Azerbaijan Journal of High Performance Computing, Vol 2, Issue 1, 2019, pp. 7-28
https://doi.org/10.32010/26166127.2019.2.1.7.28

Towards An Anonymous Incident Communication Channel for Electric Smart Grids

Anna Triantafyllou[1], Panagiotis Sarigiannidis[1], Antonios Sarigiannidis[2], Erkuden Rios[3], Eider Iturbe[3]

[1]Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 50100, Greece, atriantafyllou@uowm.gr, psarigiannidis@uowm.gr
[2]Sidroco Holdings Ltd, Limassol, Cyprus 3113, asarigia@sidroco.com
[3]Fundacion Tecnalia Research and Innovation, Derio, Spain E-20009, Erkuden.Rios@tecnalia.com, Eider.Iturbe@tecnalia.com

*Correspondence:
Panagiotis Sarigiannidis,
Department of Informatics
and Telecommunications
Engineering, University
of Western Macedonia,
Kozani 50100, Greece,
psarigiannidis@uowm.gr

Abstract

The Electric Smart Grid (ESG) is referred to as the next generation electricity power network. It is an intelligent critical infrastructure aiming to create an automated and distributed advanced energy delivery network while preserving information privacy and offering protection against intrusions. This study proposes the implementation of an Anonymous Incident Communication Channel (AICC) amongst smart grids across Europe to improve situational awareness and enhance the 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 organization. However, the technical details of the attack will be available for everyone to take appropriate countermeasures. The advantages of the AICC are the exchange of real-time security data and analysis, the circulation of best countermeasures practices, the comparison of various security solutions both from a technical and operational viewpoint and the ability to establish an open dialogue amongst anonymous peers who represent smart grid organizations (e.g., power plants) across Europe. This work focuses on the requirements of establishment, the possible obstacles, and proposed data protection techniques to be applied in the AICC. Furthermore, were explained some details of the documentation of cyber-incidents Last but not least, were also provided the benefits and the potential risks of this AICC concept.

Keyword: Smart Grid; anonymity; group signature; anonymous repository of incidents;

1. Introduction

Today the demand for electricity has gradually increased, while the electrical infrastructure has remained unchanged. The traditional power distribution network is considered to be very complicated and unsuitable to the needs of the 21st Century. To address the growing population, energy storage problems, and the demand for energy, we introduced a new grid infrastructure. The Electric Smart Grid (ESG) is the evolution of the traditional electric grid, focusing on generating and conditioning electricity, while efficiently distributing and controlling it. The principal part of the ESG that makes it smart is its Advanced Metering Infrastructure (AMI). The AMI infrastructure aims to provide reliability through real-time monitoring and efficiency in power management in cooperation with a Supervisory Control and Data Acquisition

(SCADA) system. SCADA is a control system inside the ESG, consisted of two subsystems, the energy management system (EMS) and the distribution management system (DMS) [1]. It is a system that combines both hardware and software components. The ESG infrastructure being beneficial not only to the power industries but also the consumers aims to preserve information privacy and offer protection against intrusions. However, considering its vast scale, it is reasonable to expect many vulnerabilities to exist.

In recent years, the power system has faced several cyber- attacks raising attention towards security vulnerabilities and its tremendous impact on the critical power system infrastructure [2]. The data transferred across the ESG contain sensitive information, which, if not protected from the hands of data thieves would compromise the systems productiveness and integrity. To launch an attack, the offender must first exploit entry points, and upon successful entry, different kinds of cyber-attacks can be delivered on the ESG infrastructure. Cyber-attacks could be initiated based either on device exploitation or vulnerabilities of the communication infrastructure. Offenders can be script kiddies, elite hackers, terrorists, employees, competitors, or even customers [3]. It is a fact that cyber-attacks become damaging once intruders gain access to the SCADA network. Figure 1 presents the most common cyber-attacks in the ESG environment.

Since the Smart Grid network is a hybrid of the power system and a communication network, Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are

Critical for detecting attacks concerning the communication network, while SCADA focuses on coordinating the security of the physical power system. Information sharing can significantly benefit these kinds of systems to counteract sophisticated cyber-attacks. Researchers envisioned that early detection and open information sharing between all smart grid operators could significantly reduce the cost of data breaches [5]. Many organizations are willing to join such communities of trust to protect themselves from cyber-threats better and maintain a robust cyber security posture [6].

Based on these assumptions and 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 organizations such as the EE-ISAC and the ESMIG. EE-ISAC is a joint initiative of 4 major European utility companies, together with universities, governmental bodies, and technology providers [7]. This initiative

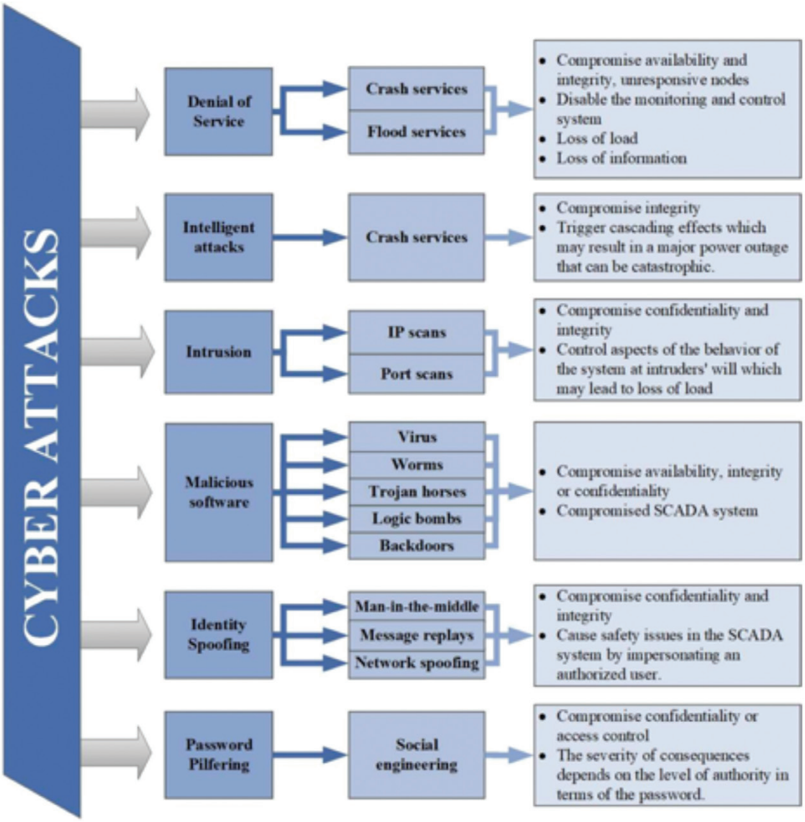

CYBER ATTACKS
Denial of Service
Crash services
Flood services
• Compromise availability and integrity, unresponsive nodes
• Disable the monitoring and control system
• Loss of load
• Loss of information
Intelligent attacks
Crash services
• Compromise integrity
• Trigger cascading effects which may result in a major power outage that can be catastrophic.
Intrusion
IP scans
Port scans
• Compromise confidentiality and integrity
• Control aspects of the behavior of the system at intruders' will which may lead to loss of load
Malicious software
Virus
Worms
Trojan horses
Logic bombs
Backdoors
• Compromise availability, integrity or confidentiality
• Compromised SCADA system
Identity Spoofing
Man-in-the-middle
Message replays
Network spoofing
• Compromise confidentiality and integrity
• Cause safety issues in the SCADA system by impersonating an authorized user.
Password Pilfering
Social engineering
• Compromise confidentiality or access control
• The severity of consequences depends on the level of authority in terms of the password.

Fig. 1: The most common cyber-attacks in the ESG [4]

aims to improve the cybersecurity and integrity of the grid by enabling trust-based data and information sharing. ESMIG is the representative of European companies which provide products, information technology, and services regarding multi-commodity metering, display, and management of energy consumption and production at consumer premises [8]. AICC will provide the opportunity for contributing organizations across Europe to broadcast sensitive information anonymously without exposing the reputation of the organization. However, the technical details of the attack will be available for everyone to take appropriate countermeasures. The advantages of the AICC are the exchange of real-time security data and analysis, the circulation of best countermeasures practices, the comparison of various security solutions both from a technical and operational viewpoint and the ability to establish an open dialogue amongst anonymous peers who represent smart grid organizations (e.g., power plants) across Europe. At this time, there are country-driven cyber incident repositories, but neither of them is focused on Smart Grid security.

This paper extends our previous work in [9] focusing on the perceived obstacles, the establishment, and the data protection techniques to be applied in the AICC. The extended work includes a more detailed presentation of the related work, the proposed data protection techniques, and enhanced bibliographic research regarding the variations of each technology during evolution. Furthermore, essential figures are provided for better understanding the concept of the AICC and the deployment of the technologies proposed. Moreover, the focus is given on the necessary components and functions of the ESG infrastructure to draw attention on existing vulnerabilities and in parallel emphasize the need for the implementation of a network of trust between contributing organizations. Last but not least, a brief categorization of the most common cyber- attacks in the ESG environment is presented.

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 analyzed, in Section V will present the benefits concerning this endeavour, 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 the trusted network for security mission operations to share sensitive information. HSIN is used to manage operations, analyze data, and send alerts and notices [10]. The Trusted Automated Exchange of Indicator Information (TAXII) is a community-driven effort that enables threat information sharing between trusted entities in the HSIN. The TAXII information is represented in XML-based Structured Threat Information Expression (STIX) language. STIX is an expressive, flexible, and extensible XML-based language that conveys potential cyber-threat information. TAXII is coordinated by MITRE, a not-for-profit organization that is leading various efforts in the security information sharing space [11]. The National Cybersecurity and Communications Integration Center (NCCIC) of the U.S. is another endeavor aiming to reduce the risk of systemic cybersecurity and communications challenges. Since 2009, NCCIC operated as a national center for cyber and communications information, technical expertise, and operational integration. Throughout 2017, NCCIC integrated like the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [12]. This structure enhances the effectiveness of NCCICs cybersecurity and communications mission based on these legacy organizations.

Moving on, in the U.S. Department of Energy, the Infrastructure Security and Energy Restoration (ISER) program takes the lead in emergency support under the National Response Framework [13]. It is up to the Energy Sector-Specific Agency for national efforts, in cooperation with public and private sector stakeholders, to enhance 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 in the manufacturing and critical infrastructure industries. The ISID data indicates that organizations that operate Supervisory Control and Data Acquisition (SCADA) and control systems should be concerned about cybersecurity. Not only has the number of incidents increased dramatically in the past five years, but the seriousness of these events appears to be growing as well [14]. Besides, the cost of an incident can be substantial. It is a fact that failing to adapt to the changing landscape of security threats and vulnerabilities will lead to the exposure of the industrial controls world to increasing numbers of cyber incidents. The result could come easily.

Be a loss of reputation, environmental impact, production, and financial loss, and even human injury.

A similarly exciting project is the Vocabulary for Event Recording and Incident Sharing (VERIS) [15]. It is a framework designed to guide the description of security incidents in a structured and repeatable manner. VERIS deals with the lack of quality information. It helps organizations to collect useful incident-related information and to share that information - anonymously and responsibly - with others.

Furthermore, a recent study [16] proposes the implementation of an International Cyber Incident Repository System (ICIRS). It is actively promoted that this system is designed, can help inform and eventually mitigate the risks of cyber- attacks to participating members. Members (governments or organizations) will be able to share information on both attempted and prior successful attacks while accessing and making use of that data to adapt to potential new security issues. Despite the fact that there are no known continental information-sharing platforms in the world, according to [16], much like in Europe, many countries, such as Australia [17], South Korea [18], Japan [19], South Africa [20], and Argentina [21], 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 endeavors for information sharing, the AICC is explicitly proposed for ESGsJ enhancement towards the prevention of cyber-security threats. Improving this intelligent infrastructure is an accomplishment that will significantly 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 [22]. 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 sure 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 [23]. Repository administrators should use transparency mechanisms judiciously

to reassure contributors about the efficient operation of security measures towards protecting 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 [22]. 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 repository’s 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 to enable automation and allow participants, the central repository, and tools to exchange threat information at machine speed. The automation of security data sharing aims to simplify and speed up the exchange, documentation, assessment, or remediation of security information [11]. Achieving interoperability can require significant time and resources, especially if sharing partners require different formats or protocols. Identifying threat information sources and entry points in the smart grids of each participating organization is a key step for this process. Taking advantage of knowledge gaps can provide a better understanding of what is needed. Also, 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 [23].

The most important feature of this project is the anonymity factor. Each smart grid organization - member, will have the ability to broadcast sensitive information anonymously without exposing the reputation of the organization. For instance, a cybersecurity 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 appropriate 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.

Regardless the basic rule of anonymization inside the channel, it would be wise for partners to handle specifications to shared information and implement policies, procedures, and technical controls to actively manage the risks of exposing sensitive information.

The development of the AICC poses significant challenges about the actual functioning of the repository and the channel. The technical team faces demanding implementation concerns that ought to be presented in a user-friendly way to the board of contributors. Repository developers could design questions for a repository input template that are relevant and easy to understand and to answer [22]. They could also consider providing data collection guidance that will allow the legal committee to approve the release of the information prior to sharing it into the repository. 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 efficiently analyze the available data of cyber-attacks. Figure 2 presents a sample of information to be stored regarding a cyber-attack by participating organizations in the anonymous repository. To protect confidentiality, appropriate repository usage should be clarified and controlled, such as enforcing prohibitions against downloading all its data or selling aggregated information. Besides, designers should consider adopting role-based access control for data display and performing metrics assessing the performance of the repository itself.

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 to be imported in the related repository.

4. Cyber-incident background

The ESG is an integration of one or more regional control centers, with each center supervising the operation of multiple power plants and substations [24]. A regional control center is a central location for analysis and control over some region of the grid, concerning either generation, transmission, or distribution [25]. Control centers typically include SCADA servers, Energy Management Systems (EMS) and Human Machine Interfaces (HMI) to monitor Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs) for gathering data from the field. What is more, the Advanced Metering Infrastructure is an integration of many technologies, providing smart connections among system operators and customers. Notably, all kinds of data being transferred across the ESG contain sensitive information, which, if not protected from the hands of data thieves would compromise the efficiency and integrity of the system. In fact, strong perimeter defense is used to prevent external adversaries from accessing information or devices within the trusted grid zone. However, as previously discussed, the size and complexity of grid networks bring forward numerous vulnerabilities as potential entry points for infiltration.

To achieve high-level availability and flexible communication architecture for the ESG is critical to mitigating attacks. Authentication, cryptographic procedures, and key management are necessary countermeasures in the ESG for protecting information confidentiality and integrity. Since the smart grid network is a hybrid of the power system and a communication network, IDSs and IPSs are critical for detecting attacks concerning the communication network, while SCADA focuses on coordinating the security of the physical power system. The AICC will provide a vast amount of valuable information leading to a considerable enhancement in the performance of IDSs and IPSs. The construction of the anonymous repository of incidents in strict accordance with all applicable legal and privacy requirements could help both private and public sector organizations better assess cyber risks, identify adequate controls, and improve their cyber risk management practices [26].

When a security incident occurs in the ESG, it is debatable what kind of information should be recorded about the incident. Nowadays, cyber incident collected data are mainly driven by compliance for reporting requirements. These results in missing valuable information or information are not recorded in a way that makes analysis easy [27]. Many organizations keep track of cybersecurity incidents in databases, in the form of excel spreadsheets, small reports or simple software solutions. Usually, each incident will contain information about when it was created and closed, who the investigator was, incident information (vector, machine type, etc.), and impact information (hours of investigation, monetary costs, etc.) in both structured entry fields and unstructured text descriptions of the incident. 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.

Based on the directions given by the Department of Homeland Security [26] the technical working group of the AICC should focus on specific data categories to establish the desired anonymous information sharing. First of all, a cyber-incident should be characterized by the type of attack. This descriptor or tag will enable the identification of the incident between others, while according to specific technical details, will be acquired by 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 to design and differentiate kinds and amounts of important cyber-security insurance by cross-referencing the severity of impacts from specific types of events that the sector experiences. Critical information is 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 particular frameworks, 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 is the information concerning what assets were implicated, and how, during the cyber incident. Most of the times, the timeline of detection can be uninformative or even misleading for cyber risk management. 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 SCADA 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 afterward, 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. Furthermore, in order to promote the identification of attack patterns, the contributor should include an attempt to identifying the multiple contributing

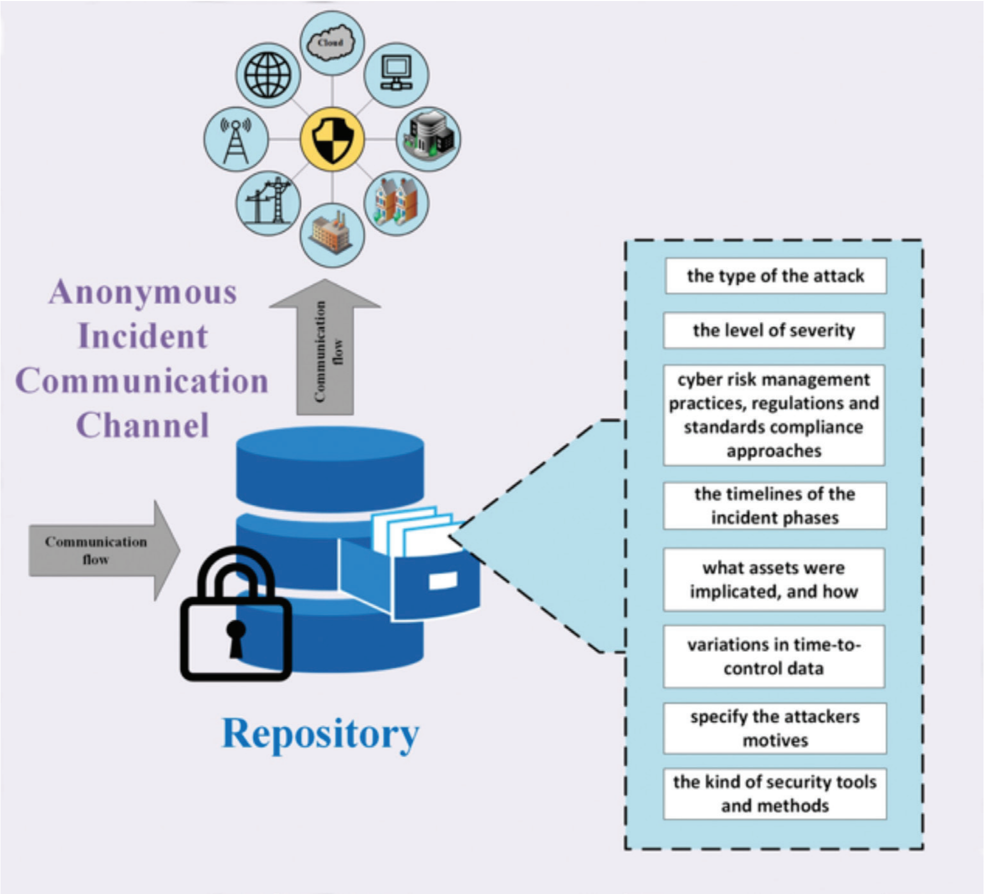

Cloud
Anonymous Incident Communication Channel
Communication flow
Communication flow
Repository
the type of the attack
the level of severity
cyber risk management practices, regulations and standards compliance approaches
the timelines of the incident phases
what assets were implicated, and how
variations in time-to-control data
specify the attackers motives
the kind of security tools and methods

Fig. 2: Cyber-attack information to be exchanged by the AICC repository

causes of the incident uploaded. It should include consistent input fields for both contributing organizations and related third-party provider control failures during each step of the progression of an incident. Any information concerning the lack of the appropriate tools, the failure or ineffective operation of a specific security tool could also prove in being very useful. Last but not least, the contributing organization should mention any long-term actions taken to stop incidents and to prevent similar future occurrences.

5. Design goals of anonymous, authenticated communication

The AICC develops the idea of utilizing 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. To safeguard the anonymity of the information provider and enforce authorization, a digital signature technique should be implemented. Also, 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.

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 can be considered as attribute authentication systems containing only one attribute to represent 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 [28]. Based on this technique, each contributing organization will have a differentiated private key to sign the uploaded data and a common group public key for verifying the signatures made available to all verifiers. Group signature schemes are commonly used in many security applications. This kind of schemes allows any member of a group of signers to sign documents on behalf of the group, while ordinary signature schemes allow only one signer. This concept was first introduced by David Chaum and Eugene van Heyst [29] in 1991.

In a group signature scheme [30] as presented in Figure 3, three kinds of participants are included:

- The group manager, for managing the memberships and generating the membership keys of group members (signers). Group Manager enables signers to sign on behalf of the group and reveals the identity of the originator of the signature when dispute. In the AICC project, the group manager could an elected member of the technical committee.
- The group members: The group member, in our case, the contributing organizations, will have separate membership keys, that can be used to sign messages on behalf of the group.
- The verifier is the receiver of the 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 [28]. The least ensures privacy, authentication, and unlinkability of users. More specifically, a general group signature scheme consists of the following four procedures [30]:

- Setup: a procedure during which the groups public key, the individual secret keys of the group members, and a secret administration key for the group manager are created.
- Sign: a procedure based on a probabilistic algorithm which returns a signature on an amount of data, by using the group members secret key.
- Verify: an algorithm which returns whether a signature is correct, based on an amount of data, the signature produced on them, and the groups public key.
- Open: If necessary, the signature can be opened so that the person who signed the data is revealed. On input, the signature and the group manager's secret administration key are needed.

According to [29], 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 to revoking the anonymity of a signer whenever necessary. In case of a dispute, the group manager can 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 the same group member produces multiple signatures. Deciding whether a signature is from an individual member or not, even after knowing

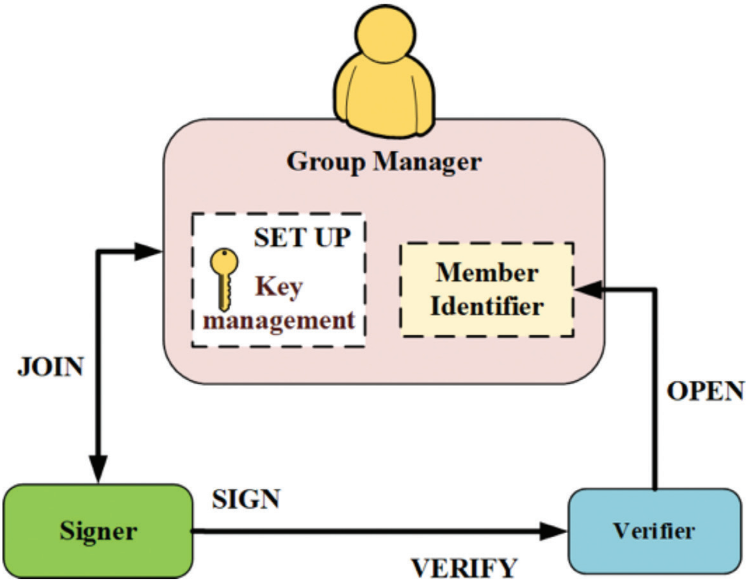


Fig. 3: The group signature scheme interactions

his secret key, must be computationally hard. Valid signatures cannot be forged and can only be created by group members. Given any valid signature, the group manager should be able to trace which user issued the signature. However, given two amounts of data and their signature, the fact that the signatures were from the same signer or not, cannot be concluded. What is more, even if all other group members (and the managers) collude, they cannot forge a signature for a non-participating group member. Last but not least, a revoked member is not able to create valid signatures on behalf of the group.

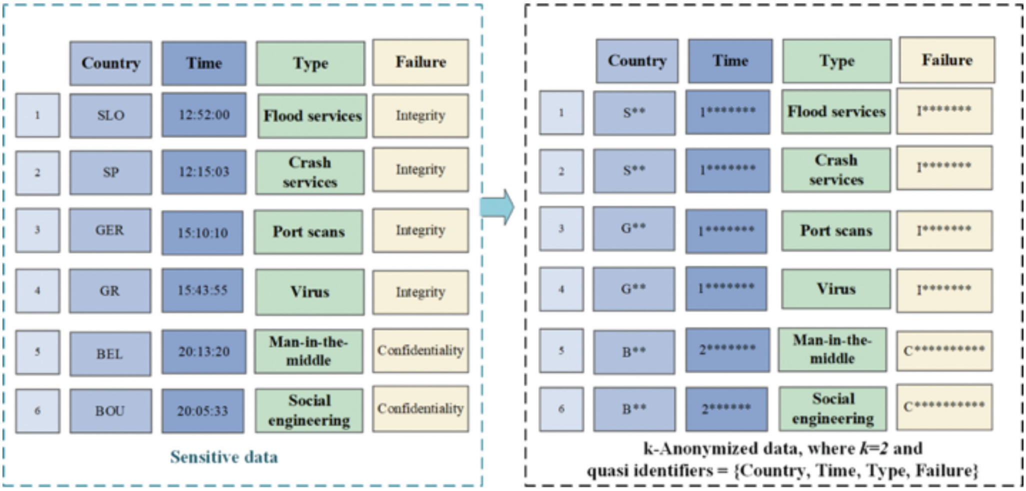
Many enhanced group signatures schemes have been proposed until now, each aiming to improve different aspects and attributes of the original scheme. In 2004, Boneh and his colleagues presented a group signature scheme based on strong Diffie-Hellman (SDH) assumption and Decision Linear assumption [31], whose length is under 200 bytes less than twice the length of an ordinary RSA signature (128 bytes) with comparable security. During that time, another and more efficient group signature scheme was suggested that extended the ability of revocation by the group manager [32]. Regarding the prevention of a single corrupt member illegally authorizing a transaction, various threshold signature schemes were also proposed. In a threshold signature scheme such as the one in [33], the group signature can only be generated when the number of participating group members is larger than or equal to the threshold value. Similar schemes presented in [33], [34], [35], [36], [37] are based on various hard problems such as RSA system, discrete logarithm (DLP), Chinese Remainder Theorem (CRT), ECDLP. However, the ones schemes in [33], [34], [37] are not considered to be secure enough, as studied in [38], [39], [40]. What is more, the group signature scheme in [35] cannot be verified by just one verifier and therefore is not practical.

Furthermore, the work in [41] presents an idea of masking group's private key to prevent group members who can collaborate to recover it but need a trusted party that use all member private keys to construct group signature and so one can argue that does not meet the requirement for non-repudiation. Various previous schemes often assumed the number of users being controlled by an adversary less than threshold number [35], [36], [40], [42] to keep groups private key safe. However, if the number of members grows, secret shared group keys will be delivered to more and more people. Therefore there are more chances for the group signature scheme to be unsecured. Based on this assumption, the research in [43] proposed two new variants of group signature protocols with and without distinguished signing authorities based on the multisignature signature scheme to reduce the signature length significantly signers public keys. The proposed protocols do not include a secret sharing and knowledge proving procedure.

Last but not least, a new property called restrictive linkability was introduced in [44], for a more advanced group signature scheme. It is a property that provides a user with control over linkability. The signer has controlled his linkability to data that he wants, so he can minimize his privacy exposure while providing necessary linkability.

Although group signature is expensive to implement, its existential anonymity, non-repudiation, and untraceability properties make it attractive for the implementation of the anonymous repository of incidents in the AICC project. More specifically, a secure hybrid threshold group signature scheme is proposed to be implemented to authenticate the identity and ensure the anonymity of contributing organizations. In [45], 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 that stores all signatures and 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. Groups' policy requires that at least t (t less than n) privilege signers must join the signing process to make a valid group signature. In the AICC project, the group manager could 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 a 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 hacker's threat. It can also reduce the risk of the unexpected transaction and provide distinct signing authority feature of multisignature internally.

However, by using group signature schemes alone, full anonymity cannot be ensured in the repository. Group- members can be identified individually by linking or matching uploaded to external data, or by recognizing unique characteristics. 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



	Country	Time	Type	Failure
1	SLO	12:52:00	Flood services	Integrity
2	SP	12:15:03	Crash services	Integrity
3	GER	15:10:10	Port scans	Integrity
4	GR	15:43:55	Virus	Integrity
5	BEL	20:13:20	Man-in-the-middle	Confidentiality
6	BOU	20:05:33	Social engineering	Confidentiality

Sensitive data

	Country	Time	Type	Failure
1	S**	1*******	Flood services	I*******
2	S**	1*******	Crash services	I*******
3	G**	1*******	Port scans	I*******
4	G**	1*******	Virus	I*******
5	B**	2*******	Man-in-the-middle	C**********
6	B**	2******	Social engineering	C**********

k-Anonymized data, where *k=2* and quasi identifiers = {Country, Time, Type, Failure}

Fig. 4: K-anonymity example for the AICC implementation

the approaches to guarantee the privacy of sharing data such as anatomization, anonymization, and permutation. Anatomization is a technique based on grouping sensitive attributes to avoid attribute disclosure using buketization [46]. On the other hand, anonymization focuses on quasi-identifiers and is used to prevent identity disclosure [47]. Anonymization preserves the original structure and field layout of the data so that they look original and realistic. Proposed anonymization techniques [48] use two approaches, including suppression, where information is removed from the data and generalization, where information is coarsened into sets.

On the other hand, 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 a large number of users [49]. Ensuring the privacy of the uploaded data in the AICC project will be implemented by an enhanced k-anonymity technique.

2) K-anonymity: K-anonymity [50], [51] 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 [50]. 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 particular set of fields called the quasi-identifier [52]. The quasi-identifier contains those fields that are likely to appear in other known data sets.

3) 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 several data categories, as referred to the previous section, to be anonymized. An example is presented in Figure 4. There are two standard methods for achieving k-anonymity, suppression, and generalization [51], [53]. Generalization involves replacing (or recoding) a value with a less specific but semantically consistent value.

4) Suppression involves not releasing a value at all. The combination of these techniques can provide safely anonymized data that doesn't 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, although higher values of k imply a lower probability of re-identification, more distortion to the data is detected, and hence more significant information loss. In general, excessive anonymization can minimize the usage of the disclosed data since the analysis produces incorrect results or becomes extremely difficult [54]. Apart from its basic application methods, k-anonymity has been studied 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 [55] 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 [56], [57] was also presented. Optimal anonymization is one which perturbs the input dataset as little as is necessary to achieve -anonymity, whereas a given cost metric typically quantifies little as is necessary. Several different cost metrics have been proposed, though most aim in one way or another to minimize the amount of information loss resulting from the generalization and suppression operations that are applied to produce the transformed dataset. The work in [56] demonstrated that optimal k-anonymity is an NP-hard problem; however, heuristic methods such as k-Optimize as given in [57] often yield productive results.

However, these techniques preserve an individual's privacy only against identity disclosure. However, they do not stop attributes disclosure. Sensitive attributes could be disclosed through various types of attacks, such as homogeneity, skewness, and semantic similarity attacks [46]. In a cyber incident database like the AICC repository, sensitive attributes may concern the entry point of the attack, the type of the attack, the assets that were implicated or the kind of security tools being used. Aiming to avoid homogeneity attacks Machanavajjhala and his colleagues in [58] 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 [59] proved that l-diversity always guarantees stronger privacy preservation than k-anonymity. The definition of l-diversity requires that each equivalence class should be associated with at least l different values for the sensitive attribute [55].

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 [47]

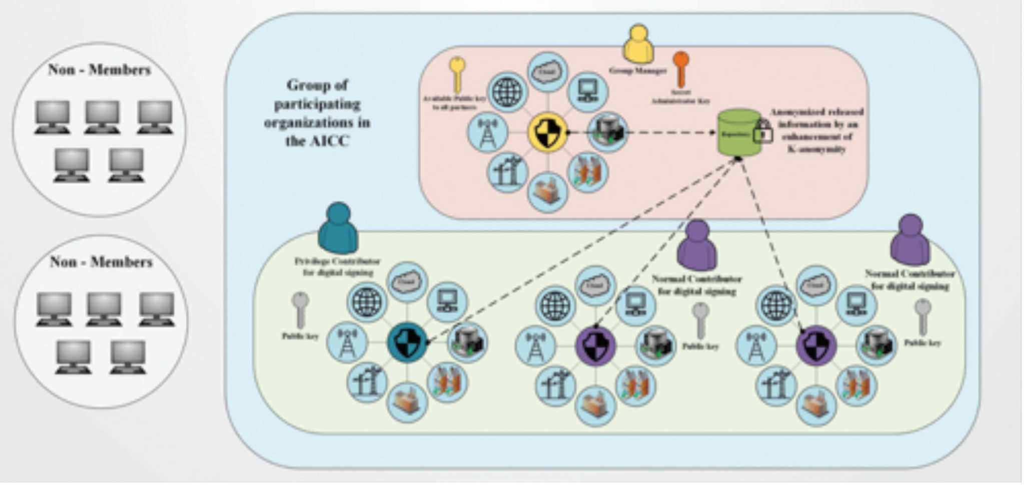

Non - Members
Non - Members
Group of participating organizations in the AICC
Available Public key to all partners
Cloud
Group Manager
Secret Administrator Key
Repository
Anonymized released information by an enhancement of K-anonymity
Privilege Contributor for digital signing
Public key
Normal Contributor for digital signing
Public key
Normal Contributor for digital signing
Public key

Fig. 5: Realisation of the AICC

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 [60], aiming to improve the efficiency of k-anonymity. This technique is considered to be more efficient than k-anonymity and has a higher degree of anonymization. K-anonymity takes more time as it has to compare records with each other to form equivalence classes. This is the part where most of the time is wasted in k-anonymization.

In 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 [46], 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 useful 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 ESGJs security, as presented in Figure 5. 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 [61].

6. Benefits of the aicc in esgs

In the ESG environment, it is expected that the cyber-physical system would be attacked resilient and help to ensure national security. The AICC provides many advantages to enhance the efficiency and reliability of the ESG infrastructure. The primary 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. Information sharing enables them to raise the awareness and security of an entire community. Cyber defense is most effective when organizations work together to deter and defend against well-organized, capable actors [23]. 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. Through knowledge maturation, the value of information that is associated with a specific incident, threat, or threat campaign increases. Information sharing could also be useful chain risk management by highlighting common supply chain cyber-security weaknesses that merit supplier and vendor attention [62]. 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 of cyber-incidents. Conclusively, smart grid organizations across Europe participating in the channel will have the ability to detect and respond to threats rapidly. This knowledge enables organizations to speed up processes inprocesses in their operationaltheir operational environment and diminish the probability of a 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 has benefits, particular challenges remain, as already discussed. 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 a consultation with experienced cyber-security personnel and knowledgeable about legal issues, internal business processes, procedures, and systems. To maintain the efficiency and reliability of the anonymous repository of incidents and mitigate any potential risk, members also need to follow carefully the directions given by the legal and technical committees.

8. Conclusion

The ESG infrastructure combines information technology with power transmission to benefit not only the industry but also the consumers, by facilitating real-time troubleshooting. Due to its vast scale and existing vulnerabilities, the power system has faced several cyber-attacks in the latest years. To enhance the security and reliability of smart grids across Europe an Anonymous Incident Communication Channel (AICC) is proposed. This attempt will enable the participating organizations to broadcast sensitive security information anonymously without exposing the reputation of the organization. The released information will be safely preserved in a repository, available to all partners. Two governing committees will be elected, a legal and a technical one, to settle and maintain the basic rules and technical procedures of the project. To ensure the anonymity of contributors a hybrid threshold group signature protocol will be used. Besides, the enhancement of k-anonymity method is proposed to preserve the privacy of the uploaded information. The primary asset of the AICC 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. Information sharing will raise awareness in cyber-security defense by evaluating the effectiveness of methods and highlight the supply chain risk management weaknesses. 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.

9. Acknowledgment

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

References

[1] Grasberg, L., & Osterlund, L. A. (2001). SCADA EMS DMS-a part of the corporate IT system. In *PICA 2001. Innovative Computing for Power-Electric Energy Meets the Market. 22nd IEEE Power Engineering Society. International Conference on Power Industry Computer Applications (Cat. No. 01CH37195)* (pp. 141-147). IEEE.

[2] Anwar, A., & Mahmood, A. N. (2014). Cyber security of smart grid infrastructure. *arXiv preprint arXiv:1401.3936.*

[3] Marmol, F. G., Sorge, C., Ugus, O., & Pérez, G. M. (2012). Do not snoop my habits: preserving privacy in the smart grid. *IEEE Communications Magazine, 50*(5), 166-172.

[4] Eder-Neuhauser, P., Zseby, T., Fabini, J., & Vormayr, G. (2017). Cyber attack models for smart grid environments. *Sustainable Energy, Grids and Networks, 12,* 10-29.

[5] L. Ponemon, "Cost of data breaches rising globally, "2015 cost of a data breach study: Global analysis," Security Intelligence

[6] Serrano, O., Dandurand, L., & Brown, S. (2014, November). On the design of a cyber security data sharing system. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security* (pp. 61-69). ACM.

[7] EE-ISAC, "European energy - information sharing and analysis center home page," accessed: 2018-06-19. [Online]. Available: http://www.ee-isac.eu/

[8] ESMIG, "Esmig - whom we are page," accessed: 2018-06-19. [Online]. Available: http://esmig.eu/

[9] Triantafyllou, A., Sarigiannidis, P., Sarigiannidis, A., Rios, E., & Iturbe, E. (2018, November). Towards an anonymous incident communication channel for electric smart grids. In *Proceedings of the 22nd Pan-Hellenic Conference on Informatics* (pp. 34-39). ACM.

[10] U.S. Department of Homeland Security, "Homeland security information network (hsin)," accessed: 2018-06-19. [Online]. Available: https: //www.dhs.gov/homeland-security-information-network-hsin

[11] Kampanakis, P. (2014). Security automation and threat information-sharing options. IEEE Security & Privacy, 12(5), 42-51.

[12] U.S. CERT - United States Computer Emergency Readiness Team, "About us page," accessed: 2018-06-19. [Online]. Available: https://www.us-cert.gov/about-us

[13] Department of Energy, "Energy security," accessed: 2018-06-19. [On- line]. Available: https://www.energy.gov/ceser/activities/energy-security

[14] E. Byres, D. Leversage, and N. Kube, "Security incidents and trends in the scada and process industries - a statistical review of the industrial security incident

database (isid)," accessed: 2018-06-19. [Online]. Available: https://www.control-global.com/assets/Media/MediaManager/ wp 07 010 semantic security.pdf

[15] VERIS - Vocabulary for Event Recording and Incident Sharing, "Veris home page," accessed: 2018-06-19". [Online]. Available: http://veriscommunity.net/index.html

[16] Joyce, A. L., Evans, N., Tanzman, E. A., & Israeli, D. (2016, October). International cyber incident repository system: Information sharing on a global scale. In *2016 International Conference on Cyber Conflict (CyCon US)* (pp. 1-6). IEEE.

[17] CERT-Australia, "Frequently asked questions," 2016, accessed: 2018- 06-19. [Online]. Available: https://www.cert.gov.au/faq

[18] National Intelligence Service Korea, "Nis home page," 2016, accessed: 2018-06-19. [Online]. Available: http://www.nis.go.kr/AF/1 7.do

[19] National Information Security Center, "National Center of incident readiness and strategy for cybersecurity home page," 2015, accessed: 2018-06-19. [Online]. Available: http://www.nisc.go.jp/eng/index.html

[20] State Security Agency-Republic of South Africa, "Computer security incident response team (csirt)," 2015, accessed: 2018-06-19. [Online]. Available: http://www.ssa.gov.za/CSIRT.aspx

[21] ICIC (Programa Nacional de Infraestructuras Crticas de Informacin y Ciberseguridad), "Qu hacemos," accessed: 2018-06-19. [Online]. Available: http://www.icic.gob.ar/

[22] "Enhancing resilience through cyber incident data sharing and analysis: Overcoming perceived obstacles to sharing into a cyber incident data repository," 12 2015. [Online]. Available: https: //www.hsdl.org/?view&did=788824

[23] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," October 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/NIST.SP.800-150.pdf

[24] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials, 14*(4), 998-1010.

[25] A. Hahn, "Cybersecurity of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation," 2013. [Online]. Available: https://lib.dr.iastate.edu/etd/13098

[26] "Enhancing resilience through cyber incident data sharing and analysis: Establishing community-relevant data categories in support of a cyber incident data repository," 9 2015. [Online]. Available: https://www.hsdl.org/?view&did=788825

[27] M. Kuypers and E. Pat-Cornell, "Documenting cybersecurity incidents," December 2015.

[28] J. J Tom, B. Alese, F. Aderonke, T., P. Nlerum, and A. D, "Performance and security of group signature in wireless networks," 05 2018.

[29] Chaum, D., & Van Heyst, E. (1991, April). Group signatures. In *Workshop on*

the Theory and Application of of Cryptographic Techniques (pp. 257-265). Springer, Berlin, Heidelberg.

[30] Agarwal, A., & Saraswat, R. (2013). A survey of group signature technique, its applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(10).

[31] Boneh, D., Boyen, X., & Shacham, H. (2004, August). Short group signatures. In *Annual International Cryptology Conference* (pp. 41-55). Springer, Berlin, Heidelberg.

[32] Camenisch, J., & Groth, J. (2004, September). Group signatures: Better efficiency and new theoretical aspects. In *International Conference on Security in Communication Networks* (pp. 120-133). Springer, Berlin, Heidelberg.

[33] Harn, L. (1994). Group-oriented (t, n) threshold digital signature scheme and digital multisignature. *IEE Proceedings-Computers and Digital Techniques, 141*(5), 307-313.

[34] Wang, C. T., Lin, C. H., & Chang, C. C. (1998). Threshold signature schemes with traceable signers in group communications. *Computer Communications, 21*(8), 771-776.

[35] Harn, L., & Wang, F. (2016). Threshold Signature Scheme without Using Polynomial Interpolation. *IJ Network Security, 18*(4), 710-717.

[36] Yu, Y. L., & Chen, T. S. (2005). An efficient threshold group signature scheme. *Applied Mathematics and Computation, 167*(1), 362-371.

[37] Mante, G., & Joshi, S. D. (2011). Discrete logarithm based (t, n) threshold group signature scheme. *International Journal of Computer Applications, 21*(2), 23-27.

[38] Michels, M., & Horster, P. (1996, November). On the risk of disruption in several multiparty signature schemes. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 334-345). Springer, Berlin, Heidelberg.

[39] Tseng, Y. M., & Jan, J. K. (1999). Attacks on threshold signature schemes with traceable signers. *Information Processing Letters, 71*(1), 1-4.

[40] Shao, Z. (2008). Repairing efficient threshold group signature scheme. *International Journal of Network Security, 7*(9), 2008.

[41] Zhao, L. S., & Liu, J. M. (2013, September). (t, n) Threshold Digital Signature Scheme with Traceable Signers against Conspiracy Attacks. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems* (pp. 649-651). IEEE.

[42] Bozkurt, I. N., Kaya, K., & Selçuk, A. A. (2009, June). Practical threshold signatures with linear secret sharing schemes. In *International Conference on Cryptology in Africa* (pp. 167-178). Springer, Berlin, Heidelberg.

[43] Tuan, H. D., Nguyen, H. M., Tran, C. M., Nguyen, H. N., & Adreevich, M. N. (2016, December). Integrating Multisignature Scheme into the Group Signature Protocol. In *International Conference on Advances in Information and Communication*

Technology (pp. 294-301). Springer, Cham.

[44] Eom, S., & Huh, J. H. (2018). Group signature with restrictive linkability: minimizing privacy exposure in ubiquitous environment. *Journal of Ambient Intelligence and Humanized Computing,* 1-11.

[45] Hung, D. T., Minh, N. H., & Hai, N. N. (2018). A Hybrid Threshold Group Signature Scheme with Distinguished Signing Authority. In *Information Systems Design and Intelligent Applications* (pp. 64-72). Springer, Singapore.

[46] Saeed, R., & Rauf, A. (2018, March). 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)* (pp. 1-7). IEEE.

[47] Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering* (pp. 106-115). IEEE.

[48] Cormode, G., & Srivastava, D. (2009, June). Anonymized data: generation, models, usage. In *Proceedings of the 2009 ACM SIGMOD International Conference on Management of data* (pp. 1015-1018). ACM.

[49] Zhou, B., Pei, J., & Luk, W. (2008). A brief survey on anonymization techniques for privacy preserving publishing of social network data. *ACM Sigkdd Explorations Newsletter, 10*(2), 12-22.

[50] Samarati, P., & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression* (pp. 101-132). technical report, SRI International.

[51] Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(05), 571-588.

[52] Dalenius, T. (1986). Finding a needle in a haystack or identifying anonymous census records. *Journal of official statistics, 2*(3), 329.

[53] P Samarati, P. (2001). Protecting respondents identities in microdata release. *IEEE transactions on Knowledge and Data Engineering, 13*(6), 1010-1027.

[54] El Emam, K., & Dankar, F. K. (2008). Protecting privacy using k-anonymity. *Journal of the American Medical Informatics Association, 15*(5), 627-637.

[55] Athiramol, S., & Sarju, S. (2017, July). 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)* (pp. 280-283). IEEE.

[56] Meyerson, A., & Williams, R. (2004, June). On the complexity of optimal k-anonymity. In *Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 223-228). ACM.

[57] Bayardo, R. J., & Agrawal, R. (2005, April). Data privacy through optimal k-anonymization. In *21st International conference on data engineering (ICDE'05)* (pp. 217-228). IEEE.

[58] Machanavajjhala, A., Gehrke, J., Kifer, D., & Venkitasubramaniam, M. (2006, April). l-diversity: Privacy beyond k-anonymity. In *22nd International Conference on Data Engineering (ICDE'06)* (pp. 24-24). IEEE.

[59] Xiao, X., & Tao, Y. (2006, September). Anatomy: Simple and effective privacy preservation. In *Proceedings of the 32nd international conference on Very large data bases* (pp. 139-150). VLDB Endowment.

[60] Prakash, B., Reddy, S. K., Singh, D., Yeshwanth, V. P. S., & Kumar, M. S. (2018). B-Anonymization: Privacy beyond k-Anonymization and l-Diversity. *International Journal for Research in Applied Science and Engineering Technology (IJRASET), 6*(03), 2018.

[61] Xiao, Y. (2007). *Security in distributed, grid, mobile, and pervasive computing*. CRC Press.

[62] DATA, C. I. (2015). ENHANCING RESILIENCE THROUGH CYBER INCIDENT DATA SHARING AND ANALYSIS.

Submitted 18.03.2019
Accepted 17.05.2019