSM as a threat.

Artificial Intelligence (AI) [7] is a system that rationally thinking and acting like a human. AI together with ML provides a lot of valuable insight [8] to the customer, product or services. AI is using big data and processes three different types of data [8] namely structured, semi-structured and unstructured data. Predicted that about 80 percent of the data [9] is unstructured and the size of unstructured data is estimated as 2.5 billion gigabytes (GB) daily. AI requires trained data from big data that require machine learning (ML) algorithms [58] to works together. ML is also playing a major role together with AI since AI requires ML [58] to process big data for modeling and prediction [59]. It has identified that AI, deep learning and machine learning are going to be in mainstream adoption [10]-[11] between 2 to 10 years. AI together with the cloud is helping businesses and services on-boarded much quickly to reef the benefit of early adoption.

Within ITSM, the service strategy, design and delivery are based on products or services we offer to the customer and it can be pre-defined to meet customer expectations without the use of disruptive technologies such as AI and ML as it can be managed using any of the service delivery platforms). The role of AI is mainly to replace humans in the form of dehumanization [12] and service operation is heavily dependent on humans. As AI and ML started to become mainstream adoption, our study proposes to deep dive to understand the extent of disruption in dehumanization in IT service operation (ITSO) and look at how disruptive in changing the service operation model.

2. LITERATURE BACKGROUND

The ITSO [13] consists of five main areas such as an event, incident, problem, access and request management.

2.1. Event Management

Event management [14] is a must to monitor customer devices, systems and networks to detect any anomalies for action. An event management system helps to forward actionable events for troubleshooting. It helps to also predict any deviation from the normal or expected service operation. It monitors service for the acceptable service level (SLA) [15]. Refer to the following figure 1 for event management processes as derived from the ITIL process framework [16].

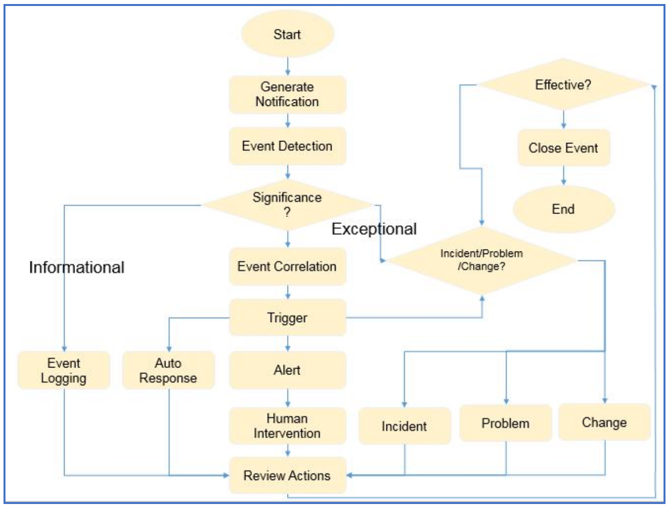

Figure 1: Event Management processes in ITSO

Refer to table 1 for the role of human and monitoring system without the use of AI/ML system in event management processes.

Table 1: Role of human and event management system

Events	**Role of Human**	**Role of the Monitoring system**	**Reference**
Generate Notification	-	Generate notification	[16]
Event Detection		Detect events	[14]
Significance of events?		Significance events such as informational, warning and exception	[14]
Informational->Logging Events		Log the event in event management	[14]
Event Correlation	Partially by user activities	Partially by system activities	Refer to figure 6 [16]
Trigger	Manual script trigger	Or scheduled script trigger by system	[16] and [14]
Alert		Monitoring system sends alert to the incident management system	[16]
Human Intervention	Alerts are normally sent by SMS and email when human intervention is needed		[14]
Logging Events -> Review Actions -> Review actions	Hardly human look at the review when huge events flooded without correlation and deduplication.	Partially it can be automated	[14]
Exceptional -> Incident / problem / change management processes			Sub-processes of incident management will be discussed in respective sections below
Effective? -> Incident / problem / change management processes			Sub-processes of incident management will be discussed in respective sections below
Effective> Close Events	Partially by human	Partially by monitoring system	[14]

2.2. Incident and problem management

An incident and problem management are the process groups in ITSO with a lot of human involvement to manage service within agreed SLA for the acceptable service availability [17]. It is a customer touchpoint in the ITSO which directly reflects customers' experience end-to-end lifecycle of the service. The incident management system or service management (SM) system will be responsible to manage customer SLA throughout the lifecycle of the service operation. There are few channels of incident escalation [5] and [14] which are mainly, proactive (by event management system) and reactive (by a human through a phone call, email or other communication channels). Problem management processes are similar to incident management processes but it helps to deep dive with root cause analysis and fixe the issue permanently to avoid recurring issues in the future. The incident management team will look at customer problems at that point in time and help to resolve them quickly. But the problem management team needs to look at repeated incidents and make sure that it is not occurring again. To have a high-level understanding of incident and problem management processes [14], refer to the following figure 2 for details.

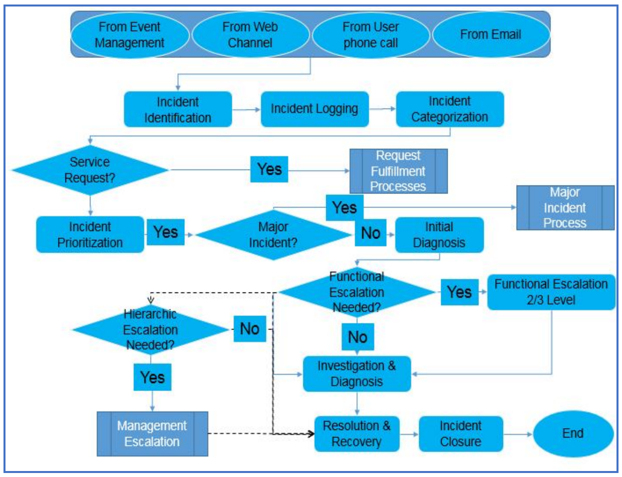

Figure 2: Incident/Problem management processes in ITSO

These processes are generally managed by the ITSM system and human. Refer to the following table 2 for the works of literature associated with incident management processes and this is analyzed based on processes in figure 2.

Table 2: The Role of Human and IMS system in IT Service Operation

Events	**Role of Human ServiceDesk (SD) or Helpdesk (HD) personnel**	**Role of incident management System (IMS)**	**Comments**
Incident identification (reactive)	Identify the incident and recording it in IMS		[14]
Incident identification (proactive)		The system handles identification of incident when automatically triggered by the monitoring system	
Incident logging (reactive)	Log the incident		[14]
Incident logging (proactive)		System logs the incident automatically	[14]
Incident categorization (reactive)	Categorize the incident		[14]
Incident categorization (proactive)		The system categorizes the incident automatically	[14]
Service Request (SR)?	Create incident Type as Service Request when escalation from the customer is SR and it follows SR processes		
Incident prioritization (reactive)	Prioritize based on issue nature		[14]
Incident prioritization (proactive)	Modify prioritization	When trigger comes from the monitoring system, it preset the defined priority (example, P1, P2 or P3) by rule	[14]
If a Major Incident?	The major incident refers to a wider outage that affects many customers. This is a separate sub-processes.		
If not Major Incident? -> Incident Diagnosis	This is at a low level (called the first level of troubleshooting) to look at the issue by Level 1 Engineer		[14]
Functional Escalation?->Level 2/3	When Level 1 is not able to resolve, the issue will be escalated to level 2/3 Engineer		[14]
Otherwise-> Investigation and Diagnosis	Done by Level 2/3 Engineer		[14]
If Management escalation Needed?	Will be escalated to management and it follows its sub-processes		[14]
Resolution and Recovery	By Level 1 Engineer to record resolution code of the issues and recover customer service		[14]
Incident Closure	This can be done my IMS system partially or human	Partially done by the system	[14]
Problem management (Root cause analysis)	Done by L2/L3 team		[14]

2.3. Access Management processes

Access Management processes are important in ITSO to protect data integrity, confidentiality and availability [14]. The service expectation from customers is to provide access at the right time and protect data in every aspect since data is intellectual property. As data is growing and data is processed [18] not only by humans as it is also processed by other intelligent agents such as robots. It is important to have secure access to data or information. Refer to figure 3 to know the access management processed [19].

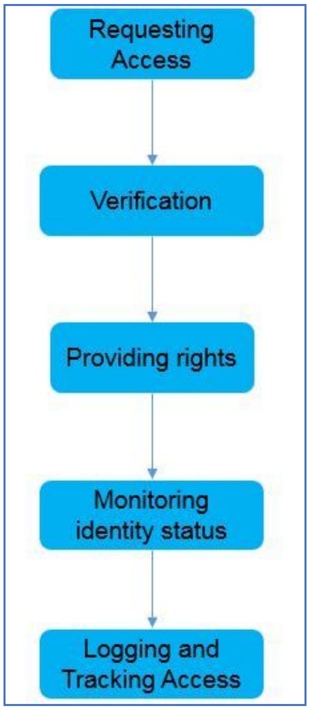

Figure 3: Access management processes in ITSO

2.4. Request Management processes

Request management processes allow the customer to place a service request and pass it to approval from business and IT service stakeholders. Then it is routed to fulfillment. The self-service portal [20] is one customer experience layer and provider to communicate service offerings to customers to place requests. The fulfillment processes are well defined and loaded into the ITSM system during customer on-boarding. Sometimes, fulfillment cannot be automated end to end as it may require human intervention or a third party. Refer to figure 4 for processes [14] related to request fulfillment.

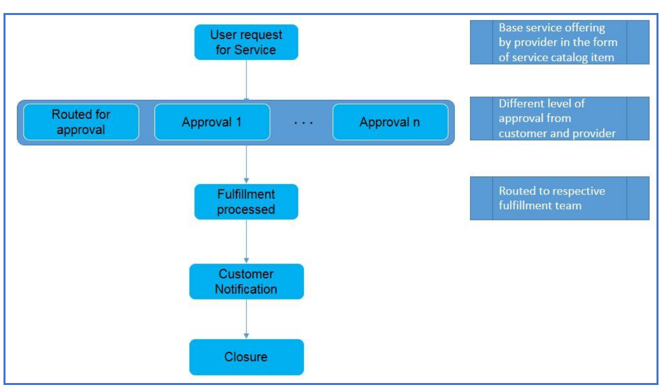

Figure 4 : Request Fulfilment processes in ITSO

3. ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

Refer to the following hype cycle [11] figure 5 which shows emerging technologies such as AI and ML which are going to be in mainstream within 2 to 10 years. Some of the consumer AI [21] in our daily life are Siri, Alexa, Google AI and so on.

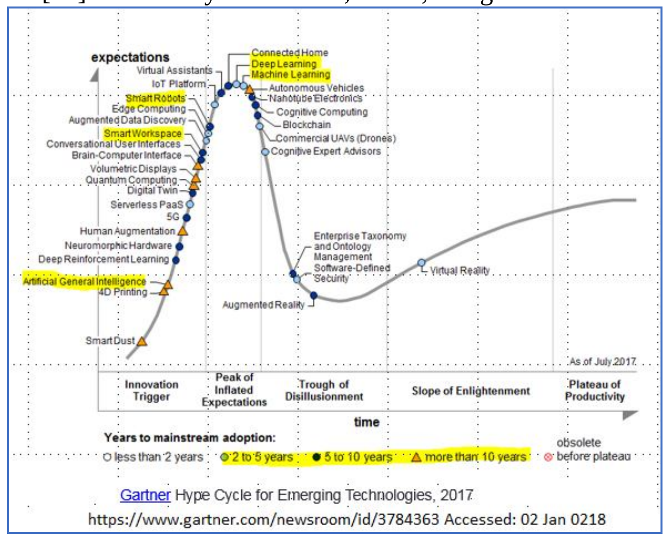

Figure 5: Gartner Hype Cycle for emerging technologies. 2017

These AIOps (AI for IT operations) products are helping to manage services in the IT service environment.

Table 3 :AIOps Products: Source- Gartner (August 2017)

Product	Stored	Streaming	Logs	Metrics	Wire Data	Document Text	Pattern Discovery	Anomaly	Causal Analysis
BMC	x	x	x	x		x	x	x	x
Correlsense		x		x	x		x	x	x
Corvil		x		x	x		x	x	x
Elastic	x		x	x	x		x	x	
ExtraHop	x	x		x	x		x	x	x
FixStream	x	x	x	x	x		x		x
(HPE)	x	x	x	x	x	x	x	x	x
IBM	x	x	x	x	x	x	x	x	x
ITRS	x	x	x	x	x	x	x	x	x
Logtrust	x	x	x	x			x	x	x
Logz.io	x		x				x	x	x
Loom Systems	x	x	x	x			x	x	x
Moogsoft	x	x	x	x	x	x	x	x	x
Rocana	x	x	x	x			x	x	
SAP	x	x	x	x	x		x	x	x
Scalyr	x		x	x			x	x	

SIOS	x	x		x			x	x	x
Splunk	x	x	x		x		x	x	x
Sumo Logic	x	x	x	x			x	x	x
VNT	x	x		x	x		x	x	X
Source: Gartner (August 2017)									

3.1. Problems in ITSO

These are some of the known problems to be solved to provide customer service within the agreed service level, run the service at low cost and delivery service within the turnaround time (TAT) [28]. There were limited studies done to address these problems. Look at the problem statement in the following table 4.

Table 4: Define Phase: Problem Statement

Item #	The problem in (ITSO)	Description	Reference
1	Duplicate incident/ticket	System or human open multiple incidents for the same issue but closed later with the resolution code as wrong/duplicate incident	[29]
2	False-positive / no fault found	System or human create or identified as an incident but no issue persists	[30]-[33]
3	Unplanned outage	Outages unplanned to solve issues when arises to bring the service up or in operation	[34]
4	Unlocalized fault	Unable to locate fault or problem	[35]
5	Long turnaround time (TAT)	Long-time has taken to resolve the issue	[28]
6	Unresolvable issues	Unable to resolve the issue and it becomes known bug to be fixed	Product bug
7	Low maturity organization	The lifecycle of incident or problem management is not matured	[36]

3.2. Data collection

The data is collected for six months from 01-01-2018 to 29-06-2018. The total number of incident records are 46, 490. The description of the dataset is as follows in table 5 below.

Table 5 Description of the dataset collected

Column Name	**Description**	**Sample value**
Number	To describe the name of the ticket/incident or case. Note: data is masked due to sensitivity. Hereafter we refer this is incident	CASE0001962742
Rep_time	Refers to the reported time of the incident	1/1/2018 12:11:00 AM
Res_time	Refers to the restoration of the incident. Means, service is restored after fixing the incident	1/1/2018 4:10:00 AM
MTTR [56]	Meantime to repair service. How much it takes to restore service [Res_time - Rep_time]. This is the calculated field from Res_time and Rep_time.	3:58:57 in HH:MM: SS
Closed.Time	The time when the incident is closed	1/1/2018 6:54
Reported. source	Channel of getting incident [Example, by email, phone, etc]	email
RES1	Restoration code. This is entered by a human while closing incident	Fault Found, No Fault Found, Wrong/Duplicate Ticket
RES2	This is the second level of restoration code entered by a human. Every RES1, there will be one or more RES2. [RES1: Fault found and RES2: Cannot Localize, or Local Loop (Singapore), or Customer, Local Loop (Overseas), etc]	Cannot Localize
RES3	This is the third level of restoration code entered by a human. Every RES2, there will be one or more RES3. [RES2: Cannot Localize and RES3: Self Recovered]	Self Recovered
Incident.type	Type of incident created or reported [Event refers to event ticket raised by a monitoring tool, Normal refers to the incident created by a human]	Event

3.3. Data Analysis

The following data analysis will be based on the problem statement in "Section 3.1 Problems in ITSO".

3.3.1. Wrong/Duplicate incident

The followings are the summary of the incident (Tabe 6) by resolution type and restoration cade is “Wrong/Duplicate incident”. There are 5,355 incidents closed with the resolution code as “Wrong/Duplicate incident”. If the system is capable to identify these incidents as duplicate or wrong, it would have been eliminated in creating an incident. The consequences are the customer will get notified that there is an incident but customers already know that there is an existing incident and support is already working on. Once a customer gets the notification, the customer will get confused with these duplicate notification. This will affect the overall SLA calculation for the customer if oversight.

Table 6: Number of incidents by Resolution

Resolution Type	Number of incidents	Percentage
Duplicate Ticket	1	0%
Enquiries	1	0%
Fault Found	24711	53%
Force Majeure	23	0%
No-Fault Found	5614	12%
NULL	1220	7%
Planned Outage	3065	7%
Provisioning	795	14%
Service Request	5700	12%
Unlocalised Fault	6	0%
Wrong /Duplicate Ticket	5354	12%
(blank)		0%
Grand Total	**46490**	0%

3.3.2. No-fault found or false incidents

The following measurement is done based on type on the incident resolution (Table 7) by incident type as “all”. There are 12 percent incidents are closed with resolution code as “No fault found”. It shows that the ITSM system is not capable to identify false-positive before the creation of an incident and it ends creating an incident and wasting time for support to troubleshoot before the closing incident.

Table 7: No-Fault found incidents

Resolution Type	Number of incidents	Percentage
Duplicate Ticket	1	0%
Enquiries	1	0%
Fault Found	24711	53%
Force Majeure	23	0%
No-Fault Found	5614	12%
NULL	1220	7%
Planned Outage	3065	7%
Provisioning	795	14%
Service Request	5700	12%
Unlocalised Fault	6	0%
Wrong /Duplicate Ticket	5354	12%
(blank)		0%
Grand Total	**46490**	0%

3.3.2.1. Event type

The number of incidents automatically triggered (Tabe 8) by the monitoring system is 26, 594 which is 57 percent of the total incident in six months. The number of incidents found as false (or no-fault found or duplicate) is 7, 497 which is 28 percent of the total event incident. These incidents are triggered by the monitoring system. Refer to table 6 with the consolidated details of data collected. Event type incident is automatically created by monitoring systems without any event correlation and noise suppression [37]. This is clearly showing that monitoring or event management system triggered wrongly without correlating existing incidents.

Table 8: Number of event incidents by Resolution

Incident type	Event	
Total number of incidents	46490	
Resolution Type	**Number of incidents**	**Percentage**
Duplicate Ticket	1	
Fault Found	15804	59%
No-Fault Found	2966	11%
NULL	742	3%
Planned Outage	1841	7%
Provisioning	476	2%
Service Request	231	1%
Unlocalised Fault	2	0%
Wrong /Duplicate Ticket	4531	17%
Grand Total	**26594**	**100%**
Percentage of event incidents	57%	

3.3.3. Unplanned outage

The outages as part of service request or fault found or even unlocalized fault are done in addition to planned outage are categorized as an unplanned outage. Refer to table 6, there is 65 percent of incidents are categorized under unplanned as it has occurred outside of the planned outage window.

3.3.4. Unlocalized fault

There are only 6 incidents (Table 7 as above) closed with the resolution code as an unlocalized fault and it is less than 0 percent of total incidents.

3.3.5. Unresolvable issues

There is no indication based on the resolution code in table 6 above. No further analysis has been since data is not available.

3.3.6. Low maturity in terms of people, culture and organization

The low maturity can be identified [36] from the processes that the organization established to manage incidents and problem management. The maturity level is not high in our current analysis as we have seen 28 percent of wrong/duplicate and no fault found incident. Overall there are 65 percent unplanned which is also an indication for low maturity as well. There are other issues identified in the below sections which are not listed in the problem section.

3.3.7. Immediately restored incident

Refer to the following table 9 for the number of the incident by resolution type and MTTR is zero. These incidents are restored by the automation engine within the same minute. Means, open time and restoration time are the same.

Table 9: MTTR equal Zero

MTTR2	0:00:00
Resolution Type	**Number of Incidents**
Duplicate Ticket	1
Fault Found	14758
Force Majeure	9
No-Fault Found	3566
NULL	334
Planned Outage	1480
Provisioning	496
Service Request	3572
Unlocalized Fault	4
Wrong /Duplicate Ticket	3165
Grand Total	**27385**

3.3.8. Breach of SLA or resolution time more than TAT

The mean time to restore (MTTR) is closely related to service level agreement [38]. The service level agreement for the services offered by this service provider is 99.5 percent. This is translated into 3 hours and 36 minutes of downtime per month. The Total number of the incident with MTTR is greater than 3 hours and 36 minutes: 6,691 (14 percent) as shown in table 10 below.

Table 10: SLA breached by Resolution Code

MTTR	➢ 3:36:00	
Total number of incident	46490	
Resolution Type	**Number of incidents**	**Percentage**
Fault Found	3617	54%
Force Majeure	8	0%
No-Fault Found	674	10%
NULL	497	7%
Planned Outage	358	5%
Provisioning	119	2%
Service Request	778	12%
Wrong /Duplicate Ticket	640	10%
Grand Total	**6691**	
Percentage of SLA breached incident	14%	

3.3.8.1. Event correlation

There are many ways to correlate events to avoid the "no-fault or false-positive" case [33]. If the event correlation is working, the subsequent incident will not be created when there is an open incident for the same service. Refer to the following incident list (sample) to show that the event correlation is not in place in the provider environment by the traditional monitoring or event management system.

Scenario:1

This scenario is measured based on the same service and customer. It was reported by the monitoring system 25 times throughout 2/22/18 to 6/9/18 (3 ½ months). Refer to the following table 11 for more details.

Table 11: Incident for the same service and customer

Number	Reported Time (A)	Closed Time (B)	Resolution Code 1	Affected Service
XX2033690	2/22/18 1:38 PM	2/23/18 9:08 AM	Cannot Localize	SVC1234
XX2065780	3/17/18 5:17 PM	3/17/18 7:16 PM	False Alert	SVC1234
XX2148691	4/19/18 1:15 PM	4/19/18 10:42 PM	Cannot Localize	SVC1234
XX2148811	4/19/18 3:29 PM	4/19/18 3:42 PM	*	SVC1234
XX2148913	4/19/18 6:27 PM	4/19/18 8:42 PM	*	SVC1234
XX2149152	4/20/18 1:27 AM	4/22/18 11:27 PM	Cannot Localize	SVC1234
XX2149842	4/20/18 7:19 AM	4/20/18 7:44 AM	*	SVC1234
XX2150155	4/20/18 9:55 AM	4/20/18 11:22 AM	*	SVC1234
XX2150818	4/20/18 6:40 PM	4/21/18 11:39 PM	Cannot Localize	SVC1234
XX2150963	4/20/18 9:33 PM	4/20/18 10:11 PM	*	SVC1234
XX2151086	4/20/18 11:47 PM	4/21/18 9:03 AM	*	SVC1234
XX2151427	4/21/18 4:44 AM	4/21/18 9:04 AM	*	SVC1234
XX21520	4/21/18 5:18	4/24/18 1:52	*	SVC1234

Number	Reported Time (A)	Closed Time (B)	Resolution Code 1	Affected Service
26	PM	AM		
XX2152917	4/22/18 5:09 AM	4/22/18 7:52 AM	Customer Issue	SVC1234
XX2155109	4/24/18 12:57 AM	4/24/18 1:28 AM	*	SVC1234
XX2155585	4/24/18 5:02 AM	4/26/18 2:19 AM	Cannot Localize	SVC1234
XX2156102	4/24/18 9:04 AM	4/24/18 9:21 AM	*	SVC1234
XX2157162	4/25/18 3:58 AM	4/25/18 11:18 AM	Cannot Localize	SVC1234
XX2174853	4/25/18 8:34 AM	4/25/18 11:38 AM	Cannot Localize	SVC1234
XX2175135	4/25/18 10:37 AM	4/25/18 11:10 AM	*	SVC1234
XX2175285	4/25/18 1:11 PM	5/4/18 1:53 AM	Local Loop (Overseas)	SVC1234
XX2187387	5/5/18 12:25 AM	5/6/18 1:02 PM	Cannot Localize	SVC1234
XX2194973	5/10/18 2:21 PM	5/10/18 11:24 PM	Cannot Localize	SVC1234
XX2197120	5/12/18 4:19 PM	5/14/18 11:04 AM	Cannot Localize	SVC1234
XX2239521	6/9/18 6:12 PM	6/19/18 5:27 AM	Scheduled Planned Maintenance	SVC1234

Scenario:2

This scenario is measured based on "MTTR = 0:00:00", Resolution Code 1= "Wrong /Duplicate Ticket" and it is for the same service and customer. It was reported by the monitoring system 12 times over the period of 5/10/18 to 5/10/18 (in a day). This is just a sample and there are many incidents matching these criteria. Refer to the following table 12 for details.

Table 12: *MTTR equal 0, Resolution code 1= "Wrong/Duplicate Ticket" and reported by monitoring system*

Number	Incident State	Reported Time (A)	Restoration time ©	Affected Service
CASE2194219	Closed	5/10/18 5:05 AM	5/10/18 5:05 AM	SVC5678
CASE2194223	Closed	5/10/18 5:06 AM	5/10/18 5:06 AM	SVC5678
CASE2194224	Closed	5/10/18 5:07 AM	5/10/18 5:07 AM	SVC5678
CASE2194226	Closed	5/10/18 5:07 AM	5/10/18 5:07 AM	SVC5678
CASE2194231	Closed	5/10/18 5:08 AM	5/10/18 5:08 AM	SVC5678
CASE2194232	Closed	5/10/18 5:09 AM	5/10/18 5:09 AM	SVC5678
CASE2194233	Closed	5/10/18 5:09 AM	5/10/18 5:09 AM	SVC5678
CASE2194235	Closed	5/10/18 5:10 AM	5/10/18 5:10 AM	SVC5678
CASE2194236	Closed	5/10/18 5:10 AM	5/10/18 5:10 AM	SVC5678
CASE2194248	Closed	5/10/18 5:19 AM	5/10/18 5:19 AM	SVC5678
CASE2194249	Closed	5/10/18 5:20 AM	5/10/18 5:20 AM	SVC5678
CASE2194279	Closed	5/10/18 5:44 AM	5/10/18 5:44 AM	SVC5678

4. FINDING AND DISCUSSION

The following findings and discussions in table 13 are based on the problem in section 3.1 and respective data analysis in section 3.3.

Table 13: Event Management with the use of AI and ML

Event Processes	**How AI / ML help**	**Reference**
Generate notification	AI capable of generating notification and integrate with the ITSM system seamlessly.	[39]
Event detection	AI engine can handle event detection and correlate and group it together based on its relationship.	[40]
Informational or warning events	AI is also capable of grouping these events together with actionable events (critical, exceptional) to have a holistic view to make sense of data to provide outage insight. ML works together with AI.	[22]
Significance, correlation and deduplication	AI works better by accessing many sources of information and enrich raw events with associated data like the customer, location, asset and related assets. Then it de-duplicate and correlate events with enriched information. AI integrates with ITSM well and correlates with the existing and open incident to decide on the new incident or update the old incident.	[23], [24]
Triggering and alerting	AI does after the correlation	[41]
Close, synchronization of event and incident state	AI predicts the state of event and incident to sync incident and event lifecycle.	[42]

As similar to event management processes, performed literature review and review of some of the product capability since limited studies were done to identify AI and ML capability in ITSO. Refer to the following table 14 for the capability of AI and ML in incident management processes.

Table 14: Use of AI and ML in Incident Management

Incident management processes	How AI / ML help	Reference
Incident logging, identification, categorization and prioritization - proactive and reactive	AI is intelligent enough to identify, categorize and prioritize incidents in an automated way to reduce human involvement. AI in the form of the virtual bot can interact with a human who reports reactive issues.	[25]-[27]
Initial diagnosis and functional escalation	AI is emerging and capable of performing troubleshooting. If a further escalation is needed, AI is capable to escalate automatically	[43], [45]
Resolution, recovery and closure	AI perform recovery and close the incident upon recovery of service	[44]

4.1. Wrong/Duplicate incident

As AI is capable of correlation and removal of duplication [23], [24], AI can avoid the creation of those 12 percent incidents (5,355 incidents) which will avoid wasting a lot of human effort in verification and closure of incident as needed to close incident event though it is duplicate. By doing so, AI help to improve the customer experience as annoying notification or false notification can be avoided.

4.2. No-fault found or false incidents

AI together with ML does correlation, de-duplication, incident identification, categorization and prioritization [22], [23]-[27], AI can avoid the creation of false-positive incidents. There is 12 percent of "No-fault found or false-positive" identified in our data collection which can be avoided by the use of AI and ML. These are all some of the examples of noise suppression.

The percentage of noise reduction is 99.9 percent which is based on Moogsoft AIOps [27] as shown in figure 6. This may differ based on the product, situation of incident and many other factors.

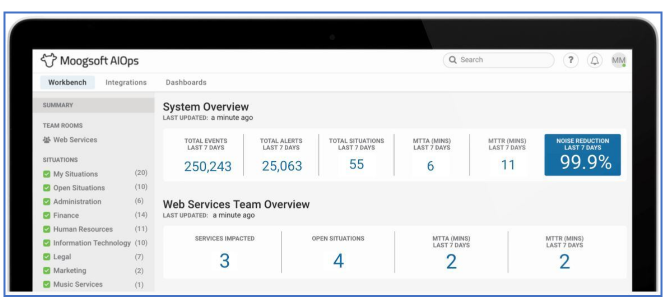

Figure 6: Moogsoft AIOps- Noise Reduction

Another example of noise suppression up to 97 percent [26] and refer to figure 7 for more details.

Figure 7: SPLUNK AIOps- Noise Reduction

AIOps system [26], [27], [46] can understand the open incident and avoid the creation of duplicate incidents. AI engine store or get dynamic CMDB information [23] upon events are received so that it can predict outage related open issues or new. Refer to figure 8 as captured from the POC setup which runs in the provider's environment (Note. Sensitive information is masked for data integrity).

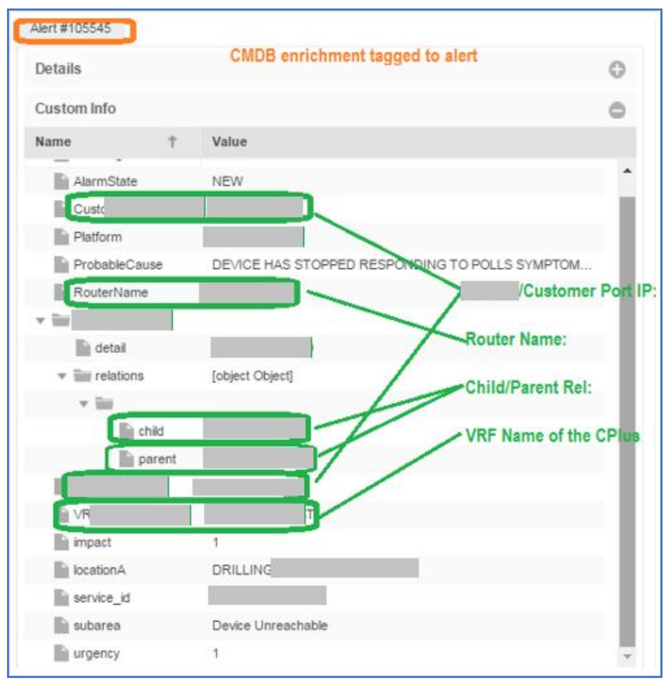

Figure 8: Data Enrichment in AIOps

It is possible to have a 33 percent reduction [43] in (MTTR) by using AI and ML. AI requires a lot of data called big data [57] which will be used by ML to learn and predict information and get the recommendation close to 100 percent.

The recommendation that AI provides is based on data that ML train and learn. When a record in dataset increases, the quality of ML will be high and AI acts on top of the ML. As referred in Gartner [55], MTTR [56] can be reduced by IMS which is faster and accurate and it can also cut noise, reduce incident acknowledgment/response time, set priorities while creating an incident, real-time collaboration and establishing clear roles and responsibilities (R&R) for the entire incident management processes.

4.3. Unplanned outage

The outages as part of service request or fault found or even unlocalized fault are done in addition to planned outage since categorized as an unplanned outage. Refer to table 6, there is 65 percent of incidents are categorized under unplanned as it has occurred outside of the planned outage window. Since AI can able to correlate data from the ITSM system [23] to know the outages and outages of related items, AI can figure out whether there is any related item affected to avoid unrelated items to be down.

4.4. Unlocalized fault

Since this is less than zero percent of total incidents our study was focusing on uncovering critical issues.

4.5. Low maturity in terms of people, culture and organization

The maturity level will be improved by AI in IT service management processes so that it can eliminate 28 percent of wrong/duplicate and false-positive incident. AI also can help to correlate existing and past historical outages to reduce 65 percent of unplanned outages.

4.6. Immediately restored incident

There is 67 percent of the incident with zero MTTR and These incidents are to be eliminated by correlation using past historical data [43]. As these incidents are related to duplicate or false positive which can be avoided by AI [22], [23]-[27], zero MTTR incidents can be avoided in ITSO.

4.7. Breach of SLA or more than TAT

The SLA is directly related to customer experience and it translates to customer retention [48]. 14 percent of SLA breached incidents are to be fixed to improve customer experience. These studies show that SLA degrades leads to customer churn [47]. The SLA is one of the important touchpoints for service provider and customer [47]. The breach of SLA can be avoided by eliminating human delay, false positive as it takes time to test to make sure it is false. Ai does well in removing false positive, remediate issues and escalate automatically to the next level. Some of the AI-capable products [43]-[45] can help to improve this area and avoid a breach of SLA.

4.8. Event correlation

Scenario:1

To avoid the false-positive incident, there might be some form of correlation or even testing to see whether the issue is temporary like network flapping [49]. The monitoring or event management system should be capable to monitor and trigger incident only when it is a genuine incident. ITSM systems are nowadays capable to suppress duplicate incidents and update existing incidents when open. But with the use of AI and ML suppression of noise is out-of-the-box capable. Refer to the figure 9 in anneure as it is captured in one of the service provider environment with the use of AI and ML, 108 events are correlated, suppressed and grouped to create just one incident.

Scenario:2

Refer to the figure 10 in annexure and this is based on one of the AI products called Splunk AIOps or ITSI [26] and it is capable of doing following sequential activities.

(1). Correlation, grouping and de-duplication: created one single event for 592 events

(2). Automated Trigger: Created only one incident (INCIDENT01854049) for these 592 events

(3, 4 and 5). Enrichment: Before the creation of the incident it has an enriched event with the affected customer, service name and location

(6). Timeline: Shows entire event escalation in timeline view

(7). Recommendation: It also provides recommendation on the probable root cause

Considering the discussion in the above sections, AI and ML can help to perform most of the event management processes as shown in the below diagram.

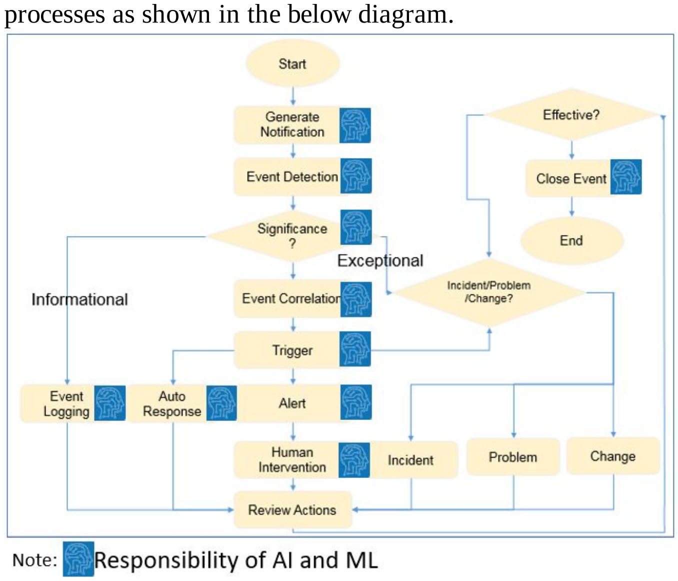

Figure 9: Role of AI and ML in Event Management processes

The following diagram is the proposed incident management processes with the role of AI and ML together with lean human involvement.

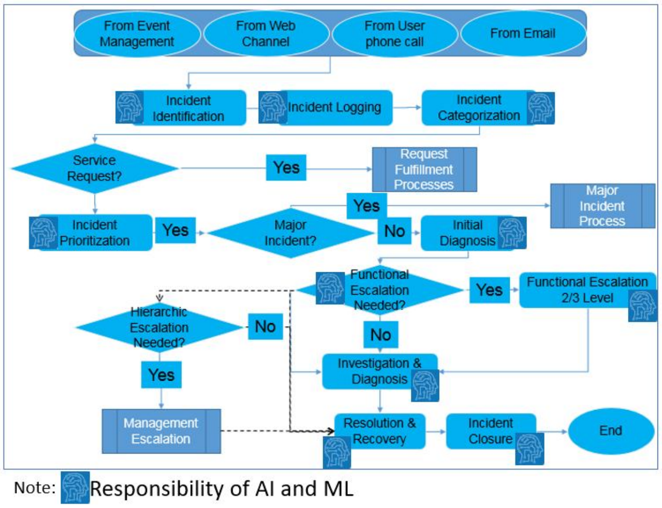

Figure 10 : Role of AI and MI in incident Management processes

The role of AI is quite disruptive as it leads to dehumanizing [12] most of the work. It will be leading to a reduction in the workforce [50] as 47 percent of the US workforce at risk within the next 10 to 20 years. AI disruptive to dehumanize the workforce in the service operation and will lead to ICT capital. But working with disruptive ICT technologies such as AI, ML, virtual assistant or even virtual engineer is quite important and relevant in terms of employability and business opportunity. 2.5 - 3 million new jobs [51] will be created by 2025 in the area of disruptive ICT technologies which include AI and ML.

These disruptions and opportunities will lead to a change in the service operating model as ICT capital substitutes labour [52] in terms of replacing repeatable human tasks. As the service industry is driven by humans and it will be getting replaced by ICT capital in the form of disruptive technologies (Gartner. 2017) where AI and ML will play a major contribution as identified in the above analysis. Bots [53]-[54] are rule-based engines right now and it will be AI-based soon. The bot can help to replace routine and repeatable task and it can work 24x7 as well.

5. CONTRIBUTION

As AI and ML are emerging, the service operating model will be important to the service provider and enterprise as it helps to redefine service operational processes cost-effectively and provide better customer experience by improving service operational processes and time to market. The contribution in this study is helping service providers and enterprises to look for AI and ML disruption and quickly change or adapt to the situation to be competitive and industry-driven.

6. FURTHER WORK

AI is an emerging technology and it is quite dynamic as it is getting matured every day. As mentioned by Gartner [11], it will be in mainstream within 2 to 10 years and it is a must to watch this disruption and emergence for future work. The collected data were limited to only incident and event management since that specific environment was not using AI and ML for access and request management at this point. Hence this study suggests having future study for access and request management in service operation which is emerging and will be disruptive as well.

7. CONCLUSION

The use of AI and ML in IT Service operation is huge and it plays a major role in event and incident management at this point. AI and ML help to manage proactive event triggering and prediction which eliminates most of the human work. Once the proactive trigger is sent to the ITSM system, AI and ML also play a role in providing recommendations so that the automation engine or human can act and fix the issue faster. It means, AL and ML together with the automation engine is quite seamless to solve customer issues without any human unless otherwise human intervention is needed for physical The use of AI and ML in IT Service operation is huge and it plays a major role in event and incident management at this point. AI and ML help to manage proactive event triggering and prediction which eliminates most of the human work. Once the proactive trigger is sent to the ITSM system, AI and ML also play a role in providing recommendations so that the automation engine or human can act and fix the issue faster. It means, AL and ML together with the automation engine is quite seamless to solve customer issues without any human unless otherwise human intervention is needed for physical hands-on like power issue and physical hardware issue.

REFERENCES

1. Narayanan, K. (2008), "Managed IT services: the role of IT standards," Information Management and Computer Security, Vol. 16 No. 4, 2008 pp. 336-359 Emerald Group Publishing Limited
2. Bichler, M. and Bhattacharya, K. (2010). “IT Service Management and IT Automation, Methods and Models for Efficient IT Operations”, Business & Information Systems Engineering, BISE Editorial
3. Wui-Gee, T., Aileen, C-S. and Mark, T. (2009). “Implementing IT Service Management: A case study focusing on critical success factors”, Journal of Computer Information Systems
4. Ahmad, N., Amer, N.T., Quataifan, F. and Alhilai, A. (2013). “Technology adoption model and a road map to a successful implementation of ITIL”, Journal on Enterprise Information Management, Vol 26 NO. 5, 2013 pp. 553-576
5. Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. and Rance, S. (2007). “The IT Infrastructure Library, An Introductory Overview of ITIL V3”, Version 1.0. itSMF
6. Business Wire. (2018). “Survey: “, available at https://www.businesswire.com/news/home/20170817005392/en/Survey-82-Percent-ITSM-Professionals-Future-Roles (accessed 05 December 2019

7. Furmankiewicz, M., Solltysik, A., Ziuzianski, P. (2015). “Artificial intelligence systems for knowledge management in e-health: the study of intelligent software agents”, Latent Trends on Systems – Volume II, ISBN: 978-1-61804-244-6
8. Kietzmann, T., Paschen, J., and Treen, E. (2018). “Artificial Intelligence in Advertising: How Marketers Can Leverage AI along the Consumer Journey”, Journal of Advertising Research
9. Rizkallah, J. (2017). “The Big (Unstructured) Data Problem.” Forbes, June 5, 2017, available at https://www.forbes.com/sites/forbestechcouncil/2017/06/05/the-big-unstructured-data-problem/#2c0d2857493a (accessed 10 December 2019)
10. CIO Journal. (2016). “An Introduction to Robotic Process Automation”, available at http://deloitte.wsj.com/cio/2016/03/13/an-introduction-to-robotic-process-automation/ (accessed 02 December 2018)
11. Gartner Report. (2017), available at https://www.gartner.com/newsroom/id/3784363 (Accessed 04 December 2019)
12. Darrell, M. (2015). "What happens if robots take the jobs? The impact of emerging technologies on employment and public policy", Center for Technology Innovation at Brookings
13. Tom R. E. and Jon, I. (2015). “Strategizing IT service management through ITIL implementation: model and empirical test”, Total Quality Management & Business Excellence, published online 19 Aug 2015, http://www.tandfonline.com/doi/full/10.1080/14783363.2015.1075872
14. UCISA. (2018). “UCISA ITIL: Introducing Service Operation”, Community in University of Oxford, available at https://www.ucisa.ac.uk/representation/activities/ITIL/serviceoperation (accessed 07 November 2019)
15. Sauve, J., Moura, A. and Marques, F., (2009). “Business Driven Design of Infrastructures for IT Services”, Journal of Network Systems Management, 17:422-456
16. Stewart, H. and Yuk-Hee, C. (2008). “Improving service management in campus IT operations”, Campus-Wide Information Systems Vol. 25 No. 1, 2008 pp. 30-49
17. Cheng, M. (2010). “Event Monitoring and service in a flat world- Benefits and challenges”, IEEE Computer Society, 1520-9202/10
18. IMI. (2018). “The future of Identity and access management”, available at https://www.identitymanagementinstitute.org/the-future-of-identity-and-access-management/ (accessed 03 December 2019)
19. UCISA ITIL-AM. (2018). “U C I S A I T I L: A Guide to Access Management” University of Oxford, available at https://www.ucisa.ac.uk/-/media/files/members/activities/itil/service_operation/access_management/itil_a%20guide%20to%20access%20management%20pdf.ashx?la=en (accessed 04 December 2019)
20. Kenneth, G., Rich, D., and Chris, M. (2018). "Magic Quadrant for IT Service Management Tools", available at https://www.gartner.com/doc/reprints?id=1-5DCA8NO&ct=180821&st=sb (accessed on 05 December 2019)
21. Kloeckner, K., Davis, J., Fuller, N.C., Lanfranchi, G., Pappe, S., Paradkar, A., Shwartz, L., Surendra, M. and Wiesmann, D., 2018. “Transforming the IT Services Lifecycle with AI Technologies”
22. Cappelli, W., Fletcher, C. and Prasad, P. (2017). “Market Guide for AIOps Platforms” Gartner Report, available at https://www.gartner.com/doc/reprints?id=1-4CKWZWO&ct=170905&st=sb (accessed on 25 November 2019
23. CMDB Enrichment. (2019). “White Paper Preview: AIOps: A Guide to operation readiness – It is all about data”, available at https://sciencelogic.com/blog/whitepaper-preview-aiops-part2 (accessed on 07 February 2019)
24. Ayoubi et al. (2018). "Machine Learning for Cognitive Network Management," in IEEE Communications Magazine, vol. 56, no. 1, pp. 158-165, Jan. 2018.DOI: 10.1109/MCOM.2018.1700560
25. Padmavathy, S. (2018). “AI in ITSM”, available at https://freshservice.com/pdf/AI-in-ITSM.pdf (accessed on 05 December 2019)
26. Splunk AIOps. (2018). “AI Powered IT service Intelligence”, available at https://www.splunk.com/en_us/software/it-service-intelligence.html (accessed 28 November 2019)
27. Moogsoft AIOps. (2018). “AI for service management and Optimal Digital Business Processes”, available at https://www.moogsoft.com/resources/aiops/white-paper/ai-it-service-management, (accessed on 29 November 2019)
28. Sunder, M. V. 2016. “Lean Six Sigma Project Management – A Stakeholder Management Perspective.” The TQM Journal 28(1): 132–150
29. Xiaoyin. W, Lu. Z, Tao. X, John. A, and Jiasu. S. (2008). An approach to detecting duplicate bug reports using natural language and execution information. In Proceedings of the 30th international conference on Software engineering (ICSE '08). ACM, New York, NY, USA, 461-470. DOI: https://doi.org/10.1145/1368088.1368151
30. PR Newswire. (2018). "New Research from Advanced Threat Analytics Finds MSSP Incident Responders Overwhelmed by False-Positive Security Alerts. PR Newswire US"
31. Interfax. (2015). “ISS incident classed by U.S. experts as false alarm - NASA. Russia & FSU General News”, p. 1
32. Bruno. T, Abrahão. J. (2012). “False alarms and incorrect rejections in an information security center: correlation with the frequency of incidents. Work”, 2012;41:2902-2907.
33. Ruiz, L. B., Siqueira, I. G., Wong, H. C., Nogueira, J. M. S., & Loureiro, A. A. (2004). Fault management in event-driven wireless sensor networks. In Proceedings of

the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems (pp. 149-156). ACM

34. Clarke, J. (2009). Resilience under attack: Techniques for continuing online business in the face of security compromise. Journal of Business Continuity & Emergency Planning, 3(3), 222–226
35. Marcu. P, Shwartz. L, Grabarnik. G and Loewenstern. G. (2009). "Managing Faults in the Service Delivery Process of Service Provider Coalitions," 2009 IEEE International Conference on Services Computing, Bangalore, 2009, pp. 65-72. DOI: 10.1109/SCC.2009.41
36. Lapão, L. V. (2011). Organizational Challenges and Barriers to Implementing IT Governance in a Hospital. Electronic Journal of Information Systems Evaluation, 14(1), 37–45.
37. Badri, L. (2010). “Development of neural networks for noise reduction”. Int. Arab J. Inf. Technol., 7(3), 289-294
38. Wu, L., & Buyya, R. (2012). Service Level Agreement (SLA) in Utility Computing Systems. In V. Cardellini, E. Casalicchio, K. Castelo Branco, J. Estrella, & F. Monaco (Eds.), Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions (pp. 1-25). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-794-4.ch001
39. Chen, Y., Yang, X., Lin, Q., Zhang, H., Gao, F., Xu, Z., Dang, Y., Zhang, D., Hang Dong, Xu, Y., Li, H., and Kang, Y. (2019). “Outage Prediction and Diagnosis for Cloud Service Systems.
40. Salas, A., Georgakis, P., and Petalas, Y. (2017). "Incident detection using data from social media," 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), Yokohama, 2017, pp. 751-755. DOI: 10.1109/ITSC.2017.8317967
41. Guo, K., Lu, Y., Gao, H., and Cao, R. (2018). “Artificial Intelligence-Based Semantic Internet of Things in a User-Centric Smart City”. Sensors 2018, 18, 1341
42. Patrick, C. (2017). “IT Alerts: From Operational Trenches to AIOps”, available at https://www.bmc.com/blogs/it-alerts-from-operational-trenches-to-aiops/ (accessed on 07 February 2019)
43. Kumar, K. (2018). “Moogsoft’s machine learning and socialized workflows are the future of service assurance”, Available at https://www.moogsoft.com/wp-content/uploads/2018/08/Moogsoft_HCL_AWS_case-study-2018.pdf (access 04 December 2019)
44. Resolve. (2017). “AIOps Integrated with Incident Resolution is Pivotal for IT Operations”, available at https://www.resolvesystems.com/blog/aiops-integrated-incident-resolution-for-it-operations/ (accessed 30 November 2019)
45. Splunk. (2017). “AI for IT: Preventing outages with predictive Analytics”, available at https://www.splunk.com/pdfs/white-papers/artificial-intelligence-and-the-future-of-it-operations.pdf (accessed 29 November 2019)
46. Bishnu, N. and Enzo, S. (2018). “AIOps for dummies”, Fixstream special edition, available at https://fixstream.com/AIOps_For_Dummies_FixStream_Special_Edition_9781119529965.pdf, (accessed on 07 February 2019)
47. Zan, M. O., Shan, Z., Li, L. I., & Ai-Jun, L. I. U. (2007). “A predictive model of churn in telecommunications based on data mining”. In 2007 IEEE International Conference on Control and Automation (pp. 809-813). IEEE
48. Bendriss. J, Yahia. B, Chemouil.P and Zeghlache. D (2017), "AI for SLA Management in Programmable Networks," DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference, Munich, Germany, 2017,pp.1-8
49. Ohara, Y., Bhatia, M., Osamu, N., & Murai, J. (2003). “Route flapping effects on OSPF. In 2003 Symposium on Applications and the Internet Workshops”, Proceedings. (pp. 232-237). IEEE
50. Jordann, T. and Sunil, J. (2017). “Digital Disruption”, Economic Development Journal / Spring 2017 / Volume 16 / Number 2
51. Swissnex. (2017). “Consulate of General of Switzerland”, India’s Booming Digital Industry, available at https://www.swissnexindia.org/wp-content/uploads/sites/5/2017/09/ICT-Report.pdf (accessed 02 December 2019)
52. Michaels, G., Natraj, A. and Reenen, J. (2014). "Has ICT Polarized skill demand? Evidence from eleven countries over twenty-five years, The Review of Economics and Statistics, March, 96(1):60-77
53. Chatbot. (2018). “Chatbot examples”, available at https://botsociety.io/blog/2018/03/chatbot-examples/ (accessed on: 16 December 2019
54. RPA (2018): “Robotic Process Automation”, available at https://en.wikipedia.org/wiki/Robotic_process_automation (accessed 16 December 2019)
55. Churchman, M. (2016). “6 Essential steps to reducing incident resolution time”, available at https://www.pagerduty.com/blog/6-steps-reducing-incident-resolution-time/ (accessed 02 December 2019)
56. Rohani, H., & Roosta, A. K. (2014). Calculating Total System Availability. Information Services Organization KLM-Air France, Amsterdam
57. Manoj. B, Sasikanth.K.V, Subbarao. M.V, Prakash. J.V, (2018), “International Journal of Advanced Trends in Computer Science and Engineering”, 7(6), November -December 2018, 87- 90 https://doi.org/10.30534/ijatcse/2018/02762018
58. Singla, M. K., Gupta, J., Nijhawan, P., & Oberoi, A. S. (2019). Electrical Load Forecasting Using Machine Learning. International Journal, 8(3).
59. Alotaibi, N. M., Abdullah, M., & Mosli, H. (2019). Agent-based Big Data Mining. International Journal, 8(1.1).

8. ANNEXURE

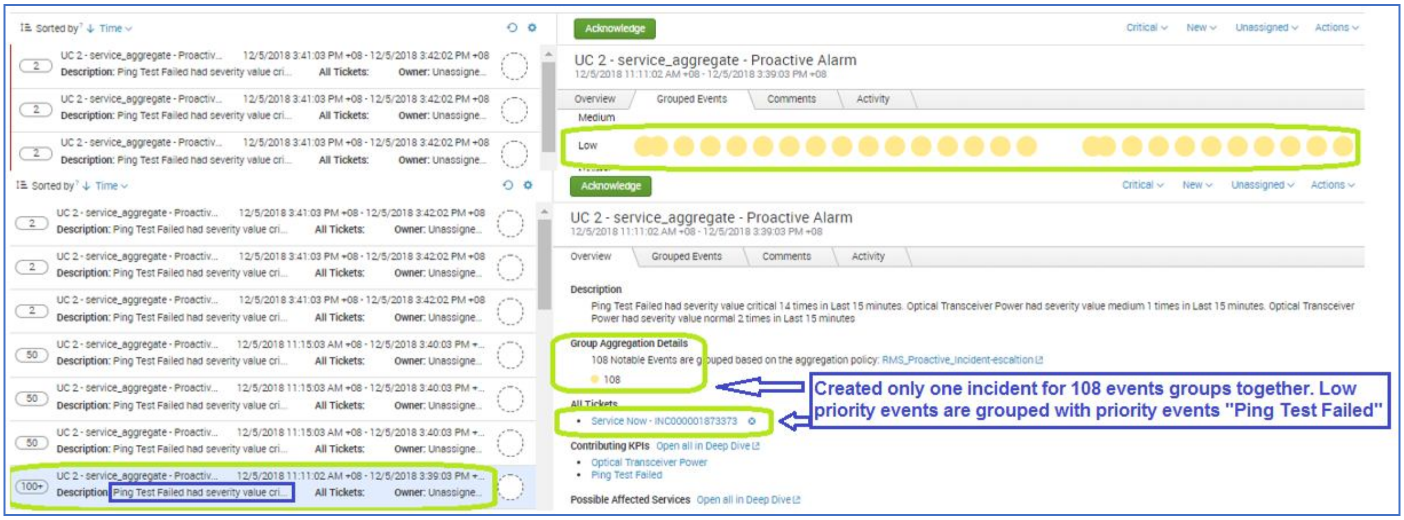

Figure 9: Correlation, suppression and grouping of events

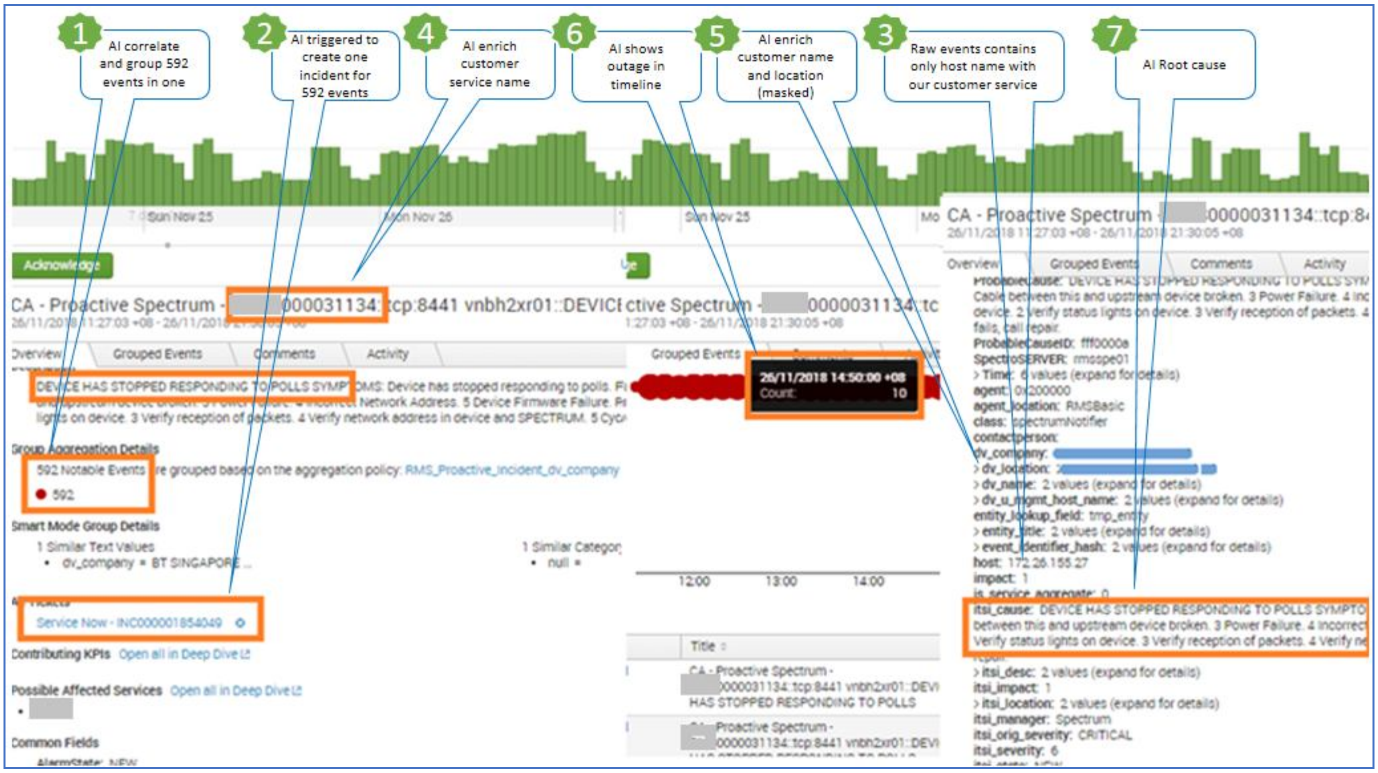

Figure 10 : End-to-End flow of AIOps in IT Service Operations