# Towards An Anonymous Incident Communication Channel for Electric Smart Grids

Anna Triantafyllou
Department of Informatics and Telecommunications Engineering, University of Western Macedonia
Kozani
atriantafyllou@uowm.gr

Panagiotis Sarigiannidis
Department of Informatics and Telecommunications Engineering, University of Western Macedonia
Kozani
psarigiannidis@uowm.gr

Antonios Sarigiannidis
Sidroco Holdings Ltd
Limassol, Cyprus
asarigia@sidroco.com

Erkuden Rios
Fundacion Tecnalia Research & Innovation
Derio, Spain
Erkuden.Rios@tecnalia.com

Eider Iturbe
Fundacion Tecnalia Research & Innovation
Derio, Spain
Eider.Iturbe@tecnalia.com

## ABSTRACT

The Electric Smart Grid (ESG) is an intelligent critical infrastructure aiming to create an automated and distributed advanced energy delivery network, while preserving information privacy. This study proposes the implementation of an Anonymous Incident Communication Channel (AICC) amongst smart grids across Europe to improve situational awareness and enhance security of the new electric intelligent infrastructures. All participating organizations will have the ability to broadcast sensitive information, stored anonymously in a repository, without exposing the reputation of the organisation. This work focuses on the requirements of establishment, the possible obstacles and proposed data protection techniques to be applied in the AICC. Furthermore, a discussion is conducted regarding the documentation of cyber-incidents. Last but not least, the benefits and the potential risks of this AICC concept are also provided.

## CCS CONCEPTS

• **Information systems**; • **Security and privacy**;

## KEYWORDS

Smart Grid, anonymity, group signature, anonymous repository of incidents

**ACM Reference Format:**
Anna Triantafyllou, Panagiotis Sarigiannidis, Antonios Sarigiannidis, Erkuden Rios, and Eider Iturbe. 2018. Towards An Anonymous Incident Communication Channel for Electric Smart Grids. In *22nd Pan-Hellenic Conference on Informatics (PCI '18), November 29-December 1, 2018, Athens, Greece.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3291533.3291559


*PCI '18, November 29-December 1, 2018, Athens, Greece*

ACM ISBN 978-1-4503-6610-6/18/11…$15.00
https://doi.org/10.1145/3291533.3291559

## 1 INTRODUCTION

The Electric Smart Grid (ESG) is the evolution of the traditional electric grid, focusing on generating and conditioning electricity, while efficiently distributing, controlling and monitoring it in real-time. Being beneficial not only to the power industries, but also the consumers, ESG also aims to preserve information privacy and offer protection against intrusions. Due to its vast scale, it is reasonable to expect many vulnerabilities to exist. Recently the power system has faced several cyber attacks which have raised the question regarding the security vulnerabilities and its large impact on the system's productiveness and integrity [5]. A detailed research on cyber attack models for ESG environments is presented in [13]. Offenders can be either elite hackers, terrorists, employees, competitors, or even customers [28]. Since the ESG is a hybrid of the power system and a communication network, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are critical for countering cyber-attacks concerning either the physical power system or the communication network or both. Information sharing can greatly benefit these kind of systems. It is envisioned that early detection and open information sharing between all smart grid operators can greatly reduce the cost of data breaches [31]. Many organizations are willing to join such communities of trust to better protect themselves from cyber threats and maintain a strong cyber security posture [35]. Based on these assumptions and in order to improve situational awareness and enhance the security of ESG, an Anonymous Incident Communication Channel (AICC) is proposed. The rationale behind the creation of this channel is to create and maintain a repository to broadcast, inform and exchange critical information about cyber-attack incidents in smart grids across Europe. The repository of incidents will be developed in line with similar organisations such as the EE-ISAC [14] and the ESMIG [17]. AICC will provide the opportunity to contributing organisations across Europe to broadcast sensitive information in an anonymous way without exposing the reputation of the organisation. However, the technical details of the attack will be available for everyone to take timely countermeasures. Despite the numerous advantages it may offer, the AICC requires careful planning. At this time there are country-driven cyber incident repositories, but neither of them is focused on Smart Grid security.

A. Triantafyllou, P. Sarigiannidis, A. Sarigiannidis, E. Rios, and E. Iturbe, "Towards an anonymous incident communication channel for electric smart grids," in Proceedings of the 22nd Pan-Hellenic Conference on Informatics - PCI '18, 2018, doi: 10.1145/3291533.3291559.

The published version is available at ACM Digital Library: https://dl.acm.org/doi/10.1145/3291533.3291559

This study focuses on the requirements of establishment and data protection techniques to be applied in the AICC. The rest of the paper is organized as follows: In Section II related works will be examined, in Section III the requirements of establishing the AICC will be discussed, in Section IV the data protection techniques proposed for the AICC will be analysed, in Section V the benefits concerning this endeavour will be presented, while in Section VI a discussion on potential risks will take place. Finally the paper is concluded in section VII.

## 2 EXISTING INFORMATION SHARING PARADIGMS

Information sharing among industry asset owners and vendors could help prevent, detect or counter cyber, personnel and physical security threats. Until now there have been a few information sharing efforts towards this direction.

The Homeland Security Information Network (HSIN) of the U.S. is resposible for sharing sensitive but unclassified information, while managing operations and sending alerts and notices [37]. The National Cybersecurity and Communications Integration Center (NCCIC) is another endeavour aiming to reduce the risk of systemic cybersecurity by served as a national hub for cyber and communications information, technical expertise, and operational integration. Moving on, in the U.S. Department of Enegy, the Infrastructure Security and Energy Restoration (ISER) program [12] enhances the readiness, resiliency, and recovery of the U.S. energy infrastructure. Accordingly in Europe there is EE-ISAC. Another similar repository of incidents is the Industrial Security Incident Database (ISID), a collection of known cybersecurity events that have occurred against control systems in the manufacturing and critical infrastructure industries [8]. Failure to adapt to the changing landscape of security threats and vulnerabilities will leave the industrial controls world exposed to increasing numbers of cyber incidents. The result could easily be loss of reputation, environmental impact, production and financial loss, and even human injury. A similarly interesting project is the Vocabulary for Event Recording and Incident Sharing (VERIS) [38]. It is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner, while sharing that information - anonymously and responsibly - with others. Furthermore, a quite recent study [23] proposes the implementation of an International Cyber Incident Repository System (ICIRS). It is strongly promoted that this system, if designed, can help inform and eventually mitigate the risks of cyber attacks to participating members. Despite the fact that there are no known continental information-sharing platforms in the world, according to [23], much like in Europe, some countries, such as South Korea [30], Japan [29] and Argentina [20], have established a national CERT, which underscores the fact that basic knowledge of cyber events and responses is available within many countries.

Based on these existing endeavours for information sharing, the AICC is proposed specifically for ESGs' enhancement towards the prevention of cyber-security threats. Improving this intelligent infrastructure is an accomplishment that will greatly benefit the whole community in the near future.

## 3 REQUIREMENTS AND PERCEIVED OBSTACLES

Cyber-threat information sharing faces several challenges. The establishment and maintenance of trust relationships between participants is the basis for efficient collaboration. All partners need to assure the integrity and confidentiality of both submitted data and system contributors, including the desire of contributors to retain control over their data and how it is used [2]. For this purpose, a governing *legal committee* will be appointed, including members of all the partners involved in the channel and repository. The committee's responsibilities will be to set and deal with all the legal and organizational requirements of the participants. It is almost certain to come across restrictions concerning the types of information that the organizations can provide to others, specifically the technical details of a cyber-attack. Settling the rules on information sharing is a delicate process since the imposition of unwarranted or arbitrary restrictions may reduce the usefulness, availability, quality, and timeliness of shared information. In the pursuit of establishing the AICC, *a technical working group* collaborating with the legal committee, should also be appointed. Its members will include experts responsible for developing the repository's data security, access policies and processes. The technical committee will be responsible for describing how the information handling designations will be applied, supervised, and enforced. These procedures should describe the roles, responsibilities, and authorities of all stakeholders [22]. Repository administrators should make judicious use of transparency mechanisms in order to reassure contributors about the security measures in place to protect the data they share. They should do so, moreover, in a way that does not provide a roadmap for malicious actors who might want to obtain and exploit that shared data [2]. Another recommended action would be to develop a pre-registration process that includes a background check based on appropriate criteria. Such a check would allow the repositoryfis governing committee, to approve or disapprove the participation of particular entities. Throughout the establishing process, participating organizations are encouraged to consult with experienced cyber-security personnel and knowledgeable about legal issues, internal business processes, procedures, and systems. Equally important is the adoption of specific data formats and protocols in order to enable automation and allow participants, the basic repository, and tools to exchange threat information at machine speed. Achieving interoperability can require significant time and resources, however if sharing partners require different formats or protocols the whole process is a lot easier. What is more, during the standards development process, early adopters need to accept the risk that it may be necessary to obtain new tools if substantial changes occur to formats and protocols [22]. The most important feature of this project is the anonymity factor. Each smart grid organization - member will have the ability to broadcast sensitive information in an anonymous way without exposing the reputation of the organisation. For instance, a cyber security incident is uploaded to the repository without knowing who the victim is and where the security incident took place. However, the technical details of the attack will be available for everyone to take timely countermeasures. Based on these assumptions the disclosure of participants' sensitive information is safeguarded by default. The

unauthorized expose of information may delay or interrupt an ongoing investigation, endanger information needed for future legal proceedings, or disorder response actions such as botnet takedown operations.

The development of the AICC poses major challenges about the actual functioning of the repository and the channel. In order to meet the goals of this project, information must be easy to understand. A dictionary of terms, ease of access to the system fields, effective visualization and data mining tools could help contributing organizations easily conduct analysis on the available data of cyber-attacks. In the following sections focus is given on the attempt of reaching the desired anonymization of AICC contributors, while exploring the documentation of ESG cyber-incidents so as to be imported in the related repository.

## 4 CYBER-INCIDENT BACKGROUND

IDSs and IPSs in the ESG can greatly benefit in cyber-attack detection concerning either the physical power system or the communication network or both. The AICC will provide a vast amount of valuable information leading to a considerable enhancement in the performance of these systems. The anonymous repository of incidents conducted in strict accordance with all applicable legal and privacy requirements, could help both private and public sector organizations better assess cyber risks, identify effective controls, and improve their cyber risk management practices [1]. In the AICC project, the documentation of cyber incidents will be addressed by the technical committee under the guidance of the legal working group. Each incident uploaded in the repository will have a specific format and will be identified by a unique identification number. The contributor will be anonymous and only the technical details of the incident will be available to the other partners.

According to [1] the technical working group of the AICC should focus on specific data categories in order to establish the desired anonymous information sharing. First of all, a cyber-incident should be characterized by *the type of the attack*. This high level descriptor or tag will differentiate the incident for ease of reference, leaving the capture of specific technical details about the incident to other data categories. Based on these tags, participating organizations can become aware of attack trends that prove to be beneficial to their internal risk awareness training. Another data category to be involved concerns *the level of severity* the incident has caused based on the industry, relative size, and other circumstances of the contributing organization. This kind of information is useful in order to design and differentiate kinds and amounts of meaningful cyber-security insurance by cross referencing the severity of impacts from specific types of events that the sector experiences. Critical information are also considered to be *the cyber risk management practices, regulations and standards compliance approaches* that the partner had in place at the time of an incident. Based on these facts the effectiveness of a particular frameworkfis best practices can be identified and enable comparisons among different types of organizations using the same framework or similar organizations using different frameworks. It is a fact that information about the full profile of a sophisticated cyber-attack tends to emerge over time. For that reason capturing the *timelines* of the incident phases is very important. Equally critical are the information concerning *what assets were implicated, and how,* during the cyber incident. However, many cyber attacks develop over weeks or months, and the date of the original compromise may never be established. Consistent *variations in time-to-control data* among ESGs components can highlight sector-specific cybersecurity strengths and weaknesses such as might be introduced by sector-unique Supervisory Control And Data Acquisition (SCADA) system and other components. Moreover, being able to *specify the attackers motives*, based on the type and volume of data compromised, and what is done with it afterwards, can help identify the risks that may be unique or common and also what controls are or are not effective in mitigating those risks. Essentials would also be the *kind of security tools and methods* used to identify and counter the attack by the contributing organization.

## 5 DESIGN GOALS OF ANONYMOUS, AUTHENTICATED COMMUNICATION

The AICC develops the idea of utilising a network of trust where sensitive information is exchanged between institutes. Beyond the policy approaches, protective technical measures will be used to ensure that shared data can only be associated with an incident and not a contributor. In order to safeguard the anonymity of the information provider and enforce authentication on access control a digital signature technique should be implemented. In addition to provide confidentiality and integrity of the sharing data stored in the repository, a privacy preserving technique should also be applied. Based on modern anonymization technologies the system can be protected against cyber-attacks itself.

### 5.1 Group Signature

There are various techniques which are based on digital signature and use their concept for communication. One of them is the group signature technique, also based on public key cryptography. Group signatures [9] can be concidered as attribute authentication systems containing only one attribute to represent a membership in a group. In terms of digital signatures, the private key is used for creating signatures and the public key is copied and handed out to validate signatures [21].

In a group signature scheme [4] three kinds of participants are included: (a) **the group manager**, for managing the memberships and generating the membership keys of group members (signers). In the AICC project the group manager could an elected member of the technical committee. (b) **the group members**, in our case the contributing organizations, will have separate membership keys, that can be used to sign messages on behalf of the group. (c) **the verifier**, who is the receiver of group signature or anyone who can check the validity of the group signature by the public key of the group. As a member of the group signature, contributors are allowed to generate signatures on behalf of other group members while their identity and location information are not known by a verifier [21]. This ensures privacy, authentication and unlinkability of users. More specifically, a general group signature scheme consists of the following four procedures [4]. Firstly, during the **setup** procedure, the group′s public key, the individual secret keys of the group members, and a secret administration key for the group manager are created. Next is the **signing** procedure based on a probabilistic

algorithm which returns a signature on an amount of data, by using the group member's secret key. Following those a signature can be either **verified**, based on an algorithm which returns whether a signature is correct or **opened** so that the person who signed the data is revealed, with the group manager's secret administration key.

According to [9], a secure group signature scheme should satisfy two basic requirements, anonymity and traceability. Anonymity demands that the identity of the signer should remain unknown to anyone verifying the signature including other group members. On the other hand, traceability offers the group manager the ability of revoking the anonymity of a signer whenever necessary. In case of a dispute, the group manager has the ability to reveal a member who signed by using his administrator secret key. However no other group member can identify the identity of the signer or determine whether multiple signatures are produced by the same group member. Many enhanced group signatures schemes have been proposed until now, like the ones in [18], [40] and [11]. Furthermore, a new property called 'restrictive linkability' was introduced recently in [16], providing a user with control over linkability.

Although group signature is expensive to implement, its existential anonymity, non-repudiation and untraceablility properties make it attractive for the implementation of the anonymous repository of incidents in the AICC project. Aiming to authenticate the identity and ensure the anonymity of contributing organizations, a secure hybrid threshold group signature scheme is proposed to be implemented. In [19], Hung and his colleagues present a new scheme based on the hardness of elliptic curve discrete logarithm problem (ECDLP) with distinguished signing authority to provide all proof of member signing processes. According to this scheme, a Distributed Centre (DC) is established for storing all signatures that calculates some secret parameters needed by signers to create signatures for each transaction. Only the group manager can open the DC when needed. To support this method, two kinds of signer are set, the privilege (n) and the normal. The scheme allows group secret key shares to be kept on limited privilege signers only while allowing new people to join the group without recalculating group public key and easy revocation. Group policy requires that at least t (t less than n) privilege signers must join signing process to make a valid group signature. In the AICC project the group manager could be an elected member of the technical committee, while the privileged members could be a subset of the legal and technical committees. Hung's scheme can provide scaling group without worrying about group secret loss and protection of the group's private key from being revealed by any set of corrupt signers or hackers' threat. It can also reduce the risk of unexpected transaction and provide distinguished signing authority feature of multisignature internally.

However, by using group signature schemes alone, full anonymity can not be ensured in the repository. Group-members can be identified individually by linking or matching uploaded to external data, or by recognizing unique characteristics. In order to ensure the integrity and confidentiality of the data in the repository of incidents a privacy preserving technique is chosen to be used. Generally, many are the approaches to guarantee the privacy of sharing data such as anatomization, anonymization and permutation. Anatomization is

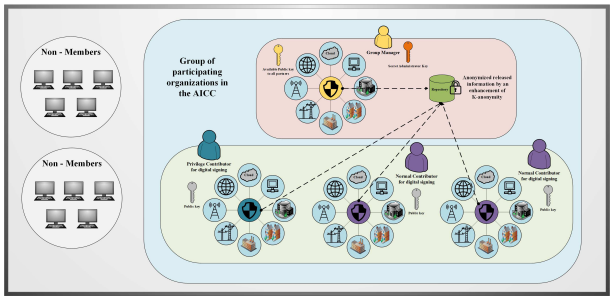


**Figure 1: Realisation of the AICC**

a technique based on grouping sensitive attributes to avoid attribute disclosure using buketization [33]. On the other hand, anonymization focuses on quasi identifiers, and is used to prevent identity disclosure [25]. Anonymization preserves the original structure and field layout of the data so that they look original and realistic. Similarly, perturbation guarantees the privacy of individuals by adding noise to the data, encrypting the data or by swapping of values. Anonymization and perturbation techniques can be considered better when compared to cryptographic techniques in terms of complexity and efficiency for large number of users [41]. Ensuring the privacy of the uploaded data in the AICC project will be implemented by an enhanced k-anonymity technique.

## 5.2 K-anonymity

K-anonymity [34],[36] is a property used to assure that the owner of the data released cannot be re-identified. Its concept was first introduced by Latanya Sweeney and Pierangela Samarati in 1998 [34]. k-anonymity provides privacy protection by guaranteeing that each record in a dataset released relates to at least k individuals even if the released records are directly linked (or matched) to external information. Based on this method, there are at least (k-1) other records in the same release whose values are indistinct over a special set of fields called the quasi-identifier [10]. The quasi-identifier contains those fields that are likely to appear in other known data sets. Each quasi-identifier tuple occurs in at least k records for a dataset with k-anonymity. Regarding the AICC project, each record released will contain a number of data categories, as referred to the previous section, in order to be anonymized.

There are two common methods for achieving k-anonymity, suppression and generalization [36]. Generalization involves replacing (or recoding) a value with a less specific but semantically consistent value. Suppression involves not releasing a value at all. The combination of these techniques can provide safely anonymized data that does not seem to be distorted. In addition, these techniques can provide the most useful data possible, depending on the released data preferences that the receiver has chosen. Furthermore, despite the fact that higher values of k imply a lower probability of re-identification, more distortion to the data is detected, and hence greater information loss. In general, excessive anonymization can minimize the usefulness of the disclosed data, since the analysis produces incorrect results or becomes extremely difficult [15].

Apart from its basic application methods k-anonymity has been studied in order to minimize the drawbacks concerning information

loss and protection against background knowledge attack and homogeneity attacks. Homogeneity attack happens when all records have the same value of sensitive attributes. As mentioned in [6] all anonymization techniques have a common drawback which is the background knowledge attack. As we are not able to predict the level of background knowledge an attacker is having about an individual, we need to compromise slightly with the information loss. In the view of minimizing the amount of information loss, a method called optical k-anonymization [27], [7] was also presented. An optimal anonymization is one which perturbs the input dataset as little as is necessary to achieve -anonymity, where 'as little as is necessary' is typically quantified by a given cost metric. However, these techniques preserve an individual's privacy against only identity disclosure. They do not stop attributes disclosure. Sensitive attributes could be disclosed through various types of attacks such as homogeneity, skewness, and semantic similarity attacks [33]. Aiming to avoid homogeneity attacks, Machanavajjhala and his collegues in [26] showed that, the degree of privacy protection is determined by the number and distribution of distinct sensitive values associated with each equivalence class. To overcome this weakness in k-anonymity, they propose the notion of l-diversity. What is more, Xiao and Tao in [39] proved that l-diversity always guarantees stronger privacy preservation than k-anonymity. The definition of l-diversity requires that each equivalence class be associated with at least l different values for the sensitive attribute [6]. Moreover, although l-diversity is useful against attribute disclosure, it is vulnerable to skewness and similarity attacks. The skewness attack is based on the possible difference in the frequency distribution of the sensitive attribute values within an equivalence class. On the other hand, the similarity attack occurs when the values of the sensitive attribute in an equivalence class are distinct but semantically similar. The authors in [25] presented the definition of t-closeness to counteract these attacks. An equivalence class is said to have t-closeness, if the distance between the distribution of a sensitive attribute in this class and the distribution of the attribute in the whole table is no more than a threshold t. T-closeness effectively limits the amount of individual-specific information an observer can learn. However, this method seems to be more efficient when dealing with numeric attributes. Since the discovery of the ultimate privacy prevention technique is still trending, b-anonymization was recently proposed by Prakash and his colleagues in [32], aiming to improve the efficiency of k-anonymity. This technique is considered to be more efficient than k-anonymity and has higher degree of anonymization. K-anonymity takes more time as it has to compare records with each other in order to form equivalence classes.

In the light of all these methods based on k-anonymity, an enhanced hybrid anonymization approach is proposed to preserve the privacy of data in the repository of incidents of the AICC project. Anatomization through Generalization (AG) proposed in [33], is a combination of the anatomization and anonymization. It utilizes the (l, e) diversity technique, which avoids semantic similarity and homogeneity attacks of sensitive attributes disclosure with high diversity degree, together with generalization and suppression. This technique is considered to be the best choice for the AICC, since its a practical and effective tool for ensuring data privacy against membership, identity and semantic similarity disclosure attacks while maintaining the utility of data. The development of the according k-anonymity technique and group signature protocol should define a single framework that efficiently contributes to the ESG's security. To this end, novel ESG security models will be the stepping stone of constructing the presented authorization policies, keeping in mind the interoperability and integration security challenges of the ESG environment [24].

## 6 BENEFITS OF THE AICC IN ESGS

The AICC enables efficiency enhancement of the ESG infrastructure, while makng it attack resilient. The major asset of the channel is the exchange of real-time security data and analysis, based on the circulation of best countermeasures practices and the comparison of various security solutions both from a technical and operational viewpoint. Benefits are obvious for the participating organizations, since they often face actors that target the same types of systems and information. Cyber defense is most effective when organizations work together to deter and defend against well-organized, capable actors [22]. The anonymous repository can provide the basis for assessments of adversary tactics on the grid, based on techniques and procedures that could link attacks to their respective sources. Information sharing could also be useful in supply chain risk management by highlighting common supply chain cyber-security weaknesses that merit supplier and vendor attention [3]. It can also enable companies to establish a baseline for reasonable cyber-security best practices, by learning about the effectiveness of methods that similar organizations have employed to avoid or re-mediate particular kinds of cyber-incidents. Conclusively, smart grid organizations across Europe participating in the channel will have the ability to rapidly detect and respond to threats. This knowledge enables organizations to speed up processes in their operational environment and diminish the probability of successful attack. As a result, large scale economies are created for network defenders, while adversaries' costs are increasing by forcing them to develop new attack methods.

## 7 POTENTIAL RISKS

While sharing cyber-security information clearly has benefits, certain challenges remain. The establishment of trust between partners is a quite delicate matter, that can be approached by considering all security precautions. Although contributing organizations may fear that other participants might compromise or use their information against them, the AICC project builds upon the anonymity of contributors and preserving the privacy of their data. In case any information is misused or stolen, it would be difficult to trace back to the contributor. Despite the security measures provided by the project, participants are encouraged to evaluate all information to be shared by considering consultation with experienced cyber-security personnel and knowledgeable about legal issues, internal business processes, procedures, and systems. In order to maintain the efficiency and reliability of the AICC and mitigate any potential risk, members need to also follow closely the directions given by the legal and technical committees.

## 8 CONCLUSION

This work proposes the implementation of an Anonymous Incident Communication Channel (AICC) to enhance the reliability and

maintain the integrity of smart grids across Europe. With the guidance of a legal and a technical committee, participating organizations will broadcast sensitive security information in an anonymous way, while safely preserving them in a repository. In order to ensure the anonymity of contributors, a hybrid threshold group signature protocol will be used. In addition, a enhancement of k-anonymity method is proposed to preserve the privacy of the uploaded information. In order to mitigate any potential risks, partners are encouraged to follow all legal regulations regarding information sharing and carefully evaluate all data to be released in the repository.

## ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 787011 (SPEAR).

## REFERENCES

[1] 2015. Enhancing Resilience Through Cyber Incident Data Sharing And Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository. (9 2015). https://www.hsdl.org/?view&did=788825

[2] 2015. Enhancing Resilience Through Cyber Incident Data Sharing And Analysis: Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository. (12 2015). https://www.hsdl.org/?view&did=788824

[3] 2015. Enhancing Resilience Through Cyber Incident Data Sharing And Analysis: Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository. (6 2015). https://www.hsdl.org/?view&did=767778

[4] Aayush Agarwal and Rekha Saraswat. 2013. A Survey of Group Signature Technique, its Applications and Attacks. *International Journal of Engineering and Innovative Technology (IJEIT)* 02 (04 2013). Issue 10.

[5] Adnan Anwar and Abdun Naser Mahmood. 2014. Cyber Security of Smart Grid Infrastructure. *CoRR* abs/1401.3936 (2014). arXiv:1401.3936 http://arxiv.org/abs/1401.3936

[6] S. Athiramol and S. Sarju. 2017. A scalable approach for anonymization using top down specialization and randomization for security. In *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*. 280–283. https://doi.org/10.1109/ICICICT1.2017.8342574

[7] R. J. Bayardo and Rakesh Agrawal. 2005. Data privacy through optimal k-anonymization. In *21st International Conference on Data Engineering (ICDE'05)*. 217–228. https://doi.org/10.1109/ICDE.2005.42

[8] E. Byres, D. Leversage, and N. Kube. [n. d.]. Security Incidents and Trends in the SCADA and Process Industries - A statistical review of the Industrial Security Incident Database (ISID). https://www.controlglobal.com/assets/Media/MediaManager/wp_07_010_symantic_security.pdf Accessed: 2018-06-19.

[9] David Chaum and Eugène van Heyst. 1991. Group Signatures. In *Advances in Cryptology — EUROCRYPT '91*, Donald W. Davies (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 257–265.

[10] Tore Dalenius. 1986. Finding a needle in a haystack or identifying anonymous census records. *Journal of Official Statistics* 2 (1986), 329âĂŞ336.

[11] Hung Dao Tuan, Hieu Minh Nguyen, Cong Manh Tran, Hai Nam Nguyen, and N Moldovyan. 2017. Integrating Multisignature Scheme into the Group Signature Protocol. (11 2017), 294–301.

[12] Department of Energy. [n. d.]. Energy Security. https://www.energy.gov/ceser/activities/energy-security Accessed: 2018-06-19.

[13] Peter Eder-Neuhauser, Tanja Zseby, Joachim Fabini, and Gernot Vormayr. 2017. Cyber attack models for smart grid environments. *Sustainable Energy, Grids and Networks* 12 (2017), 10 – 29. https://doi.org/10.1016/j.segan.2017.08.002

[14] EE-ISAC. [n. d.]. European Energy - Information Sharing and Analysis Centre Home Page. http://www.ee-isac.eu/ Accessed: 2018-06-19.

[15] Khaled El Emam and Fida Dankar. 2008. Protecting Privacy Using k-Anonymity. 15 (07 2008), 627–37.

[16] Sungwook Eom and Jun-Ho Huh. 2018. Group signature with restrictive linkability: minimizing privacy exposure in ubiquitous environment. *Journal of Ambient Intelligence and Humanized Computing* (08 Feb 2018). https://doi.org/10.1007/s12652-018-0698-2

[17] ESMIG. [n. d.]. ESMIG - Who We Are Page. http://esmig.eu/ Accessed: 2018-06-19.

[18] Lein Harn and Feng Wang. 2016. Threshold Signature Scheme without Using Polynomial Interpolation. *I. J. Network Security* 18 (2016), 710–717.

[19] Dao Tuan Hung, Nguyen Hieu Minh, and Nguyen Nam Hai. 2018. A Hybrid Threshold Group Signature Scheme with Distinguished Signing Authority. In *Information Systems Design and Intelligent Applications*, Vikrant Bhateja, Bao Le Nguyen, Nhu Gia Nguyen, Suresh Chandra Satapathy, and Dac-Nhuong Le (Eds.). Springer Singapore, Singapore, 64–72.

[20] ICIC (Programa Nacional de Infraestructuras CrÃŋticas de InformaciÃşn y Ciberseguridad). [n. d.]. QuÃĺ Hacemos. http://www.icic.gob.ar/ Accessed: 2018-06-19.

[21] Joshua J Tom, Boniface Alese, F Aderonke, Thompson , Promise Nlerum, and Anebo D. 2018. Performance and Security of Group Signature in Wireless Networks. (05 2018).

[22] Christopher S. Johnson, Mark L. Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. 2016. Guide to Cyber Threat Information Sharing. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[23] A. L. Joyce, N. Evans, E. A. Tanzman, and D. Israeli. 2016. International cyber incident repository system: Information sharing on a global scale. In *2016 International Conference on Cyber Conflict (CyCon U.S.)*. 1–6. https://doi.org/10.1109/CYCONUS.2016.7836618

[24] G. Kostopoulos, N. Sklavos, and O. Koufopavlou. 2007. *Security in Distributed, Grid, Mobile, and Pervasive Computing:A State-of-the-Art, Book Chapter: Security in Distributed, Grid, and Pervasive Computing*. Auerbach Publications, Boston, MA, USA.

[25] N. Li, T. Li, and S. Venkatasubramanian. 2007. t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In *2007 IEEE 23rd International Conference on Data Engineering*. 106–115. https://doi.org/10.1109/ICDE.2007.367856

[26] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. 2006. L-diversity: privacy beyond k-anonymity. In *22nd International Conference on Data Engineering (ICDE'06)*. 24–24. https://doi.org/10.1109/ICDE.2006.1

[27] Adam Meyerson and Ryan Williams. 2004. On the Complexity of Optimal K-anonymity. In *Proceedings of the Twenty-third ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS '04)*. ACM, New York, NY, USA, 223–228. https://doi.org/10.1145/1055558.1055591

[28] F. G. MÃąrmol, C. Sorge, O. Ugus, and G. M. PÃľrez. 2012. Do not snoop my habits: preserving privacy in the smart grid. *IEEE Communications Magazine* 50, 5 (May 2012), 166–172. https://doi.org/10.1109/MCOM.2012.6194398

[29] National Information Security Center. 2015. National Center of Incident Readiness and Strategy for Cybersecurity Home Page. http://www.nisc.go.jp/eng/index.html Accessed: 2018-06-19.

[30] National Intelligence Service Korea. 2016. NIS Home Page. http://www.nis.go.kr/AF/1_7.do Accessed: 2018-06-19.

[31] L. Ponemon. [n. d.]. Cost of Data Breaches Rising Globally, Says âĂŸ2015 Cost of a Data Breach Study: Global Analysis. https://securityintelligence.com/cost-of-a-data-breach-2015/ Accessed: 2018-06-19.

[32] B. Prakash, S. Kranthi Reddy, Daljit Singh, VBV Phani Sai Yeshwanth, and Mutukulloju Sai Kumar. 2018. B-Anonymization: Privacy beyond k-Anonymization and l-Diversity. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)* 06 (03 2018). Issue 03.

[33] R. Saeed and A. Rauf. 2018. Anatomization through generalization (AG): A hybrid privacy-preserving approach to prevent membership, identity and semantic similarity disclosure attacks. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. 1–7. https://doi.org/10.1109/ICOMET.2018.8346323

[34] Pierangela Samarati and Latanya Sweeney. 1998. *Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression.* Technical Report.

[35] Oscar Serrano, Luc Dandurand, and Sarah Brown. 2014. On the Design of a Cyber Security Data Sharing System. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security (WISCS '14)*. ACM, New York, NY, USA, 61–69. https://doi.org/10.1145/2663876.2663882

[36] Latanya Sweeney. 2002. Achieving K-anonymity Privacy Protection Using Generalization and Suppression. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* 10, 5 (10 2002), 571–588. https://doi.org/10.1142/S021848850200165X

[37] U.S. Department of Homeland Security. [n. d.]. Homeland Security Information Network (HSIN). https://www.dhs.gov/homeland-security-information-network-hsin Accessed: 2018-06-19.

[38] VERIS - Vocabulary for Event Recording and Incident Sharing. [n. d.]. VERIS Home Page. http://veriscommunity.net/index.html Accessed: 2018-06-19".

[39] Xiaokui Xiao and Yufei Tao. 2006. Anatomy: Simple and Effective Privacy Preservation. In *VLDB*.

[40] Yuan-Lung Yu and Tzer-Shyong Chen. 2005. An efficient threshold group signature scheme. *Appl. Math. Comput.* 167, 1 (2005), 362 – 371. https://doi.org/10.1016/j.amc.2004.06.089

[41] Bin Zhou, Jian Pei, and WoShun Luk. 2008. A Brief Survey on Anonymization Techniques for Privacy Preserving Publishing of Social Network Data. *SIGKDD Explor. Newsl.* 10, 2 (12 2008), 12–22. https://doi.org/10.1145/1540276.1540279