Towards Resilience Metrics for Future Cloud Applications

Marko Novak[1], Syed Noorulhassan Shirazi[2], Aleksandar Hudic[1], Thomas Hecht[1], Markus Tauber[1,3], David Hutchison[2], Silia Maksuti[1,3] and Ani Bicaku[1,3]

[1]*Austrian Institute of Technology, Vienna, Austria*

[2]*InfoLab21, School of Computing and Communications, Lancaster University, Lancaster, U.K.*

[3]*University of Applied Science Burgenland, Eisenstadt, Austria*

Keywords: Security Metrics, Technology Trend Analysis, Threat Trend Analysis, Cloud Applications, Resilience

Abstract: An analysis of new technologies can yield insight into the way these technologies will be used. Inevitably, new technologies and their uses are likely to result in new security issues regarding threats, vulnerabilities and attack vectors. In this paper, we investigate and analyse technological and security trends and their potential to become future threats by systematically examining industry reports on existing technologies. Using a cloud computing use case we identify potential resilience metrics that can shed light on the security properties of the system.

1 INTRODUCTION

Technology has become a common part of everyday life. In fact, technology is concerned with improvements in a variety of human and organizational endeavours through the design, development, and use of technologically based systems and processes that enhance the efficiency and effectiveness of our daily operations. Therefore, the analysis of technological trends is vital to all organizations for their future overall effectiveness. Cloud computing is evolving as an obvious solution for user requirements, due to their intrinsic capabilities of elasticity and resource transparency. Consequently, they are becoming increasingly mission-critical since they provide always-on services for many everyday applications (e.g., IPTV), critical industrial services (e.g., Air Traffic Control (ATC) networks), critical manufacturing services (e.g., utility networks and Industrial Control Systems) and critical real-time services (e.g., surveillance systems). This trend is emphasised in report (Dekker, 2012) published by *ENISA*, which provides specific guidelines in this area. Despite the potential benefits of cloud computing, deploying services increases various concerns because the high degree of virtualization and resource abstraction offered by cloud environments comes with a new set of challenges in terms of security and resilience. These challenges include malicious behaviour, cyber-attacks, worms and viruses-compounded with privacy and legal issues. Compared to non-cloud-based systems, understanding of the nature of challenges experienced by cloud providers is also somewhat opaque, as highlighted in the literature (Grobauer et al., 2011). Therefore, the resilience and ability of such cloud environments to remain operational in the face of challenges becomes paramount, and it should be thoroughly addressed by considering the inherent operational characteristics and investigation of technological trends that bear the potential to become future threats in cloud environments.

This paper is based on EU FP7 project SECCRIT (SEcure Cloud computing for CRitical infrastructure IT). The project aims to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments, and consequently to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for critical infrastructures (Simpson et al., 2013). More precisely, the work presented here is oriented on cloud assurance activities and resilience management activities, which includes assurance and resilience management frameworks supported by monitoring of

Novak, M., Shirazi, S., Hudic, A., Hecht, T., Tauber, M., Hutchison, D., Maksuti, S. and Bicaku, A.
Towards Resilience Metrics for Future Cloud Applications.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 1*, pages 295-301
ISBN: 978-989-758-182-3

cloud services (Shirazi et al., 2015), (Hudic et al., 2014), (Scholler et al., 2013).

2 RELATED WORK

Forecasting of the next generation technologies and their usage faces considerable difficulties. Related work in (Khajeh et al., 2010), (Khajeh et al., 2011) and (Khajeh et al., 2012) has developed research results about the cloud adaptation to other technologies. However, none of these results mention a resilience as a major issue in cloud operational context. Various monitoring systems have been developed, as in (Ballard et al., 2010), (Ibrahim et al., 2011) and (Payne et al., 2008), but likewise none of them mention resilience as a monitoring subject. Using trend analysis, a use case, and by adding a resilience as a "big thing" for better cloud operability, we believe that our work present an approach for detecting hot spots of the security issues in future based cloud applications.

3 TECHNOLOGY TREND ANALYSIS

3.1 Technology Trend Analysis Approach

The method used for collecting information with regard to technological trends and threats follow the pattern of the information collection, analysis and collation. We considered public information from research work performed by governments, organisations, and industries. This approach complies with the principles of Open-Source Intelligence. As stated in (Authorization., 2006), "OSINT is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement", applied to enable a broader view of the system, i.e., a representation of the whole system from the perspective of a related set of concerns. For the analysis of technological trends and future threats, we have used aggregation approach in order to harmonize all trends. Harmonisation of the all trend analysis results provided by the experts presents correct lines to get precise future trend analysis. In order to get summary of the results, we created cross-mapping table with technology trends and proposed sources. Raw data has been compressed and we added some simple calculation to get required results (see Figure 1).

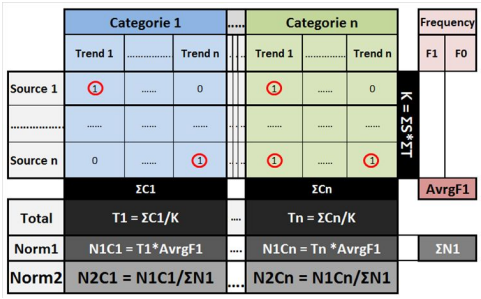

Figure 1: Calculation Model.

Relevant information is cross-mapping block indexed with "1", which presents trend identified by a corresponding source. The calculation method is structured as follows:

- Total percentage for the category is calculated with the sum of blocks indexed with "1" within category divided with the number of the trend and sources combination, $(T1 = \sum C1/K)$.
- *Normalization1* is calculated by multiplying of the total percentage with index "1" frequency average, $(N1C1 = T1 \times AvrgF1)$.
- *Normalization2*, which gets required results is calculated by dividing of the Normalization 1 value with its sum from the all categories, $(N2C1 = N1C1/\sum N1)$.

Technology trends are structured as follows:

- **Mobile Technologies** - *Internet of Things, Mobile Applications, Digital Payments, Wifi Calling, Soft SIM Cards and Beacons.*
- **Cloud Computing** - *Hybrid Cloud, Cloud/Client Architecture, Software Defined Networking (SDN), Docker and other container technologies, Agile infrastructures, Challengers to AWS, Era of personal cloud.*
- **Market and Device Diversity** - *Mobility (BYOD), Chinese brands, Telecoms Consolidation, Smart machines, Third Platform (mobile computing) and 3rd Smartphone business model (Xiaomi).*
- **Network Protocols** - *VoLTE (Voice over LTE), NFC (Near Field Communication) and 3GPP.*
- **Others** - *Wearable and 3D Printing.*

Summary of the technology trend forecast from our sources is showed in Figure 2. Percentage values represent expectation index, or more closely output of the relevant sources chosen for the future technology trend analysis.

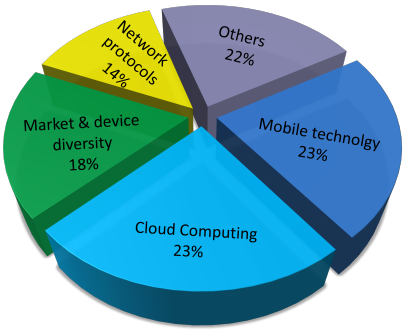

Figure 2: Technology Trends.

3.2 Future Cloud Trends

- **Big Data** - *Big Data spending will grow with video, audio and image analytic taking on more importance. Data visualisation, wireless communications, and cloud infrastructure are extending the power and reach of information* (McKinsey and Company, 2015). (KPMG, IDC (BRZ), Consol, ISreport, NetApp, UK Business Insider).
- **Hybrid Cloud** - *Bringing together personal clouds and external private cloud services is an imperative. Hybrid cloud services can be composed in many ways, varying from relatively static to very dynamic* (Gartner, 2014), (Forbes, ISreport, NetApp).
- **Cloud/Client Architecture** - *Cloud/client computing models are shifting. Increasingly complex demands of mobile users will drive apps to demand increasing amounts of server-side computing and storage capacity* (McKinsey and Company, 2015), (Gartner, KPMG, Forbes).
- **Software Defined Networking (SDN)** - *SDN is a collective term that encapsulates the growing market momentum for improved standards for infrastructure programmability and data center interoperability driven by automation inherent to cloud computing, DevOps and fast infrastructure provisioning* (Gartner, 2014), (Cisco, Forbes, Mason).
- **Docker and other Container Technology** - *As new applications for SaaS or large-scale enterprise use cases are written using the scale-out micro services model, Docker application containers have proven to be more resource efficient than VMs with a complete OS* (Insider, 2014), (NetApp).
- **Agile Infrastructures** - *Agility will be one of the most important criteria for the company's success and thus one of the trends in future. Agile system landscapes and infrastructures are required to insist about disruptive technologies and business models in a market or to require Big Data analysis amendments and adjustments* (IsReport, 2014).
- **Challenges to Amazon Web Services (AWS)** - *Companies are learning to test and experiment using this type of data. Many advanced marketing organisations are assembling data from real-time monitoring of blogs, news reports, and tweets to detect subtle shifts in sentiment that can affect product and pricing strategy* (Gartner, 2014), (UK Business Insider).
- **Era of Personal Cloud** - *The personal cloud era will mark a power shift away from devices toward services. Access to the cloud and the content stored or shared from the cloud will be managed and secured, rather than solely focusing on the device itself* (McKinsey and Company, 2015), (Gartner).

Figure 3 shows in detail a Cloud trend expectation summarised by sources.

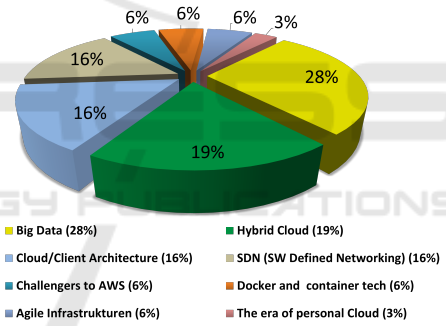

Figure 3: Cloud Computing Trends.

4 THREAT TREND ANALYSIS

Since presentation of future technology trends does not appear to be the only base of information for creation of the use case relevant for our research, we also did threat trend analysis which includes all potential future threats in technology evaluation shown in Figure 4. The process of threat trend analysis has the same approach like in previous section with sources listed in. Future threat trends are categorised as follows based on Symantec, Kaspersky, Sophos, Symantec, and SentinelOne:

- **Targeted Attacks** - *Cyber criminals developed attacks that only execute on a specific machine or set up. Since they behave like a benign application on the way to the target machine these threats*

are able to evade layers of detection mechanisms (Kaspersky, 2014).

- **Internet of Things Attacks** - *Attacks on Internet of Things devices will increase rapidly due to hyper growth in the number of connected objects, poor security hygiene and the high value of data on IoT devices* (Kaspersky, 2014).
- **Distributed Denial of Service (DDoS) Attacks** - *The installation of malicious applications and the visit malicious websites will no longer pose infection vectors which are valid exclusively for the mobile telecommunications sector. The cross-platform exploitation of vulnerabilities, will be a far greater threat to rest of the technologies* (Kaspersky, 2014).
- **Mobile Attacks** - *Mobile attacks will continue to grow rapidly as new technologies expand the attack surface and App. store abuse goes unchecked* (McAfee, 2014).
- **Beyond Windows Attacks** - *The Shellshock vulnerability will fuel non-Windows malware attacks that will continue for years. Attackers will capitalise on Shellshock by exfiltrating data, holding systems ransom, and assimilating spam bots* (McAfee, 2014).
- **New Cyber War Players** - *This refers to prediction that states will continue to use cyber-attacks as a political retaliation tool. More specifically, some states will continue to carry out brute force cyber-attacks and espionage campaigns, primarily against the other countries and human rights activists* (WebSense, 2014).
- **E-mail Attacks** - *An email exploit is an exploit embedded that can be executed on the recipient's machine once the user opens or receives the email. This allows a hacker to bypass firewalls and anti-virus products* (WebSense, 2014).

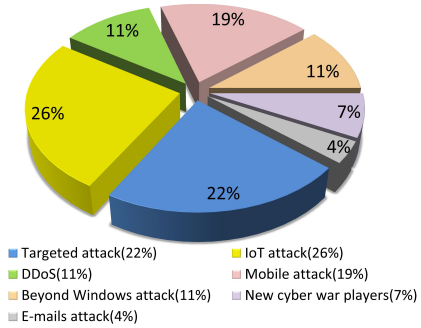

Figure 4: Threat Trends.

5 USE CASE

With the summary of the results from trend analysis we define a use case scenario which includes expected trends in the cloud computing environments including attack scenarios/vectors. A trend hybrid cloud spans at least one public and one private cloud, with the workload distributed across the two which also communicates with the cloud infrastructure provider. The client may also have a private, on-premises virtualized environment that is connected to a public cloud. Stored data on the cloud infrastructure provider present users data maintained by cloud service provider. On the other side, communication between the client and the private/public cloud service provider will be determined as a cloud/client architecture trend. The future cloud trend big data fits perfectly for the created architecture since users are constantly facing with the lack of resources. Big data is also one of the main reasons for developing hybrid technologies to the cloud. SDN is used for the realization of the networking, means that available software will maintain the resource and network usage in the proposed data centres. SDN will be based on open-source tools, like *OpenStack*. Other cloud trends like *Docker and container technologies* could be also included but the result of the cloud trend analysis exclude their relevance for the use case. The use case presented in Figure 5, is structured as: Private Cloud - Company Cloud, continuously monitoring of the user data, high-level protection, Client - Employer of the company, any employer of the company which uses any kind of service on the internet, Cloud Service Provider - Provides services across the Internet, Cloud Infrastructure Provider - Keep sensitive data from the users of the services managed by cloud service provider The threat trends relevant for our use case are:

- **Targeted Attacks** - The client can act as a "bridge" to run targeted attacks to collect sensitive information in public clouds.
- **DDoS Attacks** - According to (Kaspersky, 2014), irresponsible behaviour from the client on the open network can lead to unimaginable consequences, which would suggest the use of a private cloud infrastructure.
- **Mobile Attacks** - Because App stores present a vulnerable environment, there is a significant possibility that the client could be a victim by unwittingly downloading malicious applications.

Other attacks are either not related to our use case or did not get any attention from our sources, so for that reason we deem them to be less relevant.

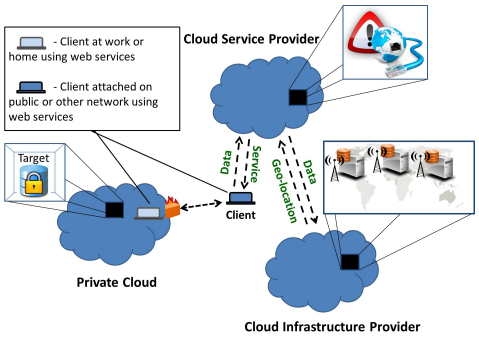

Figure 5: Use Case Scenario, Future Cloud based Applications.

6 RESILIENCE

To achieve the maximum security for our use case, we take a resilience perspective as the key concern for the overall system. In doing so, we aim to derive relevant metrics for expected hazards, weak points and attack methods in future cloud based applications.

6.1 Relation to the Use Case

Resilience is a wide-ranging concern, and can be defined as the ability of a system to provide an acceptable level of service in light of various challenges (Sterbenz et al., 2010). Resilience is supposed to be a fundamental property of Cloud service provisioning platforms. However, a number of significant outages have occurred that demonstrate Cloud services are not as resilient as one would hope, particularly for providing critical infrastructure services (Neal, 2011). The potential resilience related issues relevant to our use case include: (i) Attacks aiming to break confidentiality (e.g., sniffing and scanning) and integrity (e.g., session hijacking), and (ii) Denial of Service based on techniques, e.g., flooding attacks resulting in performance degradation, i.e., its reliability and availability.

6.2 Monitoring Metrics

It is important to define correctly the metrics that will be used in order to measure resilience. These could also be used for creating the service levels that will be agreed with the cloud provider and in order to monitor whether there are any violations of these agreements.

In this work, the metrics discussed are related to security and resilience, but others that could have an effect directly or indirectly should be added in a real scenario (assurance, legal etc.). Services offered by a provider can have one or more attributes, and these can be represented by one or more metrics. A few examples of the possible attributes and metrics used are service availability, mean time between failures, mean time to repair, mean time to invoke remediation action, mean time to recovery, scalability etc.

In relation to the use case, we argue that a systematic approach is required. Conceptually, the resilience management can be instantiated in cloud infrastructure provider, addressing management in both single and cross domain cases as sketched in use case. Such a resilience manager compose of multiple components which mainly include collector, detector, and remediation. The services offered by a provider in our use case can have one or many attributes, and they can be represented by one or more metrics. Firstly, collector collects those metrics given that cloud provider provision those resources in detector supervised part of the infrastructure and as per the resilience requirements of a tenant. In case of challenge such as Denial of service attacks, relevant metrics by collector fed into detector which consume these metrics to compute a likelihood of anomaly score and subsequently alert the remediation component. Later will then invoke actions based on policies and eventually recovering the system from challenge. These mechanisms are also supported by *IND*^{2}*UCE* framework developed within the scope of SECCRIT (Jung et al., 2015).

Figure 6 shows some of the relevant metrics for such attributes at network and service levels.

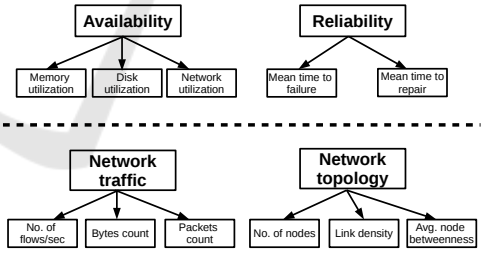

Figure 6: Example metrics for resilience.

6.3 Monitoring Solution

Monitoring is an essential component and helps to control the infrastructure by collecting and analysing data (e.g., bandwidth, disk and CPU utilisation) from various components at host and VM level. Monitoring is becoming increasingly difficult due to the changing workload patterns and scalability of cloud environments. It is becoming even harder with increasing user expectations for resilience and security. The SECCRIT consortium has proposed a resilience management framework that introduces novel mechanisms to support overall resilience to

challenges arising in cloud environments. More specifically, it introduced an online anomaly detection technique based on data density that can be applied at the cloud infrastructure level. The method is embodied by a resilience architecture that was initially defined in (Simpson et al., 2013) and further explored in (Shirazi et al., 2014) and (Shirazi et al., 2015). The framework uses monitoring API Monasca[1] that leverage high speed message queues and computational engines. It also supports authentication of all data associated with an OpenStack tenant to support multi-tenancy. Metrics and events are received by the API and published to a message queue (Kafka)[2]. The anomaly engine consumes metrics from the same message queue, predict metrics and evaluate likelihood and anomaly score as probabilities in order to provide overall resilience to challenges.

7 CONCLUSIONS

In this paper, we have analysed technological trends, and considered their potential to become future threats. We did this by means of a systematic examination of industry reports on existing and emerging technologies. Using a cloud use case we have identified potential resilience metrics that can shed light on the security properties of cloud systems. The research also gives a basic overview as to what may be expected in terms of technology futures with the aid of threat analysis for their adoption in critical infrastructure environments where there are stringent security requirements. As cloud computing is expanding very fast and new threats arising from security issues are being created, we believe that our research presents a basis for helping create more secure cloud systems.

Future work should include other relevant topics, for example assurance and legal issues, as a next step towards achieving a high security level in future cloud applications. Also, the approach should help to improve network monitoring and management systems through such a technology evaluation.

ACKNOWLEDGEMENTS

The research presented in this paper has been funded by the European Union (FP7 Project SECCRIT, grant agreement no. 312758).

[1]Monasca: www.wiki.openstack.org/wiki/Monasca

[2]Kafka: http://kafka.apache.org/

REFERENCES

Authorization., N. D. (2006). National defense authoriazation act for fiscal year 2006.

Ballard, J. R., Rae, I., and Akella, A. (2010). Extensible and scalable network monitoring using opensafe. *Proc. INM/WREN*, pages 8–8.

Dekker, M. (2012). Critical cloud computing: A ciip perspective on cloud computing services. Technical report, European Network and Information Security Agency (ENISA).

Gartner (2014). Gartner symphosium it xpo, executive summary report.

Grobauer, B., Walloschek, T., and Stocker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security and Privacy*, 9(2):50–57.

Hudic, A., Tauber, M., Lorunser, T., Krotsiani, M., Spanoudakis, G., Mauthe, A., and Weippl, E. (2014). A multi-layer and multitenant cloud assurance evaluation methodology. In *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, pages 386–393.

Ibrahim, A. S., Hamlyn-Harris, J., Grundy, J., and Almorsy, M. (2011). Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model. *Network and System Security (NSS), 2011 5th International Conference*, pages 113–120.

IDC (2014). Idc predictions 2015: Accelerating innovation and growth on the 3rd platform.

Insider, U. B. (2014). Billions of dollars are set to flow into these 7 areas of tech in 2015.

IsReport (2014). Information platform for business solutions, it forecast for 2015.

Jung, C., Schwarz, R., Rudolf, M., Moucha, C., and Eitel, A. (2015). Seccrit deliverable d4.4 policy decision and enforcement tools.

Kaspersky (2014). Next 9 security predictions for 2015.

Khajeh, H. A., Greenwood, D., Smith, J. W., and Sommerville, I. (2012). The cloud adoption toolkit: Supporting cloud adoption decisions in the enterprise. *Software Practice and Experience*, 42:447–465.

Khajeh, H. A., Greenwood, D., and Sommerville, I. (2010). Cloud migration: A case study of migrating an enterprise it system to iaas. *Cloud Computing (CLOUD)*, pages 450–457.

Khajeh, H. A., Sommerville, I., Bogaerts, J., and Teregowda, P. (2011). Decision support tools for cloud migration in the enterprise. *Cloud Computing (CLOUD)*, pages 541 – 548.

Mason, A. (2015). Global telecoms market: trends and forecasts 20152020.

McAfee (2014). Information platform for business solutions, it forecast for 2015.

McKinsey and Company (2015). Ten it enabled business trends for the decade ahead.

Neal, D. (2011). Amazon web services outages raise serious cloud questions.

Payne, B. D., Carbone, M., Sharif, M., and Lee, W. (2008). Lares: An architecture for secure active monitoring

using virtualization. *Security and Privacy, 2008. SP 2008. IEEE Symposium*, pages 233–247.

Scholler, M., Bless, R., Pallas, F., Horneber, J., and Smith, P. (2013). An architectural model for deploying critical infrastructure services in the cloud. In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, volume 1, pages 458–466. IEEE.

Shirazi, N., Simpson, S., Marnerides, A., Watson, M., Mauthe, A., and Hutchison, D. (2014). Assessing the impact of intra-cloud live migration on anomaly detection. In *Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on*, pages 52–57.

Shirazi, N., Simpson, S., Oechsner, S., Mauthe, A., and Hutchison, D. (2015). A framework for resilience management in the cloud. *e & i Elektrotechnik und Informationstechnik*, 132(2):122–132.

Simpson, S., Shirazi, N., Hutchison, D., and Backhaus, H. (2013). Seccrit deliverable d4.2 anomaly detection techniques for cloud computing.

Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., and Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265.

WebSense (2014). Websense security labs 2015.