A Survey on Cloud-based Software Platforms to Implement Secure Smart Grids

Béla Genge
"Petru Maior" University
bela.genge@ing.upm.ro

Adela Bereș
"Petru Maior" University
adela.beres@gmail.com

Piroska Haller
"Petru Maior" University
phaller@upm.ro

***Abstract*-Smart Grid has been characterized as the next generation power grid in which modern Information and Communication Technologies (ICT) will improve control, reliability and safety. Although the adoption of generic off-the-shelf ICT in Smart Grid provisions indisputable advantages and benefits, it raises several issues concerning the reliability and security of communications - the core infrastructure of Smart Grid. Cloud computing has developed and evolved over the past years becoming a real choice for Smart Grids infrastructure because of the availability, scalability, performance and interoperability that it offers. In this paper we present a survey of the existing cloud-based software platforms for implementing secure Smart Grids. Security issues like authentication and authorization of users, data encryption, availability, attacker impact, detection and trust management have received significant attention in previous work. Nevertheless, as shown in this paper, their integration and adaptation to emerging fields such as Smart Grid is still in an embryonic state. As such, we report recent advancements and software platforms specifically for Smart Grid and we outline several issues as well as suggestions for designing security-aware platforms for Smart Grid.**

***Index Terms*--Smart Grid, cloud computing, security, privacy**

I. INTRODUCTION

Nowadays, Smart Grid is commonly recognized as the next generation power grid with improved operational benefits of control, reliability and safety, and advanced two-way communication provided by the adoption of modern Information and Communication Technologies (ICT).

Although the adoption of generic off-the-shelf ICT comes with many benefits and advantages, it also raises several issues regarding the security of the core infrastructure of Smart Grid – the communications and control systems, which need to be reliable, consistent and exhibit long-lasting availability.

According to the National Institute of Standards and Technology (NIST) "cloud computing is a model for enabling ubiquitous, 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" [1]. Cloud computing is more than virtualization as it offers on-demand and measured services, rapid elasticity, pooling for resources and broad network access. This makes cloud computing a powerful candidate for secure Smart Grid infrastructures because of the reliability, high availability, scalability and performance that it offers.

Briefly, the main contributions of this paper are the following: (i) we present a survey of the existing cloud-based architectures for Smart Grid systems; (ii) we compare and evaluate these solutions against a set of basic security requirements; and (iii) we provide a detailed discussion on possible directions and approaches for designing security-aware software platforms for emerging Smart Grid.

The rest of the paper is organized as follows. Section II describes a set of basic security requirements for cloud-based platforms for Smart Grid systems. Section III presents a comparison of existing cloud-based platforms and solutions for Smart Grids. Section IV presents related surveys. Section V discusses these solutions and possible approaches for designing security-aware software platforms for emerging Smart-Grids. Conclusions are presented in Section VI.

II. SECURITY GOALS FOR CLOUD AND SMART GRID

After a thorough research on cloud-based platforms and Smart Grid systems we defined the following basic set of security requirements which need to be fulfilled in order to provide a secure cloud-based architecture for Smart Grids: confidentiality, integrity, authenticity, access control, privacy, availability, authorization and accountability.

Confidentiality is among the most important security requirements for Smart Grids. Information is considered highly sensitive and needs to be guarded from unauthorized access, use or modification, but still keeping it available for authorized personnel. This must be enforced especially on the public cloud platforms where data is stored together with others' data and can be easily tampered with. Furthermore, confidentiality is a significant property of communications between Smart Grid and cloud, and specific measures to provide it should be implemented.

Integrity ensures that data is not altered in any of the communication phases. Information must be accurate and trustworthy throughout the system. Data stored in the cloud, originating from the cloud or originating from the Smart Grid should be accurate in every state and in every step of the communication and data transfer process.

Authenticity ensures that data is coming from an authorized source and can be trusted. For this purpose, specific cryptographic measures can be implemented, e.g., Message Authentication Codes (MAC), digital signatures. However, special care must be taken in order to ensure that the same

level of authenticity is provided in all communication phases. This is a significant and challenging issue in general since the Cloud and Smart Grid represent a heterogeneous infrastructure, where devices have different computing capabilities and the deployment of Public Key Infrastructures (PKI) is not trivial.

Access Control, as its name suggests, provides the ability to setup data access control policies. In cloud platforms, especially in public clouds, data is stored in a common environment for all applications and users using that platform. Identifying the involved entities and data access policies is highly important so having the correct access control policies in place is crucial. In the Smart Grid sensitive information is generated and communicated, the remote terminal units (RTUs) as well as the smart meters control client household devices consumption and behaviour. These are critical for the availability and accuracy of the data in Smart Grid and only authorized personnel should have access to them.

Privacy ensures the protection of communicating peer's data. Electricity Grids generate a large amount of personal information about clients' electric consumption profile which is stored in the cloud. Therefore, privacy represents an important requirement for a cloud-based architecture.

Availability refers to the fact that the data needs to be available at any time. Power outages or other similar incidents shouldn't affect the clients, the system and the data should be available even in these situations. Redundancy and backup servers are solutions for an available cloud-based secure Smart Grid architecture.

Authorization is about the users and the personnel of the cloud and Smart Grid systems. Only authorized users should be permitted at any time to access sensitive information and specific operations.

Accountability represents the ability to log every operation that is done in the system. This is useful not only for history purposes but also for detecting and analysing attacks both on the cloud system and on the Smart Grid. Together with a warning system this security requirement could prevent harmful intrusions.

III. CLOUD-BASED PLATFORMS FOR SECURE SMART GRID

In this section we present existing cloud-based architectures for secure Smart Grid and proposed solutions for meeting the security of such systems.

A. D^2R

The Dynamic Demand Response (D^2R) is the result of the collaboration between the Los Angeles Smart Grid Project (sponsored by the US Department of Energy) and the Los Angeles Department of Water and Power [2].

Yogesh Simmhan et al. created a platform which is used on the University of Southern California campus microgrid in order to perform intelligent demand-side management and relieve peak load [2]. This platform is called Dynamic Demand Response (D^2R) and is targeted towards electricity power grids. In the long term, the authors intend to expand from the university microgrid to the Los Angeles power grid.

D^2R uses hybrid clouds including public and private and Infrastructure as a Service (IaaS) as well as Platform as a Service (PaaS) in order to store the data and in this way assuring its availability and scalability. D^2R also includes a secure repository to store the data collected from the sensors using authorization and authentication in order for the users to gain access to the data. Data is collected through a framework which runs on a private Eucalyptus IaaS Cloud which has 16 nodes with 8 Opteron CPU Cores connected through gigabit Ethernet [2]. Data processing is done using OpenPlanet and Hadoop MapReduce platform on private Cloud infrastructure. Confidentiality is ensured through specific cryptographic techniques.

As a recognition of the real-world impact by applying scalability principles to the Smart Grid, D^2R platform won the IEEE International Scalable Computing Challenge (SCALE) for 2012.

B. VS-Cloud

Virtual SCADA architecture for the cloud (VS-Cloud) that encompasses Cloud Computing with advanced cryptographic schemes and traditional SCADA architectures is a solution originating from University of Malaga, Spain [3].

A Smart Grid is composed of different elements like operators, remote terminal units (RTUs), advanced metering infrastructures (AMIs), sensors, SCADA systems and others which communicate and exchange data. This data needs to be controlled and safely stored. VS-Cloud was built to be the backbone of the interactions between the Smart Grid's components, controlling it and storing the sensitive information about executed actions, measurements or incidents and alarms.

VS-Cloud is focused on providing a better risk management, maintenance and auditing and an accurate forensics [3]. This is done by having specialized nodes called gateways which transmit, interpret and store the control messages from the system.

From the basic set of security requirements defined, the VS-Cloud assures availability, accountability, confidentiality, integrity and operational privacy.

Availability and accountability are provided by redundantly storing the information that is generated by the system. Consequently, in the case of a failure or of an attack the information can be retrieved, queried and used.

Data confidentiality is ensured by encryption and searchable encryption. Digital signatures and proofs of storage are used for keeping the integrity of the data. Last but not least, operational privacy is achieved by using private information retrieval, searchable encryption and anonymous routing.

C. Cryptonite

Cryptonite is part of the D^2R platform being developed at the University of Southern California in Los Angeles, USA [4]. It's a secure repository to store sensitive Smart Grid data

in the cloud based on the StrongBox model and implemented on the Windows Azure Cloud platform.

From the security goals point of view the focus is on a safe communication between the client and the storage and on providing a secure storage of the data in the cloud. Authorization and authentication of users is done based on a scalable and user-friendly model for key management with RSA public/private key pairs along with digital signatures and checksums. The accountability requirement is met and everything can be traced easily by auditing every data related operation that is done in the cloud. Confidentiality is assured in all communication phases from the client to the storage. The data is signed before being sent to the cloud. In the communication process no plaintext transfer is allowed. Furthermore, in the cloud data is encrypted using broadcast encryption.

Cryptonite is implemented on top of Microsoft Windows Azure Cloud platform and it is using the standard Azure virtual machines, BLOB files and table storage services. The authors also propose performance improvements for the communication and storage of data which were evaluated and proved to be more efficient than the Azure .NET APIs.

D. Aurelia Delfosse et al.'s work

Cloud platforms come in three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (Iaas). Aurelia Delfosse et al. from the Department of Security in Numergy, present in their work a complete security architecture for the data protection in IaaS clouds [5].

Aurelia Delfosse et al. identify the security threats and challenges for the main IaaS components. Service Layer Agreements and QoS attributes should be monitored and enforced. Attacks against XML and web services can be performed in the cloud software. Networks and Internet connectivity are also weak points because of Denial of Service (DoS), Man-In-The-Middle (MITM) attacks, IP Spoofing, port scanning and DNS spoofing. Virtualization also raises security threats like: monitoring Virtual Machines (VM) from other VM, communication between VMs, resources DoS, VMs provisioning and migration.

The authors also offer several solutions for these threats and challenges which ensure that security goals for such an architecture are met. Following we are presenting these solutions.

IPSec VPN or a Secure socket (SSL/TLS) are strongly recommended for securing the communication and data access in the cloud. IPSec will provide authentication, integrity and confidentiality at layer 3. SSL/TLS is initialized at layer 5 and at layer 6 it encrypts the rest of the communication. For securing the data storage in the cloud encryption on system, data and swap partition is proposed.

Finally, to solve the problem of authentication and authorization they consider the Public Key Infrastructure, Identity based cryptography, Identity based Signature and Private Information Retrieval.

E. Siddharth Sridhar et al.'s work

The development of a trustworthy Smart Grid requires a deeper understanding of the risks of attacks on the cyber infrastructure and power applications of the grid. Siddharth Sridhar et al. present the current research efforts aimed at enhancing the Smart Grid's application and infrastructure security [6].

The power applications are classified into three categories: Generation Control, Transmission Control and Distribution Control. For each of these a general definition of the work that it performs together with cyber vulnerabilities and existing solutions are presented.

For Generation Control is important to provide secure access control, privacy of data and high availability. These can be achieved by validating control commands and using reachability analysis to gauge the impact of data corruption.

For Transmission Control, system integrity, authenticity and availability of data are most important. False data injection attacks might to tamper data so the research in this area is mainly focused on detecting and preventing such attacks, as well as protecting the meters and making the WAN (Wide Area Network) backbone secure and dependable.

Distribution Control system is responsible for delivering power to the customer. In this system high availability if very important as well as integrity and authenticity of data and a secure access control. The availability of data is assured through load shedding. Tampering with the meters is an important problem in this system which can be resolved by smartly programming them. However, malicious LCS commands still represent a challenge.

On the cyber infrastructure the focus is on the communication and device security. Confidentiality, integrity, availability, authorization are achieved through a secure communication using encryption and VPNs. Authentication principles and protocols as well as re-keying the credentials are used to make the grid more secure.

Secure DNP3, ANSI C.12.22, IEC 61850 are some of the solutions which can be used to meet the access control security requirements. Accountability is achieved through the deployment of forensics agents, system logs, IDS (Intrusion Detection System) results and network traffic flow information.

F. Cristina Alcaraz et al.'s work

Cristina Alcaraz et al.'s work is aimed at the security of industrial sensor network-based substations in the context of the Internet of Things [7]. The researchers from the Computer Science Department of the University of Malaga in Spain and Cryptography and Security Department of Institute for Infocomm Research in Singapore, compare the existing TCP/IP integration strategies that can be applicable to such networks.

These solutions can be classified in the following two categories: stack-based and topology-based. Stack-based solutions are built on the similarities of the wireless sensor

network (WSN) stack and the Internet network stack. Topology-based is done based on the actual location of the nodes that provide access to the internet.

Three stack-based solutions are presented. The first approach is the Front-End solution in which the communication between the WSN and the Internet is done through a concentrator device. In this way the WSN can implement its own set of protocols. Most academic and commercial control systems use this type of solution.

The second solution is the Gateway solution in which a device acts as an application layer gateway. This device translates the protocols from both networks and routes the data. This solution is technically possible from 2012 with standards that support protocol tunnelling like ISA100.1.

The third approach is the TCP/IP solution where the sensor nodes implement the TCP/IP stack. This provides the ability for any internet host to open a direct connection with a specific sensor and vice versa. The drawback with this approach is that it's not any more possible to implement WSN specific substation protocols like WirelessHART. Nevertheless, other protocols that support TCP can be used, e.g., DNP3/IP or Modbus/TCP.

As for the topology-based classification two solutions are discussed: Hybrid solution where the nodes of the WSN could be a few dual sensor nodes located in the root of the network providing access to the internet and Access Point solution with a fully-fledged backbone of devices that allow nodes to access the internet in one hop.

Security-wise these solutions differ from one another. TCP/IP and Gateway solution used a distributed mechanism for authentication and authorization, while the Front-End solution uses a centralized one. TCP/IP and Gateway have efficient detection rules and an end-to-end secure channel. Front-End solution has lightweight detection rules and the channel is securely bridged at the base station. The accountability is centralized for Front-End and Gateway, while for TCP/IP is limited by the storage.

G. The Service Security Lab

Michael Menzel et al. present their cloud-based Service Security Lab that supports on-demand creation and orchestration of composed applications and services developed at the Hasso Plattner Institute in Germany [8]. The user can configure the security settings and patterns, create security configurations and execute the composed applications in the cloud. Authorization and authentication is done using WS-Trust. WS-Security and WS-Policy ensure confidentiality, integrity, authorization and authentication. Also for authentication Security Token Service and Security Policies can be chosen.

IV. RELATED SURVEYS

In their paper, Peng Yong et al. mainly provide a review on research results of secure cloud storage in which cryptographic techniques have been used to their designs [9]. It's a very comprehensive work in which different cryptographic techniques are analysed together with the degree of their adoption in the current cloud storages and the roles they play. This work was done in the Information Security Centre of the Beijing University of Posts and Telecommunications on different cloud storage platforms, analysing their roles and how the cryptographic techniques are used. These techniques are mainly used to assure the confidentiality of data and a secure access control.

Confidentiality is enforced by using searchable encryption, attribute-based encryption, identity-based encryption, broadcast-encryption, XML encryption and group encryption. At last, access control is provided by attribute-based encryption, identity-based encryption, broadcast encryption and digital signature, unique signature, group signature.

Zubair A. Baig and Abdul-Raoof Amoudi from King Fahd University of Petroleum and Minerals in Saudi Arabia did an analysis of the Smart Grid attacks and possible countermeasures. Besides from classifying the types of attacks on Smart Grids they also give a set of countermeasures [10].

Five types of attacks are identified and presented: Supervisory Control and Data Acquisition (SCADA) attacks, Smart Meter attacks, Physical Layer attacks, Data Injection and Replay attacks and Network-based attacks. These attacks affect security properties like confidentiality, integrity, availability, non-repudiation. As countermeasures to ensure integrity, availability, confidentiality and access control different algorithms developed to detect attacks on physical layer, network-based, data injection and replay are proposed. Confidentiality for smart meters can be enforced by replacing secret keys, device reconfiguration/resetting, secret key reset or by replacing the device. Secret keys also provide integrity for smart meters. Finally, replacing the device, changing the channel communication frequency or enabling ZigBee security mode can have an important impact on the availability of the smart meters.

Another research on Smart Grid threats, vulnerabilities and solutions was done by Fadi Aloul et al. The research was conducted in the Department of Computer Science and Engineering of American University of Sharjach, United Arab Emirates and the Department of Computer Science from the American University of Beirut in Lebanon, and discusses the challenges that exist in securing the Smart Grid and how the current security solutions applied are not sufficient to secure these systems [11].

The threats and attacks that they identified are the following: malware spreading, access through database links, compromising communication equipment, replay attacks, network availability, eavesdropping and traffic analysis and Modbus security issues. Also a set of solutions is proposed which could be implemented when creating a Smart Grid infrastructure which is more secure and reliable: using implicit deny policy, malware protection, using Network Intrusion Prevention and Detection Systems, Transport Layer Security (TLS), IPSec, secure communication through VPNs and Public Key Infrastructure (PKI). These solutions should

enforce authentication, authorization, access control, confidentiality, integrity and privacy security goals.

V. Discussions

In this section we compare the solutions of cloud platforms for secure Smart Grid as shown in Fig. 1. A list of possible Smart Grid attacks is provided in Table I together with the affected security properties.

As we can see from Fig. 1 a lot of emphasis is put on the confidentiality and integrity of the data. We split the security concerns and issues into three main regions: security in the cloud storage, communication security between the grid and the cloud, and last but not least security in the Smart Grid. Only two of the studied platforms offer security solutions in all three areas, most of them covering two areas, whether cloud and communication, or communication and Smart Grid.

For cloud storage the main concern is the confidentiality of the data, integrity and authorized access to the information. Availability should be implicit as most of the cloud storage providers offer redundant storage for the data, but custom solutions are also possible.

For communication between the cloud and grid again the confidentiality is the most important security property. Except for one, all platforms offer solutions to enhance the confidentiality when transferring information from the grid to the cloud or the other way around.

Smart Grid was highly studied with respect to security as it gets more and more integrated within the Internet of Things and in our everyday life, managing and controlling our electricity or water consumption. According to NIST the main security attributes for Smart Grid are availability, confidentiality and integrity [12]. Following this, almost all of the studied articles offer solutions for enforcing these security goals.

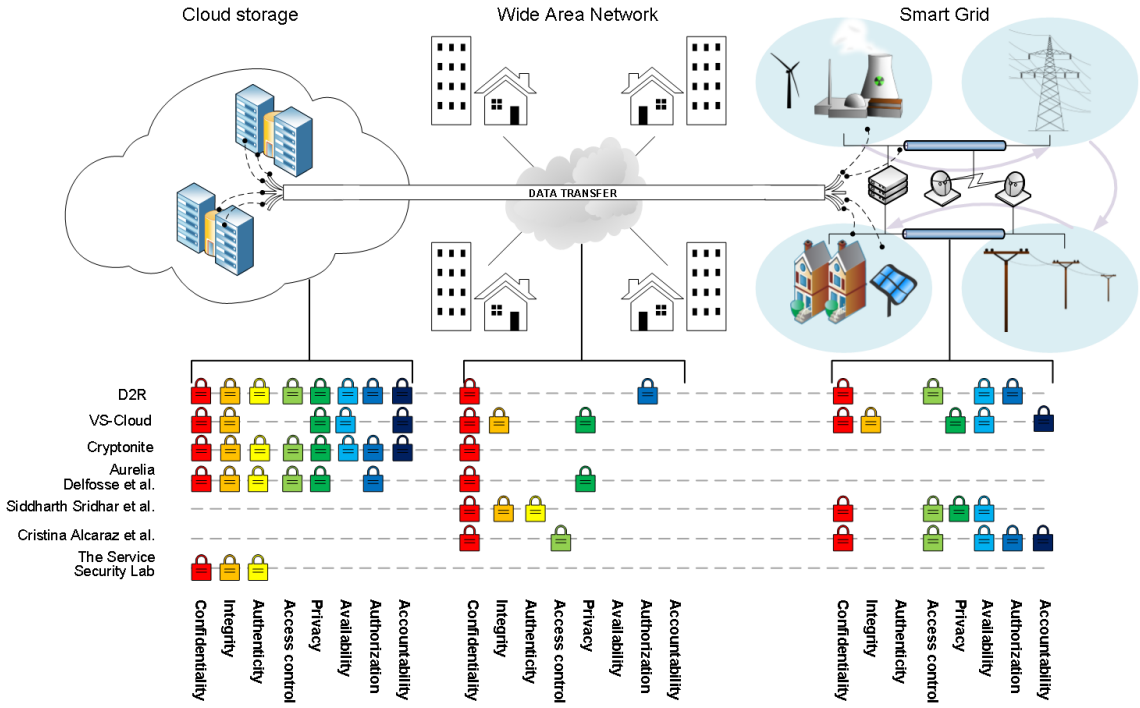

Fig. 1. Comparison of cloud-based platforms for secure Smart Grid

TABLE I
Smart Grid attack types and security properties affected

Attack type	Attack target	Attack details	Affected security property
Malware spreading and device attacks	Smart meters, RTUs, SCADA	Tampers with the devices and tries to control them	Confidentiality, integrity, privacy, availability, non-repudiation, denial of service
Data injection and replay attacks	Smart Grid data	Tries to compromise the data in the network traffic and extract private user information	Confidentiality, privacy, integrity
Eavesdropping, Man-in-the-middle-attack and traffic analysis	Smart Grid network	It aims to learn the network traffic in order to take advantage of the vulnerabilities	Confidentiality, availability, integrity, privacy, denial of service

As for the types of attacks against Smart Grids presented in Table I, we can see that almost all target the three main security properties of Smart Grid: availability, confidentiality and integrity. Few of them take advantages of the vulnerabilities of the protocols used in the grid while others tamper with the data or affect directly the physical infrastructure. For some of them a set of solutions and countermeasures were provided by the authors of the presented platforms, others are still under investigation.

Solutions to enforce integrity, authenticity and privacy of the data are a novel vulnerability measure to compare and rank topologies against false data injection attacks, developed by two researches from the Texas Tech University and the University of California respectively [13] and a generalized likelihood Ratio Detector with L_1 Norm Regulation developed at the School of Electrical and Computer Engineering of Cornell University, Ithaca [14].

A survey on bad data injection attacks in Smart Grid was done by Dai Wang et al. from Xi'an Jiaotong University in China [15]. The identified solutions for access control, integrity and privacy include dynamic key management, authentication and WSN-featured defence.

Based on the analysis beforehand, we consider that data security properties must be consistent in all communication and storage stages. More specifically, confidentiality, availability and integrity, as being the most important security properties, must be monitored in all stages. Depending on their status a set of measures and solutions should be applied.

Accountability solutions should be used more often. These provide valuable information about operations, data or possible attacks. Auditing data and activity could help in preventing most of the damages of attacks.

Even more attention should be paid to secure the communication stage. Protocols and policies should be defined to protect all parties and data involved in the communication.

The testing environment is very important and has to be chosen carefully to mimic the real life appropriately. For this purpose we propose SCYAMIX, a middleware aimed at facilitating cyber-physical security experimentation with Sensei/IoT* standard proposal and physical processes for Smart Grid [16].

VI. Conclusion

At this moment there are multiple cloud-based platforms for implementing more reliable and secure Smart Grids. Some of them are undergoing development and are already implemented in universities and microgrids.

We proposed a basic set of security requirements to be taken into account when developing these platforms. Based on our analysis few of the existing platforms enforce these requirements in their implementation. Many of them focus on providing confidentiality of data in the system.

We intend, in the future, to continue the work on the middleware for security experimentation for cloud platforms for grid taking into account the security goals we proposed. This will help us in our own implementation of cloud-based platform for secure Smart Grid.

Acknowledgements

B. Genge's work on this research was supported by a Marie Curie FP7 Integration Grant within the 7th European Union Framework Programme.

References

[1] P. Mell, T. Gance, "The NIST Definition of Cloud Computing", *NIST Special Publication 800-145*, 2011.

[2] Y. Simmhan, S. Aman, A. Kumbhare, R.g Liu, S. Stevens, Q. Zhou and V. Prasanna, "Cloud-based software platform for data-driven smart grid management", *Computing in Science and Engineering*, pp. 1-11, 2013.

[3] C. Alcaraz, I. Agudo, D. Nunez and J. Lopez, "Managing Incidents in Smart Grids a la Cloud", *IEEE 3rd International Conference on Cloud Computing Technology and Science*, pp. 527-531, 2011.

[4] A. Kumbhare, Y. Simmhan and V. Prasanna, "Cryptonite: A Secure and Performant Data Repository on Public Clouds", *Proceedings of the 2012 IEEE 5th International Conference on Cloud Computing*, pp. 510-517, 2012.

[5] A. Delfosse, J. Fanton, T. Floriani, V. Malguy, N. Marine and C. Tavernier. "Cloud Data Security and Privacy in IAAS Model", *Proc. of the 2nd International Conference on Information Technology and Computer Networks*, pp. 54-67, 2013.

[6] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid", *Proceedings of the IEEE*, Vol. 100, No. 1, pp. 210-224, 2012.

[7] C. Alcaraz, R. Roman, P. Najera and J. Lopex, "Security of industrial sensor network-based remote substations in the context on the Internet of Things", *Ad Hoc Networks*, vol. 11, issue 3, pp. 1091-1104, 2013.

[8] M. Menzel, R. Warschofsky, I. Thomas, C. Willems and C. Meinel, "The Service Security Lab: A Model-driven Platform to Compose and Explore Service Security in the Cloud", *IEEE 6th World Congress on Services*, pp. 115 - 122 , 2010.

[9] P. Yong, Z. Wei, X. Feng, D. Zhong-hua, G. Yang and C. Dong-qing, "Secure cloud storage based on cryptographic techniques", *The Journal of China Universities of Post and Telecommunications*, vol. 19, sup. 2, pp. 182-189, 2012.

[10] Z. A. Baig and A.-R. Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures", *Journal of Communications*, vol. 8, no. 8, pp. 473-479, 2013.

[11] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions", *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.

[12] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements", *NISTIR 7628*, 2010.

[13] Md. A. Rahman and H. Mohsenian-Rad, "False Data Injection Attacks with Incomplete Information Against Smart Power Grids", *Proc. of IEEE Conference on Global Communications*, 2012.

[14] O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures", *1st IEEE International Conference on Smart Grid Communications*, pp. 220-225, 2010.

[15] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun and Y. Liu, "A Survey on Bad Data Injection Attack in Smart Grid", *IEEE PES Asia-Pacific Power and Energy Engineering Conference*, 2013.

[16] B. Genge, P. Haller, A. Gligor, A.Beres, "An Approach for Cyber Security Experimentation Supporting Sensei/IoT for Smart Grid", *2nd International Symposium on Digital Forensics and Security*, 2014.