2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

Security-Oriented Cloud Platform for SOA-Based SCADA

T. Baker*, M. Mackay*, A. Shaheed†, B. Aldawsari*
*School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK
{t.baker, m.mackay, b.m.aldawsari}@ljmu.ac.uk
†Denbridge Marine Limited, Monks Ferry, Wirral, UK
amjad.shaheed@denbridgemarine.com

***Abstract*- During the last 10 years, experts in critical infrastructure security have been increasingly directing their focus and attention to the security of control structures such as Supervisory Control and Data Acquisition (SCADA) systems in the light of the move toward Internet-connected architectures. However, this more open architecture has resulted in an increasing level of risk being faced by these systems, especially as they became offered as services and utilised via Service Oriented Architectures (SOA). For example, the SOA-based SCADA architecture proposed by the AESOP project concentrated on facilitating the integration of SCADA systems with distributed services on the application layer of a cloud network. However, whilst each service specified various security goals, such as authorisation and authentication, the current AESOP model does not attempt to encompass all the necessary security requirements and features of the integrated services. This paper presents a concept for an innovative integrated cloud platform to reinforce the integrity and security of SOA-based SCADA systems that will apply in the context of Critical Infrastructures to identify the core requirements, components and features of these types of system. The paper uses the SmartGrid to highlight the applicability and importance of the proposed platform in a real world scenario.**

Keywords-component; SCADA, Critical Infrastructure, Cloud Computing, SOA

I. INTRODUCTION AND MOTIVATIONS

Current industrial distributed and Critical Infrastructure (CI) systems are based on the use of Supervisory Control and Data Acquisition (SCADA) systems to control, monitor and observe their entire processes and data. The use of SCADA systems is expected to grow massively up from €188 million in 2007 into €300 million in 2020 [1] as systems require more monitoring and control to respond quickly to unplanned situations.

State-of-the-art SCADA systems are designed to support complex monitoring via interactions among the interconnected and composed systems and services as required in next-generation architectures. For example, the EuropeAn ArchitecturE for Service Oriented Process-Monitoring and Control (AESOP) [2] project paved the way for the integration of SCADA systems with web services deployed on the cloud and used as a service, resulting in a highly complex and widely distributed monitoring system. Those services are all connected and communicate using Ethernet and the TCP/IP stack up to the transport layer, e.g. Modbus/TCP [3]. The use of TCP/IP is a very useful and logical addition to traditional SCADA systems for allowing seamless communication between services available on the web. However, relying on such a well-known and common protocol set raises the potential for cyber-attacks and/or malicious manipulation and management by external hackers. Furthermore, large scale SOA-based SCADA is distributed over large geographical distances, which makes it difficult to employ traditional physical means to secure the field network. As such, the simplest protection method might be through allocating different authorisation levels to intended roles, and assigning different roles to users. But, this solution may create an overly complex system security arrangement, as follows:

given a set of composite services	$S = \{s_1, \ldots . s_m\}$
and a set of authorisation levels	$A = \{ a_1, \ldots . a_n\}$
for a set of roles	$R = \{ r_1, \ldots . r_p\}$
assigned to a set of users	$U = \{ u_1, \ldots . u_q\}$

The above sets give many possible complex interactions between a user with system roles at various levels of authorisation for all the services: System security must therefore account for a high number of eventualities up to the product of s, a, r and u. Consequently, the complexity of the existing approaches and the security requirements for SCADA systems, such as authorisation/access control, authentication, confidentiality, integrity, auditing and availability, in CI systems [4] may lead developers in general, and users, in particular, to neglect or overlook the provision of these security features. Moreover, the possibility of legacy CI systems now being accessed online has raised new and unforeseen issues of data security to even higher levels of criticality: "*critical infrastructure systems should never have moved online*" [5]. Since there is currently neither clear identity management nor role-based authorisation associated with the utilised web services to manage the access and use of these critical systems, any resulting systems are increasingly vulnerable to cyber security attacks.

Security-as-a-service (Sec-a-a-S) is an emerging trend in utility and cloud computing paradigms [6], whereby users' get charged according to their needs and use of security features. Thus, differing levels of security can be used as a service anytime it is needed on a pay-as-you-go basis. However, with online access of CI systems, where security might be required at different stages and levels with different roles and services, the use of Sec-a-a-S will be needed very frequently, perhaps within every single process during system runtime: Thus, it will be difficult and costly to call the service and inject it in the system, unless it has been completed at design time. From the above, there are clearly a set of major hindrances to accomplishing secure SCADA-based critical infrastructure: Role based access control and different views on how systems should be configured, viewed and used [7], need to be fulfilled in order to securely use the system and current SOA

978-1-4799-8006-2/15 $31.00 © 2015 IEEE
DOI 10.1109/CCGrid.2015.37

approaches lack flexibility here. This is the motivation for our work towards developing security-oriented cloud platforms for SOA-Based SCADA systems in an attempt to protect CI services and assets stored and managed in the cloud, and offer reasonable assurances over the performance and reliability of these services.

The remainder of this paper is organised as follows: section 2 will provide a problem definition for SCADA systems, section 3 presents related work on secure cloud and SOA systems and section 4 discusses the associated network security issues. Section 5 presents our approach for SCADA oriented cloud security and section 6 analyses our system in the context of a case study of the Smart Grid paradigm. Finally, section 7 describes our work to implement a key authentication feature of our approach, and section 8 presents our testing and validation.

II. Problem Definition

Centralised SCADA systems were first designed and developed for CI monitoring purposes during the 1960s when there was considerably less knowledge and concern about information security [8]. During this period, SCADA systems were vendor-controlled and isolated from other systems: "*few people knew about SCADA installations*" [9]. These systems were originally used for collecting the necessary log-field data using industrial plant-scale Distributed Control Systems (DCS), which recorded the data and sent every reading to the control room to (re)act accordingly. So, if an alarm is raised, the control room operator would be informed via a DCS message and use the system's controls to react to the alarm appropriately. However, over time the increasing requirement for fine-grained monitoring and control over the infrastructures has resulted in SCADA systems of ever-increasing size and complexity. Moreover, by leveraging this, the threat posed by security vulnerabilities has increased radically to become a far more serious threat, from the perspective of potential, frequency, and impact [10]. Threats ranging from terrorism to more indirect attacks, have led governments and security agencies to look for more effective ways to protect and defend such services. In the UK for example, the Centre for the Protection of National Infrastructure (CPNI) was established in 2007 and it now works closely with other agencies to enforce the highest level of protection possible [11]. The most important activities in providing CI protection involve; pre-emptive analysis, assessment, and indication, warning and remediation as events occur. Mitigation, incident response, and reconstitution post-event are also important factors.

This rise in complexity, and therefore of security concerns, can be seen as a result of the rapid evolution of the SCADA architecture to enhance their capabilities to monitor and control CI systems as operator requirements expand. They arise primarily from the evolution of SCADA systems away from monolithic architectures through incremental stages of interconnectivity, as outlines below:

- The introduction of Remote Terminal Unit (RTUs) via Wide Area Networks (WAN) in the 60s;
- The deployment of distributed architectures, which allow real-time information sharing between connected units;
- The use of Wireless Sensor Networks (WSN) to monitor and signal accurate data across the whole system [12];
- The Autonomous Remote SCADA [13];
- Introduction of Cloud based SCADA, which supported additional processing complexity and scalability.

Figure 1 depicts the evolution of connectivity in SCADA systems.

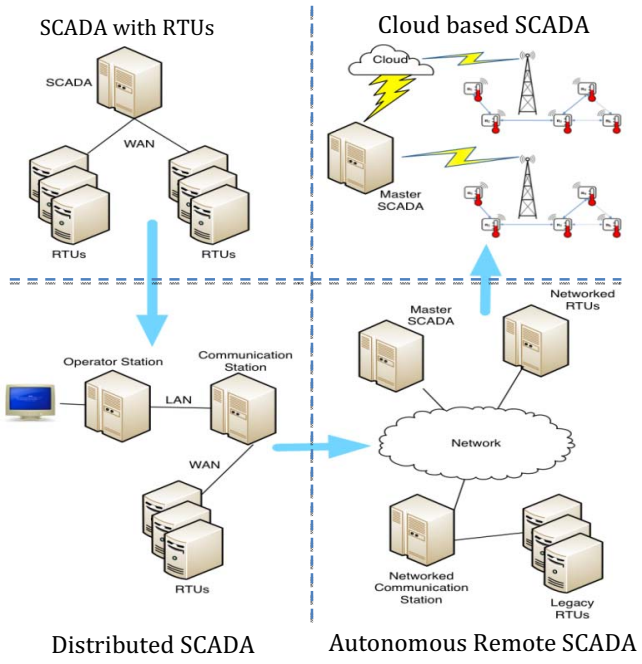

Figure 1: SCADA Systems Evolution

It has been found that an increasingly critical aspect of effectively defending CIs is to adequately protect their ICT infrastructure as an increasing number of attacks are partly or wholly conducted remotely through the Internet. One famous example was the recent cyber-attack on Iran's power generation systems by the highly modified Stuxnet virus [14]. As such, an increasing research trend is now looking at how to effectively use secure mechanisms to protect CI ICT services such as in the recently established PROTECT centre [15]. In this context, many network security mechanisms are being used or developed to enhance protection of CIs beyond the traditional deployment of firewalls and Intrusion Detection Systems (IDS). These include strong user authentication, Demilitarised Zones (DMZs), system and protocol hardening, trusted systems, and many others [16]. However, since each service requires various conflicting types of security goals such as authorisation and authentication, this model often fails to provide an effectively abstracted security layer to include the different authorisation requirements for each different service. As such, more research is needed over

time to investigate how to effectively integrate security and role-based authentication support into this model [17].

III. Related Cloud Security Work

In this section, the state-of-the-art in the areas of trusted computation platforms and CI monitoring systems and their weaknesses are discussed. First, the European SOA-Based SCADA Architecture (IMC-AESOP) is considered to highlight the need for the proposed platform; this will be followed by a discussion of the advantages and challenges of trusted platforms; how it can be applied to secured clouds for SOA-Based SCADA, and some of the major approaches that have already been put forward.

A. IMC-AESOP Approarch

IMC-AESOP for CI represents a new direction in distributed CI development that goes beyond traditional existing approaches [18]. It provides initial moves towards cross-layer service-oriented collaboration, both horizontally across cooperating devices, and vertically across systems located at different levels of the enterprise systems architecture [19]. Furthermore, IMC-AESOP is a promising step forward in prescribing how future SCADA systems and software can be designed, operate and interact with each other. As shown by the highly modularised architecture in Figure 2, AESOP focuses on how monitored systems, and their collaborative parties, can seamlessly work and monitor the message flow in a cross-layer way among interacting systems. It also highlights how new SCADA systems enable dynamic information integration from collaborative parties to make optimal decisions on unpredictable system's behaviour. The main objective of IMC-AESOP is to develop a monitoring and control approach based on utilising SOAs for very large scale distributed systems and to propose a transition path from legacy SCADA systems to those currently emerging. In brief, the IMC-AESOP architecture concentrates mainly on collaboration among cooperating objects and supports the capabilities of these objects to be strongly integrated. However, the security side of this collaboration and integration was neglected in this platform, resulting in weak/unsecured SCADA services on highly complex and widely distributed cloud networks.

B. Trusted SOA-Based Systems

Service-Oriented Architectures provide flexibility for systems to integrate loosely coupled services that are widely distributed across the web. However, due to the loosely coupled nature of the integrated services and their operations across the boundaries, security issues are now of the highest priority and represent a critical research area here. SOA-based infrastructures are vastly distributed, comprising large numbers of services, which in turn create many interconnections and interaction logs. Therefore, trust in SOA-based infrastructures must be managed in an automatic manner for use in SCADA [21] and a trust management framework for service-oriented environments has been presented in [22].

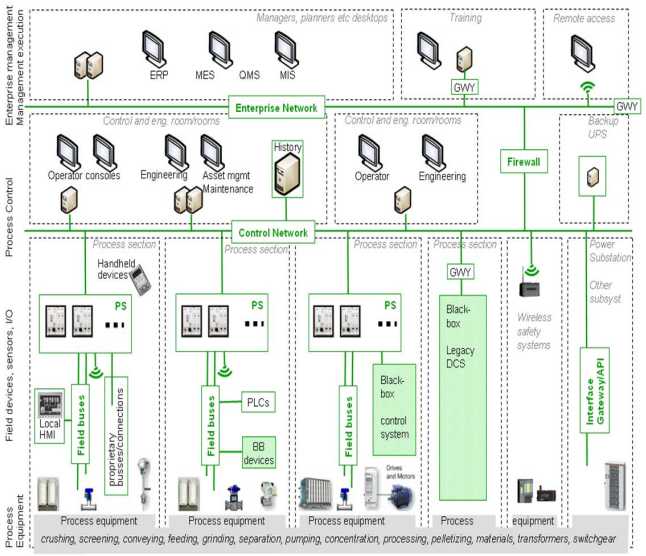

Figure 2: AESOP Architecture [20]

This, however, is described without considering the particular application scenarios with human actors in an SOA. Also, although several models define trust on interactions and behaviour, and account for reputation and recommendation, there is no fully analysed case study on the application of these models in service-oriented networks. Finally, while various theoretically sound models have been developed in recent years, fundamental research questions, such as the technical grounding in SOA and the complexity of trust-aware context-sensitive data management in large-scale networks, are still widely unaddressed.

C. Trusted Cloud-Based Systems

In the context of CIs, the introduction of the six Trusted Computing elements [23] into cloud computing could potentially provide one approach to help adequately harden the platform. This is still a very immature aspect of secure computing but there have already been a number of works aimed at designing trusted cloud computing services [24].

One of the first, most natural, areas where trusted cloud computing can be applied is in protecting the underlying infrastructure including the datacentres and interconnection networks. Obviously, the effective deployment of encrypted data storage, memory curtaining, and protected execution environments, perhaps based on some specialised form of the Trusted Platform Module (TPM) architecture, could make a significant contribution to securing cloud resources and isolating them in virtualised environments [25]. In addition, techniques such as watermarking could be used to protect shared modules and limit, or at least effectively detect, incursions. Moreover, this needs to be combined with secure end-to-end networking and trust-based reputation systems to control access to cloud resources. Ultimately, reputation systems could be combined with strong Identity and Access Management (IAM) to establish trusted network zones and enforce role-based access control.

This approach has received increasing interest in recent years as a driver to enable the movement of CIs into the cloud. Moreover, this has the advantage of potentially being cheap to implement, as it can be based on Commercial-Of-The-Self (COTS) elements, and is deployed and managed entirely by the cloud provider. Ultimately, we envision this could lead to the development of a 'Trusted Layer as a Service' (TLaaS) model whereby the cloud providers' offer trusted computing features to customers as an additional security layer and revenue opportunity.

D. Autonomous Decentralised Remote SCADA

As stated in [26, 27], and from the previous discussions, traditional centralised SCADA and its proprietary protocols represent a real problem for ubiquitous systems, which require integration with numerous services and components to scale the monitored system. Centralised SCADA systems have been characterised by relying on skilled and well-trained people to monitor the entire system behaviour based on sensors-based data collection. However, the current trend towards increasing scalability has necessitated moving the SCADA systems towards a more decentralised and widely distributed model, where it will be very hard to employ people to effectively monitor and react to failures. Thus, the autonomous management of SCADA systems has become a vital foundation to detect problems and heal the monitored systems accordingly. Autonomous SCADA systems are also becoming increasingly interconnected to and supported by COTS products [28] and open standards to be compatible with standardised networking protocols and thus integrate heterogeneous services and other enterprise solutions. While this advancement in SCADA monitoring systems is critical to minimise the need for human-intervention however, as a result, this type of SCADA system may also inherit the same security and vulnerability problems from the used COTS components and services that may be susceptible to attack. In such situations, the monitoring system of the CI will be at a high risk of failure and thus require re-assessment. The authors in [29] have highlighted the possible imminent danger of COTS components and the negative impact on CI SCADA systems.

IV. Securing the Network

In the context of widely distributed, publicly accessible systems, identifying the more general cyber security vulnerabilities and threats is of vital importance in order to protect SCADA systems. From the SOA viewpoint, all the connected systems (e.g. ERP, PLCs, legacy SCADA/DCS, devices, etc.) expose their functionalities (complex or atomic) as a service that can be composed by and interact with other entities. As such, secure network connectivity is a vital aspect of supporting CI monitoring systems, particularly SOA-based SCADA, as not only must the connection be made secure from attack but special care must be taken to prevent connection failures where reliable and consistent access to resources is mission critical. In this context, existing best practise in the field of network management is examined; including how it can be applied to Cloud Computing as a platform, the encryption mechanisms to protect the collected data, and monitoring and IPS services to secure the entire network infrastructure.

A. Network Security Approaches

As in the case of data security, traditional network security mechanisms have a strong role to play in hardening the infrastructure against attack. Securing the network is clearly a critical aspect of any production cloud service and so any public/private provider should implement firewalls, IDS monitoring, and other standard management mechanisms, to provide a sufficient level of security. Moreover, more security-conscious providers may implement Unified Threat Management (UTM) systems that can determine a range of more subtle attack characteristics and resilient networking mechanisms to automatically react by triggering remedial measures [30].

The advantage of the cloud provider hosting a range of services is that, as long as that provider implements strong security measures, the customers benefit from the underlying strength this provides; and can focus only on securing their own services. The disadvantage of course is that if these measures become compromised then the entire base of customer services is potentially also vulnerable. As such, CI customers may require additional levels of isolation from the rest of the infrastructure to minimise the potential of their service becoming compromised.

Another major aspect of network security is securing the CI data connections both into the cloud and within the cloud itself. As such, encryption will be essential to provide an acceptable level of assurance over connection security. Transport Layer Security (TLS) connections are already a standard for providing secure connections both into the cloud networks and between datacentres. However due to the potential for implementation-specific vulnerabilities to emerge, such as with the recent Heartbleed bug in some TLS implementations [30], alternatives such as IP Security (IPSec) and Application Layer security protocols such as Secure Shell (SSH) may also be necessary.

B. Resilient Networking

With the cloud network reasonably secured, the other aspect of supporting CIs is to ensure that these secure connections are both consistent and reliable. In the event that CIs move services into the cloud, they will require a constant and dependable level of connectivity as any disruptions to the service can be both costly and seriously affect the wider system performance. There are two aspects to this, a) reinforcing the current best-effort IP routing mechanisms in the Internet with additional redundancy and b) mitigating malicious denial of service attacks.

The first aspect is necessary due to the fundamental properties of IP and the Internet as a best-effort routing architecture which, while mostly reliable, offers no guarantee over end-to-end connectivity. As such, connections may be dropped or fail to establish due to technical faults, heavy load on intervening networks, routing errors, or any number of other issues. Clearly this is not sufficient where strict

requirements exist over connectivity so a range of techniques can be employed to bolster the reliability of the network. For example, QoS mechanisms may be deployed to ensure that capacity is not exceeded thereby reducing the risk of connections being refused or dropped. Secondly, route redundancy can be employed to ensure that there is always more than one path from the customer to the cloud thereby guaranteeing connectivity in the face of failures.

In the second aspect, connectivity to the cloud may be threatened by malicious activity, such as through Denial of Service (DoS) attacks as recently used by the Anonymous group in response to the arrest of Julian Assange in the wikileaks case [31]. DoS attacks attempt to overwhelm provider infrastructures by making many independent requests to a specific point in the network (i.e. a specific web server or router). DoS attacks are often made more complex to diagnose and overcome by being distributed over many sources on the Internet (via a botnet or some other mechanism), and reflected or amplified by exploiting legitimate network services. Research into effective countermeasures to detect and overcome DDoS attacks are still ongoing but, as evidenced in recent attacks on the CloudFlare system, are becoming increasingly effective.

V. An Integrated Approach to Secure SOA-Based SCADA: Innovation Perspectives

Based on the above investigation of these converging technologies, an approach to an integrated secure cloud platform that aims to embody all of the above principles is presented here. The first step is to specify the threats and requirements of CI SCADA systems and discuss how these can be addressed to pave the way for the proposed approach.

A. Cloud Computing Threats for SCADA-Based CI

The threats that SCADA-Based CIs encounter are similar to most corporate networks with the exception that there are more strict requirements over the tolerance to faults and attacks. As stated in section II, the increased number of collaborative parties in SCADA systems leads to an increased number of connections via networked systems and thus increases the system exposure to threats. The major vulnerabilities in state-of-the-art SCADA-based CIs are therefore as a direct result of the ubiquitous nature of using cloud-based networked systems and this will affect providers moving to cloud based SCADA systems, as follows:

- Ubiquitous web: the system is now able to deliver and integrate services from any location or vendor.
- Ubiquitous users: authorised users should be able to interact with the services from anywhere at any time.
- Ubiquitous agents: clients running on a wide range of devices may be responsible for making changes across the systems.

As a result, there are a number of networking threats that should be considered as relevant here:

- DDoS attacks
- Cyber threats and hacking attacks
- Espionage
- Insider attacks
- Equipment failures
- End-to-end issues
- Data loss or corruption

These threats may be innocent or malicious; however, the fundamental issue is that the CI is denied access to its data or services or that its confidential data may fall into the hands of another party. Thus, these represent the core requirements that must be met in our work.

B. Critical Infrastructure Requirements

The two primary concerns for CIs moving data into the cloud will be the security, integrity and maximised service availability. While it is highly unlikely that CI providers will move mission critical services to public cloud services, support systems and tertiary services may be more easily provisioned. In this context, the main requirements will involve**:** (a) real time support in order for such services to provide a high level of availability in case of faults and intermittent connectivity; (b) scalability so the service is able to cope with very large volumes of data being streamed at a variable rate; (c) infrastructure security to provide reasonable guarantees over the data both when it is stored in the cloud and when it is in transit; (d) high assurance e.g. reliability and resilience, to minimise downtime; (e) minimal costs of transitioning and maintaining the cloud service; (f) dynamic provisioning as the processing requirements adapt over time to cope with spikes and flash crowds; (g) legal assurances that the customer can specify and receive a fine degree of control over the service hosting and data replication strategy employed part of the Service Level Agreement (SLA).

While many of these requirements can be met intrinsically by cloud computing, there are several well-known issues introduced in this approach that are potentially critical in the case of CIs. The most critical of these issues is the relative lack of strong security and user authentication in typical cloud platforms and the limited control and monitoring of data replication and service location inside the cloud.

C. Platform Features and Functionality

Based on the requirements described above, the key features of our platform will be presented, which can support the migration of some traditional SCADA services to a secured SOA-Based SCADA on the cloud. The key assumption of the proposed solution is that all the connected systems expose their functionalities (complex or atomic) as-a-service that can be composed by and interacted with other systems subscribed to the cloud platform. The platform will be focussed on the provision of extra data integrity and security to minimise the risk of mission critical services being disrupted or taken down by equipment/network failures or attack. This will be targeted around 3 key services, Service Planning, End-to-End Security, and Monitoring and Policing. These features will be presented as a *'toolbox'* that will allow the platform to be adopted and deployed as components by a range of cloud providers and users, as shown in figure 3. However, the scope of this paper focuses on the developing a Multilevel User Access Control service as part of the Monitoring and

Policing. The monitoring and policing aspect will guard against misuse or attack via MultiLevel User Access Control (MLAC), and to ensure that the system is kept secure and the stipulations of the SLA are met. The MLAC system will replicate and extend SCADA role-based authentication schemes to determine which users can access certain parts of the platform based on their needs. The monitoring infrastructure will be distributed to provide assurances to both the customer and cloud provider that the SLA is being enforced and this can also be used to measure the effectiveness of the platform. Moreover, specialised UTM systems will be supported to secure the cloud against attacks and this will be supplemented with resilient networking services, based on Software Defined Networking mechanisms to counter recognised attack patterns.

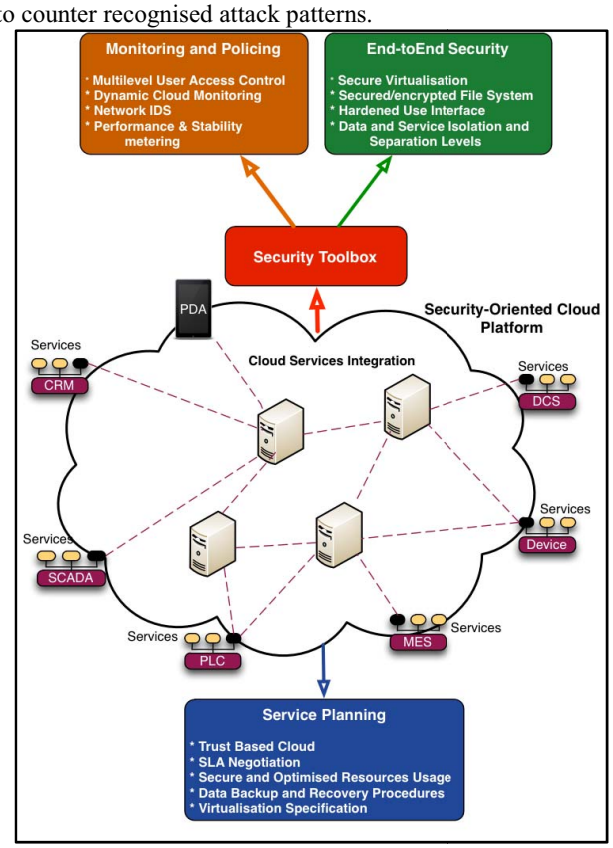

Figure 3: Key features of the proposed platform

VI. Illustrative SmartGrid Deployment Scenario

Essentially, the SmartGrid paradigm involves, among other things, enhancing the traditional power distribution grid with a far more powerful data network that gathers fine-grained information from all points in the architecture and combines this with environmental and historical data to make intelligent decisions about how to configure and route energy distribution. The core elements of this system will therefore include:

- A very large number of remote sensors that monitor the state of the network.
- A powerful computing backend that can gather and process the data to make automated decisions.
- Enhanced actuation points that can dynamically enforce the policy decisions.

The SmartGrid involves many elements that have yet to be fully-defined or standardised so there still exists a degree of uncertainty about the final architecture. For example, there is as yet no consensus over how the processing and decision-making elements will be structured and deployed, with proposals ranging from centralised SCADA-type systems such as we have today, through to fully distributed architectures. However, it has been widely accepted that a pervasive monitored infrastructure will be necessary to supplement the existing system, based on the following areas:

- Smart Meters in the home
- Sensors integrated with renewable generation systems
- Environmental monitors to determine energy production potential

Moreover, there have also been efforts within standardisation bodies towards agreeing a common data format, with IEC 61580 emerging as one potential candidate, and a general consensus that TCP/IP based communications is essential.

A. Cloud Computing within the SmartGrid

Clearly, as with any CI, the deployment or use of Cloud Computing elements here should be very carefully considered. In our scenario, we have identified that the properties of cloud platforms present a natural fit for the storage and processing of Smart Meter data to provide more information for making distribution decisions, which is similar to the model currently being proposed in the UK. In this way, regardless of the underlying control architecture, some of the storage and processing overheads of the SmartGrid are taken up by the Cloud while critical control systems are isolated and protected. For the purposes of this paper, we proposed three core functionalities to be handled by a Cloud Computing platform.

- Marshalling and storage of Smart Meter data
- Dynamic processing of data
- Provider access for service prediction

In summary, sensing devices will be configured with the 'public' interface of the cloud platform and, once suitably authenticated, will simply forward data towards that interface for processing. Once in the Cloud, the platform will be responsible for validating the data, performing any pre-processing, and storing it in a suitable format. From there, the next task will be to analyse the data and identify trends or predict generation potential or demand requirements. For example, one could envision a scenario whereby Smart Meter data is aggregated and combined with pricing schemes to predict potential demand. Finally, we expect that the distribution provider will then use this information to make real-time decisions about the configuration of their network. This 'backend' access to the cloud is the focus of our work as this will form the interface between the cloud platform and

the providers SCADA system. Of course, the specifics of this process are beyond the scope of this paper.

B. *Protecting the SmartGrid Cloud*

In this situation, the provider will still have a number of security concerns relating to integrating a Cloud platform, even in this relatively limited way. These requirements are the same as those outlined in section 5 above. This is because, even though the cloud will not directly impact on the performance of the CI, it will have requirements on how the data is held and require a certain amount of trust in the processing decisions that are presented by it. This section will discuss how elements of the proposed secure cloud platform could be applied in a meaningful way to address these issues.

1. Securing Data in the Cloud Platform

As we have highlighted above, the data stored in the Cloud in this scenario will not be mission critical or highly sensitive. However, because it is coming from users and will be used to tune the configuration of the grid and every effort must be made to secure the data. A number of mechanisms could be applied here but this will primarily involve transmitting and storing the data in an encrypted format (*end-to-end security in our platform*) to minimise the potential for unauthorised access. Depending on the cloud service used, this may ultimately be the responsibility of the cloud provider or CI provider, but it is reasonable to assume both parties should enforce this. Moreover, the CI provider may further protect user anonymity through pre-processing the data at aggregation points prior to it reaching the cloud. This could be done for example in a Home Energy Management System (HEMS).

2. Building Trust in the Cloud Service

Once we consider the integrity of the cloud platform itself, we should consider how the cloud infrastructure could be secured against attack and exploitation (*service planning in our platform*). The first issue we will tackle is how to minimise the potential for abuse, which automatically rules out the use of fully public systems. We argue that, at the very least, a remote private model should be adopted to limit the impact of shared tenant architectures. Beyond this, the cloud provider could adopt more explicit trusted computing features in the virtualisation system to negate VM exploitation, more rigorous access control to harden the user interface, and introduce more stringent IDS/IPS filtering for this part of the infrastructure to minimise network-based attacks. This aspect is largely the responsibility of the cloud provider and these features could be provided as a service to customers depending on their requirements.

3. Meeting the Service Requirements

The final requirement deals with ensuring that the cloud provider continues to meet the stipulations of the Service Agreement made with the CI provider to ensure that weaknesses are not introduced through lapses in enforcement, (*monitoring and policing in our platform*). This covers a wide range of concerns, from the storage location and replication of data, through to performance, resource allocation, and uptime issues. There is a clear need for a more effective and open monitoring infrastructure here but this is fraught with complexities, not least due to reservations from the cloud provider in publishing information about the internal state of its infrastructure. However, this is not to say the cloud providers do not and should not be actively engaged in this process and much work has been done on developing effective auditing processes to ensure that SLA stipulations are being met, whether this is communicated to the customer or not. Two solutions here may be the establishment of a trusted third party to perform this role or for the CI provider to deploy its own approach to, as far as possible, verify the Cloud providers' claims.

VII. Implementation and Testing

Based on the above, we have elected to implement and evaluate a critical element of the proposed platform in the form of authentication and access control by referring to the Monitoring and Policing part of the proposed Security Toolbox. In the scenario outlined above, it is clear that different users will have access to the cloud based on their roles in the system (e.g. consumers provide usage data, distribution providers retrieve processed data, etc) and so strong role-based authentication and access control will be critical. In the remainder of the paper we will implement a prototype for the cloud-based authentication system, which is suitable for this role and validate it through simulation.

A. *MLAC Design and Implementation*

The proposed *Multilevel User Access Control Layer (MLAC)* was developed and implemented as a simple web service along with its associated web methods, which can be used to send an authentication request to the cloud networked systems and receive a reply before accessing the system. As in any cloud-based system, beyond interacting with running services, the types of requests that can be made to utilise the available resources can be: (i) adding a new resource(s), which we implemented as a web method named *addResource* in our web service, (ii) deleting an already requested and used resource, which is implemented as another web method named *deleteResource*. In addition to those two traditional types of requests, we have also implemented a new web method, which we called here *getToken* web method, as shown in Figure 4.

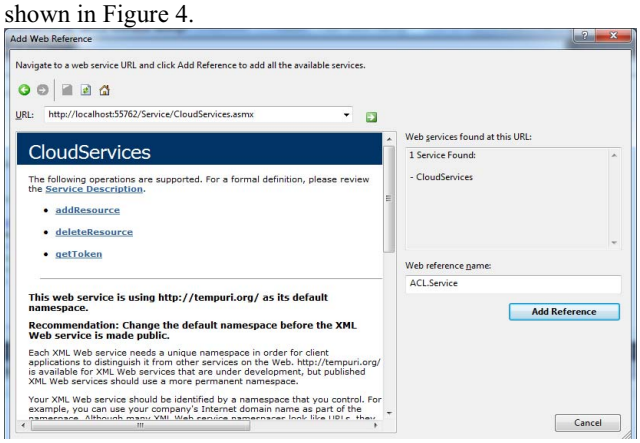

Figure 4: getToken web method

The *getToken* web method is used to increase the performance of the proposed approach by generating a token after the user credentials were first verified, so that subsequent user interactions will not need to be verified every time, but rather the token can be used to validate users' credentials. In this case, a user can stay for that session and use the token validation system for adding and deleting resources as necessary. The multilevel authorisation process and types of requests that a user can make is shown in the flowchart in figure 5. This highlights the strongly enforced authentication mechanism proposed. The new MLAC is designed to be integrated as part of the web-based user's application so that the user can seamlessly send requests to use certain SCADA nodes or services in the cloud.

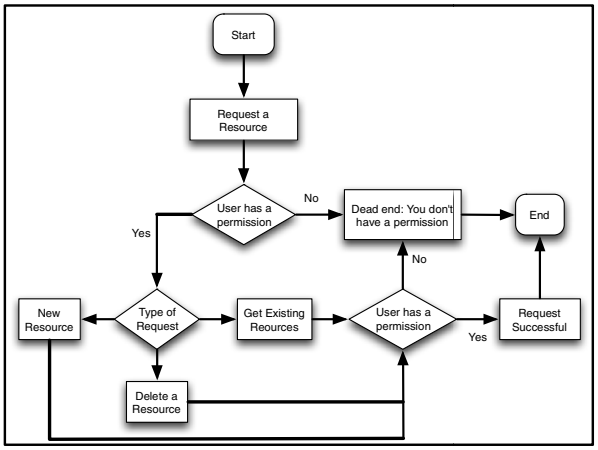

Figure 5: MLAC flowchart

Since multiple SCADA nodes may exist at the same time in the cloud, each of which is connected to a different SCADA master control, the user will be connected to the most appropriate SCADA node according to their role and credentials. This process is shown in figure 6.

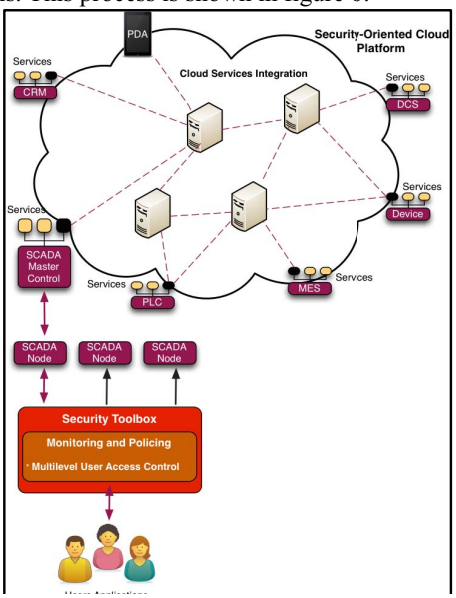

Figure 6: Access to the cloud via MLAC

Through the accessed SCADA node, the user can use the connected SCADA Master Control and thus will be fully connected to the other SCADA-based cloud resources. In brief, the system will work in this way: the MLAC system will first verify the user credentials and, if the user is valid, then grant access to one of the SCADA nodes based on the credentials and the user role.

Upon verifying the credentials, the user might be able to access the master control or otherwise can only use the SCADA node to use the service to send and receive information from the cloud. However, if a master control access is granted, then the underlying cloud resources will be accessible by the user to add, delete or modify resources as necessary. The snippet in figure 7 shows a small part of the MLAC code, in which a user can add/remove resources from the cloud. First, the user has to supply credentials to verify his/her identity. If the function returns a token then the user has been verified and can now request resources, as long as they have access to those resources.

```
ACL.Service.CloudServices service = new ACL.Service.CloudServices();
string myIPAddress = IPAddressLogic.GetMyIPAddress();
Guid token = Guid.Empty;
string status = service.ValidateUser(myIPAddress, "j.smith", "abc5671234@",out token);
if (status.Equals("Invalid IP Address"))
        {
              Console.WriteLine("You trying to access resource from invalid ip address");
        }
      else if (status.Equals("Invalid Password"))
      {
          Console.WriteLine("Username or password is wrong");
      }
      else
      {
          Console.WriteLine("User has been verified");
          string resourceStatus = service.addResource(token, "VM", 1, "Small");
          if (resourceStatus.Equals("success"))
          {
              Console.WriteLine("VM resource has been successfully added to cloud");
          }
          else
          {
            Console.WriteLine("unexpected error has occurred error status code:" + status);
          }

      }
```

Figure 7: MLAC code snippet

Access to cloud resources available to the user will be defined by the user role, as shown in the following data source schema figure.

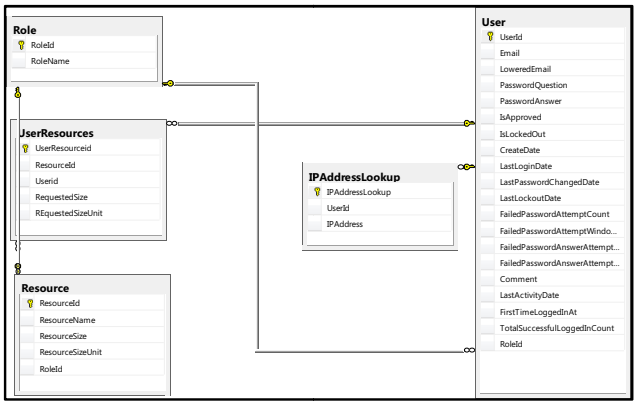

Figure 8: Data schema

VIII. Results and Evaluation

Although a full evaluation of the proposed platform is still ongoing, some preliminary results for the execution of the above MLAC features will be presented in this section. The

following testing was conducted primarily to monitor the response time of adding and removing cloud resources using the proposed approach, in comparison to doing the same functions without MLAC. As is known, introducing a new behaviour/service (e.g. MLAC in this case) to the service has a direct performance impact due to the further code interpretation needed to execute and link the new service. Our aim is to demonstrate the limited overheads of introducing MLAC to highlight that it is potentially suitable for use in real time critical systems. As such it should first be noted, via figures 9 and 10, that while adding or removing resources in the cloud, the overall system performance is less than that of the original application without MLAC. This is obviously due to the added processing time needed to execute the requests via the MLAC framework. Here, the red bars and lines represent the response time of the application using the platform in milliseconds, whereas the green represents the application without MLAC.

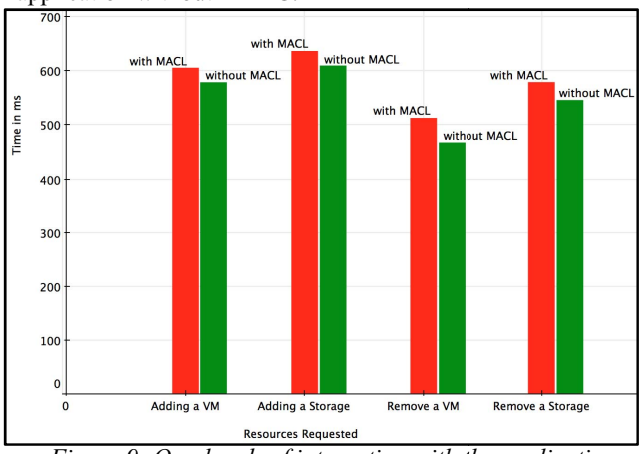

Figure 9: Overheads of interacting with the application with/without MLAC

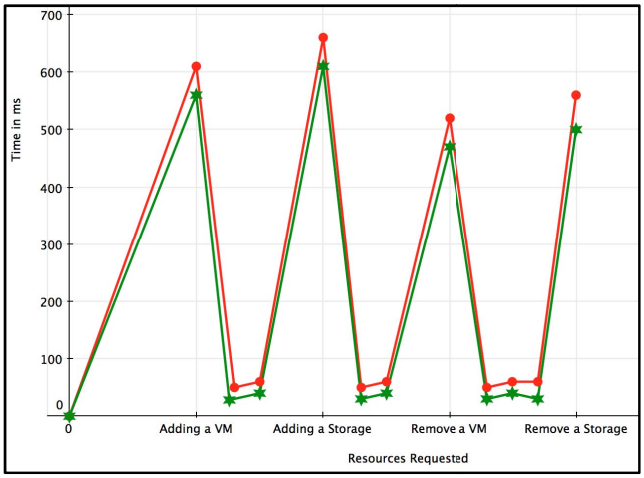

Figure 10: Overheads of interacting with the application with/without MLAC

As shown in figure 10, after the linking and execution of the MLAC in each request, the performance returns to a new standard, just slightly slower than the behaviour of the original application, which implies that overall system performance will be comparable. To verify this, we compared our how the MLAC features caused the system to scale in comparison with the standard application. To do this, we ran multiple simulations that added increasing numbers of VMs (5 – 50) to application a measured the overall performance with and without MLAC enabled. Our results, as shown in figure 11, demonstrate the impact of MLAC to be around a second in most instances and less than 2 seconds across the board. As such, we are satisfied that, at this stage, our additions do not introduce significant overheads.

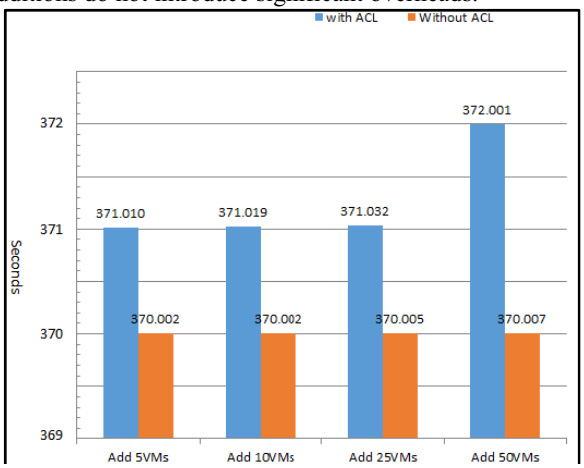

Figure 11: Scalability simulation of the application with/without MLAC

IX. Conclusions

There is a clear need for a more demonstrably secure cloud platform to drive the adoption of SOA-based services among CI providers. This must include mechanisms to secure cloud services, the end-to-end network interconnecting the users, and the cloud infrastructure itself. These issues are now starting to be tackled based on existing enterprise-strength technologies, on the basis that this can provide a reasonable level of assurance over the security of the platform while limiting the cost and complexity of the overall approach. In this paper we have identified the key aspects of this process and highlighted the requirements that must be met before it can proceed. In this way, it can be demonstrated how Cloud Computing and the end-to-end network can reasonably be made secure to support CI providers. Further, we have proposed an open platform for enabling CI support in clouds and identified the key elements of a 'security toolbox' that providers can implement and deploy to simplify this process. Finally this paper represents the first step in this area by providing an initial implementation and evaluation for a role-based authentication system but extensive further work will be necessary to validate the approach against CI provider expectations, further develop, integrate and evaluate the identified functionality, and demonstrate the strengths of the resulting platform.

REFERENCES

[1] PYL, T.V.D.: Monitoring and control. White chlorine-free paper, European Commission: Information Society and Media (Novermber 2008)

[2] consortium, T.I.-A.: ArchitecturE for Service-Oriented Process - Monitoring and Control. http://imc-aesop.eu/dl/AESOPbrochure.pdf (accessed 06 Jun 2014)

[3] Modbus, S.: Modbus TCP/IP. http://www.simplymodbus.ca/TCP.htm (accessed 6 June 2014)

[4] Dominique Kilman, J.S.: Framework for scada security policy. Technical Report SAND2005- SAND2005-1002C, Sandia National Laboratories (2005). National Nuclear Security Administration

[5] Stevenson, A.: Critical Infrastructure Systems Should Never Have Moved Online Warn Security Experts. http://www.v3.co.uk/v3-uk/news/2228538/critical infrastructure-systems-should-never-have-moved-online-warn-security-experts (accessed 6 Oct 2014)

[6] Mouftah, M.H.H.: Cloud-based security services for the smart grid. In: CASCON '13 Proceedings of the 2013 Conference of the Center for Advanced Studies on Collaborative Research, pp. 388{391. IBM Corp., (2013)

[7] Keith Stou_er, K.S. Joe Falco: Guide to industrial control systems (ics) security. Technical Report 800-82, Nantional Institute of Standards and Technology, Gaithersburg, MD 20899-8930 (June 2011)

[8] Cristina Alcaraz, G.F., Carvajal, F.: Security Aspects of SCADA and DCS Environment in Book Critical Infrastructure Protection. LNCS: 0302-9743, vol. 7130, pp. 120-149. Springer, (2012)

[9] Kim, H.: Security and vulnerability of scada systems over ip-based wireless sensor networks. International Journal of Distributed Sensor Networks Volume 2012, 10 (2012)

[10] Paganini, P.: SCADA and Security of Critical Infrastructures. http://resources.infosecinstitute.com/scada-security-of-critical-infrastructures/ (accessed 3 Oct 2014)

[11] CPNI: Centre for the Protection of National Infrastructure. http://www.cpni.gov.uk (accessed 5 Oct 2014)

[12] Action Nechibvute, C.M.: Wireless sensor networks for scada and industrial control systems. International Journal of Engineering and Technology 3(12), 1025-1035 (2013)

[13] Ltd, W.L.C.A.C.P.: Autonomous Remote SCADA. http://www.wideye.com.sg/default/index.php/remote-scada [accessed 8 June 2014

[14]. Denning, D.E.: Stuxnet: What has changed? Future Internet 4, 672-687 (2012)

[15] PROTECT: Research Centre for Critical Infrastructure Computer Technology and Protection. http://www.protect-ci.org (accessed 23 Oct 2014)

[16] Security, H.: Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies. Report, National Cyber Security Division (2009)

[17] Michael Mackay, A.A.-Y. Thar Baker: Security-oriented cloud computing platform for critical infrastructures. Computer Law and Security Review 28(6), 679-686 (2012)

[18] Programme, S.F.: IMC-AESOP Project. http://www.imc-aesop.eu (accessed 8 Oct 2014)

[19] J. Delsing, R.K. J. Eliasson, Diedrich, C.: A migration approach towards a soa-based next generation process control and monitoring. In: in 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), pp. 4472-4477. IEEE Xplore Digital Library, (2011)

[20] Stamatis Karnouskos, T.B.K.M.R.C.M.T.P.S.F.J.J.D.J.E. Armando Walter Colombo: A soa-based architecture for empowering future collaborative cloud-based industrial automation. In: IECON 2012: 38th Annual Conference of the IEEE Industrial Electronics Society; Montreal Canada from 25 to 28 October 2012, pp. 5770-5775. IEEE, Canada, Montreal (2012)

[21] Soon-Keow Chong, I.R.A.H.M.A. Jemal Abawajy: A multilevel trust management framework for service oriented environment. In: 2nd International Conference on Innovation, Management and Technology Research, vol. 129, pp. 396-405 (2014)

[22] Group, T.T.C.: Trusted Platform Module Speci_cation Version 1.2. https://www.trustedcomputinggroup.org/resources/tpm main speci_cation (accessed 2 Oct 2014)

[23]. Nuno Santos, R.R. Krishna Gummadi: Towards trusted cloud computing. In: HotCloud'09 Proceedings of the 2009 Conference on Hot Topics in Cloud Computing. ACM Digital Library, (2009)

[24]. Flavio Lombardia, R.D.P.: Secure virtualization for cloud computing. Journal of Network and Computer Applications 34(4), 1113-1122 (2011)

[25]. Philippe Gourbesville, J.Y.T.S.L.G.R. Jelena Batica, Raju, D.K.: Flood warning systems and ubiquitous computing. La Houille Blanche (6), 11{16 (2012)

[26]. Zhu, B.X.: Resilient control and intrusion detection for scada systems. Technical Report UCB/EECS-2014-34, University of California at Berkeley (May 2014)

[27]. Daniel Germanus, A.K., Suri, N.: Increasing the resilience of critical scada systems using peer-to-peer overlays.
In: Architecting Critical Systems: First International Symposium, ISARCS 2010. Lecture Notes in Computer Science, vol. 6150, pp. 161-178. Springer, (2010)

[28]. Ma, Z., Smith, P., Skopik, F.: Towards a layered architectural view for security analysis in scada systems. CoRR abs/1211.3908 (2012)

[29] Peter Schoo, V.S.M.M.P.M.H.D.H.M.D.Z. Volker Fusenig: Challenges for cloud networking security. In: The 2nd International ICST Conference on Mobile Networks and Management. 1, pp. 1-16. Springer, (2010)

[30] Codenomicon: The Heartbleed Bug. http://heartbleed.com/ [accessed 10 Jun 2014

[31] Aiko Pras, G.C.M.M.I.D.R.B.R.S.R.S. Anna Sperotto, Hofstede, R.: Attacks by \anonymous" wikileaks proponents not anonymous. CTIT Technical Report 10.41, Design and Analysis of Communication Systems Group (DACS), University of Twente, Enschede, The Netherlands (December 2010)