From Strategy to Execution: A Practical Roadmap for SME Cloud Migration

Dr. Nagaraju Kolli[1*]

[1*]PhD in Information Technology, University of the Cumberlands, 6178 College Station Drive, Williamsburg, KY 40769
[1*]kollinagaraju7@gmail.com
.
Corresponding Author Email ID: [1*]kollinagaraju7@gmail.com

Abstract:
Due to the high rate of market growth, small and medium-sized businesses (SMEs) are increasingly under pressure to modernize their IT infrastructure In 2024 the worldwide spending on cloud is estimated to reach $351.8 billion, and in 2033 the figure will increase to $1,230.8 billion. Cloud solutions provide SMEs with an economy to pay-per-use, real-time scalability, enterprise-level security, and advanced services (AI/ML, analytics), allowing them to keep up with the changing market and stay competitive in the digital economy. Poor migration planning, insufficient in-house knowledge, unexpected expenses, and regulatory burdens, however, contribute to migrations gone awry. Where migration projects cost long-term, security lapses, and operations become out of control are a point of reality. To overcome such obstacles, we present a practitioner-driven seven-step Action Framework of SME Cloud Migration: Readiness Assessment; Policy Alignment & Strategy Design; Technology Selection; Security Architecture Planning; Migration Execution; Training & Change Management; and Continuous Monitoring & Optimization. Our framework is based on best practices across industries, as well as the operational case patterns, placing smaller businesses on the path to avoiding some of the most widespread cloud pitfalls, including cost-based lift-and-shift traps, vendor lock-in, and post-migration neglect, and to maintain the long-term value of cloud through the process of steady improvement.

Keywords: *Cloud Migration Framework, Readiness Assessment, Security Architecture, Change Management, Continuous Optimization.*

1. INTRODUCTION

1.1 The Strategic Need for Cloud Computing in SMEs

Cloud computing has transformed the way small and medium-sized businesses (SMEs) run their IT systems and provide services. Because the market is growing quickly—from $351.8 billion in 2024 to $1,230.8 billion by 2033, SMEs are using the cloud as a strategic requirement. Paying for servers and data centers as you go frees up money and makes unexpected capital costs into manageable operational charges. Small and medium-sized businesses that are careful with their money require this economic flexibility[1]. Cloud platforms also let businesses increase their computing, storage, and networking resources in real time, which makes them good for times when demand suddenly goes up or when growth happens that wasn't planned for. This is because businesses don't have to wait for hardware to be bought and pay for it.Cloud services provide prices, flexibility, and security and compliance that are up to business standards, which many small and medium-sized businesses can't afford. superior than in-house systems, secure data centers, superior threat detection, and international standards protect SMEs against intrusions[2]. Built-in disaster

recovery and business continuity features keep operations safe, while seamless global access and collaboration provide teams in different parts of the world the tools they need to work together. Cloud services like AI, ML, and big data analytics finally make it possible for new ideas to come up and for companies to stand out from the competition. These benefits make it necessary for small and medium-sized businesses (SMEs) to use the cloud in order to be competitive, efficient, and strong in the digital economy[3].

1.2 Problems that small and medium-sized businesses often run into while moving to the cloud

Cloud migration is hard for small and medium-sized businesses since they don't have the resources or knowledge. Small businesses often go over budget because of the costs of moving to a new location and other costs that aren't obvious, such data egress and application re-architecting. Lean teams have a hard time keeping data safe while it is being moved, setting up cloud infrastructures correctly, and following onerous rules like GDPR and HIPAA. It's hard to plan and carry out migrations when you don't have cloud capabilities in-house, and using modern cloud services with old apps can sometimes lead to problems you did not foresee. Bad migrations may stop a business from running smoothly and hurt customer trust. The large amount of data involved makes it more likely that it will be lost or corrupted. Last but not least, SMEs need to avoid becoming locked into a vendor and get beyond any resistance from the organization as employees and management adjust to new procedures and governance structures. These problems are all interrelated; thus you need a well-organized relocation strategy that is specialized to SMEs[4].

An overview of the goals and structure .This article's goal is to provide small and medium-sized businesses (SMEs) an Action Framework for Cloud Migration that is based on academic research, industry best practices, and real-world examples. The framework has seven parts: (1) Readiness Assessment, to check how ready the business, technology, finances, and organization are; (2) Policy Alignment & Strategy Design, to set up governance structures and set migration goals; (3) Technology Selection, to pick the best mix of IaaS, PaaS, and SaaS offerings; and (4) Security Architecture Planning, to design strong Data Protection and Compliance controls. By following this step-by-step process, SMEs may avoid making mistakes while planning on the fly and confidently transform their strategic goals into cloud operational success[5].

2. An Action Framework for SME Cloud Migration

Many small and medium-sized businesses (SMEs) understand how important cloud computing is for their business, but they have trouble moving to it instead of seeing its benefits. When migrations aren't planned well enough because of financial limits, a lack of cloud skills in-house, or a lack of people, they can go beyond budget, leave security flaws, and cause disruptions. Our seven-phase Action Framework breaks the migration process down into clear, sequential phases that assist small and medium-sized businesses deal with each important aspect—technical, financial, and organizational—in turn.

Step one: Readiness Assessment

First, find out if a small business is ready for the cloud. Along with listing servers, storage, and network parts, this step must also meet with the company's goals, which might include lowering capital costs, speeding up time to market, increasing disaster recovery, or allowing remote work. It is also important to get support from senior management and to deal with resistance inside the company. To find cloud-native systems and older platforms that need to be replat formed or refactored, you need to compare a full list of hardware, software licenses, and security measures to the needs of the applications. SMEs figure out their Total Cost of Ownership by adding up their present capital and ongoing IT expenditures with the cloud

costs they plan to incur, including as provider fees, data transfer fees, refactoring costs, and training budgets. Finally, assessments of staff skills and organizational agility show that there are gaps in cloud knowledge or cultural preparedness, which leads to targeted training or working with outside groups. Automation from big cloud providers and independent portfolio analyzers can speed up this complex analysis, but it's important to have a balanced emphasis on all four areas: business, technology, finance, and people. This will help prevent problems later on[6].

Second step: Aligning policies and establishing a plan SMEs establish a formal migration strategy and governance structure after checking how ready they are. This starts with rules for protecting and categorizing data, baseline security standards, and compliance requirements for GDPR, HIPAA, or a specific industry[7]. A cost-management plan includes budgets, tagging techniques, and ways to keep an eye on expenditures so they don't grow out of hand. Identity and Access Management regulations make sure that people only have access to the information they need. The "7 R's" of migration are used to evaluate each application in the portfolio: "Rehost" (lift-and-shift virtual machines), "Replatform" (modest refactoring to use managed services), "Repurchase" (moving to SaaS), "Refactor" (full rearchitecture for cloud-native benefits), "Relocate" (VM mobility in hybrid VMware environments), "Retain" (keeping compliant or complex systems on-prem), and "Retire" (decommission)[8]. SMEs make a high-level plan for each work that takes into account time, cost, and long-term flexibility. They often start with a trial migration to evaluate the process and build trust. Detailed dependency mapping makes ensuring that related parts move together, and proactive risk planning uses rollback mechanisms to plan for security, downtime, and vendor-lock-in issues. Phase 2 makes sure that migration activities are well-planned instead of being done on the fly by tying strategic decisions to technology realities and business goals[9].

Seven-Phase Action Framework for Cloud Migration
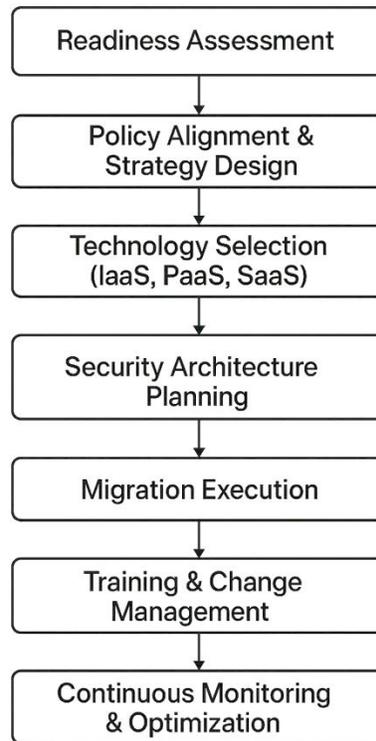
Table 1: SME Cloud Migration Strategies

This structured comparison helps SMEs make informed decisions during the strategy design phase, aligning their technical approach with their specific business context and resource realities.

Step 3: Choosing the Right Technology
After deciding on their migration goals and application strategies, SMEs choose cloud services and deployment alternatives that work for their needs, budgets, and in-house skills. IaaS gives clients full control over virtual machines, storage, and networking. PaaS maintains runtimes and platforms so teams can focus on code and data. SaaS provides preconfigured apps with low operating costs. It's customary to use IaaS for lift-and-shift workloads, PaaS for databases, and SaaS for email. Public (using hyperscale providers for cost-effective scalability), private (dedicated infrastructure for strict compliance), or hybrid installations keep sensitive data on-premises while taking advantage of the flexibility of the public cloud. Finally, small and medium-sized businesses look at AWS, Azure, GCP, or specialist clouds based on how many services they provide, how well they work, how much they cost, how secure they are, how well they support other systems, and how easy it is to integrate them with other systems. Comparisons help reduce vendor lock-in and point the way to strategies like multi-cloud, open-source portability, and containerization[10].

Step 4: Planning the security architecture Once service models and providers are in place, small and medium-sized businesses (SMEs) must make sure their cloud environment is very safe under shared accountability. They use VPCs/VNets, firewalls, VPNs, or dedicated connections to separate networks. They also need encryption while data is being sent and while it is at rest, and they set constraints for who may access what (strict roles, MFA, least privilege). Vulnerability management (patching, scanning) and real-time threat detection (logging, alerting, incident-response playbooks) are both parts of proactive defense. Strong backup and disaster recovery plans that follow GDPR, HIPAA, and PCI DSS rules can make systems more resilient. Multi-cloud posture managers or native provider solutions (Security Hub, Defender for Cloud, Security Command Center) provide you a single view of everything. By employing the cloud's built-in security features, SMEs may transform high-level security strategies into real controls that fill in gaps and exceed regulatory requirements[11].

Step 5: Move

To keep things running smoothly, SMEs plan migrations in stages. Using provider services or appliances to move large datasets over a network keeps the data safe and cuts down on downtime through checksums and synchronized replication. They employ their chosen "R" strategy—lift-and-shift automation tools (Terraform, CloudFormation) or code refactoring workflows—to deploy applications and then check them for functionality, performance, security, integration, and user approval. Dress rehearsals of noncritical workload transfers show problems early on. With live VM migration, thorough cutover preparations make the final changeover go smoothly and provide rollback options. SMEs cut down on difficulties that happen after a migration by scheduling them, automating deployments, and making sure that testing is comprehensive[12].

Step 6: Training and Making Changes

People need to use new tools and strategies for technical achievement. IT experts get technical seminars and certificates, end users get training depending on their roles, and SMEs clearly explain the benefits of cloud computing. A structured change-management program like Kotter or ADKAR makes sure that leaders support the program, sets goals and milestones, and lets people give input. Having "cloud champions" inside the company, updated documentation, and support centers after the shift all make the transfer easier and give people more confidence. SMEs make sure that staff use cloud-based workflows and that investments in technology increase productivity by addressing skills gaps and cultural obstacles[13].

Step 7:

Ongoing improvement and monitoring When you use the cloud, you start along a path of constant progress. Monitoring a SME comprises uptime, response times, resource use, security (audit logs and vulnerability scans), compliance (regular audits), and pricing (detailed billing, tagging, and FinOps processes). To get the most out of their money, they make sure that instances are the proper size, get rid of unused resources, and leverage pricing structures like spot instances, reserved capacity, and savings programs. Periodic strategy reviews connect the cloud infrastructure to changing business goals, and automatic alerts and dashboards encourage speedy changes. This never-ending cycle of watching, analyzing, and making changes keeps the cloud flexible, safe, and cost-effective. This makes migration a long-term advantage instead of a one-time task[14].

Strategy	Description	SME Pros	SME Cons	Use Case
Rehost	Lift-and-shift VMs to IaaS with no code changes	Fast; minimal skills needed	Misses cloud optimizations; possible higher run costs	Quick move of noncritical workloads
Replatform	Small app tweaks to use managed services (e.g., DB)	Some cloud benefits; moderate effort	Not fully cloud-native; requires code changes	Scaling a database via managed service
Repurchase	Swap on-prem apps for SaaS (e.g., CRM, email)	No maintenance; always up-to-date	Data migration; integration issues; lock-in	Moving to Salesforce or Microsoft 365
Refactor	Rewrite for cloud-native (microservices/serverless)	Full scalability & efficiency; future-proof	High cost; complex; needs specialist skills	Modernizing core, high-value apps
Relocate	Migrate VMware VMs to hyperscaler with vMotion/HCX	Seamless for VMware shops; leverages existing skills	VMware-only; limited native cloud features	Extending on-prem VMware to AWS via VMC
Retain	Keep workloads on-premises or current hosting	Avoids migration effort; meets compliance needs	Ongoing maintenance; limits agility	Sensitive data or legacy systems
Retire	Decommission obsolete or redundant applications	Cuts costs; simplifies estate	Risk of lost functionality; archival needed	Phasing out outdated or duplicate software

3. Real-World Case Patterns & Lessons Learned

Real-world cloud migrations for SMEs show tendencies that might help new people learn. A lot of small and medium-sized businesses (SMEs) become stuck in the "cost-driven lift-and-shift" trap, moving old programs to the cloud without changing them to save money. This method makes it easy to move quickly with minimal work up front, but bad performance, unexpected data-transfer costs, and excessive resource use lower expected savings, which leads to expensive re-engineering[15]. The "cautious hybrid evolution" keeps sensitive or difficult workloads on-premises and moves cloud-ready systems in waves to find a balance between risk and profit. SMEs start with SaaS trials or moving non-critical infrastructure to become used to the process before moving on to harder responsibilities. This staged hybrid solution takes longer to get all the benefits of the cloud, but it causes less disruption, fulfills regulatory requirements, and creates knowledge in-house[16]. Third, in the "strategic SaaS transformation," SMEs switch from on-premises tools like email, CRM, and ERP to SaaS solutions. This can save administrative expenses and take

advantage of the provider's innovation, but it needs careful vendor selection, quick data transfer to the SaaS platform, perfect connections across cloud apps, and strict change management to get users to accept it[17].

SMEs typically make mistakes like moving without a plan, not realizing how complicated their old systems are, losing control of costs because of bad FinOps procedures, ignoring security and compliance, and not testing before cutover. Strong support from top executives, thorough readiness assessments, clear goals, a staged migration strategy, rigorous testing, excellent training programs, and ongoing monitoring and optimization are all important for success[18].
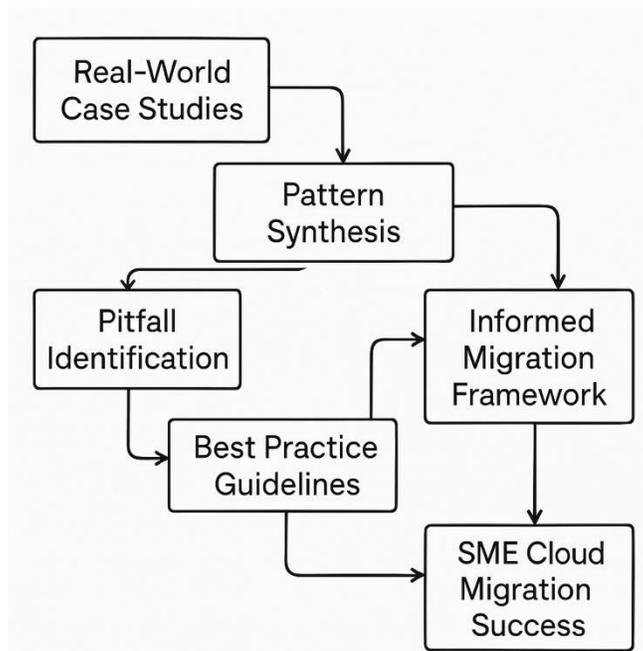
Figure 2: Real-world SME migration experiences into a practical migration framework

These insights make it easier to learn about SME cloud migration: real-world case studies help people recognize patterns that show risks and things that worked well that they can copy. This information loop makes it easier for small and medium-sized businesses (SMEs) to plan and carry out future migrations.

Table 2: SME Cloud Migration: Common Pitfalls vs. Critical Success Factors/Mitigation

Common Pitfall	Mitigation Strategy / Critical Success Factor
Lack of clear strategy and planning	Define specific business goals; develop a detailed migration roadmap; ensure IT initiatives align with business objectives.
Inadequate assessment of systems, costs, or skills	Conduct a comprehensive readiness review (technical, financial, organizational); perform TCO analysis; identify skill gaps early and plan training.
Cost overruns / poor FinOps	Create a detailed cost model upfront; establish continuous cost monitoring and optimization (FinOps); right-size resources; leverage reserved/spot pricing and discounts.

Security and compliance neglect	Architect security from the start; enforce strong IAM, encryption, and network controls; map compliance requirements; clarify shared-responsibility roles.
Insufficient expertise / skills gap	Invest in targeted staff training and certifications; engage experienced cloud partners or MSPs; validate skills during readiness.
Inadequate testing and validation	Allocate dedicated time and resources for pilot migrations; perform comprehensive functional, performance, security, integration, and user-acceptance testing before cutover.
Poor change management / weak stakeholder buy-in	Secure visible senior-management sponsorship; communicate vision and progress clearly; deliver role-based user training; address resistance proactively.
Vendor lock-in	Adopt multi-cloud or hybrid models where feasible; favor open standards and containerization; design abstraction layers for portability.
Ignoring post-migration optimization	Treat migration as ongoing: implement continuous monitoring of performance, cost, and security; schedule regular reviews and resource optimizations.

This mapping reinforces that proactively addressing known risks through the application of critical success factors, as structured within the Action Framework, is key to improving SME cloud migration outcomes[19].

4. Monitoring & Evaluation Checklist

Goal

To make sure that cloud migrations are good for business and stay healthy, small and medium-sized businesses (SMEs) require practical tools to keep track of progress and find problems early. To keep track of operations, security, compliance, and costs, this demands a short list of Readiness Assessment KPIs and a strict process after the move.

4.1 Key Performance Indicators for Migration Success

Before migrating, SMEs should set a baseline for a few critical SMART KPIs. Cost measurements include the Total Cost of Ownership, the difference between the actual and budgeted costs, and the percentages of resources that need to be right-sized or decommissioned. Average and peak application response times, system availability, and CPU, memory, and I/O utilization are all examples of performance measurements that show the degree of cloud service. Key performance indicators (KPIs) for security and compliance that lower risk include the number and severity of incidents, the average time it takes to find and fix problems, and the use of encrypted sensitive data. Adoption rates, the quantity of help desk tickets, and satisfaction surveys all demonstrate that the process is not going well. If the transfer is allowed for new ideas, operational efficiency measurements like infrastructure provisioning time, deployment frequency, and IT effort transform from normal maintenance to strategic initiatives. SMEs should focus on crucial results by finding five key indicators that are linked to their main aims[20].

Checklist for evaluation following migration Once the cloud is up and running, small and medium-sized businesses (SMEs) should set up a basic quarterly review procedure to transform raw data into action. This

usually means: Look at the baseline, budget, cost, performance, security, and user experience metrics. Find out what went wrong and why[21].

Cost Optimization Audit: Find unused resources, change the sizes of instances, and look at reserved instances and spot pricing to save expenses. Use robust access controls, widespread encryption, up-to-date vulnerability scans, and genuine regulatory audits and certifications to make sure your system is safe and compliant. Check the performance health by making sure that the auto-scaling rules meet demand and looking for problems and bottlenecks in the logs and alerts. User Feedback and Adoption: Find out if users are happy with the applications and fix any problems with training or workflows. Roadmap Alignment: Make sure that the goals for migration and the roadmap are in line with business goals and that refactoring and adopting new services are on track.

By using this review checklist as part of their daily work, SMEs turn migration into a cycle of continuous improvement. This makes sure that the cloud environment meets its goals and gets better over time. This checklist provides a simple yet comprehensive mechanism for SMEs to move beyond purely technical metrics and conduct regular, holistic reviews of their cloud investment. It helps ensure that the migration continues to deliver business value long after the initial project concludes and prompts necessary adjustments and optimizations, mitigating the common pitfall of post-migration neglect[22].

4.3 Mapping KPIs to SME Cloud Migration Objectives

To further clarify the link between measurement and strategy, the following table maps common SME migration objectives to the relevant KPIs discussed in section 4.1. This helps SMEs prioritize which KPIs are most critical based on their specific goals.

Table 3: Mapping KPIs to SME Cloud Migration Objectives

Common SME Migration Objective	Relevant Key Performance Indicators (KPIs)
Reduce IT Costs	TCO Comparison; Cloud Spend vs. Budget; Cost Savings Achieved; Cost per Resource; Resource Optimization Rate.
Improve Scalability & Flexibility	Resource Utilization (CPU, Memory); Auto-Scaling Efficiency; Infrastructure Provisioning Time; System Uptime/Availability during peak loads.
Enhance Security Posture	Number/Severity of Security Incidents; MTTD/MTTR; Vulnerability Remediation Rate; Data Encryption Coverage; Security Audit Results.
Ensure Compliance	Compliance Audit Results; Data Encryption Coverage; Access Control Violations.

Improve Application Performance	Application Response Time (ART/PRT); Error Rate; Network Latency; System Uptime/Availability.
Increase Business Agility / Innovation	Application Deployment Frequency/Time; Infrastructure Provisioning Time; IT Staff Productivity (Shift from Maintenance).
Enhance Disaster Recovery / Reliability	System Uptime/Availability; Reduction in Downtime Incidents; Successful DR Test Results; Data Recovery Point/Time Objectives (RPO/RTO) met.
Improve User Experience & Productivity	User Satisfaction Scores (CSAT/NPS); Perceived Lag/Responsiveness; Adoption Rate of New Tools; Help Desk Ticket Volume; IT Staff Productivity.

This mapping directly connects the *why* of the migration (the business objectives established in Phase 1) with the *how* of measurement (the KPIs tracked in Phase 7). It provides a practical tool for SMEs to select and prioritize the most meaningful metrics for their specific situation, ensuring that monitoring efforts are focused on demonstrating progress towards their strategic goals.

5. Conclusion

Moving to the cloud gives SMEs more agility, productivity, security, and innovation, but it's not easy. Our seven-phase Action Framework breaks down this complexity into manageable steps, starting with a readiness assessment, policy alignment and strategy design, technology selection, security architecture planning, migration execution, training and change management, and continuous monitoring and optimization. Since they have set business goals and assessed technical, financial, and organisational readiness, SMEs can choose service provision and security control models that best match their strategic purposes. Systematic change-management programs reduce disruptions through staged rollouts, trial migrations, and comprehensive testing. Finally, integrating FinOps processes and real performance and security monitoring turns a migration into a loop of continuous improvement, making cloud adoption a lasting competitive advantage. Beginning SME leaders will benefit greatly from early adopters' lessons on starting with a holistic overview of legacy systems, budgets, and internal skills instead of chasing the latest technologies; using well-defined goals to inform the selection of the desired service models, migration vehicles, and suppliers; and adopting a shared-responsibility security model that incorporates p. Because people are success's lifeblood, listening, communication, role-based training, and visible sponsorship promote adoption. Migration is just the beginning; continuous cost optimization and security posture evaluation are needed to sustain the value and flexibility that drew SMEs to the cloud. SMEs should adapt their cloud strategy to new paradigms as they emerge. Serverless and Function-as-a-Service systems require simplified architecture, embedded AI/ML services provide automation and data-driven reasoning but require governance and training, and multi-cloud deployment adds resiliency and supplier leverage but complexity. As environmental sustainability becomes more relevant in procurement agendas and cloud

decisions, providers' energy efficiency and carbon footprints must be considered. By upgrading their game plan with technical roadmaps, strategic targets, and market breakthroughs, SMEs can ensure that their cloud investments will support business agility, cost-effectiveness, and competency differentiation long-term.

REFERENCES

[1]   Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58. https://doi.org/10.1145/1721654.1721672

[2]   Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision Support Systems, 51(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

[3]   Sultan, N. (2011). Reaching for the "cloud": How SMEs can manage. International Journal of Information Management, 31(3), 272–278. https://doi.org/10.1016/j.ijinfomgt.2010.08.001

[4]   Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. (2010). Cloud migration: A case study of migrating an enterprise IT system to IaaS. IEEE International Conference on Cloud Computing, 450–457. https://doi.org/10.1109/CLOUD.2010.41

[5]   Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management, 35(2), 177–182. https://doi.org/10.1016/j.ijinfomgt.2014.01.005

[6]   Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. Electronic Journal of Information Systems Evaluation, 14(1), 110–121.

[7]   Lian, J.-W., Yen, D. C., & Wang, Y.-T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. International Journal of Information Management, 34(1), 28–36. https://doi.org/10.1016/j.ijinfomgt.2013.08.006

[8]   Tarhini, A., Ammar, H., & Tarhini, T. (2015). A large-scale study of the factors influencing the adoption of mobile banking. International Journal of Information Management, 35(4), 406–415. https://doi.org/10.1016/j.ijinfomgt.2015.01.009

[9]   Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (NIST SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

[10] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5. https://doi.org/10.1186/1869-0238-4-5

[11] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. International Conference on Computer Science and Electronics Engineering, 647–651.

https://doi.org/10.1109/ICCSEE.2012.373

[12] Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. Journal of Information Technology, 27(3), 179–197. https://doi.org/10.1057/jit.2012.17

[13] Khajeh-Hosseini, A., Sommerville, I., & Bogaerts, J. (2011). Decision support tools for cloud migration in the enterprise. Proceedings of the 1st International Workshop on Managing Operations in the Cloud (MOC'11), 132–136. https://doi.org/10.1145/1996130.1996145

[14] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6

[15] Grandon, E. E., & Pearson, J. M. (2004). Electronic commerce adoption: An empirical study of small and medium US businesses. Information & Management, 42(1), 197–216. https://doi.org/10.1016/j.im.2003.12.010

[16] Berman, S., Kesterson-Taylor, W., & Eidus, R. (2012). Cloud adoption: Measures, mechanisms, and circumstances: Insights from the field. IEEE Software, 29(5), 52–58. https://doi.org/10.1109/MS.2011.144

[17] Rai, A., Pavlou, P. A., Im, G., & Du, S. (2012). Interfirm IT capability profiles and communications for cocreating relational value: Evidence from the logistics industry. MIS Quarterly, 36(1), 233–262.

[18] Armbrust, M., et al. (2010). Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, University of California, Berkeley.

[19] Farahnakian, F., Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014). Towards autonomous management of data center resources for big data applications. International Journal of Big Data Intelligence, 1(3), 183–199. https://doi.org/10.1504/IJBDI.2014.066321

[20] Zou, D., Chen, B., Zhao, G., & De Flaviis, F. (2010). Taxonomy of virtualization and cloud computing. International Symposium on Virtualization Technologies in Distributed Computing, 157-161. https://doi.org/10.1145/1921271.1921303

[21] Kim, H., Lee, H., & Lee, I. (2013). Cloud services orchestration support system for enterprise mashup. IEEE Transactions on Services Computing, 6(4), 609–618. https://doi.org/10.1109/TSC.2012.17

[22] Cabrera, Á., & Rienda, L. (2018). Change management practices in successful information systems implementation projects. International Journal of Information Management, 38(1), 44–55. https://doi.org/10.1016/j.ijinfomgt.2017.08.006