A Conceptual Framework for Secure Cloud Migration

Srishti Ahuja and T N Nisha*
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India
Email: nisha@scit.edu*

Abstract. Cloud computing is a budding web-based technology that tends to prevail in our environment, especially in the areas of computing and information technology that require large-scale network computing. Cloud computing is a shared set of services gaining popularity due to its profitability, availability, and high production. Just on the security grounds, cloud computing's immense potential cannot be overlooked: ongoing research and the investigation of consistent, robust, and integrated cloud computing security models may be the solitary motivational pathway. There are three service and four deployment models in cloud computing. Cloud computing, together with its several advantages, also brings a much more difficult condition concerning privacy, authenticated access, data protection, etc. Because of these problems, the acceptance of cloud computing is becoming difficult in the current era. In this study, several security concerns related to reliability and data privacy, main aspects impacting cloud computing, were tackled, and recommendations on specific areas were also discussed.

Keywords: Cloud computing, Data Protection, Security Issues, Data Privacy.

1. Introduction
Software developers describe the Cloud differently than a database administrator, whereas a system administrator might have a dissimilar description. Through an Internet connection, users can access a wide range of scalable services under the Cloud. Providers like Amazon, Google, Microsoft, and countless others offer several cloud-based services that customers can pay based on service consumption and subscription. Many providers offer a wide range of cloud services, such as messaging, CRM, storage, social computing, content management, identity management, etc. Cloud computing depends on sharing resources. The Cloud is the term usually used for cloud computing. Cloud computing fulfills a broad array of purposes on the Internet, such as storage, which enables the application software's function by using these Internet-enabled devices [3]. Cloud computing can achieve consistency and economies of scale by taking benefit of resource sharing. The kinds of cloud computing can be categorized according to 2 models: deployment and service models. It is a form of data backup. Besides, it lets you work on an identical file for multiple operations of various sorts. Cloud computing simplifies usage, allowing you to overcome the restrictions of the conventional computer. Cloud computing also offers additional speed by allowing quicker access. These hosted services generally fall into three fundamental groups: "Infrastructure as a Service" (IaaS), "Platform as a Service" (PaaS), and "Software as a Service" (SaaS).
Customers use a cloud service when they need it, usually hourly [2]. This "pay-as-you-go" model has rendered the Cloud flexible so that the provider can fully monitor the services where the customer can have the services the manner they want at all times.

Some basic security threats have exploited the use of cloud computing. An example of a security threat is botnets, which are used to spread malware and spam. In 2010, almost 63% of the 761 data violations inspected by the US Secret Service happened in organizations with a hundred employees or less. Moreover, a survey conducted in 2011 by Symantec Corporation, a security system provider with more than 2,000 small and medium-sized businesses, indicated that a cyber-attack raped nearly 73%.

The prepaid computing model as a resource is one of the greatest features of cloud computing. This computing approach has enabled organizations and businesses that need computing muscle to buy as many resources as necessary devoid of the need for a hefty funds’ investment in information technology infrastructure. Cloud computing' additional benefits are greater flexibility and scalability for a comparatively even cost [5]. In the advancement of distributed systems, cloud computing is the new trend. The cloud infrastructure provides abstraction. The customer does not require understanding or experience to manage it. Cloud providers offer general online business applications accessible from servers with the help of a web browser [6].

The objectives of this study are:

- To study the subject of cloud computing.
- To study service and distribution examples of the cloud computing infrastructure.
- To identify various security challenges faced by organizations while adopting cloud computing in the real world.

This research paper reviews previous work to recognize current knowledge to meet cloud computing-related goals and related security issues. Therefore, the data used is purely secondary in this review article. The majority of the earlier research work was done with an analysis of the traditional literature. For this reason, we performed the literature review as a prime and sole research technique [4].

The aspects presented in this document are arranged to identify and discuss the cloud computing approach and the security concerns and issues that need to be considered when deploying to a computing infrastructure based on Cloud. The discussion of concepts and technical approaches to cloud computing was considered within the discussion context in this document, including architectural illustration. The security concerns intrinsic to the cloud computing approach were discussed later. Exploring cloud computing's security and technological issues has resulted in the conclusion on the general aspects of cloud computing.

1.1 Cloud Computing

Cloud Computing provides figuring resources and services on demand through a distributed architecture with scalable and centralized server resources. Just as "Internet service providers" (ISPs) provide clients with high-speed broadband to use the Internet, "Cloud service providers" (CSPs) present cloud platforms to their clients to utilize and build their web services. ISPs and CSPs both provide services. Cloud computing is a method that allows on-demand and convenient system entrance to a collective set of customizable computing resources, like storage, applications, servers, networks that can be rapidly provisioned also launched with the smallest interaction of service provider or management effort.

In the development of distributed systems, Cloud is the new trend. Before the Cloud, we utilized the grid. In cloud computing, the client does not need understanding or experience to manage the cloud infrastructure; it grants abstraction. It can be used as an Internet service with high scalability, superior performance, high computing power, and service quality. CSPs offer general e-commerce services that are accessible from servers via the web browser.
The mode of computing, also the idea of computing resources have been greatly changed by the latest advancements in the cloud computing area. In a cloud computing infrastructure, resources are often located on someone else's premises or network, and cloud users access them remotely. It may be necessary or at least feasible to store information on the Cloud remote servers for a person in a few instances, which provides the following three sensitive scenarios or states, which are of specific interest in the practical perspective of cloud computing:

- The transfer of confidential and private information to the cloud server.
- The data communication to customers' systems from the cloud server.
- The storage of customers' private information in remote cloud servers which are not client-owned.

The three afore-mentioned situations of cloud computing possess a high risk of security breaches, making study and research into the security aspects of the practice of Cloud computing a must.

1.2 Service Models
Cloud providers broadly provide three kinds of services:

i) “Software as a service” (SaaS): Also called a delivery model, wherein the software also coupled data are hosted in the Cloud set by a third party called a "cloud service provider" (CSP). You use this application on a system of someone else, just like your Gmail account.

ii) “Platform as a Service” (PaaS): You can utilize internet-based tools in this service to build applications that execute on systems software given by a different party, such as Google App Engine.

iii) “Infrastructure as a service” (IaaS): Organizations with computing resources are provided with services through this service which includes servers, networks, storage, and space in the datacenter with payment as peruse.

![Image of Service Models](image.png)

Figure 1: Service Models

1.3 Deployment Models
Figure 1 shows the Service Models. There are four Deployment Models, which are explained in the following sections:

i) Public Model: The general public is open to use this infrastructure. As the expression implies, the public cloud model generally offers resources to everybody, everywhere.

ii) Private Model: This model is meant for private groups, such as a home and an institute, to use it for their purposes. Not everyone has access to this type of service.
iii) **Community Model:** This model is a joint endeavor wherein the infrastructure is allocated among a particular group's several organizations with common motives (conformity, jurisdiction, security, etc.,) whether administered domestically or by third parties and hosted domestically or peripherally.

iv) **Hybrid Model:** A combination of private and public Cloud on the same network is called a hybrid cloud, which can be done if the private Cloud needs various essential public cloud services, such as the private Cloud, which can store data in the private Cloud and we can access it in the public Cloud. Figure 2 depicts the Cloud Deployment Models.

![Figure 2: Cloud Deployment Models](image)

### 1.4 Contribution
This study on cloud computing and related security issues contributed to business practices and research in various manners, as in:

- **Contribution to the theory:** The study made contributions to cloud computing theories, illustrating their applicability and relevance to companies in terms of security. Prospective researchers would significantly benefit in their research from the conjectural viewpoint applied to cloud computing security.

- **Contribution to research:** On research in cloud computing, the study's contributions, especially growing understanding on the security approaches employed by different organizations. Data privacy and protection strategies in different areas can be analyzed using the security issues described in the study.

- **Contribution to practice:** For smaller businesses in different sectors, this study can help ease security problems related to strategic decision-making and, among other organizations, create understanding for security problems related to cloud computing. A model cloud migration plan has also been developed, but it is purely conceptual at the moment.

### 2. Literature Review
The cloud computing concept offers dynamically scalable features over the Internet provisioned as a service. Economic gains are the Cloud's chief driver, as it guarantees to reduce capital expenditures (CapEx) and operating expenses (OpEx). However, there are still some challenges to be solved for this to become a reality. Among them are trust and security concerns, as client information needs to be stored on the Cloud and hence departs the bubble of protection of the information holder. The majority of debates on these subjects are largely motivated by disputes concerning organizational media. An article centered on technical security concerns arises from the use of cloud services and, particularly, on the core technologies employed to create these collaborations linked to the Internet between domains [7]. Cloud
Computing is a money-making, flexible, and established distribution stage for offering IT services to consumers or businesses. However, as important services are often outsourced to third parties, cloud computing presents an additional level of threat, making it challenging to uphold confidentiality also data security, maintain the availability of information and services, and exhibit conformity. Cloud computing takes advantage of numerous technologies (virtualization, Web 2.0, SOA); Their security problems are also inherited by it, discussed by the researchers, recognizing the major vulnerabilities of this kind of structure and the central risks to cloud computing and its setting found in the related literature, in addition to identifying and linking vulnerabilities and threats to possible solutions [8].

In one study, security concerns for cloud computing were discussed. The authors presented a leveled structure for protected clouds. They then focused on two of the levels, namely the data level and the storage level. The authors, particularly, talk about a system for the safe publication of third-party documents in a cloud. Also, the document discussed the safe processing of associated queries with the Hadoop and Reduce map and the employ of secure coprocessors for cloud computing.

In conclusion, the XACML implementation for Hadoop is discussed, and the belief that it will be an important aspect of secure cloud computing to build trusted applications from unreliable components [9].

The requirement for configuring expensive computing frameworks for IT-based services and solutions used by the business can be eliminated by cloud computing. It guarantees to supply a flexible, internet-accessible IT architecture for lightweight, portable machines, which would allow for a multiple augment in the capabilities or capacity of new and existing software. All information resides on a set of network resources in a cloud computing environment, allowing information to be accessed with virtual machines. Because these data centers can be anyplace on the earth away from the control and reach of customers, several privacy and security threats must be understood and resolved.

Moreover, the possibility of an event that has been observed fairly frequently in present times, a server crash, can never be denied. Several problems need to be tackled regarding security and confidentiality in a cloud computing setting. A thorough investigation was carried out. The document aimed to elaborate and analyze the innumerable unsolved problems that threaten the adoption and diffusion of cloud computing, affecting the various stakeholders related to it [10].

An article presented holistic research on security threats and problems in cloud computing. Foremost, it analyzes the effects of distinct cloud computing resources, such as multiple ownership, third-party control, and elasticity, on security requirements. Next, the Cloud's security requirements are analyzed in terms of key issues: availability, confidentiality, integrity, compliance, trust, and audit. Also, he discussed taxonomy for security problems in cloud computing. Lastly, he summarized the security problems in cloud computing using a cloud security environment [11]. Cloud computing has become a popular paradigm due to its first-class computing services at the cheap and superior performance. Cloud computing has become prevalent because of its network-centric approach, flexible infrastructure, and user-friendliness. However, its widespread use is diminished because some security problems are still unsolved by the cloud computing paradigm, which can exacerbate the service quality and the privacy of customer data. In an article, the author presented research on security concerns concerning security hazards and their solutions. The contribution pointed to examining and classifying the work systems of the major security problems and the likely countermeasures existing in the literature. A parametric assessment of the threats targeted at cloud systems was performed. Also, he compared several intrusion discoveries and avoidance structures employed to solve security problems. The methods for regulating security compliance among CSPs and confidence in cloud computing were also discussed. As security mechanisms continue to evolve, the author also presented future guidance on security problems in the Cloud and their possible countermeasures [12].

Cloud computing, a fast-growing information technology, has raised distress around the globe. Cloud computing is internet-based computing. Collective software, information, and resources are supplied to
devices and systems as required, such as the electrical grid. The fusion of network technology such as distributed computing, grid computing, parallel computing, etc., with traditional computing technology gave birth to cloud computing. The goal is to build an ideal system with great computing capacity across plenty of comparatively inexpensive computing entities and use complex business models such as SaaS, PaaS, and IaaS to deliver great computing power into end-users' hands. An article introduced the cloud computing pool and service model. This study also presented the present problems in cloud computing, like privacy, reliability, security, etc. A proposal for a solution to these problems was also presented [13]. Cloud computing technology is a novel approach that provides consumers with dramatically scalable, virtualized on-demand resources, hardware and software, and bandwidth. Consumers can generally call for cloud services through a browser or web service. Clients can afford to implement software licenses, hardware, and system maintenance through cloud computing. Alternatively, it also has some security problems. An article introduced four cloud security issues [1], which are Cloud malware injection attack, breaking XML signature elements, browser security, and flood attacks, in addition to providing potential countermeasures [14].

3. Security Concerns in Cloud Computing

Creating a classic and secure IT environment is a lot easier than the procedure of creating and managing a protected cloud space. As this technology is still in its nascent stage, fresh resources and the redistribution of existing resources are not entirely checked and carry new dangers that are still being investigated. The major threats in implementing cloud computing recognized by this study are:

i) Misunderstanding Responsibilities:

Data security is the headache of the group owning data in a traditional scenario. In the cloud computing setting, the tasks are separated among the two performers: the client and the cloud provider. There is a marvelous possibility for mistaken danger administration choices if the consumer does not know that controls are additional desirable to be accepted and cloud providers do not divulge the degree to that the security controls are executed. Different types of cloud services implemented imply various tasks for the customer and the service provider. The provider is accountable for environment security, virtualization software security, and physical security if an IaaS service model is adopted. In contrast, the consumer is answerable for securing everything else above this layer, counting functioning systems, applications, and data. Though, the provider is accountable not only for the environmental and physical security but also for every software service he employs to make available that particular software service to the customer in a SaaS cloud service model.

ii) Privacy and Data Security Concerns:

One of the significant security issues users have when they move to the Cloud is identified with keeping information protected and classified. In this sense, some issues emerge: how the information is transmitted across Cloud or from Cloud to users, etc., which is all identified as the data security lifecycle and is shown in Figure 3. This lifecycle is also present in classical design. However, in a cloud setting, its phases present higher security risks, are much more complex, and require more careful administration. In this regard, it is worth remembering that it is extremely hard to keep an eye on the cloud provider's data manipulation practices for the cloud client and make sure that the data is handled properly. Countermeasures such as data dispersion, public-private key infrastructure, data encryption, API standardization, etc., are implemented as security solutions to build a reliable and safe infrastructure to combat this threat.
Figure 3: Data Security Lifecycle

iii) Lack of Standards:
Developing a complete and universally acknowledged set of standards is difficult due to this technology's immaturity. As a result, to facilitate study and develop the specifications, many standard development organizations were established. Organizations such as the European Telecommunications Standards Institute, Distributed Management Task Force, Open Grid Forum, National Institute of Standards and Technology, There has been confusion in the market as the excitement around Cloud has created a flurry of standards and open-source activity.

iv) Interoperability Problems:
The distributed computing (Cloud) model presents a degree of asset adaptability that has never been extended. Corporations can advantage from extra computational requirements, storage space, bandwidth distribution, etc., when they also lack unlimited reserves to maintain the highest load demands. The suppliers of this service may discover the customer lock-in system alluring. However, for the clients, interoperability issues imply that they are defenseless against cost builds, the nature of administrations not addressing their requirements, the conclusion of at least one cloud administrations, supplier leaving the business, debates between with the cloud supplier. Reliability Breakdowns: One huger element of distributed computing is the unwavering quality or accessibility of applications and data. The breakdown of basic assistance that works in the Cloud affects many users. These occurrences are not uncommon and show the client's absence of power over their information. The irony is that cloud providers have laid down tall standards in terms of reliability that are seldom achieved internally. Though these disruptions concern many customers, IT decision-makers have doubts about whether the functionality presented by the Cloud can replace the desktop functionality. Also, in this sector, top organizations have established some first-class services. Other CSPs that do not boast such a well-developed infrastructure cannot easily reach these levels. Unfortunately for customers, these quality services can have higher costs and are sometimes attracted to cheaper services decision-makers are reluctant to collaborate with this supplier.

v) Malicious Insider:
A person with malicious information is an entity stimulated to make a negative impact on the mission of the business, taking actions that compromise the integrity, availability, and/or confidentiality of data. When classified information is processed exterior to the company, organizational administrators are less sentient of the threat's nature and intensity. They do not have the speedy and direct ability to manage and combat those threats. The inverse relationship between loyalty and risk is well known to security experts.
Suppose outsiders are not automatically more immoral than trusted company employees, who can also commit fraud or make mistakes. In that case, it is wise to invest in long-term company human resources with greater confidence. Malicious actions of an internal member can have a potential effect on the integrity, availability, and confidentiality of every type of information and services with an effect on in-house operations, the reputation of the organization, and the client's confidence. In cloud computing, this is especially important as cloud architectures entail certain functions, such as cloud security personnel, cloud auditors, administrators, that are very high risk.

4. Cloud Migration Framework
To overcome these Security issues, if an organization seeks to modernize mission-critical applications and plans to migrate to the Cloud as part of that process, it does not want to repeat other people's mistakes [15]. So, to maximize the likelihood of a successful migration to the Cloud, take advantage of these learning, which lead to deal with and think about a 10-step checklist of key areas. Figure 4 demonstrates the Cloud Migration Framework

![Cloud Migration Framework](image)

**Figure 4: Cloud Migration Framework**

i) **Ascertaining the migration-architect role:**
Before migration to the Cloud, establishing the role of immigration planner to chief the strength is important. The immigration architect is a position at the method planner level liable for scheduling also completing all aspects of migration; Your primary concern should include defining the refactoring necessary to successfully migrate, developing strategies for data migration, defining requirements for cloud solutions, also responsible immigration priorities as well as production change methods.

ii) **Choosing the cloud integration level:**
When a service is moved from a local, there are two migration methods: shallow and deep cloud integration.
Choosing between single and multi-cloud:
Before starting your migration to the Cloud, answer this question: Would you like to choose a sole cloud supplier also move your administration to run improved for that specific setting, or do you need your administration to be available on many cloud suppliers?

Establishing Cloud KPIs:
"Key performance indicators" (KPIs) are metrics you collect concerning your application or service to assess your expectations' performance. You may have just characterized some KPIs for your applications and administration; however, would they say they are as yet right for an application or administration when it's in the Cloud? The best KPIs for a cloud movement give you how your relocation is going, featuring noticeable or undetectable issues that might be covered up with your application. Maybe the most significant cloud movement KPIs can enable you to decide when the relocation is finished and fruitful.

Establishing performance baselines:
Define a reference metric for every KPI you have decided to measure. Decide how long you will gather information to decide the gauge. Picking a short reference period (for instance, a day) permits you to move speedier. However, you run the chance of not gathering a delegate execution test. Picking a more drawn-out period to benchmark (for example, a month) takes additional time to give more agent information.

Prioritizing migration components:
You also have to decide whether to move the whole service complex straight away or move it to the cloud service by service or component by component.

Performing any required refactoring:
You may need to accomplish additional work on your applications and administration before moving them to make them fill in as viably and productively as conceivable in the Cloud. For instance, you can refactor your application for various organizations according to the deployment requirements.

Preparing a data migration plan:
Data migration is one of the most troublesome periods of a cloud movement. The location of your information can fundamentally influence the exhibition of your application. The same is true if the data is still in place, although the service that accesses it exists in the Cloud.

Switching over the production:
There are two familiar methods: (i) Do it all at once: first, move the complete services or application to the Cloud and confirm that it is functioning properly. (ii) Do a little at a time: shift a small number of clients and then move a few more clients after testing that they are working properly in each pass. Keep on repeating this course until you transfer every one of your clients to the cloud-based application.

Reviewing application resource allocation:
There are some more things to consider once you are done moving the whole lot to the Cloud. The most important is the optimization of resources. When you assign resources (for instance, servers) statically, you are not using the full potential of the Cloud's strengths. Dynamic resource allocation has been integrated into the Cloud. When you shift to the Cloud, ensure your teams are prepared to distribute resources for your application. Additional resources are usually available from the provider in almost any quantity at any time if you need to allocate them for a cloud application, which signifies that you can
generally expect that it can be scaled as required to fulfill demand, provided dynamic scaling is supported by application architecture of your teams.

Table 1 explains how the framework addresses the six security issues. It may be used as a checklist by organizations to proceed step-by-step for their cloud migration implementation.

**Table 1: Summarized Cloud Migration Checklist**

| Misunderstanding Responsibilities | Data Privacy and Security Concerns | Lack of Standards | Interoperability Problems | Reliability Breakdowns | Malicious Insider |
|-----------------------------------|-----------------------------------|-------------------|--------------------------|-----------------------|------------------|
| Ascertaining the migration architect role | Ensure all requirements are met during migration. | Ensure all procedures are securely carried out. | - | - | Ensure monitoring of activities |
| Choosing the cloud integration level | Helps limit usage as per requirements | Helps integrating differently for different applications | - | - | - |
| Choosing between single and multi-cloud | Useful for mixed requirements. | - | Integrating to multiple cloud providers. | Useful to distribute traffic load. | - |
| Establishing Cloud KPIs | Requirements are clear from the beginning. | Ensure security is achieved through KPIs. | Ensure the implemented standards are efficient. | - | - |
| Establishing performance baselines | - | - | - | - | - |
| Prioritizing migration components | Reduces ambiguity. | - | Step-by-step prioritized integration helps reduce interoperability. | Focus on more important applications. | - |
| Performing any necessary refactoring | - | Enables gap analysis. | Helps test performance and implement changes. | Helps test performance and implement changes. | Removes unnecessary intuitions or accesses. |
| Preparing a data migration plan | Gives a clear view of how to go about migration based on organization's specific requirements. | Helps analyze sensitive areas and develop a migration plan accordingly. | Helps identify required standards. | - | - |
| Switching over the production | - | - | Gives levy to implement as required. | Provides scope for developing a contingency plan. | - |
| Reviewing application resource allocation | Removes ambiguity in user roles. | Gives access only to those who require it. | - | - | Periodically removes unwanted personnel from the system |

**5. Conclusion**

Cloud computing has a great future. However, the cloud computing approach’s benefits are more or less equivalent to the security threats embedded in it. Cloud computing is an immense opportunity and a lucrative option for companies and attackers - both sides can benefit from cloud computing. Security concerns can seriously impact cloud infrastructures. Security itself is conceptualized as a different layer in
the cloud computing model. Cloud computing will certainly grow to be the ultimate (and probably the best) model for business computing. However, security difficulties and related concerns must be addressed to make Cloud computing further practical.

To securely exploit a service-based environment, the security issues and concerns of cloud computing are intrinsic not only to the aspects of the cloud environment but also in every connected service and the forms where computing is done for both cloud service providers and customers. Security problems in cloud computing are fairly crucial and sensitive from sociological and technological points of view: technological inconsistency resulting in security breaches in cloud computing can bring about major sociological impacts.

It can be concluded without a doubt, irrespective of the nature of security problems, that the serious adverse effects resulting from security violations in cloud computing, every type of cloud computing deployment must address the security problems related to those of important security systems.

References
[1]. Kandukuri, B.R. Paturi, R. & Rakshit, V.A. (2009). Cloud Security Issues. In Proceedings of IEEE International Conference on Services Computing, pp. 517-520.
[2]. NIST. (2011). NIST Definition of Cloud Computing. National Institute of Standards and Technology.
[3]. Subha K and Kushal Reddy P, Data Sharing in Cloud Computing Based On Attribute-Based Encryption System, International Journal of MC Square Scientific Research, Vol. 9, No. 2, 2017.
[4]. Aslam K A, Smart Reading System For Visually Impaired People, International Journal of MC Square Scientific Research, Vol. 9, No. 2 2017.
[5]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., & Zaharia, M. (2009). Above the clouds: a Berkeley view of cloud computing, electrical engineering, and computer sciences. University of California at Berkeley, Technical Report No. UCB/EECS-2009-28, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html, 10.
[6]. Wang, L., Tao, J., Kunze, M., Castellanos, A.C., Kramer, D., & Karl, W. (2008). Scientific Cloud Computing: Early Definition and Experience. 10th IEEE Int. Conference on High-Performance Computing and Communications, pp. 825-830, Dalian, China.
[7]. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). Ieee.
[8]. 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.
[9]. Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy (IJISP), 4(2), 36-48.
[10]. Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388, 1-15.
[11]. Tianfield, H. (2012, October). Security issues in cloud computing. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 1082-1089). IEEE.
[12]. Khan, M. A. (2016). A survey of security issues for cloud computing. Journal of network and computer applications, 71, 11-29.
[13]. Yang, J., & Chen, Z. (2010, December). Cloud computing research and security issues. In 2010 International Conference on Computational Intelligence and Software Engineering (pp. 1-3). IEEE.
[14]. Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. International Journal of Engineering Science and Technology (IJEST), 3(4), 2672-2676.
[15]. Atchison, L. (2018, June). Preparing to Adopt the Cloud: A 10-Step Cloud Migration Checklist. Retrieved from New Relic: https://blog.newrelic.com/engineering/cloud-migration-checklist/.