An Approach for Securing Cloud-based Wide Area Monitoring of Smart Grid Systems

Luigi Coppolino[1], Salvatore D'Antonio[1], Giovanni Mazzeo[1], Luigi Romano[1] and Luigi Sgaglione[1]
[1] University of Naples ,Parthenope'
{luigi.coppolino, salvatore.dantonio, giovanni.mazzeo, luigi.romano, luigi.sgaglione}@uniparthenope.it

Abstract. Computing power and flexibility provided by cloud technologies represent an opportunity for Smart Grid applications, in general, and for Wide Area Monitoring Systems, in particular. Even though the cloud model is considered efficient for Smart Grids, it has stringent constraints in terms of security and reliability. An attack to the integrity or confidentiality of data may have a devastating impact for the system itself and for the surrounding environment. The main security risk is represented by malicious insiders, i.e., malevolent employees having privileged access to the hosting machines. In this paper, we evaluate a powerful hardening approach that could be leveraged to protect synchrophasor data processed at cloud level. In particular, we propose the use of homomorphic encryption to address risks related to malicious insiders. Our goal is to estimate the feasibility of such a security solution by verifying the compliance with frame rate requirements typical of synchrophasor standards.

1 Introduction

Future generations of Wide Area Monitoring Systems (WAMS) look at commercial cloud architectures as an opportunity to reduce costs, increase data sharing, enhance scalability, and improve availability. At the core of WAMs there are PMUs (Phasor Measurement Units), which are nowadays used in distribution network context to measure and control the status of power grid. PMUs do so through synchrophasors, i.e, time-synchronized numbers that represent both the magnitude and phase angle of the sine waves found in electricity, which are time-synchronized for accuracy. Synchrophasors enable a synchronized evaluation of the phasor through GPS radio clock, and are being extensively deployed together with network-based Phasor Data Concentrator (PDC) applications for providing a precise and comprehensive view of the status of the entire grid. PDC units are in charge of collecting data coming from different PMUs and realize the effective computation.

Prototypal solutions of Cloud-based WAM were proposed [10]. The idea is to capture sensors data on a cloud-computing platform, and leverage its facilities to archive the data into a standard data collection infrastructure, which can include standard databases or grid specific solutions such as OpenPDC [11] to track the system state in real-time by performing the variety of analyses at cloud level.

However, difficulties of sharing data in a secure and low-latency manner limits exploitation of this new powerful technology by bulk electric power grid operators.

In a cloud-based deployment, the PDC application may be exposed to a number of threats that affect both confidentiality and integrity of sensitive data going through the monitoring system. The Insider Threat [12] is a particularly worrying example. It is impersonated by a malicious employee of cloud providers that leverages the privileged position to obtain access to sensitive data [20].

Two solutions are the most accepted against malicious insiders: Trusted Execution (TE) and Homomorphic Encryption (HE). There are works proposing the adoption of TE, in particular Intel SGX, for enabling the cloudification of SCADA systems [15][16][17]. While the adoption of HE for WAMS was still poorly investigated [18].

In this paper we propose an approach that enables secure synchrophasor data processing in untrusted cloud environments. Our approach is to leverage most recent implementations of HE to create and preserve a chain-of-trust from the field data collection to the cloud processing, and ensures confidentiality, even against malicious insiders. The idea is to encrypt PMU data on field and then transmit such a data to the cloud for subsequent storage or processing Synchrophasor measurements are always kept encrypted and evaluations like phase comparisons will be performed on ciphered data. In this way risks coming from malicious cloud insiders can be addressed and the security is preserved. Unfortunately, HE suffers from a non-negligible performance overhead, which could made the adoption of this technology impossible for synchrophasor data processing, which are characterized from strict frame rate requirements. Most-recent schemes like the one adopted in this paper, i.e., TFHE [13][14], started to provide very fast results. Our goal is to evaluate the feasibility of HE towards secure synchrophasor data processing in untrusted cloud by estimating supported frame rates.

The remainder of this work is organized as follows. Section 2 provides background on HE. Afterwards, Section 3 introduces synchrophasor systems and concepts of Wide Area Monitoring. Then, Section 4 defines possible threats in cloud environment. This is followed by Section 5 where we provide our solution. Finally, Section 6 concludes the document.

2 Background

This section overviews the technology adopted in this paper to enhance the security of cloud-based WAMS, i.e., Homomorphic Encryption (HE). HE is a recent cryptographic method allowing to perform computation directly on encrypted data, without the need of decrypting it. As such, the encryption schemes possessing homomorphic properties can be very useful to construct privacy preserving protocols, in which the confidential data remains secured, not only during exchange and storage, but also during processing. In a context of data outsourcing and of cloud computing, the homomorphic encryption is a mechanism that helps to protect data against intrusions from the cloud provider itself or attacks on the cloud infrastructure. Conventional symmetric and public key cryptosystems encrypt the data such that only the authorized parties can access it. In order to perform operations on this data, one needs to decrypt it first. Contrary to the above-mentioned encryptions schemes, homomorphic encryption can be used not only as a method to protect data privacy, but also to execute algorithms directly on encrypted data. The service (cloud) provider processes the received data encrypted with the public key, performs operations over this encrypted data and sends the encrypted result to the end user, owner of the homomorphic secret key. As an example, homomorphic encryption has already been used as a key-tool in the popularization of electronic-based voting scheme. There are various application contexts in which this paradigm can be employed: private searching, keyword search, private storage, anonymous authentication, etc [19]. During the years, three types of HE algorithms were proposed:

Partially Homomorphic Encryption (PHE) [1][3], has the ability to carry out just one type of operations (e.g., addition, or multiplication). Clearly, the limitation in the type of executable computations hampered the usage of HE in practical contexts.

Fully Homomorphic Encryption (FHE) [4]. in 2009, C. Gentry, at Stanford, proposes a first credible construction, both in terms of security and theoretical efficiency which proposed the first implementation of a FHE scheme. FHE schemes are capable to perform additions and multiplications over homomorphically encrypted data (ciphertexts) which correspond to addition and, respectively, multiplication operations over the clear text messages (plaintexts). Therefore, since any function can be expressed as a combination of additions and multiplications, FHE cryptosystems could compute in theory any arbitrary function. The first barrier to the adoption of FHE cryptosystems in real-world applications was related to the computational overhead induced by the actual execution on homomorphically encrypted data. In particular, it should be noted that most of the homomorphic encryption schemes provide mainly bit-level operators, thus intrinsically low level. However, making use of recent dedicated compilation and parallelism techniques, it was possible to mitigate the performances overhead for a series of real, yet lightweight, algorithms.

The security of the system is based on the noise introduced into the ciphered text. However such a noise can quickly grow, becoming larger as more homomorphic operations are performed on a given ciphertext. When the noise reaches some maximum amount, the ciphertext becomes undecryptable. Hence, one possible solution is refreshing the ciphertext. That is, performing after each operation a bootstrapping procedure able to remove the noise. This consists in a particular decryption algorithm performed to avoid noise. Unfortunately, this first fully homomorphic cryptosystem, and more generally, any bootstrapping-based cryptosystem known so far (until very recently), are way too costly to have any practical relevance whatsoever.

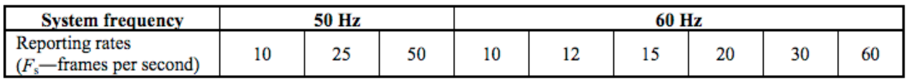
Somewhat Homomorphic Encryption (SHE), a much more efficient scheme was provided by Van Dijk et al. [5] who proposed a FHE scheme without the heavy bootstrapping procedure, i.e., Somewhat Homomorphic Encryption (SHE) over the integers. The price to pay with SHE is given by the limited number of mathematical operations that can be performed. However, in many real-world applications (e.g., medical, financial) this seems reasonable since – as Naehrig et al. [6] analysis reports – most of the evaluations required, i.e., one-time statistical functions, fits well with SHE constraints. In this work, we pursue the Van Dijk's SHE algorithm. This choice is driven by the need for a library that could be better adapted to HTEE requirements. We had to find a scheme having the following features: limited consumption of memory, fairly good performance, and support for all mathematical operations. SHE fits particularly well for our purposes. The only issue affecting SHE, i.e., the limited number of consecutive executable operations, is not a concern for the Synchrophasor use case.

3 Synchrophasor Systems for Smart Grids

Wide-Area Monitoring Systems (WAMS) of power grids is one important application from Smart Grid infrastructures. WAMS are composed of distributed measurement and control devices, characterized by a hierarchical architecture. A key component of WAMS is the Phasor Measurement Unit (PMU). This is the device in charge of electrical quantities synchronized measurements, e.g., voltage and current phasors, frequency and rate of change of frequency (ROCOF) with an accurate time-tag based on the Universal Coordinated Time generally obtained from a GPS receiver or through IEEE1588 synchronization. PMUs forward the acquired data to a Phasor Data Concentrator (PDC), which collects and aligns the provided measurements before send them next higher PDC levels. Ultimately, data arrives to a control center application where the overall status of the electric grid is evaluated.

Originally, synchronized measurements of WAMS was designed for transmission systems. After the advent of smart grid frameworks, benefits of Synchrophasor technology are moving also to the distribution network. The use of PMUs in the distribution network context represents a new challenge: the stand-alone PMUs and PDCs could be replaced by dedicated functionalities implemented in Intelligent Electronic Devices (IEDs) or by existing measurement devices upgraded in order to build an Internet of Things (IoT) network with synchrophasor functionality. In a Synchrophasor system suitable for distribution grids, several measurement devices will be necessary and, in this new scenario, the classical hierarchical architecture can be inadequate, since it can be unable to manage many PMUs and/or PMU-enabled instruments. A solution can be represented by replacing the hierarchical structure of PDCs with a less expensive and rapidly scalable structure based on cloud computing. The communication systems used by distribution system operators (DSOs) are expected to be shared and/or public. In this case, the bandwidth available for devices involved is strictly dependent on the type of communication channel adopted.

Normally, in transmission system WAMS, PMUs send data at a constant rate of 50–60 frames per second (fps) to guarantee the monitoring of dynamic events. The choice of 50 or 60 frames mean different supported frame rates (Table 1).



System frequency	50 Hz			60 Hz					
Reporting rates (F_s—frames per second)	10	25	50	10	12	15	20	30	60

Table 1 – Synchrophasor frame rate according to IEEE Std C37.118.2™-2011

The standard says: "*The actual rate to be used shall be user selectable. Support for other reporting is permissible, and higher rates such as 100 frames/s or 120 frames/s and rates lower than 10 frames/s such as 1 frame/s are encouraged*".
That is, the minimum accepted may be 1 frame per second.

4 Threats in a Cloud Environment

While, on one hand, cloud computing is capable of offering huge benefits to Smart Grid systems in terms of IT cost saving and reliability. On the other hand, it opens to a number of security risks that cannot be underestimated. As evidenced by Coppolino et al. [2], applications running in the untrusted cloud are exposed to well-known attacks, which have been around for years but that gained prominence again because of the large adoption of cloud computing. These include attacks aiming at violating: i) availability by, e.g., flooding targeted machines (Denial of Service (1)); ii) data confidentiality/integrity by, e.g., altering communication channels [21] (Traffic Hijacking (2)) or landing on the system to subsequently launch an attack (Account Hijacking (3)). Besides these, the taxonomy considers other attacks, which in turn are typical of the cloud universe. That is, those perpetrated by:

- Internal users who own a Virtual Machine (VM) and exploit flaws in the hypervisor (Shared Technologies Vulnerabilities (4)) to attack another VM instance.
- The Cloud Provider – embodied by disgruntled employees or administrators – that leverages its privileged position to get access to an unprecedented amount of information and on a much greater scale (Malicious Insiders (5)).

The latter is definitely the most worrisome category of attackers who can easily cover their actions and go undetected for years. It is even more worrying in the context of Smart Grid since the impact on the external environment could be destructive. Attacks to the integrity, e.g., could have effects on the capability to provide correct commands to the actuators, and also acquire the right measurements from sensors. This entails that operators may assume that the status of the infrastructure is normal since all measured parameters have the expected values but this is not the case. Equally important is the availability of WAMS applications. Attacks like DoS, in fact, may cause corruptions on the status of the infrastructure, hardware failures, and, more importantly monitoring service outage. In the case of critical infrastructures, e.g., this could mean risks to human lives. Finally, attacks to confidentiality would imply that the adversary either infers the current state of the Smart Grid.

5 Proposed Solution

Figure 1 reports the high-level architecture of our proposed solution. PMUs gather data from sensors deployed on-field and send it to different layers of PDCs up to the PDC gateway, at the top. This unit is in charge of encrypting data – in a homomorphic fashion – and, then, establishing a TLS secure communication with its counterpart at cloud level to create an authenticated channel. Hence, the acquired encrypted measurements are sent via this secure channel. At cloud level, the synchrophasor data is received and sent over a distributed message-based bus (e.g., ZMQ) to different Microservices (MS), i.e., small independent software units that interact each other through messages. Microservices are a new way of conceiving applications architectures, which fit much better for distributed applications like those for cloud platforms. In our work, besides providing and storing measurements, MSs perform also those mathematical functions needed by the WAMS case study.

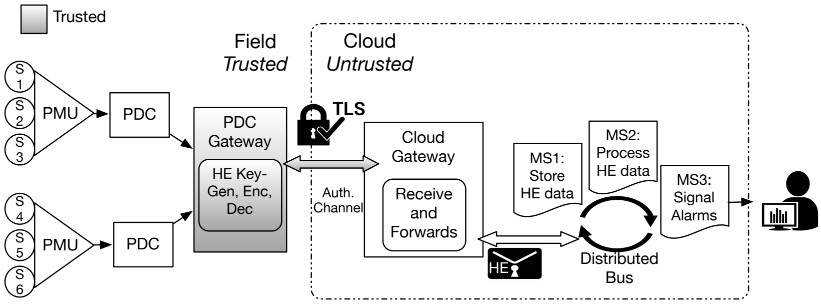


Figure 1 – Proposed Solution

In particular, we identified two mathematical operations to be realized on homomorphic encrypted data for synchrophasor evaluations, i.e.: phase subtraction and phase comparison. From a practical point of view, this meant the definition of a dedicated logical Boolean circuit – composed of gates having homomorphic support – in which ciphered bits will go through to carry out the protected computation.
Figure 2 shows the final scheme of the logical circuit used, which is composed of a full subtractor and a comparator, organized in sequence.

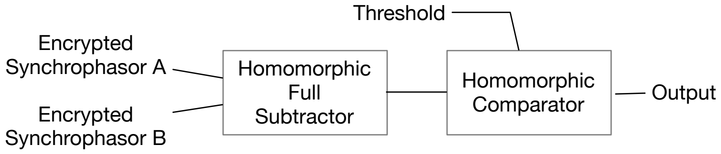

Threshold
Encrypted Synchrophasor A
Encrypted Synchrophasor B
Homomorphic Full Subtractor
Homomorphic Comparator
Output

Figure 2 – Logical circuit for HE synchrophasor evaluations

Our implementation used the widely-accepted APIs of TFHE [13], which is based on the Chillotti et. al HE algorithm [14]. It must be noticed that each gate of the logical circuit introduces an overhead. Hence, particular attention must be put on the number of gate levels to be created. The deeper is the circuit, the higher is the overhead of the overall calculus. To have an idea, we evaluated the execution time of most critical logical gates (e.g. AND, OR, MUX). We obtained that binary gates require on average 8.1ms, while the MUX took 20.4ms using an Intel Xeon E3-1270 v5 CPU with 4 cores at 3.6 GHz, having 8 hyper-threads (2 per core), 8 MB of cache, and 64 GB of memory.

To improve the performance, we took advantage of the bit-wise nature of homomorphic operations and were able to reduce the amount of computations. The system elaborates group of bits from the most significant to the least significant ones. In this way, only in the worst case, the entire word is evaluated. Moreover, we optimized the system by using a particular implementation of Fast Fourier Transform, i.e., FFTW3, which is 3x times faster than the default Nayuki implementation.

Finally, we ran tests on our developed WAMS. We used the OpenDSS comprehensive electrical power system simulation tool for simulating the WAMS data and properly evaluate the homomorphic computations. Results obtained are the following: 330.4ms in the best case and 651.3ms in the worst case. This means that the only standard rate that may be supported by a WAMS having homomorphic encryption is 1 frame per second, i.e., the minimum defined in IEEE Std C37.118.2™-2011.

6 Conclusion

This paper discussed an approach for securing Wide Area Monitoring Systems running in cloud environments, and therefore exposed to dangerous attacks from malicious insiders on sensitive data. The solution proposed leverages homomorphic encryption for executing protected synchrophasor computation. Our goal was to evaluate the feasibility of such an approach and understand the impact on the overall performances. In fact, requirements of data processing rates declared in synchrophasor standards are strict and it is important to verify the compliance of the system that works on homomorphic encrypted data.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreements No 74071 (COMPACT)

References

1. T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Proceedings of CRYPTO 84 on Advances in Cryptology, (New York, NY, USA), pp. 10–18, Springer- Verlag New York, Inc., 1985

2. L. Coppolino, S. DAntonio, G. Mazzeo, L. Romano, Cloud security: Emerging threats and current solutions, Computers & Electrical Engineering 59 (2017) 126 – 140. doi:http: //dx.doi.org/10.1016/j.compeleceng.2016.03.004
3. P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, pp. 223–238. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999
4. C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proceedings of the Forty first Annual ACM Symposium on Theory of Computing, STOC '09, (New York, NY, USA), pp. 169–178, ACM, 2009
5. M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers." Cryptology ePrint Archive, Report 2009/616, 2009. http://eprint.iacr.org/2009/616
6. M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, CCSW '11, (New York, NY, USA), pp. 113–124, ACM, 2011
7. R. Jayaram Masti, C. Marforio, and S. Capkun, "An architecture for concurrent execution of secure environments in clouds," in Proceedings of the 2013 ACM Workshop on Cloud Computing Security Workshop, ser. CCSW '13. New York, NY, USA: ACM, 2013, pp. 11–22. [Online]. Available: http://doi.acm.org/10.1145/2517488.2517489
8. P. Maene, J. Gotzfried, R. de Clercq, T. Muller, F. Freiling, and I. Verbauwhede, "Hardware-based trusted computing architectures for isolation and attestation," IEEE Transactions on Computers, vol. PP, no. 99, pp. 1–1, 2017
9. F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative Instructions and Software Model for Isolated Execution," in Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, ser. HASP, 2013
10. D. Anderson et al., "GridCloud: Infrastructure for Cloud-based Wide Area Monitoring of Bulk Electric Power Grids," in IEEE Transactions on Smart Grid. doi:10.1109/TSG.2018.2791021
11. Open Source PDC https://github.com/GridProtectionAlliance/openPDC
12. W. R. Claycomb, A. Nicoll, Insider threats to cloud computing: Directions for new research challenges, in: 2012 IEEE 36th Annual Computer Software and Applications Conference, 2012, pp. 387– 394. doi:10.1109/COMPSAC.2012.113
13. TFHE: Fast Fully Homomorphic Encryption Library over the Torus https://github.com/tfhe/tfhe
14. I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Asiacrypt 2016, pages 3-33
15. F. Campanile et al., "Cloudifying Critical Applications: A Use Case from the Power Grid Domain," 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), St. Petersburg, 2017, pp. 363-370. doi: 10.1109/PDP.2017.50
16. S. Brenner, T. Hundt, G. Mazzeo, and R. Kapitza, "Secure Cloud Micro Services using Intel SGX," in Proceedings of the 17th International IFIP Conference on Distributed Applications and Interoperable Systems (DAIS'17), 2017
17. Cerullo, G., Mazzeo, G., Papale, G., Sgaglione, L., Cristaldi, R.: A secure cloud-based SCADA application: the use case of a water supply network. In: Proceedings of the Fifteenth New Trends in Software Methodologies, Tools and Techniques, SoMeT 2016, Larnaca, Cyprus, 12–14 September 2016, pp. 291–301 2016
18. Alabdulatif, A, Kumarage, H, Khalil, I, Atiquzzaman, M and Yi, X 2017, 'Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure', IET Wireless Sensor Systems, pp. 1-11

19. Flora Amato, Francesco Moscato, Exploiting Cloud and Workflow Patterns for the Analysis of Composite Cloud Services, Future Generation Computer Systems, Volume 67, 2017, Pages 255-265, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.06.035
20. Flora Amato and Francesco Moscato. 2015. A model driven approach to data privacy verification in E-Health systems. Trans. Data Privacy 8, 3 (December 2015), 273-296
21. Flora Amato, Francesco Moscato, Exploiting Cloud and Workflow Patterns for the Analysis of Composite Cloud Services, Future Generation Computer Systems, Volume 67, 2017, Pages 255-265, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.06.035