GDPR Compliance Challenges and How to Overcome Them

Bharath Kishore Gudepu[1], Divya Sai Jaladi[2]
[1]Senior EDC Developer, State Farm, CityLine Building 1, Richardson, TX, 75085
[2]Senior Lead Application Developer, SCDMV, 10311 Wilson Boulevard, Blythewood, SC 29016, UNITED STATES

ABSTRACT

Startups and SMEs need focus, particularly technology startups; although they are fueled by innovation and advancing technology, they require improved data protection practices. This research seeks to collect data regarding the awareness of startups about the GDPR, pinpoint the main challenges encountered by technology startups in Catalonia since the GDPR's implementation in May 2018, and investigate (1) the potential correlation between the identified challenges and factors such as the number and type of employees hired, the size of the startup, the business sector, and the year of establishment; and (2) the resources, both time and financial, that startups have allocated towards compliance. The literature review identified gaps in the research and served as the foundation for examining the challenges encountered by startups due to the enforcement of the GDPR. Thirty-two challenges were identified concerning GDPR and categorized into four constructs: compliance costs, regulation complexity, government support, and process adaptation. The lack of adequate government support poses the greatest challenge for the Catalonian startups involved in the survey. This study represents one of the initial empirical investigations into GDPR compliance efforts and challenges faced by Catalan technology startups. It employs advanced statistical analysis techniques, beginning with ANOVA, and includes independent sample T-tests, correlation analysis, and regression analysis. Regrettably, the results cannot be generalized to all startups in Catalonia due to the failure to meet the required minimum sample size for representativeness; 116 responses were collected, whereas 314 were necessary to achieve the appropriate sample size. Nonetheless, this research offers a practical contribution by (1) presenting recommendations that enhance technology startups' understanding of the various challenges they need to tackle in order to comply with GDPR and (2) offering suggestions for the Catalan government to promote startup GDPR implementation.

Keywords: GDPR, Compliance, Data Privacy, Data Governance, Data Management, Data Quality, Metadata, Data Profiling, Data Security, Enterprise Data, Data Discovery

Introduction

Catalonia is one of the biggest ICT hubs in Europe and the leader destination for IED technology. This study focuses on how tech startups in Catalonia are implementing GDPR. Barcelona is the seventh hub in the European Union for future unicorns, after Paris, Berlin, Stockholm, Munich, Dublin, and Amsterdam, but before Madrid. Among Catalonian entrepreneurs, Technologies 4.0 is widely used, with 75% having taken steps to make their firm more sustainable [1-3].

In order to safeguard customers' privacy, the European Union (EU) implemented the General Data Protection Regulation ("GDPR"). The right to safety of personal data is a fundamental human right recognized in the EU Charter of Fundamental Rights. In its place and repealing the EU Data Protection Directive of 1995, the General Data Protection Regulation (GDPR) aims to establish uniform data protection standards across all EU member states and brings substantial changes to personal data and privacy.

Following an initial transition period of two years, the General Data Protection Regulation (GDPR) entered into force on May 25, 2018. We need to strike a balance between collecting personal data for commercial profit and protecting consumer data, as technological growth has made it easier to acquire more and more of it. Fast technological change and globalization have made it easier for individuals to share information about their habits and preferences, sometimes even without their knowledge or permission, and this data may easily be accessed by other companies all across the globe. Most mobile apps need access to a large quantity of personal data, shows that big data tools are becoming more common, which enables for cross-analysis of personal data. Even if a lot of those apps don't cost anything, users are nevertheless "paying" with their private information [4-9].

More data control, stronger rights, reforming how companies see and handle data, and removing trade obstacles are all goals of the General Data Protection Regulation (GDPR) for the European Union so that companies can grow more organically throughout Europe while still protecting the privacy of EU citizens' data. The General Data Protection Regulation (GDPR) is an effort to unify data protection throughout the European Union and restore faith in the online economy.

There is no doubt that all sectors of operation must know and follow the GDPR. On the other hand, IT businesses are among the most hit since they must adhere to the GDPR's regulations when handling personal data and also develop new technical solutions that meet those regulations. Despite the importance of GDPR for digital organizations, particularly SMEs and startups [10-13].

The GDPR affects big tech companies like Google and Facebook, and how important these laws are for their users. On the other hand, discussions that have concentrated on smaller tech startups have mostly concentrated on the United Kingdom. Nevertheless, it is equally important to pay attention to startups and SMEs. This is particularly true of tech startups, as they are innovation-driven, always pushing the limits of technology, but they do not yet have established data protection best practices. Startups' early choices may have detrimental consequences in the long run. As a result, it is crucial to check that tech companies' processes and inventions are solid, suitable, and acceptable. More awareness and direction from supervisory authorities is needed to help tech businesses. In order for startups to have the best chance of innovating within the GDPR framework, they should also actively participate in preventing and deterring losses. It is believed that the Supervisory Authorities are giving more attention to bigger tech companies than to smaller tech startups and SMEs; if this is true, the long-term consequences might be catastrophic [14-19].

Research on the difficulties encountered by businesses, particularly tech-based SMEs and startups, during the implementation of the General Data Protection Regulation (GDPR) has shown that such difficulties do in fact exist. Furthermore, several authors have found that the technology companies are one of the most affected ones in terms of processing data and developing technological solutions that comply with the GDPR.

An acceptable framework structure was determined through literature study, which also revealed a gap in the difficulties encountered by startups since the General Data Protection Regulation (GDPR) went into effect in May 2018.

It is still unclear, however, how tech startups fare in the three years following the GDPR's implementation, what obstacles they encountered during the regulation's implementation, whether these were related to compliance costs, regulation complexity, inadequate government support, or process adaptation, and whether there was a correlation between the difficulties startups encountered and factors like year of establishment, size, industry, and annual expenditure on GDPR compliance. Because governments can benefit from taking steps to assist companies with the difficulties of adopting GDPR, and because firms will take precautions to prevent mistakes and downsides throughout the implementation process if they are aware of the difficulties, more study is necessary.

Difficulties with the General Data Protection Regulation (GDPR)

In many companies, GDPR has sparked heated debates and discussions. According to Lindgren's (2018) research, organizations were particularly worried about the steep fines that would result from failing to adhere to the GDRP protocols. Also, some were reluctant to carry out the necessary processes because they were irritated by the GDPR legislation. Managers and workers alike worried that it would hurt the firm and its business strategies, particularly throughout the value chain's dimensions. The most difficult part of the General Data Protection Regulation (GDPR) might be putting it into practice. This is particularly true for small and medium-sized enterprises (SMEs), and for companies that hadn't previously implemented a similar level of privacy protection, this meant making extensive changes to their operations. Many companies did not have the necessary personnel on staff who were knowledgeable about privacy regulations or the new standards for the secure storage and processing of customer information. Training on data protection and privacy was thus deemed necessary by a large number of the surveyed firms. Despite seeing this as a critical component in fulfilling the new GDPR standards, many organizations lacked the additional resources necessary to handle it. Data protection layers and GDPR solutions might vary depending on whether one is talking about internal company (managers and staff) or external company (customers and network-partners) [20-23].

The GDPR implementation process and the challenges faced by companies differed depending on the companies' size, with SMEs and startups facing the highest levels of challanges. The coming into force of the GDPR has had a significant impact on how tech startups and SMEs manage their businesses. This is because the GDPR is here to stay, and the tech startups and SMEs already existing at the time of the GDPR became applicable have had to adapt the way they work to meet requirements. This has not been easy because GDPR does not provide specific guidelines to adopt its requirements. That is why every company had to find and adopt managerial and technological solutions to achieve GDPR compliance.

Challenges Encountered by Businesses Prior to the Implementation Of GDPR

E.U. companies have faced and are still facing problems with becoming GDPR compliant. Report research carried out between the 9th and the 15th of January 2018 by Populos under the order that before the entry into force of the GDPR, 60% of the

E.U. companies were not ready. The report is based on a survey of one thousand fifteen companies based in UK, Germany, France, Spain, and Italy which cover all size companies. The respondents from large companies (companies employing more than two hundred fifty people) were selected because they have been responsible for or had an impact on data protection regulations within the company or had excellent practical knowledge of data protection compliance. Respondents from SMEs (companies employing between ten and two hundred forty-nine people) and micro-businesses (self-employed and companies employing less than ten people) were selected based on seniority (management or board level). The GDPR readiness scale was quantified based on responses to queries about knowledge, understanding and actions taken concerning GDPR.

The report survey questions designed by Jonas (2018) were directed at determining the level of knowledge about where data was stored, the level of confidence in being able to consider all different databases, the measures taken to prepare for the GDPR, the level of awareness of the reputational impact of non-compliance with the GDPR, the fines resulting from the GDPR non-compliance and confidence that the company can respond to data requests within the 30-day commitment. The results of this report research show that 60% of all participating companies were not GDPR ready to deal with the challenges that GDPR compliance would pose, and that more than about a tenth (12%) of the companies were not sure was knowing where all their data was housed.

The present research because it assesses the level of GDPR compliance of companies, especially the SMEs and the tech startups, before the GDPR implementation. However, although this report is of great value for the issue of GDPR compliance, mainly on data location, it does not concentrate on tech startups but companies of all sizes based in the UK, Germany, France, Spain, and Italy. The GDPR came into force revealed that for U.K. blockchain startups the right of erasure stated under art. 17 of the GDPR was the biggest GDPR challenge they face because "you can’t eradicate [the data], you need to find a means of making the data unavailable”.

The present research as it assesses the GDPR challenges encountered by U.K. tech startups before GDPR implementation. The findings suggest that many U.K. tech startups struggled and or misinterpreted how compliance could be achieved. However, although the Norval research brings more light to the issue of GDPR challenges around the U.K. tech startups before the GDPR implementation, it does not concentrate on tech startups in Spain or Catalonia [24-27].

The TrustArc report detailed the findings of their studies on U.S. and E.U I.T and Legal professionals. TrustArc retained Dimensional Research to conduct a set of surveys which concentrated on the level of GDPR compliance on U.K. and U.S. companies before the GDPR came into force and revealed the extent of the help required for U.S. and U.K. privacy professionals to comply with these data privacy requirements TrustArc (2017). For U.S. and U.K. respondents, developing a GDPR plan topped the list. Significant investments were required for consultants, new hires and technology to meet the GDPR deadline. Difficulties encountered during implementation following the attestation of GDPR.

Dimensional Research's most recent independent report, commissioned by TrustArc in June 2018, focused on comparing the degree of GDPR compliance among companies of all sizes in the US, UK, and E.U. (non-UK countries). The report also compared the costs, efforts, most significant challenges, and motivations for becoming GDPR compliant by the deadline. Six hundred individuals with expertise in law, IT, and privacy were polled; half came from the United States, half from the United Kingdom, and the other half came from a variety of other European Union nations. Data protection accounted for a minimum of 25% of the tasks performed by each responder. Companies ranging in size from mom and pop shops to huge corporations across all major industries took part.

Finding and keeping up with GDPR compliance is a complex and costly undertaking for businesses of all sizes and in all regions, according to research from TrustArc (2018). Twenty percent said they were in compliance by May 25th, but ninety percent had begun, three quarters said they would be by year's end, and nearly all said they would be fully compliant in 2019. The good news is that a whopping 87% of businesses have stated that privacy will only become bigger at their organization, 80% want to raise their investment in digital solutions, and their GDPR budgets will stay active well beyond 2018.

Results from the study conducted by TrustArc (2018) are as follows: While general data protection regulation (GDPR) is still in its early stages, businesses are more driven by principles and the expectations of customers and other third parties than by the threat of fines and litigation. Companies have made more progress in updating policies and managing cookies than in managing vendor risk and international data transfers. Overall, GDPR has been both difficult and rewarding. While the report identifies GDPR complexity, a lack of expertise, qualified staff, and GDPR technology and tools as the top challenges, 65% of respondents are optimistic about the impact of GDPR on their business. The top three privacy priorities over the next 6-12 months are achieving, maintaining, and demonstrating GDPR compliance. Half of the respondents will seek a third party GDPR validation instead of waiting for the official GDPR certification.

Despite its usefulness, this research focuses on the degree of GDPR compliance among large and small businesses in the United States, the United Kingdom, and the European Union (excluding the United Kingdom). It doesn't address the level of compliance or the difficulties faced by startups.

How General Data Protection Regulation Impacts New and Small Firms

The implications of GDPR for small tech startups in the United Kingdom, while most discussions on data protection have concentrated on bigger tech companies like Google and Facebook and how these laws affect their users. Still, it's important to pay attention to startups and SMEs in general, and tech startups in particular, as they are innovation-driven, constantly testing new technological frontiers, but lack well-established data protection best practices. Startups' early choices may have detrimental consequences in the long run. As a result, it is crucial to check that tech companies' processes and inventions are solid, suitable, and acceptable. The tech startups might use more help from the supervisory authorities, such additional education and direction. The best chances for startups to develop within the GDPR framework can only be achieved if they actively participate in preventing harm and discouraging. Some believe that the Supervisory Authorities are giving more attention to bigger tech companies than to smaller digital startups and SMEs, which might have disastrous consequences in the long run.

In addition, IT startups and SMEs are facing difficulties in innovation due to the costs effect of GDPR. Compliance costs and data regulation can impede new entrants and dampen innovation. Small and new businesses bear the brunt of privacy regulations' financial burdens. This is particularly true for ad-supported online commodities, where price mechanisms do not mitigate the impact. Also, as the costs of compliance rise for small businesses, more innovations will be generated by larger enterprises. The ratio of venture capital to research and development expenditures is a good indicator of the number of industrial discoveries made possible by venture capitalists. Research utilizing data from Adobe Analytics measured the impact of the General Data Protection Regulation (GDPR), for a wide range of businesses in light of GDPR's impact on vital economic results. On a weekly basis, page visits fell around 4% and income fell about 8%, both of which were statistically significant. A substantial figures from an economic perspective, as a weekly revenue decrease of 8% would result in a median revenue drop of $8,000. Nevertheless, the results are not directly caused by changes in user behavior, according to the researchers. The aforementioned results clearly show the complexity and high costs of privacy laws from a researcher's point of view. Without including the substantial operational and infrastructural expenses, the data from Adobe Analytics only showed a fraction of the overall cost of GDPR compliance. To further comprehend the trade-offs, additional study is required to assess the advantages to GDPR's users.

Prior to the GDPR's implementation, not all UK IT firms were prepared to or able to maintain a continuous GDPR compliance effort. Nevertheless, digital businesses must consistently prioritize meeting their regulatory requirements. Consequently, while this analysis is valuable in and of itself, particularly since it focuses on IT startups, the inclusion of firms from the E.U., and more especially Spain, would have made it a more pertinent study.

Regardless of their size, businesses in the European Union have had and continue to have challenges in becoming GDPR compliant, according to a study report by TrustArc (2018). These challenges include the regulation's complexity, a lack of knowledge and skilled personnel, and GDPR-specific technology and tools. Achieving and maintaining GDPR compliance is an ongoing process, not a quick fix. Businesses must no longer make the costly error of ignoring the issue. In order to establish permanent automated GDPR procedures without spending as much time, money, and resources and without appointing a Data Protection Officer (DPO), notes that developing and implementing a set of best practices is a critical strategy and challenge [28-35].

The ability to get ongoing help from a DPO in the areas of compliance and best practices across the whole product lifecycle—from inception to design, implementation, and operations—makes them an invaluable asset for digital companies. Having said that, studies show that a lot of new businesses either don't think a DPO is necessary or have designated an employee from within the company to serve as the DPO, ignoring their level of data protection knowledge or autonomy within the company. Data protection regulations and procedures should be second nature to a data protection officer. That it is expensive to hire a Data Protection Officer (DPO) or Chief Privacy Officer (CPO) and that the General Data Protection Regulation (GDPR) is complicated and difficult to grasp are two possible explanations, according to the study. A CPO, is also a good idea because the lack of practical solutions to become GDPR compliant in the GDPR has been a major challenge for many firms in understanding what is necessary to become compliant. The data protection officer (DPO) is responsible for ensuring data compliance and reports to the company's upper management; the chief privacy officer (CPO) is responsible for protecting sensitive information. Instead of a DPO reporting on cost and redundancy reductions, the chief product officer (CPO) in American corporations takes on a more strategic and forward-planning role for worldwide activities. In addition, the following is how Professors Bamberger and Mulligan defined their research on American practices: "The CPOs expressed a forward-looking focus on anticipating future difficulties rather than achieving present demands. They also highlight how business organizations' privacy functions might be compromised by environmental uncertainty and genuine threats with meaningful sanctions. According to our respondents, they have a lot of influence throughout the firm, get to weigh in on big-picture business choices, and have a lot of leeway to shape how the company operates and what they're responsible for. Pages 194–1995, as cited in Bamberger and Mulligan (2015). While it's common practice for larger organizations to designate a chief privacy officer (CPO) to demonstrate to stakeholders (both internal and external) that their firm is committed to data protection compliance, startups often lack the resources to do so.

Research Deficit and Challenges to be Addressed.

Table 2.5 shows that most of the prior research in this area has focused on large companies, certain industries, and small and medium-sized enterprises (SMEs), but has ignored the specifics of what each company does and has narrowed its focus to SMEs rather than tech startups.

The dependent variable "impacts on the implementation of GDPR in pre-existing business models for SMEs" is negatively affected by the following constructs: knowledge, time, uncertainty, costs, information provision, and process adaptation. Finding that many of these tech startups struggled and/or misunderstood how compliance could be achieved and the importance of regulators' roles in providing more support, The examination of prior research about the obstacles encountered by enterprises, particularly technology SMEs and startups, in implementing the GDPR indicates their existence.

Nonetheless, there is insufficient data regarding the familiarity of technology startups with the GDPR five years post-implementation, encompassing: the primary challenges encountered during GDPR compliance, whether these challenges pertain to compliance costs, regulatory complexity, inadequate governmental support, or process adaptation, and if there exists any correlation between these challenges and factors such as the year of establishment, size, industry sector, and annual expenditures on GDPR compliance. Consequently, additional research is necessary, as identifying challenges will enable organizations to avoid errors and shortcomings during the GDPR implementation process, and it may be beneficial for governments to adopt measures to assist organizations facing difficulties in implementing GDPR.

Conceptual Framework

Due to the limited number of studies identified after applying the first four search terms, an additional string was incorporated to expand the search. The literature review assisted the author in determining a suitable framework structure and revealed a deficiency in the issues encountered by startups due to the adoption of the General Data Protection Regulation (GDPR) since May 2018.

Upon analysis of the article titles and abstracts, 27 were classified as relevant. Thirty-two challenges pertaining to GDPR were identified and categorized into four constructs: compliance costs. The researcher corroborated these problems through interviews with three Catalan companies registered with the Agency for Business Competitiveness (ACCIÓ).

Process Modification

Tim Erridge, Context Information Security In an interview conducted by Steve Mansfield-Devine, editor of Computer Fraud & Security (Mansfield-Devine, 2016), he asserts that GDPR is not a compliance framework; rather, it concerns the demonstration of due diligence in safeguarding data. Consequently, a primary task for any organization is to exhibit a pre-established cyber incident response strategy that aligns with the principles of GDPR and mitigates the danger of penalties.

The application of emergent technologies like Big Data poses challenges in achieving compliance with the GDPR. Ensuring compliance with the GDPR amidst the era of Big Data and Cloud Computing, particularly due to the extensive volume of data a controller may process for an individual data subject, especially when external third parties and multiple service providers are involved in the processing.

References

[1] Singh, V. K., Mishra, A., Gupta, K. K., Misra, R., & Patel, M. L. (2015). Reduction of microalbuminuria in type-2 diabetes mellitus with angiotensin-converting enzyme

inhibitor alone and with cilnidipine. *Indian Journal of Nephrology*, *25*(6), 334-339.

[2] Karakolias, S. E., & Polyzos, N. M. (2014). The newly established unified healthcare fund (EOPYY): current situation and proposed structural changes, towards an upgraded model of primary health care, in Greece. Health, 2014.

[3] Shilpa, Lalitha, Prakash, A., & Rao, S. (2009). BFHI in a tertiary care hospital: Does being Baby friendly affect lactation success?. *The Indian Journal of Pediatrics*, *76*, 655-657.

[4] Polyzos, N. (2015). Current and future insight into human resources for health in Greece. Open Journal of Social Sciences, 3(05), 5.

[5] Gopinath, S., Janga, K. C., Greenberg, S., & Sharma, S. K. (2013). Tolvaptan in the treatment of acute hyponatremia associated with acute kidney injury. *Case reports in nephrology*, *2013*(1), 801575.

[6] Gopinath, S., Giambarberi, L., Patil, S., & Chamberlain, R. S. (2016). Characteristics and survival of patients with eccrine carcinoma: a cohort study. *Journal of the American Academy of Dermatology*, *75*(1), 215-217.

[7] Swarnagowri, B. N., & Gopinath, S. (2013). Ambiguity in diagnosing esthesioneuroblastoma--a case report. *Journal of Evolution of Medical and Dental Sciences*, *2*(43), 8251-8255.

[8]

[9] Srinivas, N., Mandaloju, N., & Nadimpalli, S. V. (2020). Cross-Platform Application Testing: AI-Driven Automation Strategies. Artificial Intelligence and Machine Learning Review, 1(1), 8-17.

[10] Mandaloju, N., Srinivas, N., & Nadimpalli, S. V. (2020). Machine Learning for Ensuring Data Integrity in Salesforce Applications. Artificial Intelligence and Machine Learning Review, 1(2), 9-21.

[11] Mandaloju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2021). A Unified Approach to QA Automation in Salesforce Using AI, ML, and Cloud Computing. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(2), 244-256

[12] Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. Artificial Intelligence and Machine Learning Review, 2(4), 8-18.

[13] Manduva, V.C. (2021) AI-Driven Predictive Analytics for Optimizing Resource Utilization in Edge-Cloud Data Centers. The Computertech. 21-37.

[14] Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). AI-Augmented Workforce Planning: Leveraging Predictive Analytics for Talent Acquisition and Retention. Artificial Intelligence and Machine Learning Review, 2(1), 10-20.

[15] Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2021). Unifying AI and Automation: A Multi-Domain Approach to Intelligent Enterprise Transformation. Journal of Advanced Computing Systems, 1(11), 1-9.

[16] Manduva, V.C. (2021) Security Considerations in AI, Cloud Computing, and Edge Ecosystems. The Computertech. 37-60.

[17] Pasham, S.D. (2021) Graph-Based Models for Multi-Tenant Security in Cloud

Computing. International Journal of Modern Computing. 4(1): 1-28.

[18] Manduva, V.C. (2021) The Role of Cloud Computing In Driving Digitals Transformation. The Computertech. 18-36.

[19] Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Driven Self-Healing IT Systems: Automating Incident Detection and Resolution in Cloud Environments. Artificial Intelligence and Machine Learning Review, 1(4), 1-11.

[20] Manduva, V.C. (2020) AI-Powered Edge Computing for Environmental Monitoring: A Cloud-Integrated Approach. The Computertech. 50-73.

[21] Pasham, S.D. (2018) Dynamic Resource Provisioning in Cloud Environments Using Predictive Analytics. The Computertech. 1-28.

[22] Manduva, V.C. (2021) Optimizing AI Workflows: The Synergy of Cloud Computing and Edge Devices. International Journal of Modern Computing. 4(1): 50-68.

[23] Inaganti, A. C., Sundaramurthy, S. K., Ravichandran, N., & Muppalaneni, R. (2020). Cross-Functional Intelligence: Leveraging AI for Unified Identity, Service, and Talent Management. Artificial Intelligence and Machine Learning Review, 1(4), 25-36.

[24] Nersu, S. R. K., Kathram, S. R., & Mandaloju, N. (2020). Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. Revista de Inteligencia Artificial en Medicina, 11(1), 422-439.

[25] Manduva, V.C. (2021) Exploring the Role of Edge-AI in Autonomous Vehicle Decision-Making: A Case Study in Traffic Management. International Journal of Modern Computing. 4(1): 69-93.

[26] Sai, K.M.V., M. Ramineni, M.V. Chowdary, and L. Deepthi. Data Hiding Scheme in Quad Channel Images using Square Block Algorithm. in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2018. IEEE.

[27] Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. (2020). AI-Powered Workflow Optimization in IT Service Management: Enhancing Efficiency and Security. Artificial Intelligence and Machine Learning Review, 1(3), 10-26.

[28] Manduva, V.C. (2020) How Artificial Intelligence Is Transformation Cloud Computing: Unlocking Possibilities for Businesses. International Journal of Modern Computing. 3(1): 1-22.

[29] Pasham, S.D. (2017) AI-Driven Cloud Cost Optimization for Small and Medium Enterprises (SMEs). The Computertech. 1-24.

[30] Pasham, S.D. (2019) Energy-Efficient Task Scheduling in Distributed Edge Networks Using Reinforcement Learning. The Computertech. 1-23.

[31] Inaganti, A. C., Sundaramurthy, S. K., Ravichandran, N., & Muppalaneni, R. (2020). Zero Trust to Intelligent Workflows: Redefining Enterprise Security and Operations with AI. Artificial Intelligence and Machine Learning Review, 1(4), 12-24.

[32] Manduva, V.C. (2020) The Convergence of Artificial Intelligence, Cloud Computing, and Edge Computing: Transforming the Tech Landscape. The Computertech. 1-24.

[33] Pasham, S.D. (2020) Fault-Tolerant Distributed Computing for Real-Time Applications in Critical Systems. The Computertech. 1-29.

[34] Mandaloju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2021). Overcoming Challenges in Salesforce Lightning Testing with AI Solutions. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(1), 228-238.

[35] Nersu, S. R. K., Kathram, S. R., & Mandaloju, N. (2021). Automation of ETL Processes Using AI: A Comparative Study. Revista de Inteligencia Artificial en Medicina, 12(1), 536-559.