Security and Privacy in Cloud Computing: Challenges and Opportunities

Venkata Koteswara Rao Ballamudi[1*], Harshith Desamsetti[2]

[1]Sr. Software Engineer, High Quartile LLC, **USA**
[2]Department of Computer Science, Northern Illinois University, IL 60115, **USA**

[*]E-mail for correspondence: venkata.bvk@gmail.com

Received: July 07, 2017 **Accepted:** Nov 27, 2017 **Published:** Dec 31, 2017
Source of Support: Nil **No Conflict of Interest:** Declared

ABSTRACT

ICT advancements have made cloud computing popular and successful. Cloud computing lets corporate users relocate and utilize the pay-as-you-go price model's scalability. However, outsourcing data and business applications to the Cloud or a third party creates security and privacy concerns, which are crucial to cloud adoption. Researchers and impacted organizations have offered several security measures to address security issues in the literature. Cloud computing security and privacy are extensively covered in the literature. Unfortunately, literature efforts lack flexibility in mitigating numerous threats without contradicting cloud security aims. The literature has also focused on security and privacy issues and has yet to give technical solutions. Research on technical remedies to security concerns has yet to explain their origins. This paper introduces security and privacy challenges that require adaptive solutions without compromising cloud security. This research evaluates the literature, including its adaptability to future threats and how cloud security conflicts have invalidated their models. The essay uses STRIDE to highlight cloud computing security issues from a user perspective. It also analyses literature-based inefficient solutions and recommends secure, adaptive cloud environments.

Keywords: Cloud Computing, Security Issues, Privacy, Cloud Computing Model, Cloud Security

INTRODUCTION

For several years, a cloud picture has been utilized on system graphs. Cloud computing technology allows computing resources to be accessible through the Internet. Cloud computing focuses on internet software, data storage, and processing power. Cloud computing lets firms dynamically increase their capacity without investing in new infrastructure, training new IT staff, or buying new licensed software to automate procedures. IT capabilities are expanded. In recent years, cloud computing has gone from a potential business idea to a fast-growing IT innovation. All personal and business data is stored in the Cloud, raising security concerns. Cloud computing has helped many companies save IT costs and focus on their core competencies rather than IT infrastructure (Lal, 2015). Cloud services are suitable for companies with changing consumer bandwidth needs. Due to the versatility of cloud services, users can scale up and down depending on their needs. This agility can provide cloud-computing companies an edge over competitors. Due to data security concerns, customers still need help moving their corporate activities to the Cloud despite its many benefits. Cloud services are internet-based and serve many clients daily. Therefore, they can become overwhelmed and experience technical outages. When a web connection is lost, users cannot access their applications, servers, or cloud data, which can momentarily halt company processes. Data centralization and resource security may increase security, but concerns remain about losing control over sensitive data and cloud service provider-stored data security. Consumers may suffer if suppliers need adequate security systems. Many cloud providers must expose their infrastructure facilities to consumers, making it difficult to assess their security procedures. Section 2 reviews related cloud computing security literature. Section 3 discusses cloud computing security, specifically Software as a Service, Platform as a Service, Infrastructure as a Service, and deployment methodologies. Section 4 discusses enterprises' cloud computing resource management difficulties, and section 5 concludes the work (Čapek, 2012).

Models for Cloud Deployment

Cloud hosting deployment methods are based on ownership, scale, and access. It describes the Cloud. Most firms are willing to use the Cloud since it cuts costs and regulates operations.

- **Public Cloud:** This hosting offers Cloud services over a public network. This Model accurately depicts cloud hosting. A cloud service provider delivers services and infrastructure to several clients. Customers need to have a say in infrastructure location. Public and private clouds may have similar structural designs, except for the security supplied by Cloud hosting companies for public cloud services (Mandapuram, 2016). The public Cloud is suitable for load-management businesses. The public cloud approach is cost-effective due to lower capital and operational costs. Dealers may offer free or pay-per-user licenses. Public cloud users pay together. Customer earnings come from economies of scale. Public clouds like Google offer free services.
- **Private Cloud:** Also called internal Cloud. This cloud computing platform is implemented on a secure cloud environment and protected by a corporate IT department firewall. Private clouds allow only authorized users and give organizations more data control. Physical machines hosted inside or externally supply resources from a separate pool to personal cloud services. A private cloud is best for businesses with unpredictable needs, critical administrative tasks, and uptime needs. The private Cloud does not require additional security restrictions or bandwidth limits like the public Cloud. Clients and cloud providers have control over infrastructure and increased security due to restricted user access and networks. Eucalyptus Systems is a good example.
- **Hybrid Cloud:** Integrated cloud computing. It could be two or more private, public, or community cloud servers connected yet remaining independent. Hybrid clouds can cross provider boundaries and not be classified as public, private, or community clouds. It lets users add capacity and capabilities by assimilation, aggregation, and customization with other cloud services. In a hybrid cloud, in-house or external providers manage resources. It adapts the workload between the private and public clouds to meet organizational needs. Third-party, public clouds can host non-critical resources like development and test workloads. Critical and sensitive tasks should be kept within. Organizations may process massive data with a hybrid cloud. Hybrid cloud hosting is scalable, flexible, and secure.
- **Community Cloud:** The setup is shared by many banks and trading corporations in cloud hosting. It is a multi-tenant architecture shared by several enterprises with comparable computing concerns. These community members often share performance and security concerns. Communities aim to meet commercial goals. Community cloud can be hosted outside or internally and managed by third parties. Community cloud saves money since community organizations split the expense. Companies recognize cloud hosting has excellent potential. To be great, use the proper cloud hosting. Knowing the business and analyzing demands is necessary. Choosing the right cloud hosting lets us achieve business goals.

Cloud Computing Service Models

Software as a Service (SaaS): Software as a Service (SaaS) is experiencing significant expansion. The client is responsible for accessing the application's user interface when using a software delivery model known as software as a service (SaaS), which uses the Internet to distribute software applications that a third-party vendor manages. There is no need to download or install SaaS programs because they may be run directly from a web browser; nevertheless, these applications require plugins. The consumer can deploy an application on a cloud infrastructure thanks to the provider (Desamsetti, 2016a). Because it utilizes a web-based distribution architecture, SaaS eliminates the requirement that apps be installed and operated locally on individual PCs. Because vendors can handle everything, including applications, runtime, data, middleware, operating system (OS), virtualization, servers, storage, and networking, this architecture makes it simple for businesses to increase their maintenance and support capabilities, some of the most popular SaaS services are email and collaboration, as well as applications connected to healthcare. The majority of interfaces offered by SaaS companies are browser-based. APIs are typically also made available to developers as well. The primary advantage of using a SaaS platform is that no upfront capital is required to purchase servers or software licenses. The application developer must maintain a single program that serves multiple customers.

Infrastructure as a Service (IaaS): Infrastructure as a Service, or IaaS, is a method for monitoring and controlling distant data center infrastructures (Desamsetti, 2016b). These infrastructures include computation (virtualized or bare metal), storage, and networking. Users can purchase IaaS on a consumption basis, comparable to other utility billing forms. Users of an IaaS service are the ones who are ultimately responsible for applications,

data, runtime, and middleware. It is still possible for providers to manage virtualization, servers, storage, and networking. IaaS companies also offer additional services, such as databases, messaging queues, and other services, on top of the virtualization layer.

Platform as a Service (PaaS): The phrase "platform as a service" (Platform as a Service) is a type of cloud computing service that offers a platform to customers, enabling them to design, run, and manage applications without the hassle of having to construct and maintain the underlying infrastructure. The Cloud Service Provider takes care of their customers' lower-level infrastructure, network topology, and security concerns, so there is no need for anyone to worry about these things. The operating system (OS), virtualization, and PaaS software can be managed by third-party companies using this technology. The developers work on the programs. Applications that use PaaS automatically inherit characteristics of the Cloud, like scalability, multi-tenancy, SaaS enablement, high availability, and more. This paradigm is advantageous to businesses since it reduces the amount of coding required, automates business policies, and assists in the process of converting applications to a hybrid model (Keegan et al., 2016).

SECURITY IN THE CLOUD COMPUTING

Because of its wide variety of uses, cloud computing has recently attracted the attention of academics concerned about maintaining data storage, administration, and processing safety. Cloud computing raises questions about the confidentiality and integrity of outsourced data. Outsourced applications and data to the Cloud have unlimited security boundaries and infrastructure. This is because of the Cloud's dynamic abstraction and scalability (Lal, 2016). The multi-tenant nature of cloud computing and the sharing of virtualized resources is another significant problem with adopting cloud computing from a security perspective. Cloud service providers such as Google, Microsoft, and Amazon have recently significantly improved their cloud computing infrastructure and services to accommodate more end users. The fact that cloud databases typically include critical sensitive information will, despite this, lead the issue of privacy and security to become an increasingly pressing concern. As a result of the dangers that have been analyzed, the confidence level in using the Cloud is decreasing (Gutlapalli, 2016a).

Unethical cloud computing: Users have access to various utilities provided by the architecture of cloud computing, including storage and bandwidth capacities. However, the cloud infrastructure needs complete control over utilizing these resources. This allows malevolent users and attackers to exploit the Cloud's flaws. Users with malicious intent abuse cloud resources by concentrating their attacks on specific attack sites and launching DDoS, password cracking, and captcha-solving farm attacks. Because of the high user engagement these levels require, these dangers mainly affect the PaaS and IaaS layers.

Malicious insider attackers: Attacks that hostile insiders generate have been one of the most overlooked attacks, even though this form of attack has been the most destructive, hitting all layers of the cloud infrastructure. A malevolent insider who has high-level access can get root power to network components and then manipulate sensitive and confidential data by using data (Gutlapalli, 2016b). This assault offers several security risks since intrusion detection systems and firewalls can circumvent them by treating them as normal activities and thinking they are not malicious. As a result, there is no risk that they will be discovered.

Programming interface vulnerabilities: Publishing application programming interfaces (APIs), which allow for simple deployment or the creation of software programs, is included as part of the cloud services that facilitate user engagement at all levels. The cloud architecture's complexity is increased by adding these interfaces, which give an additional layer. Unfortunately, these interfaces bring vulnerabilities in the APIs, which malevolent users can exploit via backdoor access. These vulnerabilities can impact the fundamental processes of cloud architecture (Dekkati & Thaduri, 2017).

The leaking and loss of data: Cloud computing raises several serious risks, one of the most critical of which is the possibility of data leakage due to the continuous movement and transfer of information through untrusted networks. Theft of data has emerged as the most significant risk facing the information technology industry, and it costs businesses and their customers an enormous amount of money every year in lost revenue. Ineffective authentication and encryption methods, inefficient data storage facilities, and a lack of disaster recovery planning are the primary contributors to data loss.

Distributed technology vulnerabilities: Because the multi-tenant architecture provides virtualization for shared on-demand services, several users can share a single application as long as all of those users have access to the system. However, due to security flaws in the hypervisor, unauthorized third parties can take control of otherwise lawful virtual machines. These vulnerabilities can also disrupt the fundamental processes of the cloud architecture, resulting in changes to the Cloud's normally expected behavior (William & Lee, 2016).

Services and unauthorized access to accounts: This refers to the capability of a malicious intruder to divert traffic from a legitimate website to a website that the intruder controls. After gaining access to the legitimate website with the reused credentials, malicious intruders can perform phishing attacks and steal users' identities.

The threat posed by an anonymous profile: Cloud computing services can reduce the time and effort required to set up and maintain hardware and software. On the other hand, this creates risks for security compliance, hardening, auditing, patching, and logging processes and requires an understanding of internal security measures. A considerable danger of confidential information being leaked can be posed to an organization by the presence of a threat posed by an anonymous profile.

The Cloud's underlying infrastructure is distributed and shared, making it challenging to develop a self-security model that protects the confidentiality and integrity of stored data. To gain privileges or root access within a network, adversaries take advantage of the security challenges posed by cloud architecture and use advanced approaches. Attacks against cloud systems can be made possible through flaws in the Internet Protocols, such as the man-in-the-middle attack, ARP spoofing, DNS poisoning, and Internet Protocol (IP) spoofing. ARP poisoning is one of the most significant flaws in the IP protocol stack. Because the Address Resolution Protocol does not frequently demand Proof, unscrupulous users can exploit this vulnerability and redirect legitimate users' outward and inbound traffic. The research literature has documented session states in Web services that use the HTTP protocol and several strategies for abusing session management. These approaches include session hijacking and session ridding. Application module information can be obtained by exploiting injection attack vulnerabilities such as those in the operating system and SQL injection. These application modules may constitute the central part of an organization's data hosted in the Cloud and may contain sensitive private information. Sometimes, the availability of the Cloud and its capacity to perform its functions depend on the methods used to secure the supplied APIs. Insecure application programming interfaces (APIs) can result in attacks against HTML services, such as browser phishing, and malevolent users can initiate SSL certificate spoofing.

Attacks of the DoS and DDoS variety compromise the safety of cloud services. Launching a DDoS attack on a system can have the effect of disrupting both the Quality of Service and the access that is granted to legitimate users. Intrusion Detection Systems, often known as IDS, are utilized to thwart Distributed Denial of Service attacks. An intrusion detection system's objective is to provide an additional layer of defense or security against malevolent users who take advantage of the weaknesses in computing systems by sending alerts to users whenever aberrant behavior is detected. IDSs are necessary to identify any disturbances to cloud services.

Cloud Computing Model Challenges

Organizations adopting and using cloud computing for optimal resource management face several hurdles since people still need to determine its legitimacy. According to a 2008 International Data Corporation report, the main barriers to firms using Cloud Computing are:

Security Issues: Security concerns have slowed cloud computing adoption. Many find it intimidating to save organizational data, execute it using software on someone else's hard disk, and use someone else's CPU. Common security risks threaten an organization's data and software, including data loss, phishing, and remote machine use. The multi-tenancy paradigm and communal computing resources in cloud computing have created new security concerns that demand enhanced security techniques. Hackers can build up a Cloud service and offer client businesses more reliable infrastructure services at a lower cost to start an attack (Fernandes et al., 2014).

Costing Model Issues: Cloud users must balance computation, communication, and integration. Migration to the Cloud model can significantly reduce infrastructure costs. Still, it raises data communication costs, such as shipping an organization's data to and from the public and community Cloud, and the cost per computing resource used. This cost is incredibly high if the consumer company chooses a hybrid cloud deployment architecture to disseminate data across public/private/community clouds. Thus, on-demand cloud computing is only helpful for CPU-intensive tasks.

Charging Model Issues: Flexible computing resources have made cost inquiry more complicated than in typical data centers, which use static computing. Additionally, client organizations now analyze virtual server costs instead of physical ones. SaaS cloud providers may find it costly to build architecture where a single software application serves several customers. The cost of adding new features for intensive customization, performance and security improvements for concurrent multi-user access, and dealing with the complexities caused by the above software changes are among them (Lal & Ballamudi, 2017). Thus, SaaS providers must weigh the benefits of multi-occupancy, such as decreased overhead from paying off, fewer on-site software licensing, etc. The profitability and sustainability of SaaS cloud providers in cloud environments depend on an innovative and practical billing model.

SLA Issues: After moving their core business activities to the Cloud, cloud consumer organizations must ensure the quality, accessibility, dependability, and performance of their computing resources. Consumer organizations must get delivery assurance from service suppliers. Service Level Agreements (SLAs) between cloud providers and users usually supply these. The challenge is defining SLA details with enough granularity, specifically the tradeoffs between articulacy and multifaceted nature, to cover many of the client's desires and be easy to weigh, confirm, assess, and implement by the cloud resource allocation and management mechanism. IaaS, PaaS, and SaaS cloud products should also have various SLA meta requirements. Cloud providers also face implementation challenges. Advanced SLA mechanisms must also incorporate user input and customization highlights into the SLA assessment framework.

Cloud Interoperability Issues: Current cloud offerings provide different ways for clients, apps, and users to collaborate with the Cloud, causing the "Foggy Cloud" problem. Vendor locking inhibits customers from choosing from multiple vendors/offers to increase resources at different organizational levels, significantly hindering cloud ecosystem development. Furthermore, proprietary cloud application programming interfaces make integrating cloud services with an organization's traditional frameworks difficult. Interoperability aims to comprehend perfectly smooth data movement across clouds and between cloud and local applications of a client enterprise. Soft cloud computing requires compatibility on many levels. First, optimize IT assets and computing resources. Organizations typically need to preserve in-house IT assets and capabilities for core competencies while outsourcing marginal operations and activities to the Cloud. Second, outsourcing marginal functions to cloud services from diverse providers may be more significant for optimization. Standards help solve interoperability issues. Interoperability has yet to be a priority for significant industry cloud vendors as cloud computing occurs (Aithal & Pai, 2016).

NETWORK PROBLEMS

Computing in the Cloud makes use of the Internet and other remote computers to store and manage data to execute a variety of applications. All information is uploaded through the use of this network. Thaduri has said that concerns regarding the security of networks in the Cloud are a primary emphasis. It offers consumers on-demand access to virtual resources, high bandwidth, and software. The network architecture of this Cloud is susceptible to a wide variety of threats and vulnerabilities, including cloud malware injection attacks, browser security difficulties, flooding assaults, lock-ins, incomplete data erasure, data protection, and XML signature element wrapping (Thaduri et al., 2016).

XML Signature Elements Wrapping: An extremely well-known assault on an online service. This safeguards the identification value and the hostname from the unlawful party, but it cannot secure the position in the documents. The attacker is going after the computer, acting as the host by sending SOAP messages containing jumbled data so the user of the host computer won't comprehend it. The XML Signature wrapping attack modifies the information contained within the signed portion of a message but does not alter the signature itself. This would prevent the user from gaining any comprehension.

Security for Browsers: The client will communicate the information on the network using their browser. These browsers protect the user's identity and credentials by utilizing SSL technology. However, hackers operating from the intermediary host can retrieve these credentials by employing sniffing software installed on the intermediary host. One should only have one identification, but that lone certificate should have the ability to prove one's identity to varying degrees of certainty, which can be accomplished by acquiring approvals in a digital format.

Attacks from Flooding: In this form of assault, the intruder quickly requests a substantial number of cloud-based resources to flood the Cloud with many requests for these resources. According to research that IBM conducted, the Cloud can grow in proportion to the number of submissions made. It will expand to satisfy the demands of the invader, thereby rendering the resources inaccessible to the typical consumers.

SQL Injection Vulnerability: The insertion of harmful code into an SQL code is an attack, an act considered malicious in cloud computing. Through this type of assault, the intruder can get illegal access to a database and other confidential information. Any kind of SQL database is vulnerable to attack using the technique known as "SQL injection." Because development must emphasize security, SQL injection, and other vulnerabilities are possible. This is one of the reasons why.

OPPORTUNITIES FOR CLOUD COMPUTING MODEL

Cost Savings to the Management: Utilizing, maintaining, and upgrading the information technology system with this approach results in the lowest total cost. Through the usage of cloud computing, a company may, without a doubt, obtain fiscally innovative and on-premise information technology services without the need to purchase or evaluate hardware equipment or software, as well as without the need to recruit in-

house IT employees to keep up and benefit from in-house infrastructure. A significant monetary outlay is required for a business to purchase a software license. When corporations have several people using the software, the cost of the license payments might quickly become too expensive for them. On the Cloud, it is available at far cheaper rates; as a result, the business can reduce its overall expenditures on information technology. Consequently, the company can concentrate on the most important tasks without spending additional money on IT staffing and training (Mona & Sharma, 2014).

Pay as per Use: It is pretty reasonable for the consumer firm because various options accessible, such as a one-time purchase or pay-as-you-use, are available. When additional cloud resources are needed, the consumer company can place a demand for them, and they can be released when they are not being utilized.

Unlimited Storage space: Customers can access virtually infinite storage space when they save their data on the Cloud. As a result, there is no longer any need to be concerned about running out of storage space. (for example, Google Drive)

Supports green computing: The utilization of available computer resources in a manner that is both more beneficial to the environment and more conducive to energy conservation. Utilizing pre-built computing resources adapted to an organization's specific requirements unquestionably helps it lower its monthly electricity costs. Not only does it save money on power, but it also saves money on the resources that are needed to cool down computers and other components. This results in a lower emission of potentially harmful substances into the environment.

Scalability / Flexibility: Organizations can start with a relatively modest cloud deployment, grow it quickly, and then scale it back if necessary. In addition, the versatility of cloud computing enables consumer firms to use extra resources as needed, allowing them to satisfy their requirements.

Backup and Recovery: Services that use several redundant backup sites can enable both the continuity of corporate operations and the recovery from any disaster. Compared to storing the same data on a physical device, backing up this data and restoring it is a relatively much more straightforward process, thanks to the fact that all the data is saved in the Cloud (Hatem et al., 2014).

Work from anywhere and Mobile Accessible: We can access information from any location with an Internet connection, the appropriate credentials, and access rights. This helpful function enables the user to circumvent barriers imposed by time zones and physical areas, resulting in higher productivity due to systems that are accessible within an infrastructure that is available from any site.

Easy and Rapid Deployment: Cloud computing can rapidly deploy the desired or necessary setup. If the technology the customer needs is available, the system setup can fully function in just a few minutes. It is easy to implement programmed software integration because the user or decision maker only needs to select the programming services and applications that are the most appropriate for the firm. APIs, which do not require program installations on users' local computers, are used to gain access to the data.

CONCLUSION

Computing in the Cloud is a relatively new notion that offers several advantages to the people who utilize it. However, this brings up specific security concerns, potentially limiting its application. This will be easier for businesses to transition to using the Cloud if they understand the risks associated with cloud computing. Since cloud computing uses many different technologies, it also inherits those systems' security flaws. Traditional online applications and virtualizations have been examined. However, some solutions given by cloud computing still need to be developed or exist. We have discussed the many security concerns associated with cloud models such as IaaS, PaaS, and IaaS. These concerns vary based on the Model. According to the information presented in this article, the two areas of most significant concern regarding cloud computing security are storage and networks. Cloud computing users have a substantial issue regarding virtualization, making it possible for several users to share a single physical server. Some assaults are directed at virtual network infrastructures. This distinction, which is critical for understanding these challenges, has been the primary focus of our attention. Another essential component of cloud computing is the use of many tenants.

REFERENCES

Aithal, P. S., & Pai, V. T. (2016). Concept of Ideal Software and its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME), 1*(1), 826-837. http://doi.org/10.5281/zenodo.160908

Čapek, J. (2012). Cloud Computing and Information Security. *Scientific Papers of the University of Pardubice. Series D. Faculty of Economics and Administration, Pardibuce 24*, 23-30.

Dekkati, S., & Thaduri, U. R. (2017). Innovative Method for the Prediction of Software Defects Based on Class Imbalance Datasets. *Technology & Management Review*, *2*, 1–5. https://upright.pub/index.php/tmr/article/view/78

Desamsetti, H. (2016a). A Fused Homomorphic Encryption Technique to Increase Secure Data Storage in Cloud Based Systems. *The International Journal of Science & Technoledge*, *4*(10), 151-155.

Desamsetti, H. (2016b). Issues with the Cloud Computing Technology. *International Research Journal of Engineering and Technology (IRJET)*, *3*(5), 321-323.

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., Inácio, P. R. M. (2014). Security Issues in Cloud Environments: a Survey. *International Journal of Information Security*, *13*(2), 113-170. http://doi.org/10.1007/s10207-013-0208-7

Gutlapalli, S. S. (2016a). An Examination of Nanotechnology's Role as an Integral Part of Electronics. *ABC Research Alert*, *4*(3), 21–27. https://doi.org/10.18034/ra.v4i3.651

Gutlapalli, S. S. (2016b). Commercial Applications of Blockchain and Distributed Ledger Technology. *Engineering International*, *4*(2), 89–94. https://doi.org/10.18034/ei.v4i2.653

Hatem, S. S., wafy, M. H., El-Khouly, M. M. (2014). Malware Detection in Cloud Computing. *International Journal of Advanced Computer Science and Applications*, *5*(4), 187-192. http://doi.org/10.14569/IJACSA.2014.050427

Keegan, N., Ji, S-Y., Chaudhary, A., Concolato, C., Yu, B. (2016). A Survey of Cloud-Based Network Intrusion Detection Analysis. *Human-centric Computing and Information Sciences*, *6*(1), 1-16. http://doi.org/10.1186/s13673-016-0076-z

Lal, K. (2015). How Does Cloud Infrastructure Work?. *Asia Pacific Journal of Energy and Environment*, *2*(2), 61-64. https://doi.org/10.18034/apjee.v2i2.697

Lal, K. (2016). Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs. *American Journal of Trade and Policy*, *3*(3), 121–126. https://doi.org/10.18034/ajtp.v3i3.663

Lal, K., & Ballamudi, V. K. R. (2017). Unlock Data's Full Potential with Segment: A Cloud Data Integration Approach. *Technology & Management Review*, *2*(1), 6–12. https://upright.pub/index.php/tmr/article/view/80

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement*, *7*(1), 50–57. https://4ajournal.com/article/view/76

Mona, M. A., Sharma, P. (2014). Cloud Computing: a Collaborative Green Platform for the Knowledge Society. *VINE: Very Informal Newsletter on Library Automation*, *44*(3), 357-374. http://doi.org/10.1108/VINE-07-2013-0038

Thaduri, U. R., Ballamudi, V. K. R., Dekkati, S., & Mandapuram, M. (2016). Making the Cloud Adoption Decisions: Gaining Advantages from Taking an Integrated Approach. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *3*, 11–16. https://upright.pub/index.php/ijrstp/article/view/77

William, U., Lee, U. (2016). A Fortress of Clouds: Copyright Law, the Computer Fraud, Abuse Act, and Cloud Computing. *Southern Law Journal*, *26*(2), 191-232.

--0--

SOCIAL SCIENCE RESEARCH NETWORK
2171 Monroe Avenue, Suite 203, Rochester, NY 14618, USA
http://www.ssrn.com/en/
AJTP Link: http://www.ssrn.com/link/American-Journal-Trade-Policy.html