Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 8 No. 2, June, 2017 - www.cisdijournal.org

A Review of Cyber Security Risk Management from Service Oriented Architecture to Fog Computing

[1]Akinwumi D.A., [2]Alese, B.K., [3]Akingbesote, A.O. & [2]Oluwadare, S.A.
[1]ICT Application Centre, AdekunleAjasin University, Akungba-Akoko, Ondo State, Nigeria.
[2]Department of Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria
[3]Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Ondo State, Nigeria.
david.akinwumi@aaua.edu.ng, kaalfad@yahoo.com, oluwamodimu2012@gmail.com, samoluwadare@futa.edu.ng

ABSTRACT

Cyber security is among the most complex and rapidly evolving issues and has been the focus of organizations, researchers and government of nations. Cyber security is the preservation of confidentiality, integrity and availability of information in the Cyberspace. Cyber security risk management is the process of managing or reducing potentially harmful and uncertain events that posse as threats to cyber security. It involves looking at what could go wrong on the cyber space and deciding on ways to prevent or minimize their occurrences or effects. The advancement in technology has allowed for the management of cyber risk from Service-Oriented Architecture (SOA) to Fog Computing. In this research, a detailed literature review is presented on the work done in the area of cyber security risk management on these computing concepts. An overview of the key features of the concepts is given and a systematic strategy towards addressing the shortcomings is then introduced. Finally, some future research issues especially on cyber security risk management in the concept of Fog computing are discussed.

Keywords: Cybersecurity; risk management, Service-Oriented Architecture;Grid computing; Cloud computing; Fog Computing.

CISDI Journal Reference Format
Akinwumi D.A., Alese, B.K., Akingbesote, A.O. & Oluwadare, S.A. (2017): A Review of Cyber Security Risk Management from Service Oriented Architecture to Fog Computing.. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 8 No 2. Pp 111-122.
Available online at www.cisdijournal.org

1. INTRODUCTION

Risk is present everywhere and demands efficient management strategies. Risks associated with cyber activities are called cyber risks. Cyber risk is among the most complex and rapidly evolving issues with which organizations, researchers and government of nations must contend with [1]. Security threats are common in recent times and a violation can result into serious consequences which are indication of the importance of cyber security risk management to services provided over the Internet. Presently, there is a proportionate increase in the number of users of cyber space and the number of cyber criminals has also increased. This explains the reason why increasing organizations' reliant on information systems and the Internet has resulted in increased cyber security risks management in all the concept of computing that provide services via the Internet.

Reports of major cyber attacks and damage to organizational IT infrastructure have become increasingly common in recent years and developments in mobile technology, cloud computing, Fog computing and social media continue to impacts the IT risk landscape [2]. Consistent cyber security risk management ensures cost-effective management of risks with high priority to be aggressively managed so as to provide better risk reporting and informed decision making [3]. Managing cyber security risk may not result in the elimination of all risks but is effective for determining and understanding risk rating of events and putting the right processes or controls in place [4]. This research takes a systematic review of cyber security risk management from service oriented architecture to fog computing.

Section 2 of this paper presents the review of Service-Oriented Architecture in relation to cyber security risk management while the review of some research works on cyber security risk management as applied to Grid and Cloud computing is presented in Sections 3 and 4. Section 5 focuses on the review of Fog Computing and propose a game theory approach to cyber security risk management in the concept of Fog computing and the conclusion is drawn in Section 6.

2. SERVICE-ORIENTED ARCHITECTURE (SOA)

In recent times most software capabilities are delivered and consumed as services through a service-based interface. There is a probability of everything becoming a service. The service is an essential publishing construct and should be adopted at the point of each significant interface. Service-Oriented Architecture (SOA) allows us to manage the usage these services. SOA can be described as something that makes use of multiple services to perform a specific task[5]. In [6]Service-Oriented Architecture is defined as a style of designing a standard and technology-based independent distributed computing paradigm and architecture where services are provided to the other components through a communication protocol over a network. The services represent reusable business functionality through standard interfaces; service consumers compose applications using those services. The goal for a SOA is a worldwide network of collaborating services[7]. The adoption of SOA is highly imperative so as to provide the deliverables of business and IT by Web Services. These benefits are delivered through the creation of a Service Oriented Environment that is based on the Services that can be published, discovered and used in a technology neutral and standard form. The policies, practices, and frameworks must ensure that the right services are provided and consumed. In addition, existence of at least minimum of two different processes must be ensured for providers and consumers.

In recent times, researchers have applied SOA to various domains to enable dynamic Web services composition in order to flexibly support business processes within and across organizations. For example,[8] proposed the concepts of Web-services based workflows, [9]matching mechanisms, and in [10] context-aware Web services is conceptualized[11][12]. presented the concepts of Web-services using WSDL-S and ontologies. These researches focuses on ubiquitous computing, mobile computing, e-Commerce, supply chain management, knowledge and document management which has bring various benefits of SOA and Web services to the limelight. In this regards, Papazoglou and Van den Heuvel [13] propose a comprehensive service life-cycle methodology for applications to enhance management practices. For example, the customer relationship management is proposed in [14].

Service-Oriented Architecture and web services implementation in the military is on the pipeline[15].This is achieved as a result of breakthrough in research through the development of models, methodologies and specifications that have help programmers to integrate application into selected SOA, including the installation of security appropriate to SOA[15]. The increasing dependence of business organization on SOA, have necessitate the need to apply a comprehensive and dynamic security strategy by organizations so as to keep abreast of the evolving security threats[16]. Security threats are common in recent times and a violation can result into serious consequences which is an indication of the importance of SOA security. [17] Propose a solution for risk management in SOA, the methodology addresses the assessment of the likelihood and the risks impact as well as profiling of information assets. In [18]the authors proposed some security standards for web services as applied to SOA and risk management. The standards include: (i) Security Assertion Markup Language (SAML) and Electronic Business using eXtensible Markup Language (ebXML), (ii) Web Services Security, XML-Signature and XML Encryption in the message layer standards. (iii) Transport Layer Security (TLS) / Security Socket Layer (SSL).

The benefits of a SOA according to[19] include:

i. Provision of application functionality as services in order to enable the integration of existing applications, thus, improving the value of existing software assets.
ii. redundancy in IT infrastructure can be avoided
iii. It enhances a quick response to changes in business processes and interoperability
iv. simple standards that define the available interfaces and structure of data that is conveyed across those interfaces
v. platform and language-independent interfaces based on these standards, which allow applications to invoke services operating on any device supporting the SOA regardless of the hardware platform, operating system, or implementation language
vi. clear separation of service interface from implementation, thus allowing many service upgrades to occur without impact on service users
vii. message-oriented communication allowing distribution across a wide area
viii. loose coupling between services, minimizing interdependencies and reusability
ix. mechanisms for discovery of services available and for establishing connections with services

The authors in [20]argued that SOA benefits proposed in[19]is based on single or multiple case studies that range from infrastructure to operational, organizational, and strategic benefits. The authors however, opine that the findings have neither been systematically consolidated into a framework nor validated by means of a broader empirical view. Another challenge of SOA is the new threats it introduces to information security which poses new challenges for security professionals[17]. As a result of the challenges, it becomes difficult sometime for programmers to guarantee insurance services and SOA architectures. Similarly, joining the SOA architecture with protocols allowed through firewalls security can pose serious security risk[17]. While the SOA have been successfully applied in different domain, especially in the business sector, SOA demand for high computational power, high cost of maintaining the equipment and human resources is a big challenge[21],[22].These limitations led to the creation of the Grid computing.

3. GRID COMPUTING

Various architectural enhancements exist for increasing computer network speeds and storage capacity. However, effective utilization of computing power is very low. Numerical and data intensive problems that require a variety of heterogeneous resources are not available on a single computer[23]. Grid Computing offers a solution to this challenge. Grid computing is the voluntary use of under-utilized resources available over the network, balancing out the utilization by exploiting parallelism and providing a means for solving highly intensive problems in real time.

In [24]Grid computing is defined as a distributed system with non-interactive workloads having a variety of levels of virtualization of computer resources from multiple locations to reach a common goal. The concept of Grid can be viewed as a technology that manages sharing and trust. Sharing is done through coordinated resource sharing in a virtual environment between participants with varying degrees of prior relationships and trust, while trust within a virtual environment is strictly defined by the sharing rules governed by security policies[25]. The grid virtualizes heterogeneous and geographically disperse resources is depicted in Figure1.

The conceptualization of the Grid architecture is the drawing of computational power from a distributed pool of resources by consumers seamlessly and ubiquitously[26].

According to [24] the following benefits of Grid computing has been the major motivation for using Grid:

i. Exploiting underutilized resources
ii. Parallel CPU capacity
iii. Virtual resources and virtual organizations for collaboration
iv. Access to additional resources
v. Resource balancing
vi. Reliability and Management

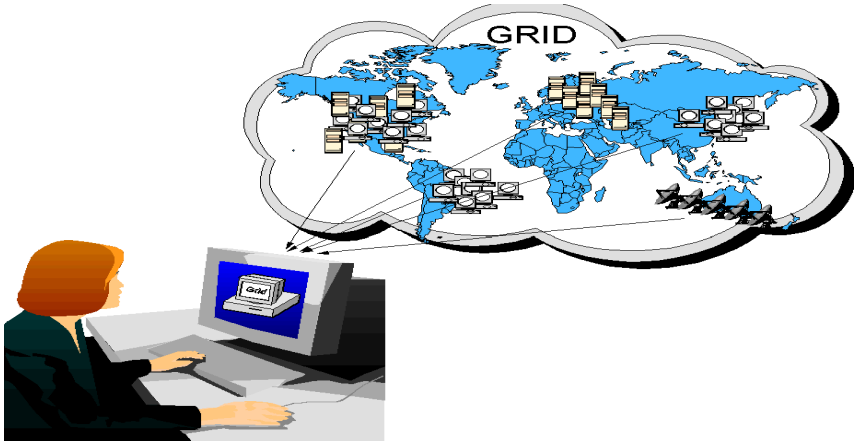

Figure 1: The grid virtualizes heterogeneous and geographically disperse resources[24]

Grid computing have been applied into the market place, for example in [26] the Grid market place allows for the purchase of computational power by consumers through the use of middleware or a resource allocation broker. [27],[28] identified the distinguishing features of the Grid Marketplace as follows:

i. Collaboration among members of the Grid community with the use of powerful middleware.
ii. Integration of different heterogeneous hardware infrastructure.
iii. The distributed paradigm and
iv. Secure access through the use of a powerful security mechanism to grant the right delegation.

Grid markets have been viable in terms of high performance[29],[30]. However, lack of a distributed and robust resource allocation mechanism, inability to provide a good accounting mechanism and inability of the architecture to fully cope with the business world has been some of the major challenges of Grid markets [31],[32],[33].

In[34]a framework for enabling autonomic application management in Grids is introduced to address the constant growth and increasing scale complexity of dynamic and heterogeneous components in computational Grids. In this regards, a good number of Grid systems have been proposed[34], for example is the Aneka Federation system [35], a Grid application development and execution environment called Askalon[36], AutoMate [34],Condor-G [37] which combines the inter-domain resource management protocols of the Globus Toolkit and the intra-domain resource and job management mechanisms of Condor. Other Grid systems includes; Grid bus Workflow Management System (GWMS) [38]that helps users to execute their workflow applications on Grids, Nimrod/G [39]is a Grid middleware environment for building and managing large computational experiments over distributed resources, Pegasus Workflow Management System (PWMS) [40]supports large-scale data management in physics experiments, Taverna [41] focus to exploit Grid technology to develop high-level middleware for supporting data-intensive in silicobioinformatics experiments using distributed resources and Triana [42] which allows integration of Triana with multiple Grid services and interfaces.

The author in [25] pointed out the challenges of Grid computing and the propose some solutions as depicted in Table 1.

Table 1: Challenges of Grid Computing and Solutions[25]

Grid attributes	Challenges	Solution
Trust (security is built on trusted parties	how to trust virtual organization members and its agents	proxy credentials provided by a trusted parties in public key infrastructure
Sharing of applications and data	incompatible machines and OS, need to limit access	virtualization, Grid resource allocation policies
Grid interoperability	incompatible protocols	XML-based protocols and open standards
Reliability and robustness	Grid-based systems can be brittle	two-phase commit, transaction-based protocols
Quality of service (QoS)	need end-to-end resource management, transactions	budgeting of cycles, bandwidth, and storage capacity

Considering the several areas where Grid computing have been applied, it is could be observed that Grid computing cannot achieve more without additional hardware or resources, Grid computing cannot introduce parallelism in applications and it also requires configuration rather than mere installation[23].Grid computing allows sharing resources, principally for scientific applications[43]. However, Grid computing does not heavily use virtualization, as a result, users have less control and the Grid system is less flexible and more complex. This challenges led to the emergence of the Cloud computing.

4. CLOUD COMPUTING

The implementation of virtualization technology by cloud computing to attain the goal of providing computing resources as a utility has been a distinguishing factor for the cloud paradigm [44].In 2009, NIST defines Cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[43]. Cloud computing can be categorized based on delivery and deployment models as depicted in Figure 2.Cloud computing consist of three layers; the lowest layer that provides basic infrastructure support service is Infrastructure as a Service (IaaS), the middle layer is Platform as a Service (PaaS) that provides platform oriented services and environment for hosting user's applications. The topmost layer is Software as a Service (SaaS) that provides a complete

application offered as service on demand [45],[46],[47].Depending upon the customers' requirements any of these cloud service models can be deployed [46]as (1.) Public Cloud which is managed by a third party service provider to provide a cloud infrastructure to many customers.(2.) Private Cloud is managed either by the organization itself or third party service provider to provide a cloud infrastructure to a specific customer using the concept of virtualization.(3.) Community cloud is managed by several organizations or a third party to provide shared infrastructure and (4.) Hybrid Cloud composed of two or more cloud deployment models linked in a way that data transfer takes place between them without affecting each other.

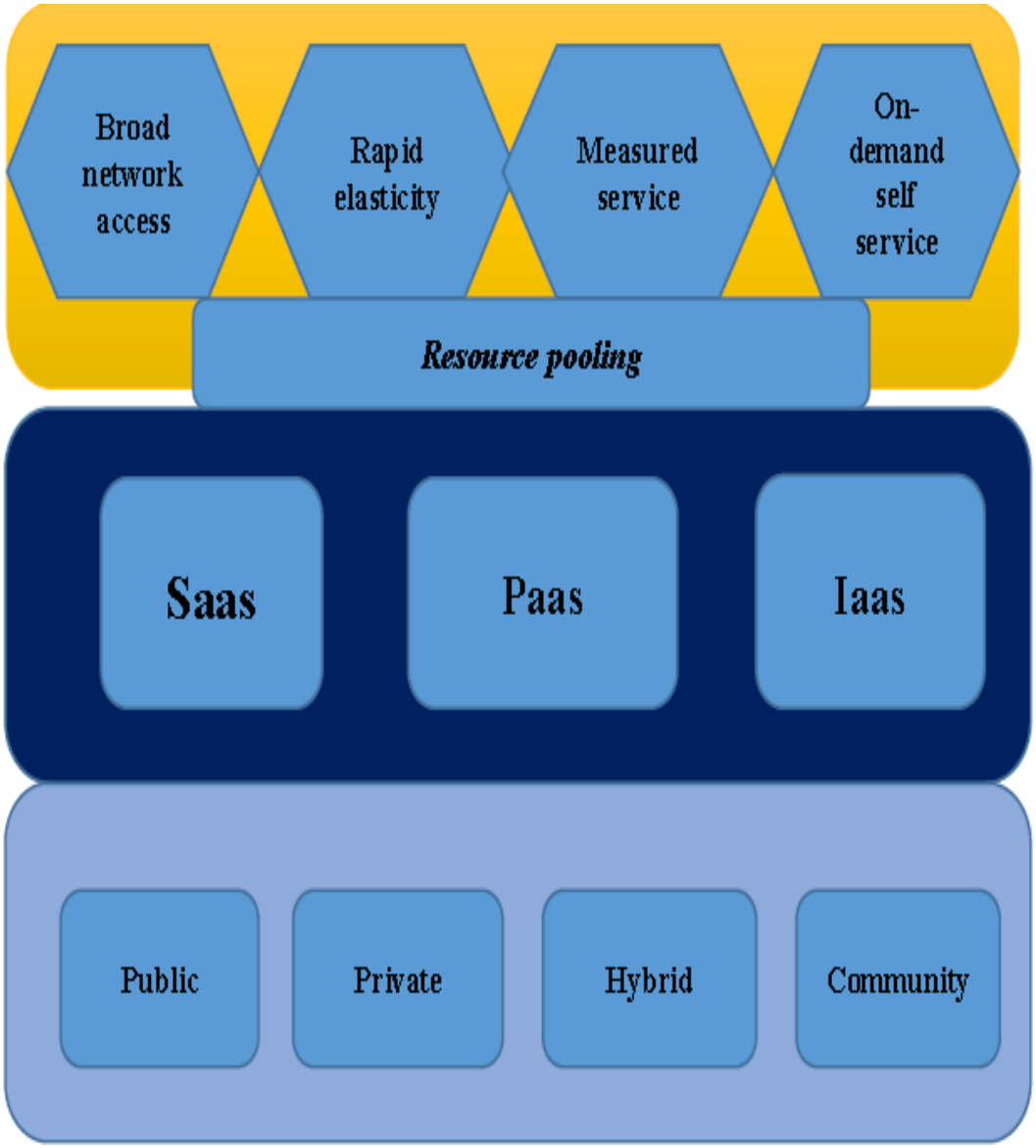

Figure 2: Cloud computing categorized [44]

The benefits of Cloud Computing

i. No up-front investment: pay as you go, utility-based pricing
ii. Lowering operating cost: easy to rapidly add and remove resources, no need to dimension for peak load
iii. Elastic: highly scalable
iv. Easy to access: often web-based (for SaaS, and management for I/PaaS)
v. Reduce risks and contracts out expertise: lower staff training/Hardware maintenance costs
vi. computing resources are pooled together by service providers to help their numerous customers and dynamically allocate or reallocated the resources according to customer demand [44].

Cloud computing poses some challenges to both the users and cloud providers, for example, the issue of standards for cloud services especially PaaS, monitoring, security and systemic risks are users challenge while automatic scaling, VM migration and Server consolidation are providers challenge [43]. IaaS, PaaS, and SaaS models have different impact on application security [48]. In this regards, despite the tremendous business and technical advantages of cloud computing, security issue has been a major challenge[49]. The security issues identified in [50] are:

i. Outsourcing: Users may lose control of their data, hence appropriate mechanisms is required to prevent cloud providers from using customers' data in a way that has not been agreed upon in the past.
ii. Extensibility and Shared Responsibility: There is a balance between extensibility and security responsibility for customers in different delivery models.
iii. Virtualization: There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.
iv. Multi-tenancy: Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.
v. Service Level Agreement: The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time.
vi. Heterogeneity: Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.

Network penetration, packet analysis session and access control faults are some of the security risks posed to the cloud computing environment[51],[52].[53],[54],[55]discussed security issues associated with the cloud computing as insufficiency in security providers, availability, attacks by other clients, and reliability issues, wrapping attack, flooding attack and the authors analyzed the possible security solutions. In[56]Denial of Service (DoS) attacks, man-in the-middle cryptographic attacks, authentication attacks and inside-job is discussed.

The authors in[57]propose Advanced Cloud Protection System (ACPS) to tackle security issues in the Cloud while [58],[59]tackle the issues by presenting a model for random computations and outsourcing data that ensure integrity, verifiability and confidentiality. [60]focused on integrity protection issues in the clouds. [61] proposed a system protecting personal information using role-base and attributed- base access control models that improve the security of the cloud and access control that guarantee the cloud availability, confidentiality and integrity.

Various authors have used different approaches to solve security issues in Cloud, for example, [62]proposed an approach of provider-compulsory deterministic execution to protect shared cloud from timing channels that is able to avoid implementation of timing. [63]developed a technique to identify application DOS attack using a new constraint-based group testing model. [64] presented several approaches to mitigate risks that arises from sharing physical infrastructure between mutually distrustful users. [65]presented data protection scheme with public auditing scheme that involves four algorithms including sig gen, key gen, gen proof, and verify proof. [66]developed an algorithm for secure third party publications of documents in the cloud.[67] proposed a method which gives access to user using elliptic curve cryptography encryption to preserve data files and to safeguards the privacy and security of data stored on cloud.

In attempt to manage cyber security risks on the cloud, SalesForce.com[68] implemented some security measures to avoid unauthorized access to its platform by sending a security code to the registered customer every-time the same account is accessed from same or different IP-address and the user needs to provide the security code at the time of logging in, in order to prove the identity of the user. In [69] a detailed analysis of various steganographic techniques and their application using different cover media is carried out. Steganography is a technique which can be used to hide confidential information within a plain text, image, audio/video files or IP datagrams in a TCP/IP network in order to secure the data-in-transit. Detecting unauthorized access in the cloud using tenant profiles is also presented in [70].

Performance unpredictability has been observed as an issue in Cloud computing, for example, I/O performance [71].The research proposed a method to improve I/O performance as improve architecture and operating systems so as to efficiently virtualized interrupts and I/O channels.The authors in [71]also opined that flash memory can be used to improve I/O performance which is a type of semiconductor memory that preserves information even when powered off. Flash memory is much faster to access; it uses comparatively less energy and can sustain many more I/O operations than disks. However, the performance of the system is a factor in cloud computing, the cloud service providers may run short of capacity either by allowing access to too many virtual machines or reaching upper throughput thresholds on their Internet links because of high demand arising from the customers. This affects the system performance and also adds to the latency of the system.

Latency has been a major issue in cloud computing[72]. The factors that contributed to the latency in the cloud are (1.) encryption and decryption of the data when it moves around unreliable and public networks. (2.) data flow around different clouds (3.) congestion (4.) packet loss and (5.) windowing. Congestion adds to the latency when the traffic flow through the network is high and there are many requests that need to be executed at the same time. Windowing is a message passing technique whereby the receiver has to send a message to the sender that it has received the earlier sent packet and hence this additional traffic adds to the network latency[72],[73].

There are quite a number of unresolved issues that need to be addressed in cloud computing. For example is the Internet accessibility, the Internet has been the major factor towards the cloud computing evolution and without having the Internet access the cloud cannot offer any reasonable service. Latency, the distance from the source adds up to the longer time intervals observed in case of data transfer and other network related activities because of an increase in the number of intermediate network components. Also, applications running on mobiles in a mobile cloud computing platform should be intelligent enough to adapt to the varying network capacities and these should be accessible through different platforms without suffering any data loss. In addition, Cloud computing involves virtualization hence the need for user authentication and control across the clouds since existing solutions are not able to handle the case of multiple clouds[46].These challenges brought the emergence of Fog Computing.

5. FOG COMPUTING

Cloud computing offers customers a range of computing services through the "pay-as-you-go" model by providing an efficient alternative to owning and managing private data centres [74]. Cloud computing also saved the enterprises and their end users storage resources, computation limitation and network communication cost. However, this has become a challenge for latency-sensitive applications [75]. In addition, the emergence of IoT makes the current Cloud computing paradigm inefficient to satisfy customers' requirements of mobility support, location awareness and low latency[26].

Fog (Edge) computing is a promising computing paradigm that extends cloud computing to the edge of networks. In [26] Fog Computing is defined as the architecture that extends Cloud computing and services to the edge devices. Fog provides data, compute, storage, and application services to end-users in a similar way to Cloud computing but with distinct characteristics. Fog computing is an evolution of Cloud. This new evolution emanated from the era of mainframe which was then based on client–server solution that was distributive in nature. Technological advancement moves us from client-server solution (Distributive) to cloud solution (Centralized). But we are back to distributive as we move from cloud based solution to Fog based.

A typical Fog architecture [76] consist of three layers; the cloud layer, the Fog layer and the client layer as presented in Figure 3. The Fog layer extends the cloud to the edge devices. This consists of localized servers that are close to the consumers (Applications). These servers use a pro-active method to forecasts the mobile consumers' demand on information and pre-cache the most desirable contents [77]. The Fog layer serves as an intermediary between the cloud and the application layer. In this layer several Fog servers can be connected to each other using the IP core technology.

Fog computing has helped to provide solutions to cloud limitations[26] in the followings ways:

i. Reduction in data movement across the network resulting in reduced congestion
ii. Elimination of bottlenecks resulting from centralized computing systems
iii. Improved security of encrypted data as it stays closer to the end user.

Basically Fog computing offer the following advantages [75]:

i. The Fog proximity to end-users.
ii. The dense geographical distribution and its support for mobility.
iii. Fog provides low latency, location awareness, and improves quality-of-services (QoS) and real time applications.

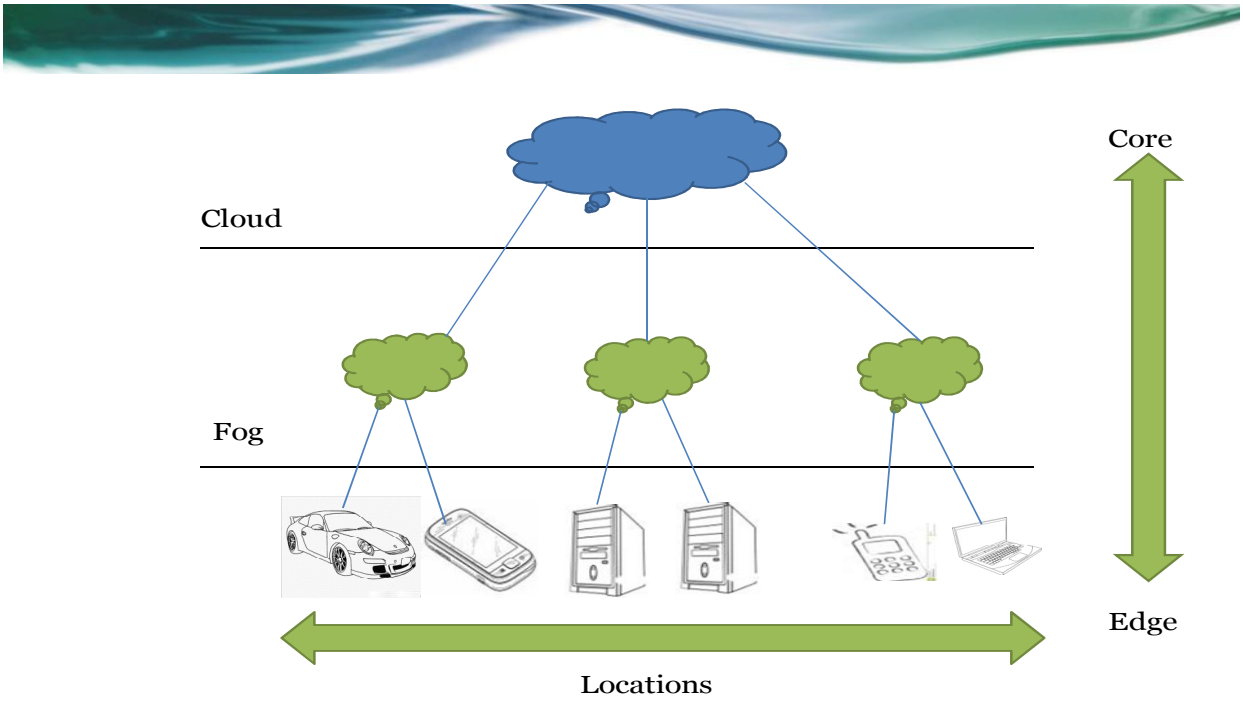

Figure 3: Fog Architecture [76]

Cyber security risk management solutions has been proposed in the context of Grid computing [78] and Cloud computing[76]. However, these solutions may not suit for Fog computing because Fog devices work at the edge of networks. The working surroundings of Fog devices will face with many cyber threats which do not exist in well managed Cloud. Mobility between Fog nodes, and between Fog and Cloud is an issue [76], especially in the context of cyber security risk management since Fog devices are geographically distributed over heterogeneous platforms. Hence, optimizing service mobility across platforms is still a challenge.

Authentication at different levels of gateways as well as at the edge devices is a major security issues. An attacker can either tamper with the edge devices or give false report. There are some solutions proposed by various researchers to solve authentication issue. For example, [79]presented a public key infrastructure (PKI) based solutions which involve multicast authentication. [80]proposed some authentication techniques using Diffie-Hellman key exchange while in [81]intrusion detection techniques is applied in Fog Computing. Intrusion in Grids is detected using either a signature-based method in which the patterns of behaviour are observed and checked against an already existing database of possible misbehaviors. Intrusion is also captured using an anomaly-based method in which an observed behaviour is compared with expected behavior to check if there is a deviation. The authors in [82]presented an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by attackers. The algorithm detects intrusion by using principal component analysis to separate power flow variability into regular and irregular subspaces.Another security issue in Fog computing is the Man-in-the-middle attack in which gateways serving as Fog devices is compromised or replaced by fake gateways [83].

[76] used man-in-the-middle attack as a proof of concept to expose the security issues in Fog computing. Man-in-the-middle attack is very stealthy in Fog computing because the attack consumes only a small amount of resources in Fog devices. The authors examine the memory consumption and the CPU utilization of gateway during the attack and show that if man-in-the middle attack does not greatly change the features of the communication, it is proofed to be a stealthy attack. The research also shows that man-in-the-middle attack is simple to launch but difficult to be addressed. Consequently, protecting Fog devices from compromise is a difficult task. Other unresolved issues include the estimation of specific risks arising from cyber attacks in order to prioritise effective control in the concept of Fog computing as well as the design of a competent Fog-based game-theoretic model for cyber security risk management. Most cyber security risk management techniques based on game theory have been applied to solve Computer Networks, Grid computing and Cloud computing. However, how this could be applied in the concept of Fog computing is yet to be fully discussed.

6. CONCLUSION

The review of the trends in computing paradigm and how to manage cyber security risk in each concept has been presented. The paper studied the current state of art from service oriented architecture to Fog computing. Some recent research works on cyber security risk management that are presented with focus on the motivations, objectives, methodologies and some short comings. The pros and cons of each paradigm that led to the emergence of the other computing paradigms have been examined. In view of the fact that technology changes, threats to cyber security also changes and hence, the need for continuous monitoring and managing of the cyber security is highly needed. The contribution of this paper is on some shortcomings identified in each of the technologies we have discussed in the concepts of cyber security risk. This, we hope will be of great benefits to scholar to identify some gaps for their research.

REFERENCES:

[1] O. Adeyinka, "Internet Attack Methods and Internet Security Technology," *Second Asia Int. Conf. Model. Simulation, May 2008*, vol. 13, no. 15, pp. 77–82, 2008.
[2] L. D. Deloitte, "Audit Committee Brief," 2013.
[3] L. Gordon, "Cyber-security management," 2014.
[4] K. Diana, "Application Security Risk Management and the NIST Cybersecurity Framework," 2014.
[5] D. Youseff, L; Butrico, M; Da Silva, "Toward a Unified Ontology of Cloud Computing," in *Grid Computing Environments Workshop*, 2008, pp. 1–10.
[6] G. Lewis and D. Smith, "A Research Agenda for Service-Oriented Architecture (SOA): Maintenance and Evolution of Service-Oriented Systems," no. March, 2010.
[7] D. Sprott and L. Wilkes, "Understanding Service-Oriented Architecture," no. January, 2004.
[8] J. M. BUHLER, P.A., and VIDAL, "Towards Adaptive Workflow Enactment Using Multiagent Systems," *Inf. Technol. Manag.*, vol. 6, no. 1, pp. 61–87, 2005.
[9] M. S. Juhnyoug, L., and Park, "Integration and Composition of Web Service-Based Business Processes," *J. Comput. Inf. Syst.*, vol. 44, no. 1, pp. 82–92, 3AD.
[10] W. E. B. Services, "What Can Context do for Web Services?," vol. 49, no. 12, pp. 98–103.
[11] J. Y. Sayah and L. Zhang, "On-demand business collaboration enablement with web services," vol. 40, pp. 107–127, 2005.
[12] A. Šaša, "Ontology-Based Knowledge Management in Service-Oriented Systems," vol. 35, no. 1, pp. 105–118, 2011.
[13] W. J. Papazoglou, M.P., and Van Den Heuvel, "Life Cycle Methodology," *Commun. ACM*, vol. 50, no. 10, pp. 79–85, 2007.
[14] M. B. Shah, J.R., and Murtaza, "EffectiveE Customer Relationship Management Through Web Services," *J. Comput. Inf. Syst.*, vol. 46, no. 1, pp. 98–109, 2005.
[15] R. W. M. and W. C. Lewis, "Risk Management Framework for Service-Oriented Architecture," in *IEEE International Conference on Web Services, Los Angeles, CA*, 2009, pp. 1000–1003.
[16] I. TIPNIS, Ajay. LOMELLI, "Security – a Major Imperative for a Service-Oriented Architecture.," 2009.
[17] E. L. & P. C. da S. Monteiro, "A Risk Management Model for Service - Oriented Architecture," *Int. J. Adv. Comput. Technol.*, pp. 53–61, 2009.
[18] S. BADR, Youakin. BIENNIER, Frederique. NASSAR, Pascal. BANERJEE, "Challenges of Security Risks in Service-Oriented Architectures," 2013.
[19] G. Lewis and L. O. Brien, "SMART : The Service-Oriented Migration and Reuse Technique," no. September, 2005.
[20] F. A. Goetz Viering, Christine Legner, "The (LACKING) Business Perspective on SOA –Critical Themes in SOA Research," pp. 1–10.
[21] and S. V. R. Buyya, C. S. Yeo, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities," *Proc. - 10th IEEE Int. Conf. High Perform. Comput. Commun. HPCC*, pp. 5–13, 2008.
[22] and R. N. C. R. Buyya, R. Ranjan, "Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities," *Int. Conf. High Perform. Comput. Simul*, pp. 1–11, 2009.
[23] M. Joshi, "Grid Computing," no. April, pp. 1–17, 2005.
[24] J. Bart, M. Brown, K. Fukui, and N. Trivedi, *Introduction to Grid Computing*. 2005.
[25] A. T. Spring, "Concepts and Architecture of Grid Computing," 2008.
[26] A. O. Akingbesote, "Survey on The Performance Evaluation of E-Marketplaces," *Comput. Inf. Syst. Dev. Informatics Allied Res. J.*, vol. 7, no. 3, 2016.
[27] L. . K. and T. Kiss, *Distributed and Parallel Systems*, vol. 777. Boston: Kluwer Academic Publishers, 2005.
[28] and J. B. R. Wolski, J. S. Plank, "g-Commerce – Building Computational Marketplaces for the Computational Grid," 2000.
[29] I. F. and N. T. Karonis, "A Grid-Enabled MPI: Message Passing in Heterogeneous Distributed Computing Systems," *Proc. IEEE/ACM SC98 Conf.*, pp. 1–11, 1998.
[30] and S. D. S. Pardeshi, C. Patil, "Grid Computing Architecture and Benefits," *Ijsrp.Org*, vol. 3, no. 8, pp. 3–6, 2013.
[31] P. F. Grimshaw, A. S., Wulf, W. A., French, J. C., Weaver, A. C., Reynolds Jr, P. F. and Reynolds, "Legion : The Next Logical Step Toward a Nationwide Virtual Computer e pluribus unum -- one out of many Technical Report CS-94-21, University of Virginia," 1994.
[32] and M. L. D. Thain, T. Tannenbaum, "Distributed computing in practice: The Condor experience," *Concurr. Comput. Pr. Exp.*, vol. 17, no. 2–4, pp. 323–356, 2005.
[33] K. N. and R. Buyya, "Enterprise grid computing: State-of-the-art TGrid Computing and Distributed Systems Laboratory, The University of Melbourne," 2005.
[34] M. Rahman, R. Ranjan, R. Buyya, and B. Benatallah, "A taxonomy and survey on autonomic management of applications in grid computing environments," no. May, pp. 1990–2019, 2011.
[35] B. R. Ranjan R, *Decentralized overlay for federation of enterprise clouds*, Li K (ed.). Hershey, PA, U.S.A.: IGI Global, 2009.

[36] A. T.F., "A tool set for cluster and grid computing," *Concurr. Comput. Pract. Exp.*, vol. 17, no. 2–4, pp. 143–169, 2005.
[37] T. S. Frey J, Tannenbaum T, Livny M, Foster I, "Condor-G: a computation management agent for multiinstitutional grids," *Tenth IEEE Int. Symp. High Perform. Distrib. Comput. U.S.A.*, 2001.
[38] B. R. Yu J, "Gridbus Workflow Enactment Engine, Grid Computing: Infrastructure, Service, and Applications," C. J. (eds). Wang L, Jie W, Ed. U.S.A.: CRC Press, 2009.
[39] G. J. Buyya R, Abramson D, "Nimrod/g: An architecture for a resource management and scheduling system in a global computational grid," in *Proceedings of 4th International Conference on High Performance Computing in Asia–Pacific Region (HPC Asia 2000)*, 2000.
[40] L. A. Deelman E, Singh G, Su M, Blythe J, Gil A, Kesselman C, Mehta G, Vahi K, Berriman GB, Good J and K. D. Jacob JC, "Pegasus: A framework for mapping complex scientific workflows onto distributed systems," *Sci. Program.*, vol. 13, no. 2, pp. 219–237, 2005.
[41] W. A. Oinn T, Addis M, Ferris J, Marvin D, Senger M, Greenwood M, Carver T, Glover K, Pocock M and L. P, "Taverna: A tool for the composition and enactment of bioinformatics workflows," *Bioinformatics*, vol. 20, no. 17, pp. 3045–3054, 2004.
[42] W. I. Taylor I, Shields M, "Resource management of triana p2p services," *Grid Resour. Manag. Wiley-InterScience Netherlands*, 2003.
[43] F. Taïani, "Cloud Computing," vol. 1, no. May, pp. 7–18, 2010.
[44] Y. Abdul, A. S. Aldeen, M. Salleh, and M. Abdur, "State of the art Survey on Security Issues in the Cloud Computing Architecture Approahes," vol. 75, no. 1, 2015.
[45] L. Lo Meiko Jensen, Jorg Schwenk, Nils Gruschka and Iacon, "On technical Security Issues in Cloud Computing," in *Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009)*, 2009, pp. 109–116.
[46] R. Bhadauria, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," vol. 47, no. 18, pp. 47–66, 2012.
[47] I. L. B.P. Rimal, Choi Eunmi, "A Taxonomy and Survey of Cloud Computing Systems," in *Intl. Joint Conference on INC, IMS and IDC*, 2009, pp. 44–51.
[48] H. John, "Security Guidance for Critical Areas of Focus in Cloud Computing," 2009.
[49] F. Gens, "IT Cloud Services User Survey, part 2: Top Benefits and Challenges," 2008.
[50] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges , Approaches and Solutions State-of-the-art Survey on Cloud Computing Security Challenges , Approaches and Solutions," *Procedia - Procedia Comput. Sci.*, vol. 37, no. September, pp. 357–362, 2014.
[51] V. Subashini, S., & Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.
[52] & D. Kulkarni, G., Gambhir, J., Patil, T. and A., "A security aspects in cloud computing.," *IEEE Int. Conf. Comput. Sci. Autom. Eng.*, pp. 547–550, 2012.
[53] S. Chhikara, "Analyzing Security Solutions in Cloud Computing," vol. 68, no. 25, pp. 17–21, 2013.
[54] K. A. Challa, "Cloud Computing Security Issues with Possible Solutions," pp. 340–344, 2012.
[55] V. Nirmala, "Data Confidentiallity and Integrity Veriffication using User Autthenticator scheme in cloud," 2013.
[56] B. Seunghwan, J., Gelogo, Y. E., & Park, "Next Generation Cloud Computing Issues and Solutions," vol. 5, no. 1, pp. 63–70, 2012.
[57] R. Lombardi, F., & Di Pietro, "Secure virtualization for cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1113–1122, 2011.
[58] & Sadeghi, A., Schneider, T., Winandy, M. and G. Horst, "Token-Based Cloud Computing," vol. 2, pp. 417–429, 2010.
[59] D. Zissis, D., & Lekkas, "Addressing cloud computing security issues.," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.
[60] P. A. Lombardi, F., & Moro, "Transparent Security for Cloud," pp. 414–415, 2010.
[61] T. T. Mon, E. E., & Naing, "The privacy-aware access control system using attribute-and role-based access control in private cloud," *4th IEEE Int. Conf. Broadband Netw. Multimed. Technol.*, pp. 447–451, 2011.
[62] B. Aviram, A., Hu, S., & Ford, "Determinating Timing Channels in Compute Clouds," *Comput. Inf. Sci.*, 2010.
[63] D. S. Varma, P. R. K., & Krishna, "Application Denial of Service Attacks Detection using Group Testing Based Approach," *Int. J. Comput. Sci. Commun. Networks*, vol. 2, no. 2, pp. 167–171, 2012.
[64] S. Ristenpart, T., Tromer, E., & Savage, "Hey , You , Get Off of My Cloud : Exploring Information Leakage in Third-Party Compute Clouds.," 2009.
[65] M. Gowrigolla, B., Sivaji, S., & Masillamani and R., "Design and auditing of Cloud computing security," *2010 Fifth Int. Conf. Inf. Autom. Sustain.*, pp. 292–297, 2010.
[66] & Hamlen, K., Kantarcioglu, M., Khan, L. and B. Thuraisingham, "Security Issues for Cloud Computing," *Int. J. Inf. Secur. Priv.*, vol. 4, no. 2, pp. 36–48, 2010.
[67] A. Kumar, A., Lee, B. G., Lee, H., & Kumari, "Secure storage and access of data in cloud computing," *Int. Conf. ICT Converg.*, pp. 336–339, 2012.

[68] Sales-force.com, "Secure, Private and Trustworthy: Enterprise Cloud Computing with Force.com," 2012.
[69] B. Soumyendu Das, Subhendu Das and S. S. Bandopadhyay, "Steganography and Staganalysis: Different Approaches," *Int. J. Comput. Inf. Technol. Eng.*, vol. 2, no. 1, 2008.
[70] Jason Nikolai, "Detecting Unauthorized Usage in a Cloud using Tenant Profiles," 2010.
[71] R. G. Michael Armbrust, Armando Fox, A. K. Anthony D. Joseph, Randy Katz, I. S. Gunho Lee, David Petterson, Ariel Rabkin, and M. Zaharica, "A View of Cloud Computing", Communications of the ACM," vol. 53, no. 4, 2010.
[72] Neal Leavitt, "Is Cloud Computing Really Ready for Prime Time?," *IEEE Comput. Soc. CA, USA*, vol. 42, no. 1, pp. 15–20, 2009.
[73] R. Minnear, "Latency: The Achilles Heel of Cloud Computing," *Cloud Expo Artic. Cloud Comput. Journal.*, 2011.
[74] A. K. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz and and M. Z. G. Lee, D. Patterson, A. Rabkin, I. Stoica, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[75] and S. A. F. Bonomi, R. Milito, J. Zhu, "Fog computing and its role in the internet of things," *Proc. First Ed. MCC Work. Mob. Cloud Comput. ser. MCC'12. ACM*, pp. 13–16, 2012.
[76] I. Stojmenovic, "The Fog Computing Paradigm : Scenarios and Security Issues," vol. 2, pp. 1–8, 2014.
[77] and M. D. E. Bagtug, M. Bennis, "Living on the Edge: The Role of Proactive Caching in 5G Wireless Networks," *IEEE Commun. Mag.*, vol. 52, pp. 82–89, 2014.
[78] W. Wang and Z. Lu, "Survey cyber security in the smart grid: Survey and challenges," *Comput. Netw*, vol. 57, no. 5, pp. 1344–1371, 2013.
[79] and A. Lo Y. W. Law, M. Palaniswami, G. Kounga, "Wake: Key management scheme for wide-area measurement systems in smart grid," *Commun. Mag. IEEE*, vol. 51, no. 1, pp. 31–44, 2013.
[80] and Y. N. Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, "Toward intelligent machine-to-machine communications in smart grid," *Commun. Mag. IEEE*, vol. 49, no. 4, pp. 60–65, 2011.
[81] and M. R. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, "A survey of intrusion detection techniques in cloud," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2013.
[82] and N. B. J. Valenzuela, J. Wang, "Real-time intrusion detection in power system operations," *Power Syst. IEEE Trans.*, vol. 28, no. 2, pp. 1052–1062.
[83] and D. Y. L. Zhang, W. Jia, S. Wen, "A man-in-the-middle attack on 3g-wlan interworking," *Commun. Mob. Comput. (CMC), Int. Conf.*, vol. 1, pp. 121–125, 2010.