INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Incident Response Support Systems

Miguel Ângelo Rodrigues do Sacramento e Sousa

Master in computer engineering

Supervisor:
PhD Carlos Eduardo Dias Coutinho, Assistant Professor
ISCTE - Instituto Universitário de Lisboa

September,2024

TECNOLOGIAS
E ARQUITETURA

Department of Information Science and Technology

Incident Response Support Systems

Miguel Ângelo Rodrigues do Sacramento e Sousa

Master in Computer Engineering

Supervisor:
PhD Carlos Eduardo Dias Coutinho, Assistant Professor
ISCTE - Instituto Universitário de Lisboa.

September, 2024

Dedico à minha família pelas horas
perdidas e pelo apoio incansável.

Resumo

Os Sistemas de Gerenciamento de Tecnologias de Informação – *Information Technology Service Management* (ITSM) – são ferramentas ou soluções de software que ajudam na organização e gerenciamento dos serviços inerentes as tecnologias de informação, dando suporte à resolução de incidentes de tecnologias de informação, mantendo operacional e funcional o parque informático dessas organizações.

Os sistemas ITSM atualmente funcionam de modo completamente manual: os utilizadores, por meio de canais de comunicação (email, telefone, aplicação especialista, etc.), abrem incidentes no helpdesk ou contact center, de modo manual; subsequentemente, as equipas de gestão do serviço de apoio ao cliente criam incidentes na ferramenta ITSM. A primeira equipa de incidente é a "primeira linha", onde os incidentes podem ser resolvidos se o tema é do domínio dessa equipa. Caso essa equipa de primeira linha não seja capaz de resolver o incidente, o incidente é transferido para a segunda ou terceira linhas, que podem ser mais técnicas ou especialistas, para resolverem os incidentes.

O modo tradicional de resolver incidentes é difícil de operar, e consome muito tempo, devido à operação manual e dependente de muitos recursos humanos, o que torna a solução cara de operar.

Esta investigação ambiciona resolver este problema, usando a DSRM (Design Science Research Methodology) para investigar uma nova solução para uma resolução automática de incidentes usando tecnologia de nuvem e Generative AI (GenAI, também conhecida por LLM).

Palavras-chave: Sistemas de Suporte, resposta a incidente, automático, autónomo.

Abstract

Information Technology Service Management (ITSM) are tools or software solutions that assist in the organization and management of services inherent to information technologies, by helping solving incidents and keeping the IT portfolio of organizations operational and running.

ITSM systems currently work in a completely manual way, where users, via communication channels (email, phone, specialized application, etc.), open incidents in the helpdesk or contact center; subsequently, the customer service management teams manually create incidents in the ITSM tool. The first incident team is the “first line,” where incidents can be resolved immediately if the topic is in the knowledge domain of that team. If the first line team is not able to solve the incident, it is transferred or routed to second or third lines teams, which may be more technical or specialized in the incident resolution domain.

This traditional way of resolving incidents is difficult to operate and time consuming due to the underscored manual operation, and dependent on a lot of human resources using manual operations, which makes the solution expensive to operate.

This research aims to solve this problem, using the DSRM (Design Science Research Methodology) to investigate a new theoretical solution for an automatic incident resolution information system using cloud technology and Generative AI (GenAI, also known by LLM).

Keywords: Support Systems, incident response, automatic, autonomous.

Index

Table of Contents

Index of Figures

List of figures

Table of acronyms

List of acronyms	
Abbreviation	**Definition**
AI	Artificial Intelligence
AIR	Automatic incident resolution
API	Application Programming Interface
AIOPS	Artificial Intelligence for Information Technology Operations
BSM	Business Service Management
CNNs	Convolutional Neural Networks
DB	Database
DSRM	Design Science Research Methodology
DevOps	Development and IT Operations
GCNs	Graph convolutional networks
I&O	Infrastructure and operations
ID	Identification
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service management
IMS	Incident management software
GenAI	Generative AI
LLM	Large Language Model
MS	Monitoring Software
ML	Machine Learning
MOF	Microsoft Operations Framework
MTTR	Mean Time to Resolve
MSOs	Medium and small sized organizations
NLP	Natural Language Processing
RPA	Robotic process automation
RNN	Recurrent Neural Networks
VM	Virtual Machine
POC	Proof of concept

CHAPTER 1

Introduction

In the ever-evolving landscape of organizational management, the role of Information Technology (IT) has become increasingly pivotal. At the heart of every efficient IT strategy lies the Information Technology Service Management (ITSM) system, a comprehensive framework designed to oversee and streamline the vast array of services and infrastructure that underpin daily operations. Traditionally, these systems have relied on a passive ticketing approach, where users report incidents after they occur(Heikkinen & Jäntti, 2012). However, a paradigm shift has occurred with the emergence of proactive ITSM solutions, which leverage agents embedded within organizational infrastructure to automatically detect, report, and in some cases, resolve incidents in real time.

The transition from passive to active incident management within ITSM frameworks presents a significant opportunity for organizations to enhance operational efficiency, reduce costs, and optimize resource allocation. By automating routine tasks that would otherwise require human intervention, companies stand to benefit from streamlined processes, decreased downtime, and a more agile response to emerging issues (Engemann & Miller, 2024). This shift not only alleviates the burden on human resources but also enables personnel to focus their expertise on higher value, strategic initiatives, fostering innovation and driving competitive advantage in an increasingly dynamic market landscape.

However, despite the potential advantages offered by automated incident resolution, challenges persist in effectively implementing and optimizing these systems (Tae & Hung, 2020) . One of the key hurdles facing service providers is ensuring seamless integration and functionality of automated agents within existing ITSM infrastructure. Moreover, concerns regarding data security, reliability, and the potential for false positives necessitate careful consideration and robust safeguards to mitigate risks and ensure the integrity of automated incident management processes.

Nevertheless, the imperative to embrace automation within ITSM frameworks is undeniable. By harnessing the power of advanced technologies to augment and optimize traditional IT service delivery models, organizations can unlock new levels of efficiency, agility, and competitiveness (Sahid et al., 2017). As we navigate an increasingly digital future, the adoption of automated incident resolution mechanisms represents a critical step towards realizing the full potential of ITSM systems and empowering organizations (Jäntti & Hotti, 2016) to thrive in an everchanging business landscape.

Incident resolution in ITSM involves several steps (Al-Hawari & Barham, 2021): detection, logging, categorization, prioritization, investigation, resolution, and closure. Manual handling of these steps can be time consuming and error prone.

Generative AI refers to artificial intelligence systems capable of generating text, images, or other media in response to prompts. In the context of ITSM, Generative AI can assist in generating responses to incidents, categorizing issues, and suggesting solutions.(Frick et al., 2019)

This research work proposes to have monitoring agents in integrated monitoring and ITSM solutions that can automatically create events from IT portfolio, automatically transforming problems to ITSM incidents, and attempting to solve those incidents automatically proposing solutions inferred from the use of Generative AI.

The goal of the proposed solution is to have monitoring software integrate with incident management software, where events are generated automatically into incidents, and having incident management software integrated with generative AI API, where generative AI, can make inference about solutions for the related events/incidents. Solutions are triggered based on the previously incidents errors and resolution documentation of the technology manufacturers when previously trained the LLMs models of generative AI.

According to the ID or code, Generative AI, will trigger solutions based on the errors generated in the events when matched with the errors codes and solutions that were trained previously the LLMs. Besides that, it will be possible to insert repetitive tasks to be executed by the ITSM integrated tools, like agents in IT endpoints to automatically solve incidents by using scripts or robotic process automation (RPA) routines.

Learning from historical data from one or several or other ITSM systems will input machine learning incorporated within ITSM with a complete set of data to classify and prioritize resolution information to apply in any scenarios where this solution is applied and suitable to be applied.

Currently in the technology market there are some tools which publicize the autonomous resolution of an incident, from fetching the event failure, opening the incident ticket into the ITSM, solving the issue after some configured time to run the solution, and after that, closing the incident. But currently, when using those tools, we can see that these automatic tools have difficulties in categorizing the incidents and automatically solving them, and it turns most of time to manual execution for human intervention.

The advantages of the proposed solution in this research are to have integrated the monitoring software and the incident management software, and when an when an event is raised in the monitoring software it automatically is transformed in an incident in the incident management software, besides that with the integration of the incident management software and the Generative AI API, solutions previously trained in the LLM according to the manufacture errors codes when mapped with the incident events errors code could be raised and triggered as solutions to solve the incidents in the End-points technologies.

1.1 Research Methodology

This dissertation aims to analyze and discover practical implementation and impact of an automatic ITSM resolution solution to help organizations become more productive and liberate IT teams from repetitive tasks, liberating it to more complex tasks, to accomplish this goal it was chosen Design Science Research to aid provide the direction of a conceptual model and in the presentation of the scientific research artifacts.

For the application of DSRM, as the problem is already defined, from the four options: "problem-centered approach," "objective-centered approach," "design and development-centered approach" and "client/context initiated solution," the selected option was "problem-centered approach."

The first phase, Identify problem and motivate, in phase when the problem is defined, in this dissertation, this phase is described in the abstract and in the introduction.

The second phase defines objectives of a solution, objectives of a solution are defined, the objectives and defined in section 2.1 and chapter, where objectives based on the literature review are defined and described.

The third phase which is Design and development, with the focus in the development o f a solution, describes the development of a solution to the problem previously identified, is presented in chapter 3,

For the fourth phase, the demonstration phases, with the goal of finding a suitable context for the problem or use an artifact to solve the problem, was presented in chapter 4, an artifact, built using cloud technology and a solution for the design previously discovered.

For the evaluation phase, observe how effective and efficient the solution presented previously solved the problem, was described and presented in chapter 5.

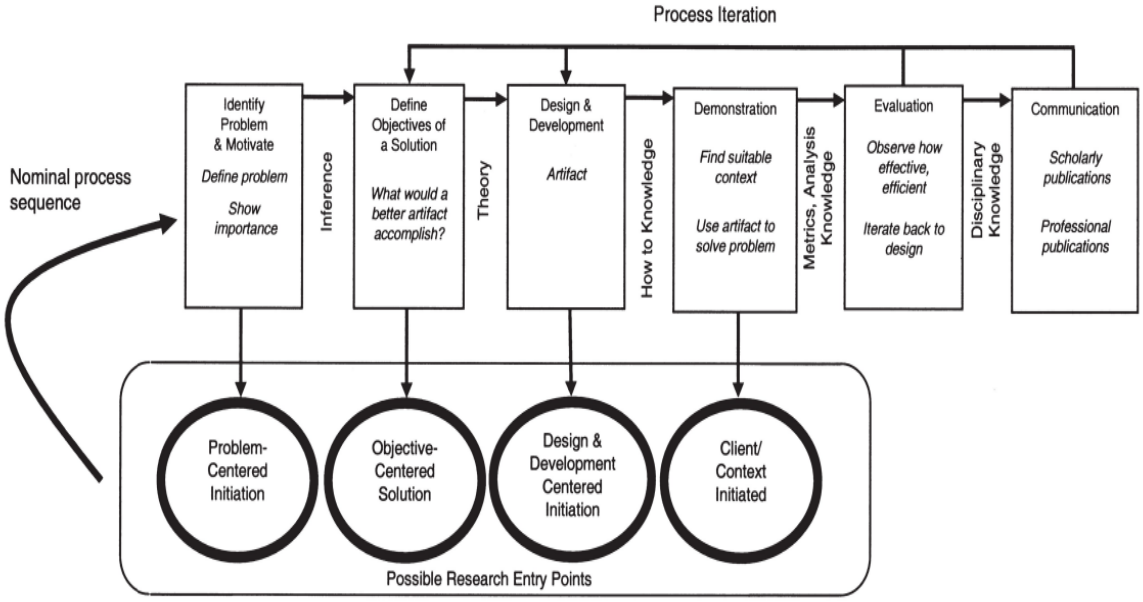

Figure 1. Design Science Research Methodology; (Peffers et al., 2008)

As stated in figure 1, above related to the application of DSRM, in the design and development phase, it is possible to iterate back to previous phase, the define objectives of a solution. and in the evaluation and communication phases it is possible to iterate back to both phases define objectives of a solution and design and development phases, to adjust the requirements of those phases and be possible to iterate again with the next phases.

1.2 Research Question

To elaborate a theoretical proposal for an automatic incident management system in this dissertation, the following research question was formulated.

How can Generative AI and LLM be effectively leveraged for optimizing IT incident management resolution processes, with a focus on developing intelligent systems that enhance identification, classification, and automated resolution of diverse IT incidents?

.

CHAPTER 2

Literature Review

2.1 State of the Art/Literature Review

To conduct the literature review of related works it was conducted a series of research in Springer, Elsevier and IEEE explore.

The research was conducted in the same way in the three databases, it was done using keywords.

The query used for the keywords were the following:

("Support Systems" OR "incident response" OR "ITSM") AND ("Automatic" OR "Autonomous") AND ("Machine Learning" OR Generative AI OR LLM OR Artificial Intelligence)

Besides the query by keywords a filter was used to illustrate the relevant work among the diversified results, including (Articles, written in English, from 2018 or later, in the area of Computer Science, in the area of Engineering, in the area of Artificial Intelligence, free and paid) and exclusive (Not being articles, Written in other than English, older than 2018, Not in an area of computer Science, Not in an area of Engineering, Not in the area of Artificial Intelligence, paid works) .

According to the results of the keywords and the filter applied it was obtained sixty-three papers, related to the application of machine learning and artificial intelligence to Information Technology Incident management.

2.2 Base ITSM technologies (alternatives analysis)

This subject was researched in several papers to make a review of base ITSM technologies to find solutions.

The process of adopting IT Service Management (ITSM) frameworks, particularly focusing on how ITSM improves efficiency, service quality, and alignment between IT and business goals. It explores common ITSM frameworks like ITIL (Information Technology Infrastructure Library) and examines the steps required to implement them effectively within IT departments. The article highlights the benefits of ITSM, including streamlined workflows, enhanced customer satisfaction, and better incident management. Additionally, it addresses challenges such as employee resistance, the need for proper training, and the investment of time and resources required for successful ITSM implementation(MacLean & Titah, 2023)

The article above provides a thorough overview of ITSM benefits but tends to downplay the potential complexities and risks associated with its implementation. While it addresses challenges like resistance and resource allocation, it does not delve deeply into potential long-term drawbacks or the possibility of organizational misalignment postimplementation. The focus on large-scale benefits could oversimplify the process for smaller organizations with limited resources. Furthermore, the article could have benefited from case studies or real-world examples to give a more nuanced understanding of ITSM's impact across different industries and contexts. Overall, while informative, the article's analysis remains surface level and lacks a deeper exploration of ITSM's potential pitfalls(MacLean & Titah, 2023)

Service Oriented IT Management: Benefit, Cost, and success factors, focuses on the concept of managing IT systems through a service-oriented approach. It explores the benefits of aligning IT services with business objectives, emphasizing improved efficiency, enhanced customer satisfaction, and better resource allocation. The article also discusses the costs involved in adopting a service-oriented IT model, such as infrastructure investment and training, while presenting key success factors including strong leadership, a sharp vision, and continuous monitoring. The aim is to demonstrate how IT services can be leveraged as strategic assets for organizational growth and agility.(Hochstein, Tamm, et al., 2005)

The article effectively highlights the advantages of service-oriented IT management, but it could provide more detailed analysis of the potential challenges organizations face during implementation. While it underscores cost considerations, it tends to overlook the complexities of integrating legacy systems and potential resistance to change from stakeholders. Furthermore, the emphasis on leadership and vision as success factors is valid, yet the article could benefit from discussing the specific metrics or tools that can be used to measure success. Overall, while informative, the article could be more comprehensive in addressing both the risks and practicalities of adopting a service-oriented IT approach.(Hochstein, Tamm, et al., 2005)

ITIL as Common Practice Reference Model for IT Service Management, Formal Assessment and Implications for Practice, examines ITIL (Information Technology Infrastructure Library) as a standard framework for IT service management (ITSM). It focuses on assessing ITIL's effectiveness and influence on organizational practices, evaluating its strengths and limitations in achieving IT service optimization. The authors provide a formal assessment of ITIL by reviewing its practical adoption, discussing its alignment with business needs, and highlighting its contributions toward process standardization. Moreover, the article discusses implications for IT service professionals, offering insights into how ITIL can support decision making and service improvements.(Hochstein, Zamekow, et al., 2005)

The article succeeds in providing a comprehensive evaluation of ITIL, clearly articulating its value as a widely adopted model for ITSM. However, the article could benefit from a more balanced discussion of potential challenges and limitations in ITIL implementation, such as rigidity or over standardization, which may hinder innovation in dynamic environments. Additionally, while the formal assessment of ITIL is thorough, more empirical data or case studies could have added depth to the argument by showing real world scenarios where ITIL either succeeded or faced practical limitations. The article overall presents ITIL as a strong framework but could include more nuanced perspectives on its adaptability and scalability in diverse organizational contexts.(Hochstein, Zamekow, et al., 2005)

Impact of IT Service Management Frameworks on the IT Organization, discusses the significance of implementing IT Service Management (ITSM) frameworks within IT organizations. It explores how ITSM frameworks, such as ITIL (Information Technology Infrastructure Library), can streamline IT processes, improve service delivery, and align IT services with business goals. The article highlights the positive effects of adopting these frameworks, including increased efficiency, enhanced communication, and better resource management. Additionally, it examines the challenges that organizations face in adopting ITSM frameworks, such as resistance to change, the complexity of implementation, and the need for continuous training and process optimization.(Marrone & Kolbe, 2011)

The article provides a solid overview of the benefits and challenges of implementing ITSM frameworks, it could benefit from a deeper exploration of specific case studies or empirical evidence that support its claims. The discussion on the challenges is generic, lacking detailed insights into how organizations can practically overcome resistance to change or complex implementation. Furthermore, the article assumes that adopting an ITSM framework will inherently lead to improvements without adequately addressing the variability in outcomes based on organizational culture, IT maturity, or resource availability. A more nuanced examination of how different frameworks perform in varying contexts would have enriched the analysis, making it more applicable to diverse IT environments.(Marrone & Kolbe, 2011)

Information Technology Service Management Models Applied to Medium and Small Organizations: A Systematic Literature Review" explores the application of IT service management (ITSM) models in medium and small sized organizations (MSOs). Through a comprehensive review of existing literature, the study aims to understand how ITSM frameworks, traditionally developed for large enterprises, can be adapted or optimized for smaller organizations. It identifies key challenges, benefits, and constraints associated with implementing ITSM in MSOs and examines specific models like ITIL and COBIT to assess their effectiveness in improving operational efficiency, service quality, and business alignment in smaller firms.(Melendez et al., 2016)

The article provides valuable insights into an underexplored area, ITSM, in medium and small organizations. By conducting a systematic literature review, it highlights the need for tailoring traditional ITSM models to meet the unique needs and limitations of MSOs, such as resource constraints and simpler IT infrastructures. However, the article could have benefited from a more in-depth analysis of specific case studies or empirical data to illustrate the practical challenges faced by MSOs in adopting these models. Additionally, while the review identifies existing gaps, it falls short in offering actionable recommendations or frameworks specifically designed for MSOs, which would have made its conclusions more impactful for both practitioners and researchers.(Melendez et al., 2016)

2.3 Other solutions in the market

The research papers described in this section provide an overview of other solutions that exist in the market which are focused on Information Technology Service Management of IT services operations.

Magic Quadrant for IT Service Management Tools by Gartner evaluates the competitive positioning of IT service management (ITSM) tool vendors based on their ability to execute and completeness of vision. It provides a framework for understanding which platforms lead the market, particularly for infrastructure and operations (I&O) leaders. The 2022 report highlights ten key vendors in the ITSM space, with ServiceNow and BMC consistently positioned as leaders due to their innovative capabilities, AI integration, and comprehensive service operations. Vendors like Atlassian and Ivanti also hold notable positions, with strengths in workflow management and customer service automation.(Matchett et al., 2017)

Gartner's Magic Quadrant is a valuable tool for decision making, it has limitations. The evaluation methodology favors large, established vendors, potentially sidelining smaller, niche players that may offer more tailored solutions for specific needs. Additionally, the report's emphasis on AI and automation trends highlights the growing shift toward digital transformation, but it may overlook the practical challenges companies face when implementing such advanced technologies. Therefore, while Gartner's insights are thorough, users should balance them with specific organizational needs and market trends to make informed decisions. (Matchett et al., 2017)

ServiceNow ITSM Overview provides a comprehensive summary of ServiceNow's IT Service Management (ITSM) platform, highlighting its capabilities in streamlining IT processes and improving service delivery. It discusses key features like incident, problem, and change management, along with knowledge management and self-service portals. ServiceNow's ITSM tools aim to enhance operational efficiency, minimize disruptions, and drive automation across IT departments. The platform's integration capabilities and data driven insights are emphasized as pivotal in transforming traditional IT service operations into more agile, responsive frameworks that align with business objectives.(ServiceNow, 2020)

The article offers a solid introduction to ServiceNow's ITSM, but it lacks a deeper examination of potential challenges or limitations of the platform, such as implementation complexity, cost concerns, or customization difficulties. While the article is informative in showcasing the advantages and features, it could benefit from a more balanced view by addressing potential pitfalls that organizations might face during adoption. Additionally, the focus remains primarily on the platform's offerings without discussing how it compares to other ITSM solutions in the market, which would provide readers with a more holistic perspective on the available options.(ServiceNow, 2020)

IBM Maximo Asset Management is a comprehensive software solution designed to manage physical assets across various industries. The system provides tools to oversee the lifecycle of assets, from procurement to disposal, allowing organizations to improve maintenance, optimize performance, and reduce costs. It integrates asset tracking, work management, inventory, and procurement, offering real time data analytics to support decision making. Maximo is known for its scalability, flexibility, and ability to handle complex asset management tasks, making it suitable for industries such as manufacturing, transportation, energy, and utilities.(Fahmi, 2016)

While IBM Maximo offers robust functionality and can significantly enhance operational efficiency, its complexity can be a barrier for smaller businesses or those without a dedicated IT infrastructure. The system's broad feature set often requires extensive customization and a learning curve, which can lead to higher implementation costs and longer deployment times. Furthermore, while its integration capabilities with other enterprise systems are a strength, these integrations can sometimes be challenging to implement without expert support. Despite these potential drawbacks, Maximo remains a powerful tool for organizations that need to manage large, diverse asset portfolios and are equipped to handle its technical demands.(Fahmi, 2016)

Aligning Business Service Management to Goals, An Integrated Approach at BMC Software" discusses how BMC Software adopted an innovative strategy to align its Business Service Management (BSM) with organizational goals. It details the integration of BSM tools and practices within the company's broader business strategy, enhancing service delivery and improving operational efficiency. By aligning IT services more closely with business objectives, BMC was able to streamline processes, improve decision making, and deliver more value to its customers. The article highlights the importance of adopting a holistic, purposeful approach to business service management for sustained competitive advantage.(Richardson & Mahfouz, 2011)

The article provides a thorough and practical insight into how BMC Software successfully implemented BSM strategies, but it may lack a deeper exploration of the challenges and risks associated with such integration. While the focus on aligning BSM with business goals is commendable, the article primarily showcases the benefits without adequately addressing potential pitfalls, such as the complexities of cultural change, resistance from employees, or the costs of transitioning to a new system. Furthermore, while the case study is relevant, it could benefit from broader examples across different industries to give a more diverse perspective. Overall, the article is insightful but could use more balance by including both the successes and challenges of aligning BSM with organizational goals.(Richardson & Mahfouz, 2011)

2.4 Tools that may be used in the solution.

The research papers in the section provide a list of tools and techniques that may be used in the proposed ITSM solution to solve the ITSM manual incident resolution problem.

The Utilization of Artificial Intelligence for Improving Incident Management explores how artificial intelligence (AI) technologies are being integrated into incident management systems across various sectors. It highlights the potential of AI to enhance response times, streamline communication, and facilitate better decision-making during incidents. The article discusses several case studies where AI has successfully improved incident detection, prioritization, and resolution, emphasizing its role in predictive analytics and real time monitoring. By showcasing various AI tools and methodologies, the article aims to illustrate the transformative impact of AI on incident management, leading to increased efficiency and effectiveness in handling emergencies.(Frick et al., 2019)

The article effectively outlines the benefits of integrating AI into incident management, it tends to overlook some critical challenges and limitations associated with such technologies. For instance, reliance on AI may lead to overconfidence in automated systems, potentially undermining human judgment during crises. Moreover, the article could provide a more balanced view by discussing the ethical implications of AI in incident management, such as data privacy concerns and the risk of algorithmic bias. Additionally, while case studies are useful, they may not represent the full spectrum of incidents faced by organizations, leaving readers with a narrow understanding of AI's applicability. A more comprehensive approach that includes potential drawbacks and varied case studies would enhance the article's credibility and depth.(Frick et al., 2019)

Adopting Artificial Intelligence in ITIL for Information Security Management—Way Forward in Industry 4.0" explores the integration of Artificial Intelligence (AI) within the Information Technology Infrastructure Library (ITIL) framework to enhance information security management in the context of Industry 4.0. It discusses the challenges faced by organizations in managing information security and the potential benefits of incorporating AI technologies, such as machine learning and data analytics, to improve threat detection, incident response, and risk management. The authors present a conceptual model for implementing AI in ITIL processes, emphasizing the importance of aligning Ai driven strategies with business objectives to foster a proactive security posture.(Rajagopal & Ramkumar, 2023)

The article provides a comprehensive overview of the benefits and challenges associated with integrating AI into ITIL for information security management. It may overlook some critical factors that could affect implementation success. For instance, the discussion could benefit from a deeper exploration of the ethical implications of AI in security management, including biases in algorithms and the potential for overreliance on automated systems, which could lead to complacency among human operators. Additionally, the proposed conceptual model lacks practical case studies or empirical evidence that could substantiate the claims made regarding AI's effectiveness in enhancing information security. A more balanced approach that includes potential pitfalls alongside benefits would provide a clearer picture of the complexities involved in this integration, making the article more valuable to practitioners seeking to navigate the evolving landscape of information security in Industry 4.0.(Rajagopal & Ramkumar, 2023)

Machine Learning in IT Service Management explores the transformative impact of machine learning (ML) technologies on the processes and efficiency of IT service management (ITSM). It discusses how ML algorithms can analyze vast amounts of data generated within IT environments, enabling predictive analytics that enhance decision making and problem solving. The article outlines specific use cases where ML improves incident management, service desk operations, and change management, showcasing the potential for automation and improved user experience. Furthermore, it highlights the challenges organizations face in integrating ML into existing ITSM frameworks, including data quality, privacy concerns, and the need for skilled personnel.(Zuev et al., 2018)

The article presents a comprehensive overview of the benefits and challenges of implementing machine learning in IT service management, it could benefit from a deeper exploration of the potential ethical implications and biases inherent in ML algorithms. The discussion primarily focuses on operational efficiency and productivity, which, although crucial, may overlook the importance of human factors and the need for a balanced approach that prioritizes user privacy and trust. Additionally, the article could provide more concrete examples or case studies that illustrate the successful implementation of ML in diverse organizational contexts, which would strengthen its arguments and provide practical insights for IT managers. Overall, while the article serves as a useful introduction to the subject, a more nuanced analysis would enhance its depth and relevance in the rapidly evolving field of IT service management.(Zuev et al., 2018)

Performance of Machine Learning Algorithms for IT Incident Management explores the effectiveness of various machine learning (ML) algorithms in the context of managing IT incidents. It analyzes multiple algorithms, including supervised and unsupervised learning techniques, and evaluates their performance based on metrics such as accuracy, precision, recall, and F1score. The study presents a comparative analysis of the algorithms' capabilities in automating incident classification, prioritization, and resolution, emphasizing the potential for improving efficiency and reducing response times in IT service management. By leveraging real world incident data, the research highlights the practical implications and benefits of implementing machine learning in IT incident management processes.(Prihandono et al., 2020)

The article provides valuable insights into the application of machine learning in IT incident management, several areas warrant further consideration. The research primarily focuses on performance metrics without delving deeply into the context of how these algorithms adapt to the ever-changing nature of IT incidents, which can vary significantly in complexity and scale. Additionally, the article could benefit from a more comprehensive discussion on the challenges and limitations of deploying these algorithms in real world scenarios, such as data quality issues, algorithm interpretability, and the need for continuous learning. Furthermore, the comparative analysis, while informative, might overlook the influence of domain specific factors that could affect the performance of machine learning algorithms in different organizational contexts. Addressing these aspects would provide a more holistic understanding of the potential and limitations of machine learning in enhancing IT incident management.(Prihandono et al., 2020)

Automation of Incident Response and IT Ticket Management by ML and NLP Mechanisms, explores the integration of machine learning (ML) and natural language processing (NLP) technologies to enhance the efficiency and effectiveness of incident response and IT ticket management processes. It discusses how these advanced technologies can streamline ticket classification, prioritize incidents based on urgency, and automate responses to common issues, thus reducing the workload on IT support teams. The article also highlights the potential for ML and NLP to analyze historical ticket data to identify patterns and improve future incident handling, leading to a more proactive approach in IT service management.(Subbarao et al., 2022)

The article presents a compelling case for the use of ML and NLP in automating incident response and IT ticket management, it could benefit from a more nuanced exploration of potential challenges and limitations. For instance, the article primarily focuses on the benefits of automation, such as increased efficiency and reduced response times, but it overlooks issues like the quality of the training data for ML algorithms and the potential for bias in NLP applications. Additionally, the article could address the importance of human oversight in automated systems to ensure that complex or sensitive issues are handled appropriately. By providing a balanced view that includes both advantages and drawbacks, the article would better equip readers to understand the full scope of implementing these technologies in real world IT environments.(Subbarao et al., 2022)

Classification and Pattern Extraction of Incidents: A Deep Learning Based Approach" explores the application of deep learning techniques for the classification and analysis of incident data. The authors present a novel framework that utilizes various deep learning models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to effectively categorize incidents and extract meaningful patterns from complex datasets. Through empirical studies, the research demonstrates the effectiveness of these models in improving accuracy and efficiency compared to traditional machine learning methods. Additionally, the article discusses the significance of incident classification in various domains, such as cybersecurity and emergency response, highlighting the potential of deep learning in enhancing decision making processes.(Sarkar et al., 2022)

The article presents a comprehensive approach to incident classification using deep learning, it may fall short in addressing the limitations and challenges inherent in deploying these models in real world scenarios. For instance, the reliance on extensive labeled datasets may hinder the practicality of the proposed methods, especially in fields where data scarcity is an issue. Furthermore, the discussion on interpretability and transparency of deep learning models is minimal; without a clear understanding of how these models derive their classifications, stakeholders may be reluctant to trust the results. Additionally, the potential biases in the training data could lead to skewed outcomes, which is a critical consideration in sensitive applications like cybersecurity. Overall, while the research contributes valuable insights into deep learning applications for incident classification, a more nuanced exploration of its limitations and ethical implications would strengthen the article's impact.(Sarkar et al., 2022)

Automatic Thai Ticket Classification by Using Machine Learning for IT Infrastructure Company, explores the application of machine learning techniques in automating the classification of service tickets within an IT infrastructure company in Thailand. It discusses the challenges associated with manual ticket classification, such as inefficiency and potential errors, and presents a machine learning framework designed to enhance accuracy and speed in processing incoming support requests. The study employs various algorithms to analyze and categorize tickets based on their content, demonstrating a significant improvement in operational efficiency. (Khowongprasoed & Titijaroonroj, 2022)

The article presents a compelling case for the use of machine learning in automating ticket classification, it could benefit from a more comprehensive evaluation of the methodologies employed. Although it outlines the machine learning models used, such as decision trees or neural networks, there is a lack of detailed discussion regarding the selection criteria for these models, their performance metrics, and potential limitations. Additionally, the practical implications of implementing such a system in real world scenarios are not fully addressed, including considerations of data privacy and the need for human oversight in complex cases. A more nuanced analysis of these factors would provide a deeper understanding of the effectiveness and applicability of machine learning in IT service management.(Khowongprasoed & Titijaroonroj, 2022)

Machine Learning Supervised Analysis for Enhancing Incident Management Process explores the application of supervised machine learning techniques to improve incident management within organizations. It outlines the traditional challenges faced in incident management, such as inefficient data handling and slow response times, and presents machine learning as a viable solution to streamline these processes. The authors detail various machine learning algorithms and their effectiveness in analyzing historical incident data, predicting incident trends, and automating responses. By leveraging data driven insights, the article argues that organizations can significantly enhance their incident management capabilities, leading to faster resolution times and improved overall operational efficiency.(Mustapha et al., 2020)

The article presents a compelling case for integrating machine learning into incident management processes, it falls short in addressing some critical challenges associated with implementation. For instance, the discussion lacks a thorough examination of the potential barriers organizations may face, such as data quality issues, the need for skilled personnel, and the complexities of integrating machine learning systems with existing IT frameworks. Furthermore, the article could benefit from empirical case studies or quantitative analyses demonstrating the effectiveness of the proposed machine learning methods in real world scenarios. Additionally, ethical considerations, such as data privacy and algorithmic bias, are not adequately addressed, which are crucial aspects of deploying AI technologies in incident management. Overall, while the article offers valuable insights, a more balanced approach that considers both the advantages and challenges of machine learning in incident management would enhance its credibility and applicability.(Mustapha et al., 2020)

explores the application of machine learning techniques to enhance the ticketing process by addressing the complexities inherent in ticketing datasets. It aims to determine the optimum features that influence ticketing decisions, thereby improving the efficiency and effectiveness of eticketing systems. By analyzing various datasets, the authors apply different machine learning algorithms to identify significant patterns and features that can optimize the ticketing experience for both consumers and service providers. The study underscores the importance of data preprocessing and feature selection in achieving accurate predictions, providing insights into how machine learning can streamline operations in eticketing platforms.(Mohd Jamaludin et al., 2023)

The article presents a relevant and timely topic, particularly given the increasing reliance on digital solutions in various sectors, its analysis could be strengthened by a more comprehensive discussion of the limitations and challenges associated with machine learning in eticketing. The authors primarily focus on the algorithms and feature selection methods but do not sufficiently address potential biases in the dataset or the implications of overfitting, which could significantly impact the reliability of the findings. Furthermore, the article could benefit from a comparison with existing solutions or frameworks to illustrate the practical implications of the proposed machine learning strategies. Overall, while the study provides valuable insights into feature optimization in eticketing, it would be enhanced by a more nuanced understanding of the complexities and limitations of the methodologies employed.(Mohd Jamaludin et al., 2023)

Empowering Recommender Systems in ITSM: A Pipeline Reference Model for Ai Based Textual Data Quality Enrichment" discusses the integration of artificial intelligence (AI) techniques to enhance the effectiveness of recommender systems within IT Service Management (ITSM). It presents a comprehensive pipeline reference model that outlines the processes and methodologies for enriching textual data quality, which is crucial for generating reliable recommendations. The authors emphasize the importance of data quality in driving decision making processes and propose a systematic approach to improve data through various Ai based techniques, including natural language processing (NLP) and machine learning. By focusing on enriching textual data, the article aims to provide a framework that ITSM professionals can utilize to create more accurate and user centric recommendations.(Reinhard et al., 2023)

The article presents a well-structured pipeline reference model for enhancing recommending systems in ITSM, it could benefit from a more extensive discussion on the practical challenges and limitations of implementing such Ai based solutions in real world scenarios. Although the theoretical foundation is solid, the authors do not address potential barriers such as data privacy concerns, the need for significant computational resources, or the skill gaps in ITSM teams regarding AI technologies. Additionally, the reliance on textual data quality raises questions about the model's adaptability to various data formats and sources commonly encountered in IT environments. A more balanced perspective that includes these practical considerations would enhance the article's applicability and provide ITSM professionals with a more comprehensive understanding of the implications of adopting Ai driven recommender systems.(Reinhard et al., 2023)

Towards Intelligent Incident Management: Why We Need It and How We Make, explores the critical necessity for intelligent incident management systems in today’s fast paced, technology driven environments. It discusses the increasing complexity of incidents in various sectors, including IT and public safety, and highlights how traditional incident management approaches often fall short in addressing these challenges. The authors advocate for integrating advanced technologies like artificial intelligence and machine learning to enhance incident detection, response, and recovery processes. They present a framework for implementing intelligent incident management that emphasizes proactive measures, real time data analysis, and improved communication among stakeholders.(Chen et al., 2020)

While the article effectively outlines the pressing need for intelligent incident management and offers a forward-thinking framework, it could benefit from a more detailed examination of potential challenges in implementation. The reliance on AI and machine learning, while promising, raises concerns regarding data privacy, ethical implications, and the need for comprehensive training for personnel. Additionally, the article could have included case studies or empirical data to support its claims about the effectiveness of intelligent systems, making the arguments more persuasive. Overall, while the vision for intelligent incident management is compelling, a balanced discussion of both the opportunities and risks involved would provide a more nuanced perspective on this evolving field.(Chen et al., 2020)

Classification and Pattern Extraction of Incidents: A Deep Learning Based Approach" presents a novel framework utilizing deep learning techniques for the classification and pattern extraction of incidents, particularly in the context of data from incident reports. It explores the effectiveness of various deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), in analyzing incident data, identifying key features, and classifying incidents into predefined categories. The authors employ a robust dataset to validate their approach, demonstrating that their deep learning model significantly outperforms traditional methods in terms of accuracy and efficiency, thus providing valuable insights into incident trends and facilitating better decision making in incident management.(Sarkar et al., 2022)

The article presents a compelling case for the application of deep learning in incident classification and pattern extraction, it falls short in addressing several critical aspects. First, the generalizability of the findings is questionable, as the study relies on a specific dataset that may not fully represent the diverse nature of incidents encountered in real world scenarios. Additionally, the authors do not sufficiently discuss the limitations of deep learning models, such as their opacity and the potential for bias in training data, which could lead to erroneous classifications. Furthermore, the practical implementation of these models in operational settings is not thoroughly explored, leaving readers with unanswered questions about the integration of such advanced techniques into existing incident management systems. Overall, while the framework proposed is innovative, a more comprehensive discussion on its applicability and limitations would enhance the article's contribution to the field.(Sarkar et al., 2022)

The article "Machine Learning Approach to Quick Incident Response" explores the application of machine learning techniques in enhancing the efficiency and speed of incident response in various domains, particularly in cybersecurity. It discusses the challenges organizations face in managing incidents, including the high volume of data and the need for real time analysis. The authors present several machine learning models designed to automate and improve the detection, classification, and prioritization of incidents, thus enabling faster decision making and resource allocation. By leveraging historical incident data, the proposed models aim to reduce response times and improve overall incident management effectiveness.(Nila et al., 2020)

The article presents a compelling case for integrating machine learning into incident response strategies, it could benefit from a deeper exploration of potential limitations and challenges associated with implementation. The reliance on historical data for training machine learning models raises concerns about data quality and bias, which could affect the accuracy of incident predictions. Additionally, the article briefly touches on the need for human oversight in the decision-making process, yet it does not adequately address how organizations can balance automation with the expertise required for effective incident response. Furthermore, practical case studies or examples demonstrating the successful application of these models in real world scenarios would strengthen the article’s claims and provide readers with tangible insights into the feasibility and impact of these approaches.(Nila et al., 2020)

The article "Machine Learning in IT Service Management" explores the transformative role of machine learning (ML) technologies in enhancing IT service management (ITSM) practices. It discusses various applications of ML in areas such as incident management, problem resolution, and service optimization, highlighting how these technologies can automate processes, predict service outages, and improve user experience. The article also delves into the integration of ML with existing ITSM tools, emphasizing the benefits of data driven decision making and increased operational efficiency. Real world case studies and examples illustrate the practical implementation of ML in ITSM environments, showcasing the potential for reduced costs and enhanced service delivery.(Zuev et al., 2018)

While the article effectively outlines the benefits and applications of machine learning in IT service management, it may oversimplify some of the challenges associated with implementation. For instance, it glosses over the complexities of data quality, integration with legacy systems, and the need for a cultural shift within organizations to adopt Ai driven solutions. Additionally, the article could benefit from a deeper exploration of ethical considerations and the potential risks of reliance on automated systems, such as bias in decision making or job displacement. By providing a more balanced view that addresses both the advantages and potential pitfalls of ML in ITSM, the article would offer a more comprehensive understanding of the topic.(Zuev et al., 2018)

The article "Predicting Help Desk Ticket Reassignments with Graph Convolutional Networks" explores the application of advanced machine learning techniques, specifically graph convolutional networks (GCNs), to enhance the efficiency of help desk operations. It addresses the challenges associated with ticket reassignments, which often lead to delays and customer dissatisfaction. By leveraging GCNs, the authors aim to create a predictive model that can accurately forecast when and why tickets are likely to be reassigned based on various attributes, such as ticket history, relationships between tickets, and the expertise of help desk agents. The study presents a comprehensive analysis of the model's effectiveness through experiments on real world datasets, demonstrating its potential to optimize help desk workflows and improve response times.(Schad et al., 2022)

While the article presents a novel approach to predicting help desk ticket reassignments using graph convolutional networks, it could benefit from a more thorough discussion of the limitations and potential biases inherent in the data used. The reliance on historical ticket data may inadvertently reinforce existing patterns or biases in ticket handling, which could lead to inequities in service response. Additionally, the implementation of GCNs, though promising, might require significant computational resources, raising questions about scalability in larger organizational settings. The article could also delve deeper into the implications of these predictions for human decision making, considering how automated predictions might interact with the intuition and expertise of human agents. Overall, while the findings are significant, a more nuanced exploration of these factors would strengthen the article's contribution to the field.(Schad et al., 2022)

Process Automation 2.0 with Generative AI Framework discusses the evolution of process automation, highlighting the integration of generative AI technologies into traditional automation frameworks. It explores how generative AI enhances existing automation capabilities by enabling more intelligent decision making, improving process efficiency, and reducing operational costs. The authors illustrate this transformation through real world examples and case studies, demonstrating the potential of generative AI to not only automate repetitive tasks but also to create adaptive systems that learn and evolve. Additionally, the article emphasizes the importance of collaboration between humans and AI, suggesting that a synergistic approach can lead to innovative solutions in various sectors.(Mandvikar & Achanta, 2023)

While the article presents a compelling overview of the benefits of integrating generative AI into process automation, it could benefit from a more critical examination of the potential challenges and ethical considerations associated with this technology. For instance, issues such as data privacy, algorithmic bias, and the implications of reduced human oversight are mentioned but not deeply explored. Furthermore, the article focuses on the positive outcomes of generative AI, potentially overlooking the risks that come with its implementation, such as job displacement and the need for substantial upskilling in the workforce. A more balanced approach that addresses these concerns would provide a fuller understanding of the landscape of process automation in the age of AI, fostering a more informed discussion about its future trajectory.(Mandvikar & Achanta, 2023)

Towards Intelligent Automation (IA): Literature Review on the Evolution of Robotic Process Automation (RPA), Its Challenges, and Future Trends, provides a comprehensive overview of the development and progression of RPA technologies within the broader context of intelligent automation. It reviews existing literature to trace the evolution of RPA, highlighting key advancements, methodologies, and applications across various industries. The article also identifies significant challenges that organizations face in implementing RPA, such as technical limitations, integration issues, and workforce resistance. Furthermore, it discusses future trends in intelligent automation, emphasizing the potential for enhanced efficiency, improved decision making, and the integration of artificial intelligence (AI) to create more adaptable and autonomous systems.(Siderska et al., 2023)

The article offers valuable insights into the evolution of RPA and its future trajectory, it may lack depth in addressing the socioeconomic implications of automation on the workforce. The analysis of challenges tends to focus on technical and operational aspects, potentially underestimating the human factor and the necessity for organizational change management strategies. Furthermore, while the discussion on future trends is thought-provoking, it could benefit from a more critical examination of ethical considerations surrounding the deployment of intelligent automation. By incorporating these perspectives, the article could provide a more holistic view of the impact of RPA and intelligent automation, encouraging organizations to adopt a balanced approach that considers both technological advancements and their implications for employees and society.(Siderska et al., 2023)

2.5 AI Technologies Applied to ITSM

2.5.1 Automated Incident Management

Chatbots and virtual Agents; (Godse et al., 2018): AI driven chatbots can handle routine queries, provide instant support, and escalate complex issues to human agents. They use Natural Language Processing (NLP) to understand and respond to user requests.

Self-Healing Systems; (Ugwuanyi et al., 2020): AI systems can detect anomalies and trigger automated responses to resolve issues without human intervention. This includes automated patching, restarting services, or reallocating resources.

2.5.2 Predictive Analytics

Incident Prediction: AI algorithms analyze historical incident data to predict future issues, enabling pre-emptive actions to prevent downtime. Machine Learning (ML) models can identify patterns and predict potential failures.

Root Cause Analysis: AI can sift through large datasets to identify the root causes of recurring incidents, reducing the time and effort required for human analysis.

2.5.3 Enhanced User Experience

Personalized IT Support: AI can tailor support based on user profiles and previous interactions, providing a more customized support experience.

Automated Knowledge Management: AI can curate and update knowledge bases automatically, ensuring that support agents and users have access to the most relevant and UpToDate information.

2.6 Key Players and Solutions

2.6.1 ServiceNow

AI and ML Integration: ServiceNow's ITSM solution incorporates AI to automate routine tasks, provide predictive analytics, and enhance decision making processes. Features like Virtual Agent and Predictive Intelligence streamline incident management and improve user experience.(ServiceNow, 2020)

2.6.2 BMC Helix

Cognitive Automation: BMC Helix uses AI for cognitive automation, offering capabilities like predictive service management, anomaly detection, and automated resolution. The platform's AI driven insights help in proactive problem resolution.(Hertvik, 2016)

2.6.3 IBM Watson AIOps

AI for IT Operations: IBM Watson AIOps applies AI to monitor, detect, and resolve IT incidents in real time. The platform integrates with ITSM tools to provide predictive alerts and root cause analysis, enhancing incident management efficiency.

2.6.4 Atlassian Jira Service Management

Intelligent Automation: Atlassian's solution leverages AI for automation of repetitive tasks, intelligent ticket routing, and predictive analytics. Integration with Opsgenie and other tools enhances incident response and management.

2.6.4 Micro Focus SMAX

Machine Learning: Micro Focus SMAX utilizes ML to provide automated ticket categorization, intelligent virtual agents, and predictive analytics. The platform's AI capabilities support faster incident resolution and improved service delivery.

2.6.5 Industry Trends and Future Directions

Increased Adoption of AI: Organizations are increasingly adopting AI driven ITSM solutions to enhance operational efficiency and user satisfaction.

Focus on Proactive Management: AI is shifting ITSM from a reactive to a proactive approach, with a focus on preventing incidents before they occur.

Integration with DevOps and AIOps: ITSM is integrating more closely with DevOps practices and AIOps platforms to provide a unified approach to incident management and operational efficiency.

Continuous Learning and Improvement: AI models in ITSM are continually learning from new data, improving their accuracy and effectiveness over time.

CHAPTER 3

Technology Stack and Solution Architecture

3.1 Technology Stack

A new paradigm of computing environment known as cloud computing is being used by organizations worldwide, where the information technology infrastructure is being hosted in cloud computing environment, taking precedence over the more traditional approach of hosting the IT resource on-premises.

Organizations are using a diversified set of computing constructs from pure cloud hosting to hybrid cloud computing environment.

The goal in this dissertation is to use a hybrid approach for cloud environment to implement the proposed solution, using hybrid cloud, specifically azure cloud, with resources created in the cloud and other resources created on-premises as depicted in figure 2.

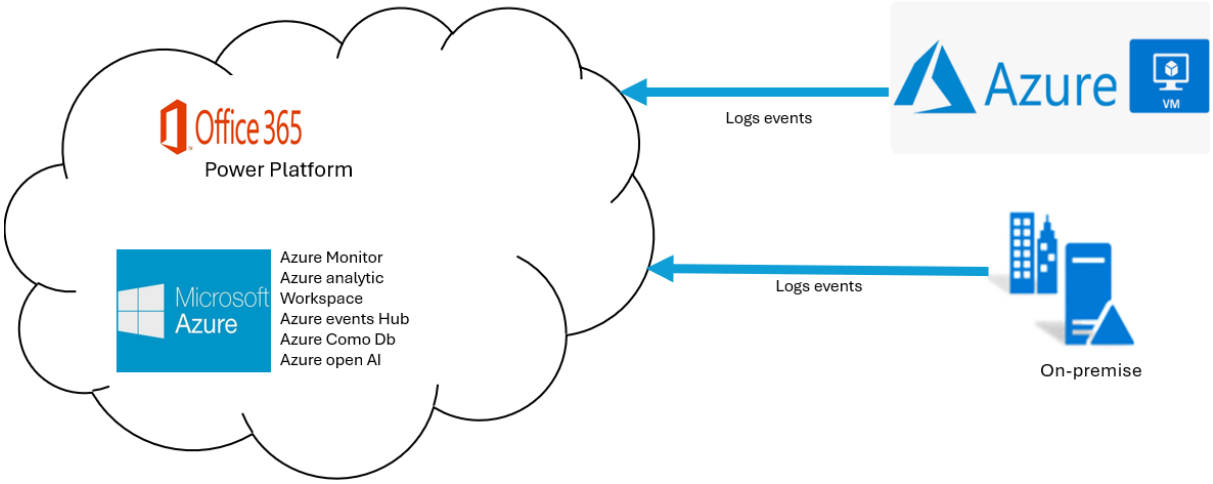

Figure 2. Cloud Technology Stack

Monitoring Software: with the scope of simulating the monitoring software to collect events in the technological environment, the monitoring software from "Microsoft" Azure Monitor was chosen.

Azure Monitor is a comprehensive monitoring solution for collecting, analyzing, and responding to monitoring data from your cloud and on-premises environments. You can use Azure Monitor to maximize the availability and performance of your applications and services. It helps you understand how your applications are performing and allows you to respond to system events manually and programmatically.

Azure Monitor collects and aggregates the data from every layer and component of your system across multiple Azure and non-Azure subscriptions and tenants. It stores it in a common data platform for consumption by a common set of tools that can correlate, analyze, visualize, and/or respond to the data. You can also integrate other Microsoft and non-Microsoft tools.

Incident management software; The incident management software allows you to manage the incident lifecycle from the capture, classification, routing, resolution and closure of the incidents generated in the IT portfolio, usually associated with a service management framework such as ITIL (Information Technology Infrastructure Library) and service levels agreed between the service provider and the customer(s) are associated. To demonstrate this solution in this dissertation, the Microsoft PowerApps platform was chosen.

Power Apps is a collection of apps, services, and connectors, as well as a data platform, which provides a quick development environment for you to build custom apps for your business needs. Using Power Apps this, you can quickly create custom business applications that connect to your data stored in the underlying data platform (Microsoft Dataverse) or in many online and on-premises data sources (such as SharePoint, Microsoft 365, Dynamics 365, SQL Server,etc).

3.2 Solution Architecture

The goal is to implement an ITSM that automatically receives incidents from events logs by agents monitoring collect the events logs from the IT portfolio (applications, databases, virtual machines, networks, storage, cloud resources), automatically transform the logs into incidents, those incidents stay in the state of new incident, and automatically, the generative AI, takes the new incidents and search for the wiki or ITSM solution database, find a solution in historical data or in large language model, finding the solution, sends the feedback resolution to the endpoint agent with the information correlated to the incident and the endpoint agent, applies the solution and sends a message to ITSM to change the status of the incident from new to solved. All new incidents without solution will be routed to the correct team for manual intervention.

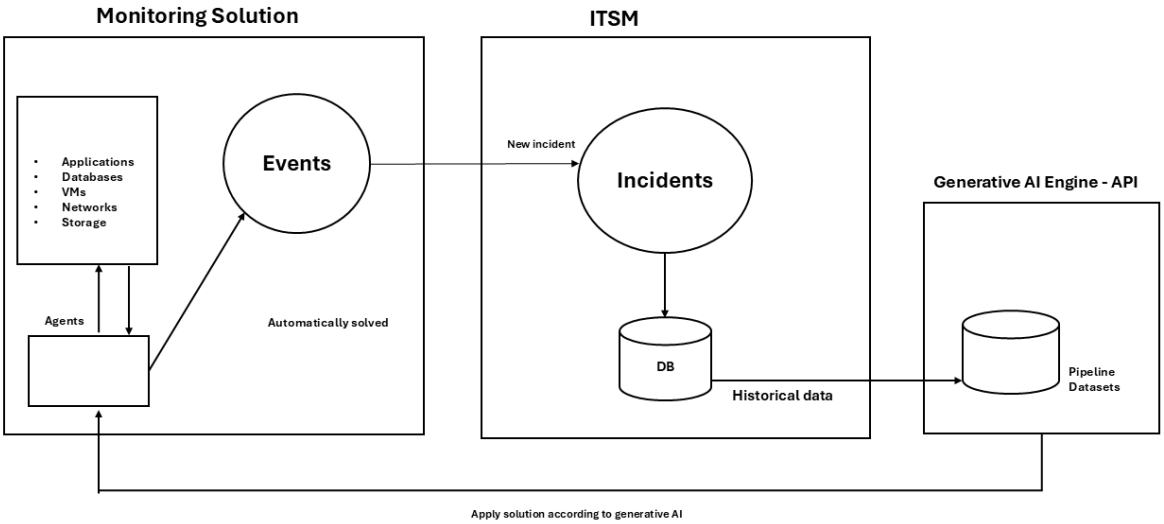

Figure 3. Automatic incident resolution theoretical proposal

3.3 Description of the process solution.

Applications, network devices, databases, and operating systems generate logs commonly called events.

Monitoring software through monitoring agents captures events.

The monitoring software is interconnected to the incident management solution/software, and the events generated are automatically turned into incidents.

The monitoring agent, due to the integration between the monitoring software and the incident management solution, is also an operator of the incident management solution.

New incidents generated through events in the incident management solution are automatically assigned to the agent's name.

New incidents are compared to the incident management solution's database or wiki to see if they are correlated incidents and if they have the same solution.

If the incident is correlated and there is a solution in the database or wiki of the incident management solution, the ITSM agent/operator automatically triggers the solution through a solution that may be a script with specific steps in the form of robotic process automation, for example: restart a certain service of an application or database that for some reason was paralyzed, or apply a more complex solution in script mode or with predetermined resolution.

After applying the solution to the device, application, or database, the monitoring agent/operator automatically closes the incident, and it stays in the closed state.

If there is no correlated incident through a Generative AI API interconnected to the incident management solution, the incident is sent to Generative AI to generate a solution for that incident. Generative AI is previously trained with the error code and solution documentation of the manufacturers of the computer solutions so that they have the correct response to a given incident.

Generative AI generates the solution for resolution of the incident in the form of a script and/or applied as Robotic process Automation, and is stored in the database, is sent to the agent/operator of the incident management solution to apply the solution to the end device.

Incidents with no solution presented by generative AI, nor with a solution correlated to incidents already resolved, stay in the state for manual resolution but assigned to the ITSM agent/operator, where they must be manually reassigned to the technical team for resolution.

For the solution to be possible to implement, the monitoring software and the incident management solution must be interconnected, so that each relevant event generated can be created automatically.

In addition to integration, the monitoring management solution should be interconnected to Generative AI, through an API to consult the incident solution. Those solutions can be stored in the database and through a comparison process with the log which generated the incident be applied as a solution to the incident.

On the other hand, Generative AI should be trained in manufacturers' incident error codes regarding the devices, software or applications they have on the market and respective solutions for the error codes.

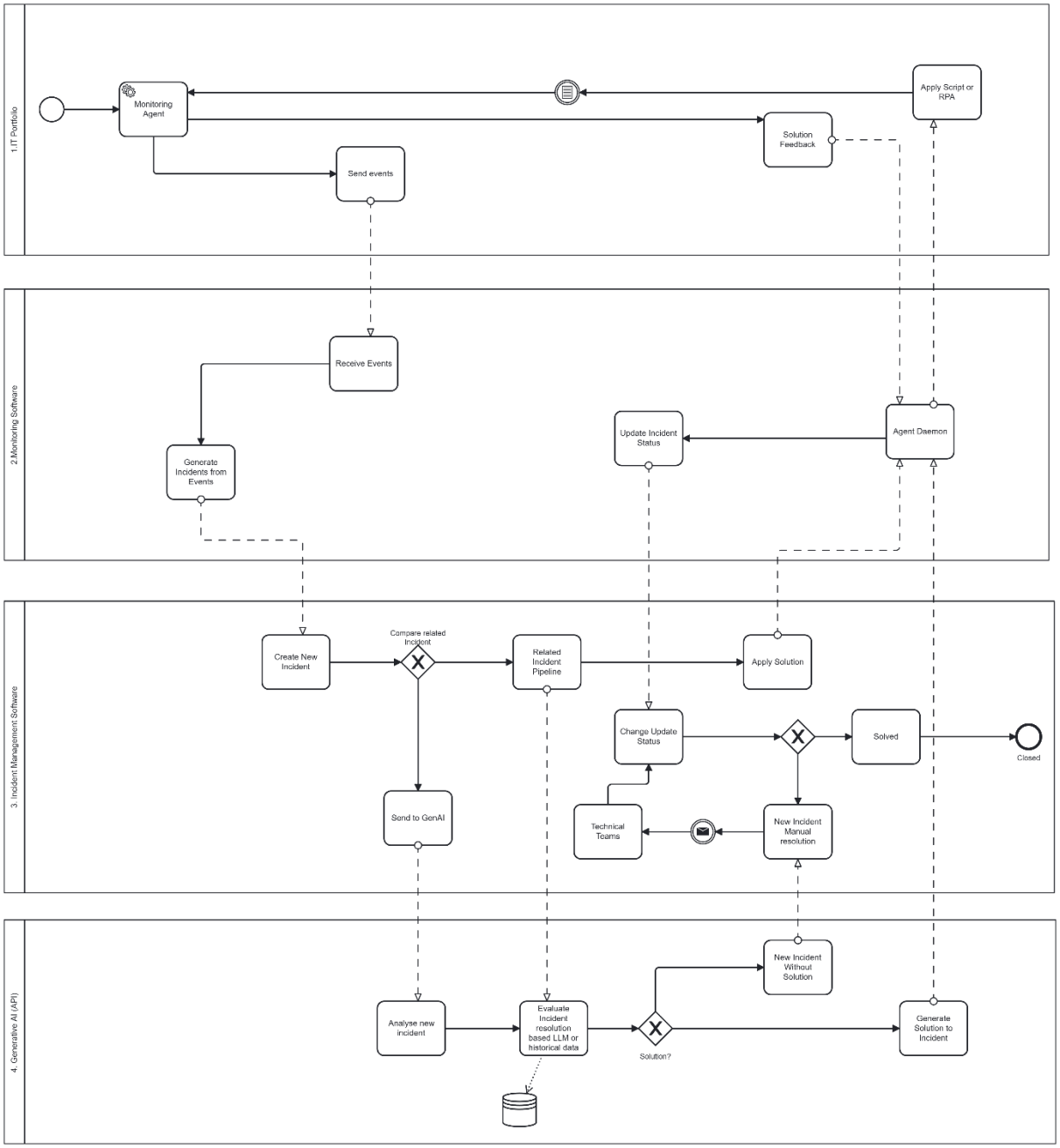

Figure 4. Process architecture

3.3.1 Description of the process described in Figure 1

1. IT Portfolio; Primarily, monitoring agents installed capture events logs from IT portfolio (applications, databases, network devices, etc)

2.Monitoring Software; The events captured from monitoring agents are sent to monitoring software and captured in the database, monitoring software, which is integrated with incident management software, send events to incident management.

3.Incident management software; capture events and transform into incidents as new events becomes new incidents.

Related solved incidents; if incident is solved previously and there exists a solution in the database it is a related incident, and the solution is picked up and sent to agent to apply the referred solution.

4.Generative AI (API); New events/incidents captured are sent to generative AI to provide a solution. Incidents with solution, the solutions are sent to the Agent daemon to apply the solution to the end device. Incidents without solution are sent to the incident management software and stays in manual state for manual resolution by the IT Teams.

3.4 Constituent parts of the incident response support system.

As a proposed solution for the automatic incident resolution information system, in this dissertation the following constituent parts of this system are proposed, where each of the parts can be considered as a sub-project.

1. Monitoring Software.
2. Incident management software.
3. Interconnection between monitoring software and incident management software.
4. Integration of incident management software and generative AI API

3.4.1 Monitoring software

The monitoring software consists of a client-server architecture, where the server(s) with front-end interconnected to the database(s), communicate with agents installed on the monitored devices and send customized monitoring metrics to be sent to the central server(s) interconnected by a communication network.

3.4.2 Incident management software

Incident management software allows you to record, classify, route, solve and close occurrences of failures in the IT portfolio associated with the organization's information technology infrastructure, incident management software is based on a service management framework, such as ITIL (Information Technology Infrastructure library) or MOF (Microsoft Operations Framework).

3.4.3 Integration between monitoring software and incident management software

To achieve the functionality of automatic incident management system automation, the monitoring software must be integrated or be an integral part of the incident management software.

The integration between monitoring and incident management software is crucial for

The events captured by the monitoring software in the automatic incident management system should be automatically captured by the monitoring software and be automatically transformed into an incident.

3.4.4 Integration of incident management software and Generative AI Engine via API.

For new incidents, the proposed solution for automation depends on integration with the generative AI engine, so that generative AI can infer a solution to the incident.

CHAPTER 4

Solution Implementation

4.1 Overview

The goal of this dissertation is to demonstrate a feasible solution for the design and development phase using cloud technology to build an artifact.

Demonstration of steps for POC (Proof of concept) for a proposed solution using cloud technology to create an artifact.

4.2. Monitoring software.

According to the process, present in chapter 3, of this dissertation, as monitoring software to demonstrate the proposed solution, azure monitor will be used, then the general steps for parametrization of azure monitor will be presented, from the collection of events on information technology resources to the recording of logs into cosmos db database.

Through the process

4.2.1 Azure monitor and IT resource.

In the Azure console, create the resources needed to be monitored (database, virtual machine, application, etc.)

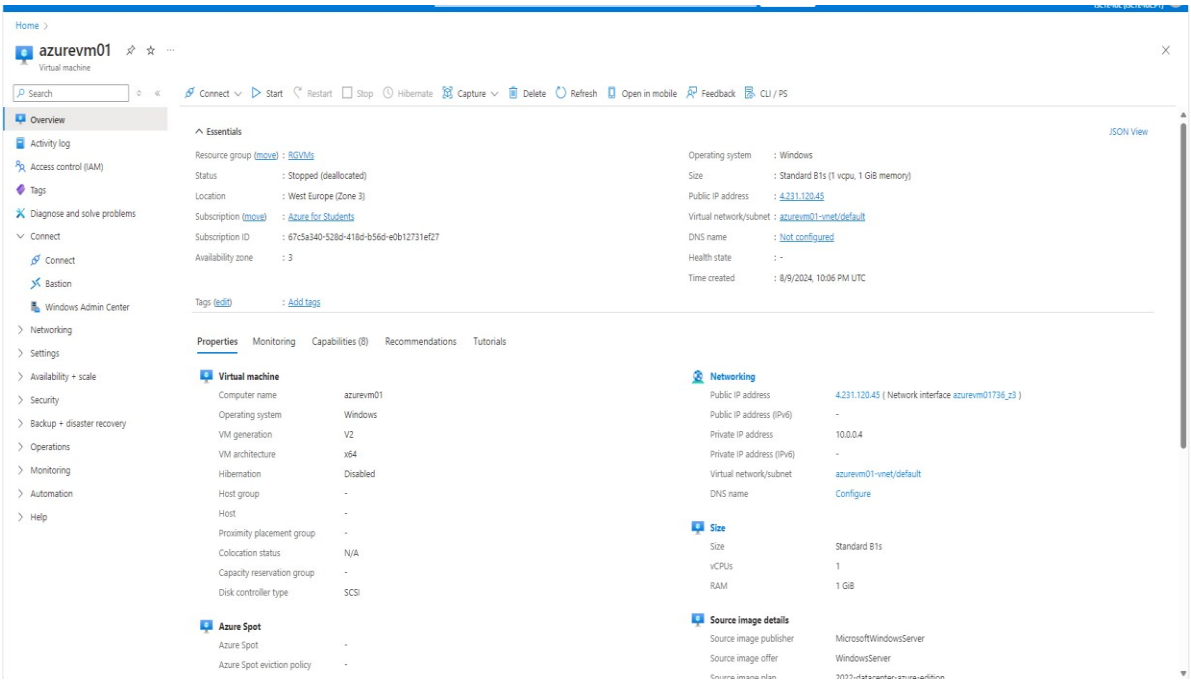

Figure 5. IT resource created in Azure.

Create a Log Analytics workspace; using azure console create a log analytics workspace and associate or activate the log analytic agent of the resource previously created.

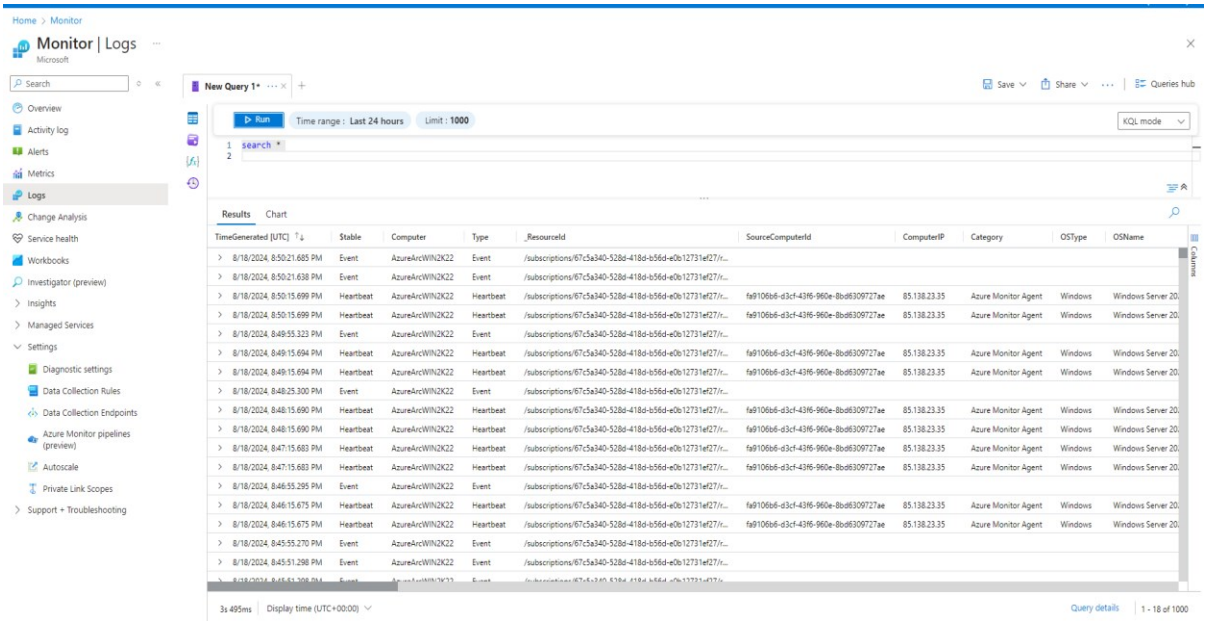

Figure 6. Logs captured from Azure monitor.

In the case of Azure VM or Azure Arc-Enabled server. Others resource created in others clouds would be considered azure-arc enabled, in this case it is used Data collection rules, to create monitoring logs and send to the destination Workspace.

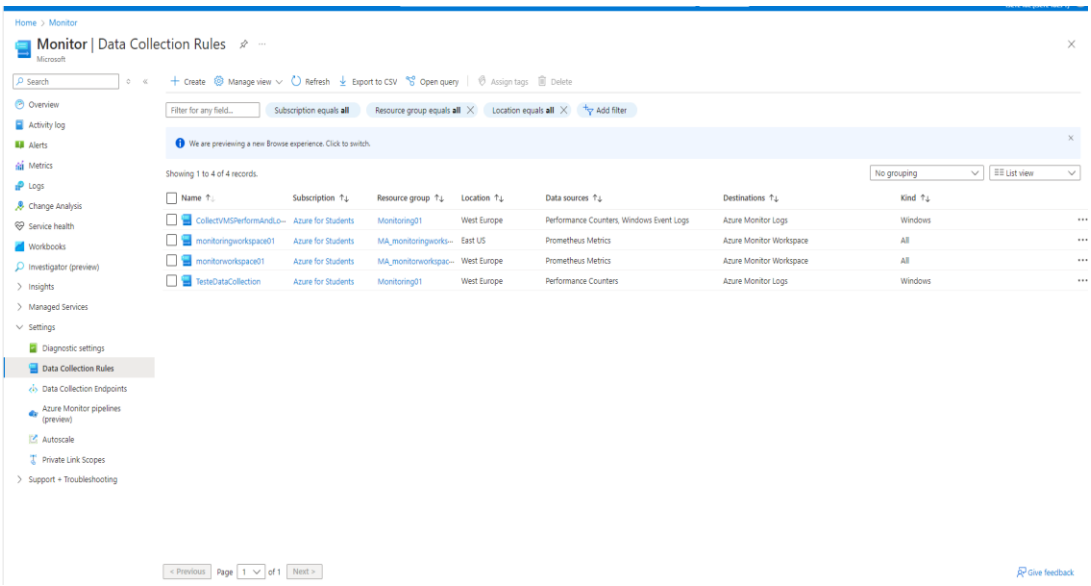

Figure 7. Data collection rules

4.2.2 Azure monitor and azure event hubs integration.

In the azure console, go to log analytics workspace and select Data Export and create an export rule, export the data to event hubs, previously the event hubs namespace must be created before exporting the events logs.

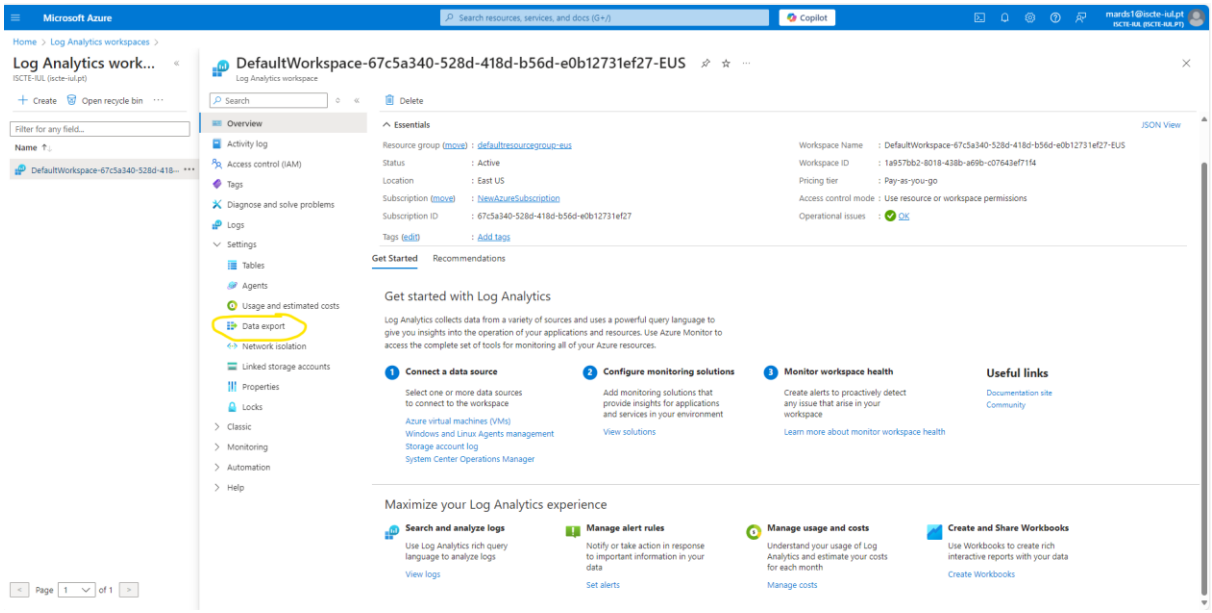

Figure 8. Export data to Azure event Hubs.

Log analytics workspace; is a data store into which you can collect any type of log data from all your Azure and non-Azure resources and applications.

Azure event hubs is a native data-streaming service in the cloud that can stream millions of events per second, with low latency, from any source to any destination.

4.2.3 Azure event Hubs to Cosmos DB integration.

Azure Monitor logs sent to Azure Event Hubs are saved in JSON format.

Azure Cosmos db is a globally distributed, multi-model database service. Azure Cosmos db supports several data types, one of which is JSON. Therefore, in this case it saves the logs in JSON format in the Cosmos db database.

The json file uses the following format:


```
[
  {
   "TimeGenerated": "2023-11-13T08:42:50Z",
   "fields": {
    "Buffer pool": "15.90",
    "Cache (objects)": "0.60",
    "Cache (sql plans)": "35.60",
    "Other": "48.10"
   },
   "name": "Memory breakdown (%)",
```

```
  "tags": {
    "host": "telegraf",
    "servername": "WIN-MVE00BSRF5S",
    "type": "Memory clerk"
  }
 },
 {
  "TimeGenerated": "2023-11-13T08:42:50Z",
  "fields": {
    "Buffer pool": "72744960.00",
    "Cache (objects)": "2842624.00",
    "Cache (sql plans)": "162807808.00",
    "Other": "220069888.00"
  },
  "name": "Memory breakdown (bytes)",
  "tags": {
    "host": "telegraf",
    "servername": "WIN-MVE00BSRF5S",
    "type": "Memory clerk"
  }
 }
]
```


For the integration between Azure Event Hubs and Cosmos db, was used azure stream analytics job to send log data from azure event hubs to Cosmos db database.

In the Azure stream analytics console, select Process data, and select the option Materialize data in cosmos db, create a job and select the event hubs data source and fields, select cosmos db destination as output, select the cosmos db subscription, select database in cosmos db and connect.

4.3. incident management software.

From the logs stored in the Cosmos db database, powerapps is used to simulate the incident management software and interconnect the events saved in json format, with the highlight for new incidents. In this way the events generated would be considered as new incidents.

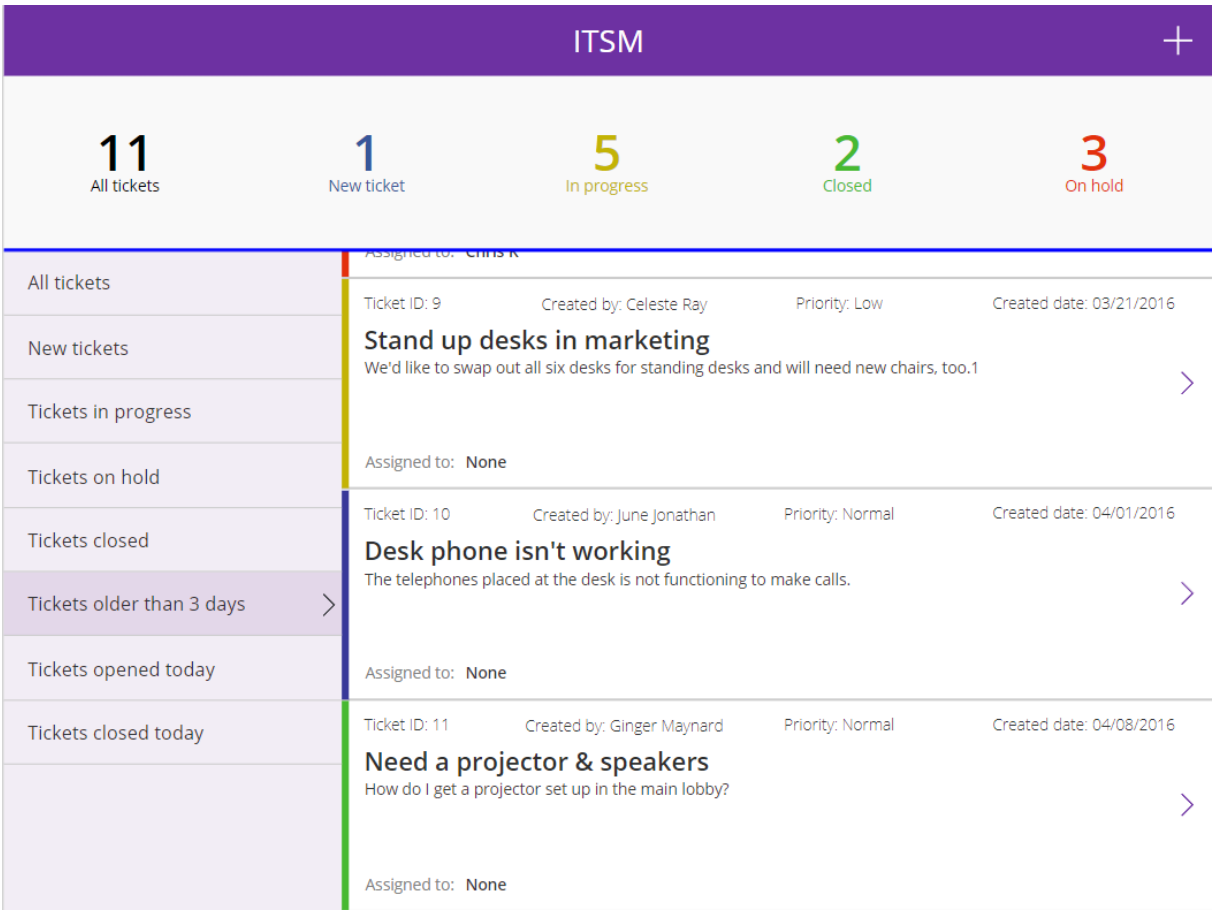

Figure 9. Simulation of incident management software

4.3.1 Integration between Cosmos db and PowerApps

To simulate the incident management software and store the new incidents (event logs) that needed to be shown as new incidents in powerapps application user interface.

The integration was done by the existing "Azure cosmos db" connector in Powerautomate.

In powerautomate, the flow was created using the connector, and in the "GetAllDocument" property to generate a flow to send data to Powerapps, in powerapps the data is shown in the "gallery" which is a control.

The powerplatform connector "Azure cosmos db" is a premium connector.

CHAPTER 5

Conclusions and future work

5.1 Discussion of the results

In the proposed solution presented to solve the automatic incident response system using the cloud computing environment, it was found that the integration between the monitoring software, the incident management software and then the integration between the incident management software and the Generative AI engine is required.

The ideal solution for the complexity of the project presented would be to develop a customized development artifact of the monitoring software integrated with the incident management software and the subsequent integration with the generative AI engine or another machine learning classifier engine.

In the steps presented in the previous chapter, it was verified that with the proposed solution the incidents/logs are written to the cosmos db database, and the subsequent logs can be ingested for inference in Azure OpenAI for computation of a solution. However, the topic of applying the solution generated by Generative AI or alternatively a machine learning classifier model, which is considered as future work, remains open.

Although the artifact created in chapter 4, in the demonstration phase did not reach all the functionalities designed in the Design and Development phase, it is concluded that it is open to develop an artifact with better coverage for Design and Development, but at the Design and Development phase, it was global view and the complexity of how an automatic incident resolution system should work, with the support of generative AI or another machine learning classification model, splitting it into layers of abstraction.

5.2 Future Work.

Create a solution database generated by openAI and save it in cosmos db. Make this solution database available in powerapps as a solution for the generated logs/incidents.

Create a mechanism using powerautomate or azure logicapps so that it is possible to apply the resolution generated by generative AI or classifier model, on the devices or applications where the events were generated, from the solutions saved in Cosmos db.

Bibliographic References

Al-Hawari, F., & Barham, H. (2021). A machine learning based help desk system for IT service management. *Journal of King Saud University - Computer and Information Sciences*, *33*(6). https://doi.org/10.1016/j.jksuci.2019.04.001

Ali, A., & Soomro, T. R. (2014). Bridging gape between ITSM, IT-governance and information security to meet business needs. *Research Journal of Applied Sciences, Engineering and Technology*, *7*(23). https://doi.org/10.19026/rjaset.7.881

Chen, Z., Kang, Y., Li, L., Zhang, X., Zhang, H., Xu, H., Zhou, Y., Yang, L., Sun, J., Xu, Z., Dang, Y., Gao, F., Zhao, P., Qiao, B., 林庆维 Q. L., Zhang, D., & Lyu, M. R. (2020). Towards intelligent incident management: why we need it and how we make it. *2020 Foundations of Software Engineering*, 1487–1497. https://www.microsoft.com/en-us/research/publication/towards-intelligent-incident-management-why-we-need-it-and-how-we-make-it/

Engemann, K. J., & Miller, H. E. (2024). Toward revealing concealed risks for agile IT service management practices. *Information Systems and E-Business Management*. https://doi.org/10.1007/s10257-023-00666-8

Fahmi. (2016). IBM Maximo Asset Management System. *19 Juni*.

Frick, N., Brünker, F., Ross, B., & Stieglitz, S. (2019). The Utilization of Artificial Intelligence for Improving Incident Management. *HMD Praxis Der Wirtschaftsinformatik*, *56*(2).

Godse, N. A., Deodhar, S., Raut, S., & Jagdale, P. (2018). Implementation of Chatbot for ITSM Application Using IBM Watson. *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*. https://doi.org/10.1109/ICCUBEA.2018.8697411

Heikkinen, S., & Jäntti, M. (2012). Identifying IT service management challenges: A case study in two IT service provider companies. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*. https://doi.org/10.1109/DEXA.2012.32

Hertvik, J. (2016). *What is ITIL? A Simple Primer for Understanding ITSM and ITIL – BMC Blogs*. Bmc Blogs.

Hochstein, A., Tamm, G., & Brenner, W. (2005). Service-oriented it management: Benefit, cost and success factors. *Proceedings of the 13th European Conference on Information Systems, Information Systems in a Rapidly Changing Economy, ECIS 2005*.

Hochstein, A., Zamekow, R., & Brenner, W. (2005). ITIL as common practice reference model for IT service management: Formal assessment and implications for practice. *Proceedings - 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, EEE-05*. https://doi.org/10.1109/EEE.2005.86

Iden, J., & Eikebrokk, T. R. (2014). Using the ITIL Process Reference Model for Realizing IT Governance: An Empirical Investigation. *Information Systems Management*, *31*(1). https://doi.org/10.1080/10580530.2014.854089

Jäntti, M., & Hotti, V. (2016). Defining the relationships between IT service management and IT service governance. *Information Technology and Management*, *17*(2). https://doi.org/10.1007/s10799-015-0239-z

Khowongprasoed, K., & Titijaroonroj, T. (2022). Automatic Thai Ticket Classification By Using Machine Learning For IT Infrastructure Company. *2022 19th International Joint Conference on Computer Science and Software Engineering, JCSSE 2022*. https://doi.org/10.1109/JCSSE54890.2022.9836250

MacLean, D., & Titah, R. (2023). Implementation and impacts of IT Service Management in the IT function. *International Journal of Information Management*, *70*. https://doi.org/10.1016/j.ijinfomgt.2023.102628

Mandvikar, S., & Achanta, A. (2023). Process Automation 2.0 with Generative AI Framework. *International Journal of Science and Research (IJSR)*, *12*(10). https://doi.org/10.21275/sr231021200626

Mansor, M., Wan Adnan, W. A., Abdul Wahid, R., & Hamid, J. (2021). Step by Step Implementation of DSRM for Personalization of Reading. *International Journal of Humanities, Management and Social Science*, *4*(1). https://doi.org/10.36079/lamintang.ij-humass-0401.212

Marrone, M., & Kolbe, L. M. (2011). Impact of IT Service Management Frameworks on the IT Organization. *Business & Information Systems Engineering*, *3*(1). https://doi.org/10.1007/s12599-010-0141-5

Matchett, C., Doheny, R., & Gonzalez, K. (2017). Magic Quadrant for IT Service Management Tools. *Gartner*.

Melendez, K., Dávila, A., & Pessoa, M. (2016). Information technology service management models applied to medium and small organizations: A systematic literature review. In *Computer Standards and Interfaces* (Vol. 47). https://doi.org/10.1016/j.csi.2015.10.001

Mohd Jamaludin, S. Z., Khan Majahar Ali, M., Vun Shiung Wong, E., Ismail, M. T., & Ibrahim, N. F. (2023). Solving Complexity Dataset in e-Ticketing using Machine

Learning to Determine Optimum Feature. *Malaysian Journal of Fundamental and Applied Sciences*, *19*(6), 1068–1081. https://doi.org/10.11113/mjfas.v19n6.2921

Mustapha, A., Mostafa, S. A., Hassan, M. H., Jubair, M. A., Khaleefah, S. H., & Hassan, M. H. (2020). Machine learning supervised analysis for enhancing incident management process. *International Journal of Emerging Trends in Engineering Research*, *8*(1 1.1 Special Issue), 199–204. https://doi.org/10.30534/ijeter/2020/3181.12020

Nila, C., Apostol, I., & Patriciu, V. (2020). Machine learning approach to quick incident response. *2020 13th International Conference on Communications, COMM 2020 - Proceedings*. https://doi.org/10.1109/COMM48946.2020.9141989

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee. (2008). Peffers et al. (2008) A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*.

Prihandono, M. A., Harwahyu, R., & Sari, R. F. (2020). Performance of machine learning algorithms for IT incident management. *2020 11th International Conference on Awareness Science and Technology, ICAST 2020*. https://doi.org/10.1109/iCAST51195.2020.9319487

Rajagopal, M., & Ramkumar, S. (2023). *Adopting Artificial Intelligence in ITIL for Information Security Management—Way Forward in Industry 4.0*. https://doi.org/10.1007/978-981-99-2115-7_5

Reinhard, P., Li, M. M., Dickhaut, E., Peters, C., & Leimeister, J. M. (2023). Empowering Recommender Systems in ITSM: A Pipeline Reference Model for AI-Based Textual Data Quality Enrichment. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13873 LNCS*, 279–293. https://doi.org/10.1007/978-3-031-32808-4_18

Richardson, B. F., & Mahfouz, A. Y. (2011). Aligning business service management to goals: an integrated approach at BMC Software. *Journal of Technology Research*, *2*.

Sahay, R. (2020). Azure Monitoring. In *Microsoft Azure Architect Technologies Study Companion*. https://doi.org/10.1007/978-1-4842-6200-9_5

Sahid, A., Maleh, Y., & Belaissaoui, M. (2017). An agile framework for ITS management in organizations. A case study based on DevOps. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3167486.3167556

Salvaris, M., Dean, D., & Tok, W. H. (2018). Deep Learning with Azure. In *Deep Learning with Azure*. https://doi.org/10.1007/978-1-4842-3679-6

Sarkar, S., Vinay, S., Djeddi, C., & Maiti, J. (2022). Classification and pattern extraction of incidents: a deep learning-based approach. *Neural Computing and Applications*, *34*(17). https://doi.org/10.1007/s00521-021-06780-3

Schad, J., Sambasivan, R., & Woodward, C. (2022). Predicting help desk ticket reassignments with graph convolutional networks. *Machine Learning with Applications*, *7*. https://doi.org/10.1016/j.mlwa.2021.100237

ServiceNow. (2020). *ServiceNow ITSM overview*. ServiceNow.

Siderska, J., Aunimo, L., Süße, T., von Stamm, J., Kedziora, D., & Aini, S. N. B. M. (2023). Towards Intelligent Automation (IA): literature review on the evolution of Robotic Process Automation (RPA), its challenges, and future trends. *Engineering Management in Production and Services*, *15*(4). https://doi.org/10.2478/emj-2023-0030

Subbarao, M. V., Venkatarao, K., & Suresh, C. H. (2022). AUTOMATION OF INCIDENT RESPONSE AND IT TICKET MANAGEMENT BY ML AND NLP MECHANISMS. *Journal of Theoretical and Applied Information Technology*, *100*(12), 3945–3955.

Tae, C. M., & Hung, P. D. (2020). A Collaborative Web Application Based on Incident Management Framework for Financial System. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12341 LNCS*. https://doi.org/10.1007/978-3-030-60816-3_32

Ugwuanyi, F. O., S. O, A., & Anigbogu, K. S. (2020). SELF-HEALING SYSTEMS: APPLICATION AND METHODOLOGIES-A REVIEW. *International Journal of Research -GRANTHAALAYAH*, *8*(9). https://doi.org/10.29121/granthaalayah.v8.i9.2020.1306

Zuev, D., Kalistratov, A., & Zuev, A. (2018). Machine Learning in IT Service Management. *Procedia Computer Science*, *145*. https://doi.org/10.1016/j.procs.2018.11.063