C. Alcaraz, I. Agudo, D. Nuñez, and J. Lopez, "Managing Incidents in Smart Grids 'a la Cloud", *IEEE CloudCom 2011*, pp. 527-531, 2011.
http://doi.org/10.1109/CloudCom.2011.79
NICS Lab. Publications: https://www.nics.uma.es/publications

Managing Incidents in Smart Grids à la Cloud

Cristina Alcaraz, Isaac Agudo, David Nuñez and Javier Lopez
Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz, isaac, dnunez, jlm}@lcc.uma.es

October 29, 2015

Abstract

Over the last decade, the Cloud Computing paradigm has emerged as a panacea for many problems in traditional IT infrastructures. Much has been said about the potential of Cloud Computing in the context of the Smart Grid, but unfortunately it is still relegated to a second layer when it comes to critical systems. Although the advantages of outsourcing these kinds of applications to the cloud is clear, data confidentiality and operational privacy stand as mayor drawbacks. In this paper, we describe some security mechanisms, and specifically, some cryptographic schemes, that will help in a better integration of Smart Grids and Clouds. We propose the use of Virtual SCADA in the Cloud (VS-Cloud) as a means to improve reliability and efficiency whilst maintaining the same protection level as in traditional SCADA architectures.

Keywords: Smart Grid, SCADA systems, Incident Management, Cloud Computing, Cryptography, Searchable Encryption

1 Introduction

Today's society relies on a set of critical infrastructures (CIs), which provide services that are essential for the good performance of other CIs, such as energy control and distribution systems. Every day millions of watts of electricity are channelled from power suppliers to power consumers. Any disruption of such services could involve a significant change in the performance of other infrastructures, seriously affecting our social and economic welfare [15].

In order to efficiently and intelligently generate, distribute and administer power consumption to end-users, a new electrical network architecture, known as Smart Grid, starts to be introduced in the literature. According to the NIST [14], a Smart Grid is a complex infrastructure composed of seven main domains: (i) customers (citizens or utilities), (ii) market, (iii) service providers, (iv) operations, (v) bulk generation, (vi) distribution and (vii) transmission.

Each domain encompasses a set of elements (e.g. customers, operators, software and hardware components, etc.) whose interactions and relationships ensure a dynamic

cooperation and information exchange. Unfortunately, this interaction may involve certain architectural complexities and interdependence links, which may trigger serious consequences when part of the control is partially or permanently disrupted within the Grid. The propagated effect, known as *cascading effect*, could leave parts of the system isolated or domains without any functionality. For this reason, it is necessary to provide solutions that help the entire system to recover its control on time, irrespective of the type and criticality of the situation.

Taking advantage of the distributed and scalable nature and the on-demand provisioning of computing resources offered by Cloud Computing, a new model for Smart Grid based on such a paradigm is proposed in this paper. Our idea is to ensure a transparent control and service delivery in every case, in either a normal or extreme situation.

In this paper, we introduce a Virtual SCADA architecture for the Cloud (VS-Cloud) that encompasses Cloud Computing with advanced cryptographic schemes and traditional SCADA architectures. The main novelty of our scheme is the redundant storage of sensitive information within the Cloud, guaranteeing its accessibility at all times. However, we cannot avoid that the proposed solution also has to fulfil a set of requirements, such as scalability, availability and reliability of services and resources, performance in real-time and security. While some of them are the direct responsibility of the cloud provider and, hence, out of the scope of this paper, we will discuss to what extent our model compromises or facilitates them.

The paper is organised as follows: Section 2 presents the challenges faced by the next generation of energy distribution systems. Section 3 exposes our proposal, as well as the security requirements that it must meet. Section 4 describes the applicability of Searchable Encryption schemes for building a secure Incident Management System for VS-Cloud. Finally, Section 5 concludes the paper and future work is outlined.

2 Smart Grids: New Needs to Advance in the Energy Control and Distribution

Continuing with the model proposed by the NIST [14], part of the functionality of a Smart Grid is associated with the remote control of power substations that ensure efficient energy generation and distribution to residential area complexes. The control is basically managed by a centralised system known as SCADA (Supervisory Control and Data Acquisition) system [1]. Although this control forms a unique entity, it has a special influence on the rest of the domains (particularly on generation, transmission and distribution systems) by supervising operational activities in the entire Grid. Given that its importance is essential for reaching a good performance within the Grid, all our effort will mainly focus on SCADA systems.

A SCADA system is a critical control system in charge of monitoring other CIs, such as energy systems. The critical nature of these controlled infrastructures means that a SCADA system must guarantee *resources and services availability* at all times. For this reason, the main control network is responsible for receiving and properly registering measurements and alarms from remote substations located very close to

controlled CIs, as well as managing control tasks through commands. To this end, every substation has to be configured with special elements known as Remote Terminal Units (RTUs), whose main function is to collect data streams from sensors and perform actions on the controlled infrastructure.

Then, it is quite clear that a SCADA system plays an essential role within a Smart Grid architecture, not only to control substations from any geographical point but also to directly control the performance and needs of the rest of the domains of a Smart Grid. This demand is managed through specialised infrastructures called Advanced Metering Infrastructures (AMIs), which act as an interface between the real world and the SCADA system, in addition to enabling a suitable collection and distribution of information to customers and other entities, such as pricing of electricity or load reductions due to power peaks.

In the model proposed by NIST, the Internet is a crucial communication infrastructure for the control and interconnection between domains of a Smart Grid architecture. Indeed, it provides a set of benefits for supervision, such as global connectivity between the system entities, flexibility in data acquisition and management, data dissemination, maintenance, diagnosis and Web interfaces to visualise data streams and resources in real-time. In addition, the use of open standards and open Web protocols, such as HTML and HTTP(S), also help to significantly reduce costs in terms of hardware, software, time, personnel and field operations [16].

Despite the migration to IP-based technologies and the standardisation of IP-based automation protocols, the nature of these systems and their protocols are still very limited, specially with respect to security. For example, current SCADA systems typically use Modbus/TCP, DNP3 and IEC-104 for the control and automation, and ICCP/TASE2.0 for the intercommunication between telemetry control systems. Unfortunately, these protocols show a significant lack of strong-agreement procedures, authentication services and integrity services [1], which could put at risk the operational integrity and the overall security of the system. For instance, an intruder could alter critical variables or parameters, or change highly-sensitive information such as alarms in order to change the normal behaviour of the system.

For this reason, we believe that future control solutions for renewable energy systems will have to take into account a minimum set of operational requirements in order to ensure a secure and suitable control of domains. Some of these requirements are listed below.

- Operational control with a minimum delay for ensuring *performance* in (near) real-time and quality of service.
- *Resource and service availability*.
- *Availability, integrity and confidentiality of operational information*. Note that the protection order for a critical control system is very different to the protection order for a conventional system (i.e. confidentiality, integrity and availability). Confidentiality issues do not entail major security risks in comparison to unavailable information or resources, or an intentional manipulation of critical messages (alarms, measurements or commands).

- Business continuity by ensuring *survivability and critical-safety* in the presence of failures, errors or threats within a domain.

Our main goal and contribution in this paper is to provide an attractive and robust approach that allows the control system to continue with its services in a secure manner irrespective of the type of situation (either normal, threatening or emergency), continuously providing critical services delivered by controlled CIs and demanded by the end-users.

3 VS-Cloud: Advantages of a Virtual SCADA centre in the Cloud

The main idea behind this paper is the definition of a system where different elements of the Smart Grid (such as operators, RTUs, sensors, utilities, SCADA systems, and others) can directly interact with each other through a unique and common cloud, called *Virtual-SCADA Cloud* (*VS-Cloud* from now on). Basically, VS-Cloud could be considered as the backbone of the control system by redundantly storing any type of information generated by the system, such as incidents/alarms, measurements and executed actions/processes. Thus, operational data streams are not only registered by the SCADA centre, but also they are registered by VS-Cloud.

The way of registering and locating operational data streams within the cloud forms part of the goal of VS-Cloud of providing a set of reliable and secure operational services, such as:

- A *suitable SCADA incident management* and a *fast response* to face critical situations by redundantly storing and registering relevant evidence of the entire system within VS-Cloud. Thus, when substations are targeted or disrupted, their individual elements, such as sensor nodes and RTUs, could directly interact with the cloud to recover operational information that may help the system to estimate the actual situation and its consequences, and take over the control as soon as possible.

- *Advanced search of SCADA incidents* without going through the SCADA centre. Thus, operators in the field could directly operate with the system as soon as possible by obtaining an incident list in real-time from the cloud and according to a certain search priority parameters, such as the time or the criticality of an alarm.

- *Operational privacy* by strategically storing operational data streams and hiding their exact location within the cloud. The goal would be therefore to hide real weaknesses of a critical system and deceive adversaries (including the cloud provider).

- *Integrity* of the information stored in the cloud, both at an atomic level (stages of individual transference and storage to/from the cloud) and at a dataset level (the data stored within the cloud as a whole).

- *Accountability* by registering within VS-Cloud any operational information together with information related to the sender node. These registers allows operators and engineers to know existing evidence within an affected domain/system at all times and from anywhere, and thereby take a suitable action accordingly.

Summing up, this approach seems to be a promising solution for the control of future power generation systems. This is thanks to the operational information redundancy and its management within the cloud, providing a better *risk management, maintenance and auditing* and a most accurate *forensics*, as well as ensuring rapid attendance to critical situations. This continuous protection does not only cover the control system but also the rest of the domains in the Smart Grid, controlling any emergency situation and avoiding any type of repercussion on the performance of other CIs and on the welfare of our society and economy.

3.1 Redundancy and Emergency Control in VS-Cloud

For an efficient management of SCADA alarms/incidents through VS-Cloud, specialised intermediary nodes (i.e. gateways) with enough computational resources to compute different control message formats are required for our approach. The reason for this is mainly due to the heterogeneous nature of SCADA network architectures where different elements, technologies and communication protocols coexist to reach the same goal: monitoring and supervision. For example, there are currently some IP-based SCADA protocols such as Modbus/TCP, DNP3, IEC-104, ICCP and other proprietaries ones, as well as wireless industrial communication protocols such as ISA100.11a, WirelessHART or ZigBee [2].

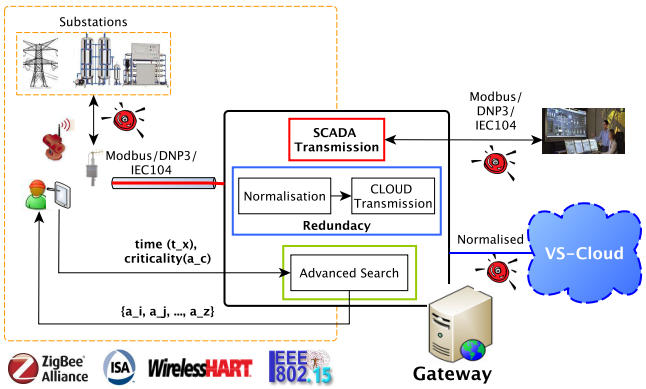

Figure 1: The gateway and its components

The are several main functionalities of the gateway within our model. Firstly, this gateway allows the system to interpret and translate control messages between different networks (e.g. translating incoming ISA100.11a messages from a WSN to Modbus/TCP messages for a SCADA network, and viceversa); and secondly to provide a

customizable way for managing SCADA incidents. To be able to meet these goals, the gateway is composed of three basic components (see Figure 1): (i) a *SCADA Transmission* component, (ii) a *Redundancy* component, and (iii) an *Advanced Search* component.

The SCADA transmission component is in charge of transmitting any operational information to the SCADA system, whereas the redundancy component is responsible for replicating such information within VS-Cloud. In order to normalise control messages to the same format, the redundancy component first operates the *Normalisation* component to combine and represent different data inputs in the same generic format, and then transmits the normalised message to the cloud. Regarding the advanced search component, it is in charge of dynamically resolving specific queries according to a set of parameters, such as range of time or frequency of a specific type of evidence with a determined priority level.

This way of redundantly storing sensitive operational information would also allow the entire system to recover the control of its affected areas by permitting other control systems to directly access VS-Cloud and obtain all the evidence that had occurred before an anomalous event. The idea is to create a precise reconstruction of a situation and deal with it accordingly. Depending on the criticality of the situation, the system will have to warn a field operator through a handheld device or to take control using a specific SCADA protocol.

However, there is an important aspect to take into account within this approach: the information security. We cannot forget that the stored information within the VS-Cloud is highly-sensitive and it requires, on the one hand *operational privacy*, and on the other hand, *availability*, *integrity* and *confidentiality*. Availability is the main expected benefit gained from outsourcing the management of incidents to the cloud, so it is out of the scope of this paper; therefore, our next goal and main focus in the following Section will be to analyse existing security solutions for the rest of the properties.

3.2 Meeting the Security Requirements of VS-Cloud

In this Section, we briefly describe some techniques that could used to guarantee the security requirements of VS-Cloud, i.e. operational privacy, integrity and confidentiality.

Searchable Encryption is a recent concept that deals with searches over encrypted data, enabling a server to execute queries without having to decrypt the data, and ideally, without learning any information about it. This way, it is possible to outsource the storage of data to an untrusted party while preserving both confidentiality and searching capabilities. We will look at this technique in detail in Section 4.1.

Private Information Retrieval enables a client to retrieve information from a database without revealing any information about the requested data to the server [7]. The goal of these protocols is to hide from the server what items are of interest to the client, rather than refraining the server from reading the data. Private Information Retrieval techniques could be of use in VS-Cloud to provide operational privacy, since it would prevent the cloud provider from finding out which part of the data is more valuable.

Digital Signatures are widely used cryptographic schemes that enable a sender to "sign" a document or message, in such a way that both authenticity and integrity of

data can be verified by the recipient. Digital Signatures could be used in our VS-Cloud proposal to provide data integrity, as well as authentication of data producers (e.g. RTUs, sensor nodes, etc.); however, this solution does not scale well to large amounts of data, as it is infeasible to check the signature for every item of the VS-Cloud database. For this reason, more recent solutions, such as Proofs of Storage protocols, are more suitable for solving this issue.

Proofs of Storage are a type of cryptographic protocols that allow a client to check the integrity of large amounts of data stored in a server, without retrieving it, thus achieving reduced communications and storage overhead [3, 12]. We could use this technique for checking the integrity of the whole dataset of incidents in our VS-Cloud proposal.

Anonymous Routing techniques, such as Tor [9], are designed to provide anonymity to online communications. These techniques could be used for concealing the source of communications in our VS-Cloud setting, thus enhancing operational privacy; this way, potential attackers (and even the cloud provider itself) should not be able to trace, locate or identify VS-Cloud users, such as operators, RTUs or sensor nodes.

Table 1: Cryptographic solutions for security properties of VS-Cloud

Property	**Cryptographic solution**
Data confidentiality	Encryption, Searchable Encryption
Integrity	Digital Signatures (atomic data integrity), Proofs of Storage (dataset integrity)
Operational Privacy	Private Information Retrieval, Searchable Encryption, Anonymous Routing

As we can see, there are several cryptographic techniques that could be of use for providing the desired security properties to VS-Cloud, which are summarised in Table 1. However, in this paper we will focus exclusively on Searchable Encryption, since this technique on its own would provide several interesting properties for an Incident Management System, namely: (i) data confidentiality, (ii) searching and filtering capabilities, and (iii) operational privacy.

Section 4 provides an in-depth insight of Searchable Encryption and its applicability to our proposal. However, we consider that a thorough study of the rest of the presented techniques, as well as others that are not considered here, would be of interest to our proposal.

4 Searchable Encryption for an Incident Management System

As we have already stated, in this paper we will analyse the characteristics of some *searchable encryption* schemes that could be of use for providing data confidentiality

to an Incident Management System that is outsourced to the cloud, while preserving search and filter capabilities.

We propose an architecture in which data confidentiality is provided through cryptography, like the one proposed in [13], where the authors describe a high-level architecture that enables to build a secure cloud storage service from an untrusted cloud provider combining three recent cryptographic techniques, namely searchable encryption, proofs of storage and attribute-based encryption. Their proposal stands at a high level and does not go into to details regarding specific cryptographic primitives or procedures, but offers an interesting initial approach to the cloud storage problem through the use of cryptography. In our setting, we will only consider the use of searchable encryption, in order to provide both data confidentiality and search capabilities.

4.1 An Overview of Searchable Encryption

Basically, a Searchable Encryption scheme is a set of cryptographic primitives that enables, apart from encryption, the possibility of searching for keywords over the encrypted data through the creation of *trapdoors*; these trapdoors are cryptographic tokens that must be handed to the server in order to perform a specific query. There are two main types of searchable encryption schemes: symmetric and asymmetric.

Symmetric Searchable Encryption schemes (SSE) assume that the data is encrypted with the same master key that will be used during searching, which makes them appropriate for scenarios where there is only one party involved or where the master key can be shared between several parties [4, 8]. The latter, among other aspects, proposes a multi-user version for symmetric searchable encryption (MSSE), which enables multiple parties to search over the data encrypted by a single user; in addition, this variant allows the data owner to create and revoke search permissions dynamically.

Asymmetric Searchable Encryption schemes (ASE) are based on a pair of public and private keys, so that any party that knows the public key is able to encrypt and add data to the server, but only the party in possession of the private key can generate trapdoors for searching for keywords over the encrypted data [5]. There are several ASE schemes with advanced search functionalities [6], which enable conjunctive, subset or range queries. However, the great limitation of most ASE schemes is that they do not provide any means to decrypt the data, although recent proposals tackle this issue [10, 11].

4.2 Analysis of Searchable Encryption schemes

In this Section, we will analyse the suitability of the different types of Searchable Encryption schemes with respect to the requirements and characteristics of our VS-Cloud proposal.

An ASE scheme can be used in a setting where there are multiple parties that are exposed to physical attacks, such as tampering or node capture, in the case of wireless sensor networks [2]; in such scenario, a master key cannot be freely distributed without posing a new security risk. Although these parties are necessary because of their role as data producers, there is no need to grant them any search privileges over the data. In this setting, the public key of the Incident Management System is known by

the data producer parties for adding data to the repository; if one of the data producers is compromised, or if the communications are eavesdropped, data confidentiality is maintained, since it is encrypted with the public key, although an attacker might be able to generate fake data. The private key will be held only by an auditing authority, that will be able to create and distribute search trapdoors to authorised auditors. As is mentioned in Section 4.1, there are several ASE schemes that provide more advanced search functionalities, such as range and conjunctive queries. It is important to remember that few ASE schemes provide decryption capabilities; data recoverability is a crucial characteristic for a redundant information system, so it would be unacceptable for us to lack such functionality. For this reason, we will only consider ASE schemes that enable decryption. It can be seen that ASE schemes provide more functionalities with respect to searches and deployment scenarios, at the expense of their limitations regarding data recoverability and efficiency.

In contrast, SSE schemes are created under the assumption that the same party generates and consumes the data; for this reason, it only requires a master key, which must be distributed to all the data producers. Most SSE schemes are less functional with respect to queries than ASE schemes, since, to the best of our knowledge, there are no symmetric schemes that handle range or subset queries. In the same fashion as regular encryption, symmetric schemes are much faster than asymmetric ones, making them more appropriate when efficiency is a critical requirement. However, if an attacker discovers the key, he will then be able of encrypting, searching and decrypting data. SSE schemes could be useful in any setting where there is a low risk of the master key being disclosed. In the case of our Incident Management System, each party may be a SCADA centre, whose security measures could be considered high enough to share the same secret key. These centres would be capable of generating encrypted data and outsourcing it to VS-Cloud, providing search trapdoors to authorised operators, and decrypting the data stored in the cloud in case of an emergency or a forensic analysis.

The last option that we will consider in this paper is to use the multi-user symmetric searchable encryption scheme (MSSE) proposed in [8]. The main advantage of this variant is that it provides a means to dynamically grant and revoke search privileges to an arbitrary group of users; in previous schemes, once a trapdoor is generated, it can be used indefinitely for searching for a certain keyword. The MSSE scheme could be of use in the same scenarios as the SSE, and additionaly, in settings where search permissions may be revoked as time goes on. Being based on a symmetric scheme, MSSE is also more efficient than ASE.

It can be seen that none of the schemes provides all the desired capabilities for VS-Cloud, since current schemes are often designed to solve one specific problem (e.g. range queries, conjunctive queries, etc.). However, the MSSE approach differs from the others, since the multi-user feature is added on top of a regular SSE scheme, and thus, it can be redefined for other SSE solutions (e.g. schemes that have support for conjunctive queries).

5 Conclusions and Future Work

In this paper, we have described the VS-Cloud architecture for Smart Grid management in the Cloud. Our primary goal when defining this architecture was to take advantage of all the benefits of Cloud Computing whilst retaining the same level of protection of traditional management schemes for Critical Infrastructures. We have described the requirements for this new architecture, as well as some techniques that could be of use for our proposal. Among these techniques, we have focused on searchable encryption; for future work, we plan to explore the other ones. Although current searchable encryption schemes are limited with respect to functionality and efficiency, we envisage this area as a key component of future secure storage solutions; research on this area is active and new schemes may arise in the near future.

We are currently planning to implement several searchable encryption schemes in a real cloud setting, in order to develop a comparative benchmark of these schemes that will give a more realistic comparison of the cited schemes. We also plan to use real data collected from existing SCADA systems in order to contextualise the comparison.

Acknowledgments

The work in this paper was partly sponsored by the EC Framework Programme as part of the ICT PASSIVE project (http://ict-passive.eu/) and by the Spanish Ministry of Science and Innovation through the ARES project (CSD2007-00004).

References

[1] C. Alcaraz, G. Fernandez, R. Roman, A. Balastegui, and J. Lopez. Secure Management of SCADA Networks. *New Trends in Network Management, CEPIS by Novática (ATI, Spain)*, 9(6):22–28, December 2008.

[2] Cristina Alcaraz and Javier Lopez. A security analysis for wireless sensor mesh networks in highly critical systems. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 40(4):419–428, July 2010.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 598–609. ACM, 2007.

[4] L. Ballard, S. Kamara, and F. Monrose. Achieving efficient conjunctive keyword searches over encrypted data. *Information and Communications Security*, pages 414–426, 2005.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In *Advances in Cryptology-EUROCRYPT 2004*, pages 506–522. Springer, 2004.

[6] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. *Theory of Cryptography*, pages 535–554, 2007.

[7] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. *Journal of the ACM*, 45(6):965–981, 1998.

[8] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 79–88. ACM, 2006.

[9] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium*, pages 21–21. USENIX Assoc., 2004.

[10] T. Fuhr and P. Paillier. Decryptable searchable encryption. *Provable Security*, pages 228–236, 2007.

[11] D. Hofheinz and E. Weinreb. Searchable encryption with decryption in the standard model. Technical report, Cryptology eprint archive, report 2008/423, 2008.

[12] A. Juels and B.S. Kaliski Jr. Pors: Proofs of retrievability for large files. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 584–597. ACM, 2007.

[13] S. Kamara and K. Lauter. Cryptographic cloud storage. *Financial Cryptography and Data Security*, pages 136–149, 2010.

[14] NIST. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Realease 1.0. NIST Special Publication 1108., January 2010.

[15] P. Peerenboom and R. Fisher. Analyzing Cross-Sector Interdependencies. In *40th Annual Hawaii International Conference on System Sciences, HICCS*, pages 112–119. IEEE Computer Society, 2007.

[16] M. Smith. Web-based Monitoring & Control for OilGas Industry. SCADA's Next Step Forward, Pipeline & Gas Journal, Online News, 2001, Retrieved on March 2011.