New dimensions of Cloud Security with Infrastructure and Intelligence Impact

Bhal Chandra Ram Tripathi[1] and Krishna Prasad R[2]
Global Academy of Technology, Bengaluru Karnataka 560098, India
rkp_rgp@yahoo.co.in

Dr. Satish Kumar T
BMS Institute of Technology, Bengaluru Karnataka 560064, India

Visheshwar Pratap Singh
Aegis School of Business, Data Science and Telecommunication, Mumbai, Maharashtra, India

Abstract. Cloud Computing has evolved as a major form of computing these days. The cloud computing possess the characteristics such as scalability, security, reliability which makes it a choice to complex solutions. The industries are transiting from the physical sources to the virtual sources which is due to the cloud computing. The immense reliance on cloud computing has started creating certain thinkable issues such as security, handling, transmission. The clouds are a piece of virtual technology, highly susceptible to external attacks producing shear pressure on the service providers to deal with. The challenges are not only fixed to professional environment but with the use of the technology to all humanity, it is entering to the personal environment too. The cloud computing takes the support of external intelligence such as use of Artificial Intelligence to help it in making a more resistive to the external disturbances.

Keywords: Cloud Computing, Artificial Intelligence, Scalability, Cloud Security

1 Introduction

For years the Internet has been represented on network diagrams by a cloud symbol until recent times when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. The cloud has provided many a good features but the deep penetration of its reachability in lifestyle has started capturing the major security issues. The issues arising from the malware attacks to the data inconsistency are becoming issue of handling. The scalability of the cloud is the most eminence feature, which makes the organization and mass attraction, but the security breach is other truth of the clouds.

From one point of view, security should improve due to centralization of data and increased security-focused resources. On the other hand, concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a proposal to more specific different security issues and the associated challenges [1] that has emanated in the cloud computing system. The use of intelligence in the environment of the vendor or in the management of the cloud providers can make a more susceptible computing.

Cloud computing has five key attributes, which grant it some advantages over similar technologies and these attributes include:

- *Shared Resources:* The resources are centralized mounted in data centres, providing access to all as per needs.[18]
- *Massive Scalability:* Cloud computing can take the opportunity to handle the large domain of system simultaneously. It increases its horizon when needed.
- *Elasticity:* Gives freedom user to demand and use the services; the user has no bounding to permanently keep it.[2]
- *Pay as you go:* Users pay according to their use.
- *Self-provisioning of resources:* Users self-provision resources, such as additional systems (processing capability, software & storage) and network resources.

2 Security Threats and Risk in Cloud Computing

Cloud computing can be considered as word which has all in it. The word, which gives solution to all the problems such as API, site management, etc. But the scenario is different from the other prospect; the eruption of certain demands has made to compromise certain features by the environment in delivering services. The most sought of risk compromised is of security. The indirect growth of the services has made the compromising in the protocol suit of the transfers, which allows the third parties to infiltrate in the network and play with the data. The access is not only fixed until the runaround but also to the modifications, which produces major setbacks. Today everyone is making the system to remember the credentials such as passwords, id's such that next time the system automatically takes appropriate steps to reach the user at desired place but in performance it's an easies way to compromise the security. The data stored by system is automatically being transferred to cloud, which is not well reliable. The presence of supporting and well-known technologies such as Artificial Intelligence is now somewhere supports in the security breaches due to movement from human led to chip led thinking. The issues are serious and organizations such as Google, IBM are working to overcome them but the vast reachability makes the path complex to the solution. The cloud, which is a large cluster of space with the processing capacities, always surrounded by the security vulnerabilities. The vulnerabilities arise

due to infrastructure bleaks, outsourcing of center credentials, compromising of professional agreements. The artificial intelligence is playing a vital role in handling the threats along with providing intelligence to the cloud. The preprocessing of the logins using the intelligence that works on the MAC id and Personal ID of the user around the infrastructure to make a record of activity and deciding the vulnerability.

The major vulnerabilities are now produced can be taken into two forms as – Threats, Risks.

2.1 Threats

Cloud computing today is facing the great threat through malware attacks. The threats are moving from professional to personal information. These thread risk vulnerabilities come in various forms. The Cloud Security [4,5] Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing as depicted in Figure 1, and it identified the flowing seven major threats:

1. Abuse use of Cloud Computing
2. Unknown Risk Profile
3. Data Loss/Leakage
4. Insecure Programming Interfaces
5. Shared Technology Vulnerabilities
6. Account, Service & Traffic Hijacking

2.2 Risks

Cloud looks like a more easily accessible place but there are certain risk associated with it. The organizations using the services by cloud are very incapable to physically access the data stored or know the form in which the data is stored. The cloud stores a number of trade information, credentials, professional data, etc., which makes it a sensitive place but the infrastructure, is finally with the governing organization. The risks are also increasing with the increasing intelligent solutions such that they are allowing the attackers to penetrate inside the cloud and cause attacks. However, the Intelligence be used around direction to resist attacks.

3 Cloud Computing Service Delivery Model and Intelligence

Following the cloud deployment models, the models tell the important aspect in consideration of the security features. The model play an important role in an infrastructure security, the model with less authentication is more prone to vulnerabilities than those models with more credential matchings. The modification in the models with respect to handle the vulnerability can make the secure environment and the use of Artificial Intelligence is the most appropriate choice for it. The three

main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) as depicted in Figure 2.

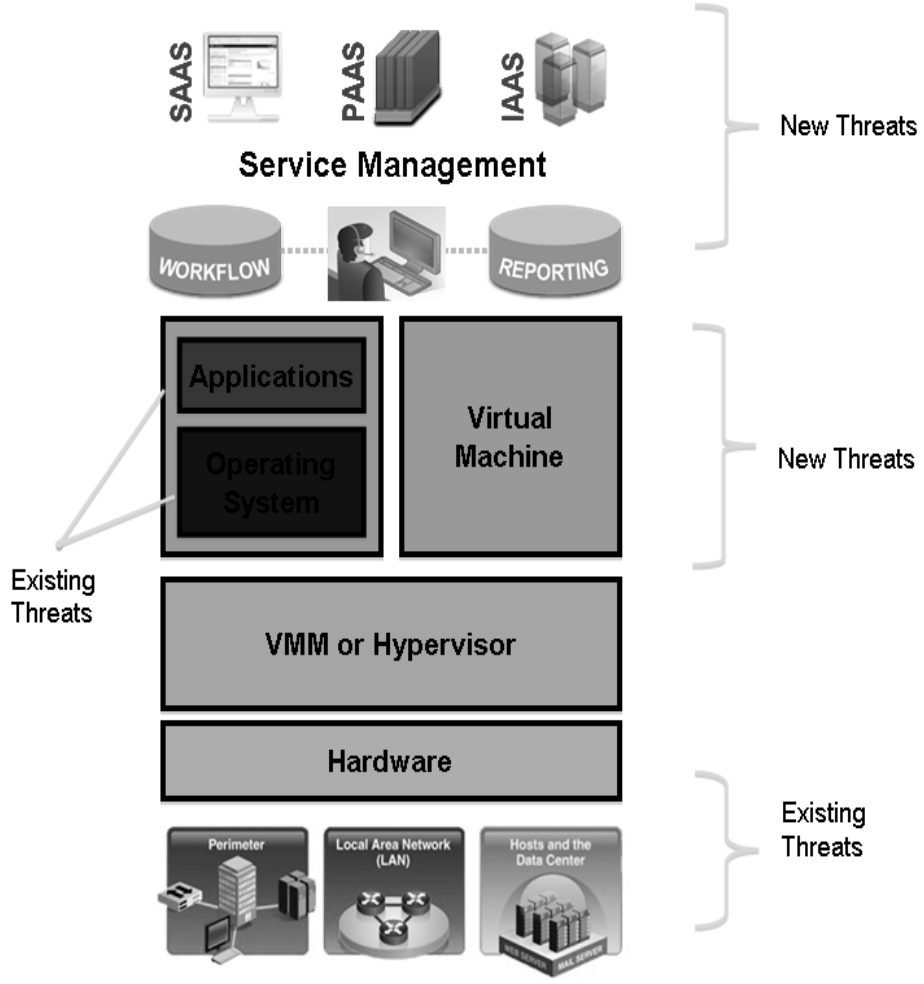

Figure 1. Cloud threads known and discovered

3.1 Infrastructure as a Service

Infrastructure as a Service is a simple implementation of the cloud services and performing the computing. The services provided by it are termed as *"pay and use";* the organizations can use the services by the cloud when they need it by just performing simple monetary transactions and keeping aside the inner complex functionalities of the cloud. The cloud model permits fast transacting organizations to focus on their core model keeping aside the storage and processing functionalities by the associated cloud.

IaaS and other associated services have also enabled startups focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS makes a layer over its infrastructure, which prevents the outside to know the inner hardware transactions and associativity's. The layer makes the use of "Intelligent Authentication" to make the lesser prone computing. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

3.2 Platform as a Service

This is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design 3

to building applications to deployment to testing to maintenance. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. The underneath services are hidden with there complexity from the outer capital but the use of "Proportionate Access" can overcome the issues of security to a level. The Proportionate Access will all the access but improves the security by 40%-50%. The Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks [10][11] such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental.

3.3 Software as a Service

The model has gained a great response due to its customer relief infrastructure. The organizations account this model as it is capable of hosting the application in the cloud and providing access to the customer base. The model is capable to handle the traffic of application access as well as data access. Trusting the reliability of the model; there are 80% web infrastructure relying on this and providing services to the trusted user base. SaaS has adopted the "*pay-as-you-go"* subscription model providing the ease of access to the large customer base and monetary relief. But there are certain vulnerabilities related to security and data present in the model. The model perhaps hosts the application but due to its global presence is highly susceptible to the malware attacks and the impingement of malwares. The service providers if not using the appropriate cryptographic and authentication solutions would lead to compromise the

trust and the authenticity of hosted application. The use of layered authentication and sophisticated protecting infrastructure would lead to a 60%-70% protection but its the The models are capable of capturing the relevant user base; but the issues related to security and data needed to be handled appropriately. The cloud models from IaaS through SaaS are having bleaks in the layered protection. The proposed model tends to produce a layer of public-private protection. Cloud vendors [18] and clients' need to maintain Cloud computing security at all interfaces.

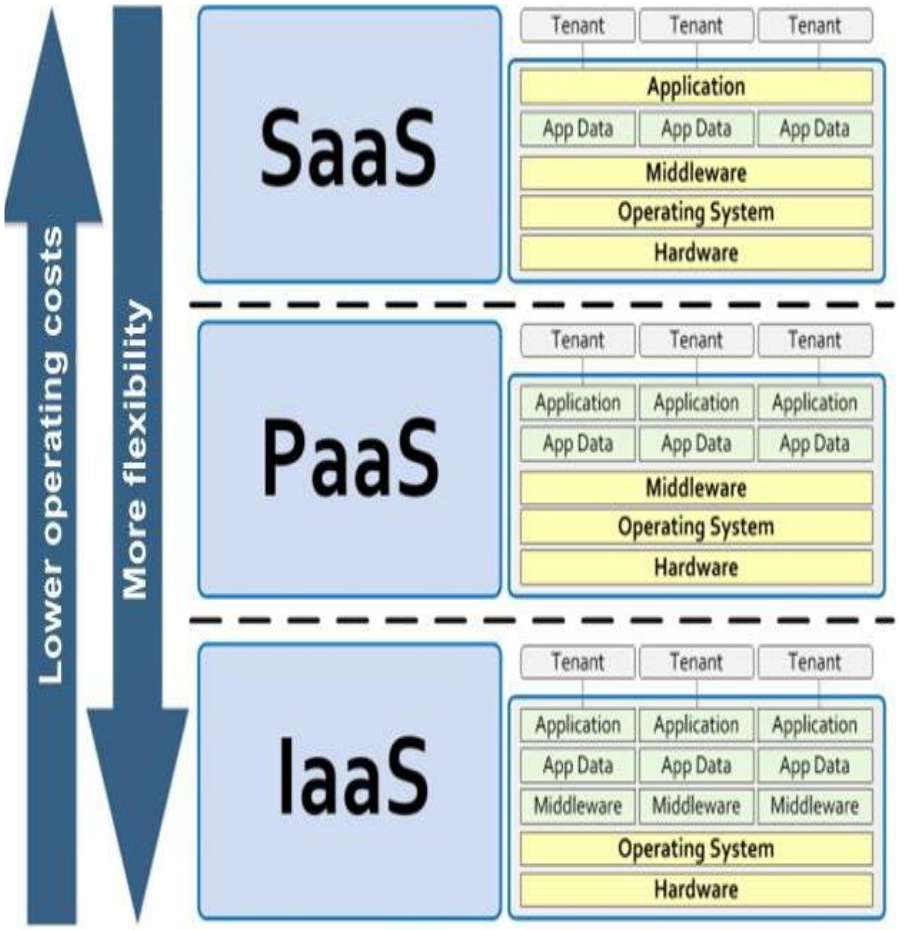

Figure 1. Cloud Service Delivery Models

4 Cloud Computation Implementation Criterion and Intelligent Security

The increased demand of the cloud has given a vital choice of its implementation. The user make a choice of implementation but the security is to be essential prime attribute, which regarded as the long duration sustainability.

4.1 Steps to Cloud Security

Edwards (2009) stated that, with the security risk and vulnerability [17] there are certain steps needs to follow in the path to attain a secure bridge to the cloud infrastructure:

- Decide the model and infrastructure of the cloud as per the usage. Decide on the security measures and layered optimizations.[12]
- Demand Transparency by making sure that the cloud provider should be providing the security levels and updates. The proper trials related to security should be conducted and the regular reports to be created.
- The service providing organizations should persist a rigid firewall and the security features and ability to handle any sudden malware eruptions.
- Consider the Legal Implications by knowing how the laws and regulations will affect what you send into the cloud.
- Perform transitions through the environment of cloud regularly asking the proposed issues and making the relevant pitches.[13]
- Use of appropriate surrounding with the inner servicing makes an measurable impact along with the use of analytics.

4.2 Criterion of Computing

Gartner, Inc., the world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud-computing user should address with cloud computing providers (Edwards, 2009) before adopting:

- User Access: Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major companies should demand and enforce their own hiring criteria for personnel that will operate their cloud computing environments.
- Regulatory Compliance: Demand for the details regarding the regulations from the service providers of the cloud.

- Data location: Enterprises need to take care of fixing of the data in the cloud. The positioning needs to be relevant with respect to cluster of usage demands. [16]
- Data Segregation: The data sent from user to the cloud should be acknowledged regularly. The key security features added to it needs to be acknowledged back to the service taker such that it can plan certain proposals for the further improvements to the organization.[15]
- Disaster Recovery Verification: In extreme conditions of failure; the client should know how the data will be recovered (i.e. multiple hopping). This is important credential, as the data cannot risked in any condition.
- Disaster Recovery: Recovery should from top to bottom without compromising any set of data.
- Long-term Viability: Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application.

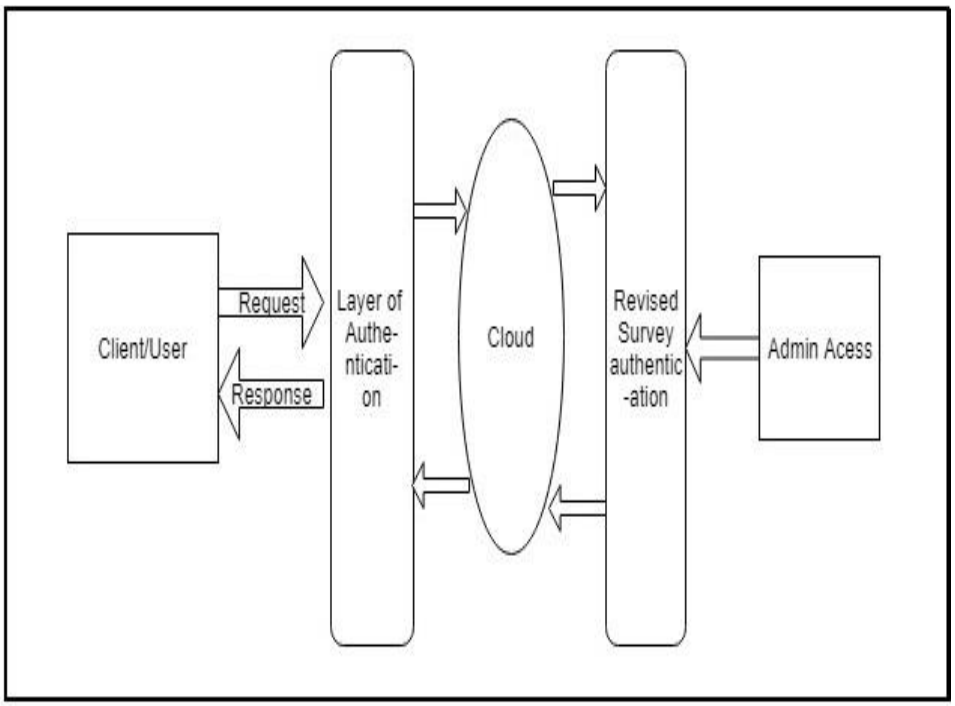

Figure 3. Proposed Secure Model of Cloud

The context of Figure 3 is a model, which is capable of handling the vulnerabilities and issues with cloud data with efficiency of 80%-92%. The cloud is made secure through the over way authentication combining the layered gateways and firewall. The algorithm is developed for gateway protocol suites and network transmissions. The "Graph – g1" shows a clear impact of the measures applied on the cloud environment. It depicts an threshold upon which the optimization in inversely proportional to the time. The use of algorithms, which are application based on AI, ML, DA platforms, will be a best way to encompass the security issues.

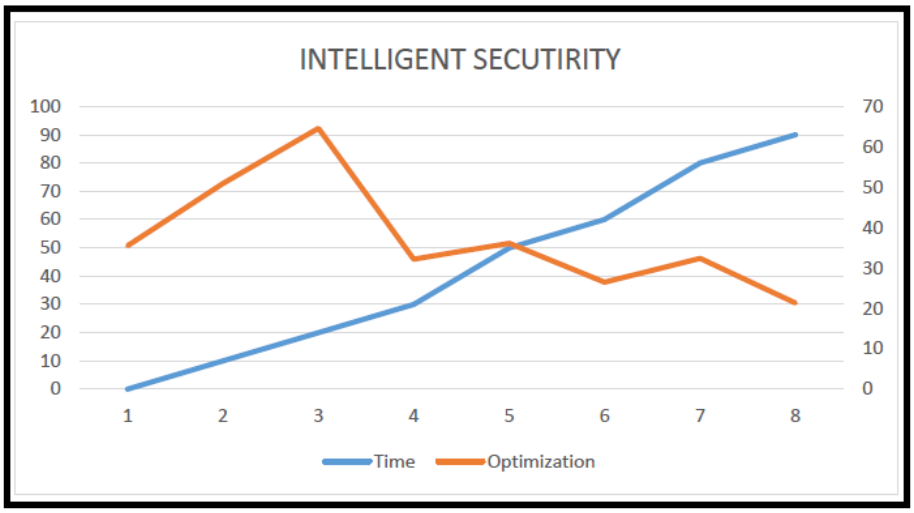

Fig. 2. Graph-g1

5 Conclusion

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges that are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

References

[1] Mather T, Kumaraswamy S, Latif S (2009) *Cloud security and privacy*: an enterprise perspective on risks and compliance. O'Reailly Media, Sebastopol, CA, USA

[2] Jensen M, Schwenk J,Gruschka N, LoIacono L (2009) On technical security issues in cloud computing. Cloud Computing. In: *IEEE international conference* on 0:109–116

[3] Casado M, Freedman MJ, Pettit J, Luo J, McKeown N, Shenker S (2007) Ethane: taking control of the enterprise. SIGCOMM Comput Commun Rev 37(4):1–12. http://doi.acm.org/10.1145/1282427.1282382

[4] Bernstein D, Ludvigson E (2009) Networking challenges and resultant approaches for large scale cloud construction.In: Grid and pervasive computing conference, workshops the 0:136–142. http://doi.ieeecomputersociety.org/10.1109/GPC.2009.10

[5] Pffaf B, Pettit J, Koponen T, Anidon K, Casado M, Shenker S (2009) Extending networking into the virtualization layer. In: ACM SIGCOMM's hot topics in networks(HotNets)workshops.
http://conferences.sigcomm.org/hotnets/2009/papers/hotnets2009- final143.pdf

[6] Verendel V (2009) Quantified security is a weak hypothesis: a critical survey of results and assumptions. In: NSPW '09: *Proceedings of the 2009 workshop on new security paradigms workshop*, pp 37–50. ACM, New York, NY, USA. http://doi.acm.org/10.1145/1719030.1719036

[7] Krautsevich L, Martinelli F, Yautsiukhin A (2010) Formal approach to security metrics.: what does "more secure"mean for you? In: ECSA'10: *Proceedings of the fourth European conference on software architecture*, pp 162–169. ACM, New York, NY, USA. http://doi.acm.org/10.1145/1842752.1842787

[8] Ibrahim, Amani S., James Hamlyn Hamlyn-harris, and John Grundy. "*Emerging security challenges of cloud virtual infrastructure*." (2010).

[9] Ferris, James Michael. "*Extending security platforms to cloud-based networks*." U.S. Patent No. 8,977,750. 10 Mar. 2015.

[10] Erway, C. Chris, et al. "*Dynamic provable data possession*." ACM Transactions on Information and System Security (TISSEC) 17.4 (2015): 15.

[11] Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "*Security in cloud computing: Opportunities and challenges*." Information Sciences 305 (2015): 357-383.

[12] Wang, Boyang, Baochun Li, and Hui Li. "*Panda: public auditing for shared data with efficient user revocation in the cloud*." Services Computing, IEEE Transactions on 8.1 (2015): 92-106.

[13] Baumann, Andrew, Marcus Peinado, and Galen Hunt. "*Shielding applications from an untrusted cloud with haven*." ACM Transactions on Computer Systems (TOCS) 33.3 (2015): 8.

[14] Sari, Arif. "*A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications.*" Journal of Information Security 6.02 (2015): 142.

[15] Hashem, Ibrahim Abaker Targio, et al. "*The rise of "big data" on cloud computing: Review and open research issues*." Information Systems 47 (2015): 98-115.