Direct Debit Frauds: A Novel Detection Approach

Gaetano Papale[1], Luigi Sgaglione[1] , Gianfranco Cerullo[1], Giovanni Mazzeo[1],
Pasquale Starace[1] and Ferdinando Campanile[2]
[1]*Department of Engineering, University of Naples "Parthenope", Naples, Italy*
[2]*Sync Lab S.r.l., Naples, Italy*

Keywords: Data Fusion, Real-time Correlation, Data Analytics.

Abstract: Single Euro Payments Area (SEPA) is an initiative of the European banking industry aiming at making all electronic payments across the Euro area as easy as domestic payments currently are. One of the payment schemes defined by the SEPA mandate is the SEPA Direct Debit (SDD) that allows a creditor (biller) to collect directly funds from a debtor's (payer's) account. It is apparent that the use of this standard scheme facilitates the access to new markets by enterprises and public administrations and allows for a substantial cost reduction. However, the other side of the coin is represented by the security issues concerning this type of electronic payments. A study conducted by Center of Economics and Business Research (CEBR) of Britain showed that from 2006 to 2010 the Direct Debit frauds have increased of 288%. In this paper a comprehensive analysis of real SDD data provided by the EU FP7 LeanBigData project is performed. The results of this data analysis will conduct to define emerging attack patterns that can be execute against SDD and the related effective detection criteria. All the work aims at inspire the design of a security system supporting analysts to detect Direct Debit frauds.

1 INTRODUCTION

Payment systems are in rapidly evolution. And so are payment frauds. Whenever a new payment method is introduced, the fraudsters try to take advantage of loopholes and security vulnerabilities that each novel system brings with it. European Union has developed the Single Euro Payment Area (SEPA), where 500 million of citizens, businesses and the European Public Administrations can make and receive over 100 billion no-cash payments every year (EPC, 2002). SEPA Direct Debit (SDD) is a service that allows consumers to make in euro payments using a single bank account and a single set of instructions. A common standard, if on one hand translates into efficiency gains for businesses and public administrations, facilitating access to new markets and reducing costs, on the other hand, the simplification of the payment process increases the risks for the users. The SDD service is not free from cybercrime attacks. A study conducted by Center of Economics and Business Research (CEBR) of Britain, on behalf of Liverpool Insurance Company, showed that from 2006 to 2010 the Direct Debit frauds have increased of 288%, with an expected growth of 57% for the next three years (FINEXTRA, 2010). The magnitude of these evidences is related to the lack of knowledge on the part of financial institutions with respect to the types of threats that an attacker can implement. The paper is organized as follows: Section 2 presents the works found in literature that approached to the issues in SDD payments and electronics ones; in Section 3 an in-depth analysis of the SEPA standard and an accurate description of the phases to set-up a Direct Debit transaction is presented. Particular emphasis is given to the almost absence of security mechanisms that a financial institution puts in place to protect his users from unauthorized or fraudulent SDDs. Section 4, starting from the information reported in the previous sections, analyzes the vulnerabilities of the SDD process due to the adoption of Creditor Mandate Flow Model (CMF). Section 5 proposes a categorization, in four misuse cases, of attacks that a fraudster can execute against an unaware SDD's user. To this aim, we have analyzed over than 2TB of real SDD data, provided within the framework of EU FP7 European LeanBigData project. Section 6

Papale, G., Sgaglione, L., Cerullo, G., Mazzeo, G., Starace, P. and Campanile, F.
Direct Debit Frauds: A Novel Detection Approach.
In *Proceedings of the 6th International Conference on Cloud Computing and Services Science (CLOSER 2016) - Volume 1*, pages 380-387
ISBN: 978-989-758-182-3

outlines effective detection criteria to the previously identified attack patterns and finally, Section 7 shows future research directions.

2 RELATED WORK

Direct Debit frauds are a modern topic in the scientific community and, at the beginning of our work, we were aware that no literature concerning this argument was available. However, several are the publications relating the detection of threats against other forms of electronic payment. In (D'Antonio, 2015) (Coppolino, 2015) authors describe the advanced cyber threats, specifically targeted to financial institutions and propose an approach based on combining multiple and heterogeneous data to detect frauds against a Mobile Money Transfer (MMT). The research presented in (Raj, 2011), denotes that in real life fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. The work presents a survey of various techniques (Data mining, Fuzzy logic, Machine learning...) used in credit card fraud detection. (Patidar, 2011) shows that the frauds tend to be perpetrated to certain patterns and the use of Neural Network to detect fraudulent transactions is presented. The paper (Duman, 2011) suggests a novel combination of the two well-known meta-heuristic approaches, namely the genetic algorithms and the scatter search to detecting credit card frauds. The method is applied to real data and very successful results are obtained compared to current practice. The research presented in (Allison, 2005) proposes an analysis of the identity theft and the related crimes.

3 SEPA DIRECT DEBIT TRANSACTIONS

SEPA is the area where citizens, businesses, governments and other economic actors can make and receive euro payments. The jurisdiction of the SEPA scope currently consists of the 28 EU Member States (List, 2015), the members of European Free Trade Association-EFTA (Iceland, Liechtenstein, Norway and Switzerland), plus Monaco and San Marino. The goal of the SEPA project includes the development of financial instruments, standards, procedures and infrastructures to enable economies of scale. This paper is focused on SEPA Direct Debit transactions (SDDs), one of the services provided by SEPA. Typical examples of SDD transactions are services that require recursive payments such as pay per view TV, gym subscription and energy distribution. The actors involved in an SDD transaction are:

- **Creditor**

In the SEPA Direct Debit (SDD) schema is the person or company who has a credit that will be satisfied by collecting funds from the Debtor's bank account through an SDD transaction.

- **Debtor**

In the SEPA Direct Debit (SDD) schema is the person or company who has a debit that satisfies by providing funds from his/her bank account to the Creditor's bank account by means of an SDD transaction.

- **Creditor's and Debtor's banks**

They represent the respective banks of Creditor and Debtor.

When a Creditor must draw funds from another person's bank account, to set up the process, he/she has to acquire an SDD mandate from Debtor and advise his/her bank about it. During each transaction, the Creditor sends a direct debit request (with information about the amount of the transaction) to his/her bank that will start the process to request the specified amount from Debtor's bank account. The Debtor must provide only the signature of the mandate, but has no prior acknowledgement about the direct debit being in charge to his/her bank account. Usually, the Creditor sends a receipt to the Debtor by using a best effort service, so no guarantee about delivery time and delivery itself is provided. In this process, the Debtor will have knowledge of an unauthorized direct debit only when the funds have already been withdrawn and after reception of his/her bank statement. This of course exposes the Debtor to a large number of possible frauds. For these reasons, with SEPA, in case of unauthorized transactions due to errors or frauds, a Debtor can request refund until 8 weeks from the SDD deadline or 13 months in case of an unauthorized SDD. The SDD process (Figure 1) is characterized by the following steps:

- **Acquisition**

1) The mandate is signed by the Debtor and is notified to the Creditor Bank.

- **Validation**

1) The Creditor Bank sends a validation request for the received mandate to the Debtor Bank.
2) The Debtor Bank receives the validation request and returns its validation.

- **SDD request**

1) The Creditor generates a receipt at least 14 working days before its deadline.
2) The Creditor sends an SDD request to its bank (at least 11 working days before in case of first SDD request, 9 for subsequent requests).
3) The Creditor Bank sends an SDD request to the Debtor Bank which checks the correctness of the request and if no problem occurred, the bank debits the SDD on Debtor's account.

- **Interbank Clearing**

1) The Debtor Bank communicates the result of SDD request to the Creditor Bank.
2) In case of positive response, the Creditor Bank credits the amount of the transaction on Creditor's account.

The standard adopted by SEPA to compose SDD requests is the ISO 20022 (Goswell, 2006), a multi-part International Standard performed by ISO Technical Committee TC68 Financial Services. It defines a modelling methodology to capture in a syntax-independent way financial business areas, business transactions, and associated message flows. Also, it sets a central dictionary of business items used in financial communications and fixes a set of XML and ASN.1 design rules to convert the message models into XML or ASN.1 schemas, whenever the use of ISO 20022 XML or ASN.1-based syntax is preferred. In Italy, from the 1st of February 2014, domestic credit transfers, banking and postal direct debits (RIDs) were replaced by the corresponding SEPA instruments. In particular, for the SDD request, the "CBIBdySDDReq.00.01.00" standard which is provided by the Interbank Corporate Banking (CBI) consortium is used.

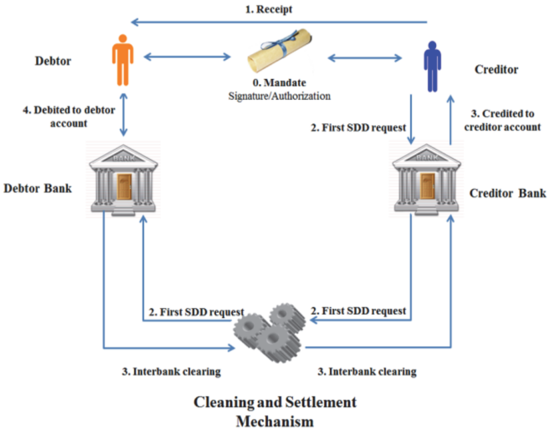

Figure 1: SEPA Direct Debit process.

In Listing 1 an excerpt of real SDD data is shown.

```
<Cdtr>
    <Nm>Cred_Name Cred_Surname </Nm>
      <PstlAdr>
      <TwnNm>Cred_Town</TwnNm>
      <Ctry>Cred_Country</Ctry>
      <AdrLine>Cred_Addr</AdrLine>
      </PstlAdr>
         <Id>ITXXX100000857072000YYY</Id>
</Cdtr>
    <CdtrAcct>
     <Id>
<IBAN>IT58Z0000000001000000000884</IBAN>
     </Id>
    </CdtrAcct>
<Dbtr>
    <Nm>Deb_Name Deb_Surname </Nm>
      <PstlAdr>
      <TwnNm>Deb_Town</TwnNm>
      <Ctry>Deb_Country</Ctry>
      <AdrLine>Deb_Addr</AdrLine>
      </PstlAdr>
         <Id>AAABBB88A08B777R</Id>
</Dbtr>
<DbtrAcct>
     <Id>
<IBAN>IT48Y0000000001000000000884</IBAN>
     </Id>
</DbtrAcct>
   <RmtInf>
    <Ustrd>Gym Subscription</Ustrd>
   </RmtInf>
```

Listing 1: Excerpt of SDD data in ISO 20022 format.

It contains the information of Creditor and Debtor. Within the <Cdtr> tag, the "Id" field represents the Creditor Identifier (CI, 2015) on 23 digits.

In particular, from digit 8 to digit 23 is defined the VAT number of the company. An analogous structure is used for the Debtor, but the "Id" field is on 16 digits and represents the fiscal code of the user. In the real data that we have analyzed, every ISO 20022 xml file contains a trace of purpose of the transaction (i.e. gym or pay-tv subscription) within the field "Ustrd".

4 ISSUES IN SEPA TRANSACTIONS

The SEPA Direct Debit transactions, as any other form of electronic payment, are not immune from attacks of fraudsters. At the basis of each SDD fraud there is the "Identity Theft", of either the Debtor's identity or the Creditor's identity. Identity Theft is a relatively new phenomenon for which there is no universally recognized definition, but overall can be defined as a crime where someone:

"*knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another* *person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation law ...*" (Finklea, 2010).

The major weakness of the SEPA Direct Debit process is at the beginning of the procedure, in particular during the phase of signing the mandate. In fact, as shown in Figure 2, a fraudster can authorize the SDD mandate in place of the Debtor. This illegal activity, also known as "Mandate Fraud", allows benefiting products or services without paying for it, while the Debtor will recognize the fraud after the direct debit was performed. The management of the mandate can follow two different models:

- **CMF** – Creditor driven Mandate Flow
- **DMF** – Debtor driven Mandate Flow

CMF provides that the mandate is stored with the Creditor and it is the unique model in four European countries (Germany, Spain, Netherland and UK). DMF, unlike the previous, provides that the mandate stays with the Debtor's bank and is adopted in Finland, Greece, Malta, Slovenia, Slovakia, Hungary, Latvia and Lithuania. In Italy and in the remaining countries of SEPA area, CMF and DMF coexist, but the European Policy Centre (EPC) has unilaterally decided that the SEPA model would be based on CMF. The same European Consumer's Organization (BEUC), through a letter to the members of European Parliament (MEPs) dated 25 January 2010, has raised the issue by defining SEPA's Creditor Mandate Flow Model (CMF) "massively open to fraud". With the CMF model, the consumer's bank (i.e. Debtor's bank) does not have control over the mandate, so the risk of fraud is higher (BEUC, 2011). This model prevents the Debtor's Bank from intervening once a payment has left an account, with the consequence that the

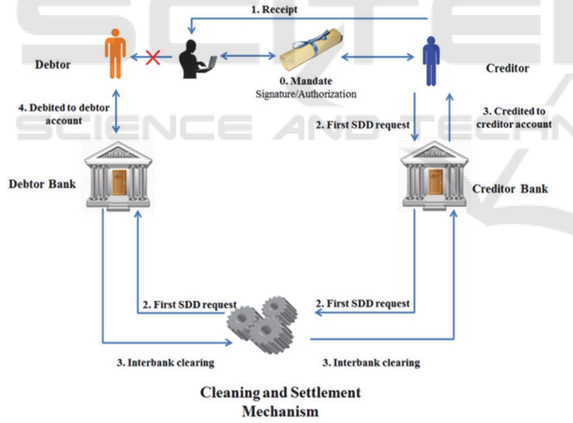

Figure 2: Mandate Fraud.

Creditor is in full control of the transaction. Furthermore, the reduced amount of information required to activate a transaction, allows even to the less savvy criminals to perpetrate a fraud. The precondition of an SDD fraud is an identity theft. There are different techniques to steal personal information of the victim, as reported in (Pardede, 2013), several that don't need high technical expertise (i.e. Dumpster Diving) and other more sophisticated (i.e. Spoofing and Phishing).

5 FOUR MISUSE CASES

In this section will be described four misuse cases in the SDD transactions. The classification was conducted in order to develop, in future, a support system to recognize SDD frauds with a high detection rate and a low occurrence of false-positives. To categorize the frauds, we have examined a huge amount of real data. This data have been obtained within the LeanBigData project (Project, 2014). LeanBigData is an European project that has as goal the building of an ultra-scalable and ultra-efficient integrated big data platform addressing important open issues in financial, cloud data and social media big data analytics. Over than 2 TB of data transactions properly anonymized have been analyzed and, from the observation of different attack patterns, we have extracted four misuse cases. The misuse cases will be schematized with indications about the actors involved in the fraud, the preconditions to execute it, a description of the misuse case and the fraudster's goal. To allow a better understanding of the misuse cases, it is appropriate to divide the services that can be connected to an SDD transaction into two categories:

- Location-unbound
- Location-bound

The "location-unbound" category identifies services that can be provided at any location and therefore do not require the physical presence of the Debtor (e.g. pay-per-view, smartphone fee) while, the term "location-bound" indicates all services necessarily provided at a specific place and requiring the physical presence of the user at a specific place, for example a gym subscription.

Misuse Case 1: Location-unbound Service Fraud

- **Actors:** Debtor, Creditor and Fraudster.
- **Objective:** The goal of the Fraudster is to perpetrate an identity fraud against the Debtor to

benefit of a "location-unbound" service, without paying for it.

- **Preconditions:**

1)The Fraudster steals Debtor's identity.
2)The Fraudster signs a mandate for a location-unbound" service instead of the legitimate user.

- **Description:**

1)The Fraudster, impersonating a Debtor, requests a direct debit on the Debtor's account for a "location-unbound" service.
2)The Fraudster, to activate the SDD process, signs the mandate with the stolen identity of the Debtor.
3)The Debtor's bank, once verified the correctness of the data into SDDs, transfer the cost of the service from Debtor's account.

Misuse Case 2: Location-bound Service Fraud

- **Actors:** Debtor, Creditor and Fraudster.
- **Objective:** The goal of the Fraudster is to perpetrate an identity fraud against the Debtor to benefit of a "location-bound" service, without paying for it.
- **Preconditions:**

1)The Fraudster steals Debtor's identity.
2)The Fraudster signs a mandate for a "location-bound" service instead of the legitimate user.

- **Description:**

1)The Fraudster steals the identity of a Debtor and, by using such identity, requests a payment for a "location-bound" service to the unaware Debtor.
2)The Fraudster, to activate the SDD transaction, signs the mandate with the stolen identity of the Debtor.
3)The "location-bound" service provided by real Creditor has a location of use very far from usually places visited/lived by the Debtor.
4)The Debtor's bank, that has the duty of checking only the correctness of format and data into the SDD request, validates the transaction.

Misuse Case 3: Fake Company Fraud

- **Actors:** Debtor and Fraudster.
- **Objective:** The goal of the Fraudster is to perpetrate an identity fraud against the Debtor, without provide to him/her any "location-bound" or "location-unbound" service.
- **Preconditions:**

1) Fraudster and Creditor is the same actor.
2) The Fraudster steals Debtor's identity.
3) The Fraudster signs a mandate for a service instead of legitimate user.

- **Description:**

1) A fake company, registered as biller for SDDs, requires a direct debit for a service to an unaware Debtor.
2)The Fraudster, to activate the SDD transaction, signs the mandate with the stolen identity of the Debtor.
3) The Debtor's bank, that is not able to verify the reliability of Creditor, accepts the SDDs.

Misuse Case 4: Cloning Company Fraud

- **Actors:** Debtor and Fraudster.
- **Objective:** The goal of the Fraudster is to activate a direct debit on the Debtor's account for a "location-unbound" service regularly subscribed by Debtor, but that will not provide.
- **Preconditions:**

1) Fraudster and Creditor is the same actor.
2)The Fraudster contacts the Debtor and obtains "legally" his/her identity.
3)The Debtor authorizes the mandate for the service.

- **Description:**

1)The Fraudster, using a company name slightly different from another well-known by the Debtor, contacts the Debtor and proposes to him/her the subscription for an "unbound" service.
2)The Debtor is interested to the service, subscribes it and provides its personal and banking details.
3)The Debtor's bank, given that the cloning company is registered as a biller and the mandate is properly signed, activates the fund transfer.
4)The Debtor will be aware of the fraud only when after several days the service still has been not provided (within the account statement there is not anything of irregular).

6 A MULTI SENSORS APPROACH TO RECOGNIZE FRAUDOLENT TRANSACTIONS

In the last years, despite the recommendations by the part of European Banking Committee (EBC) to improve the security of SDD payment process, the financial institutes have not yet put in place valuable solutions to recognize fraudulent transactions. The banking fraud detection systems currently have low performance because they separately control only the format correctness of the direct debit requests and the data therein specified. The multi sensors approach proposed in this work, is driven by the Joint Directors Laboratories (JDL) Data Fusion model (Blash, 2013) and involving its Source Preprocessing, Object Refinement and Situation Refinement levels. In order to discern a malicious operation from a legitimate one, is necessary categorizing each incoming SDD for topic and collect, within of a profile, more information as possible on Debtor and Creditor. Finally, through several detection criteria targeted on the misuse cases previously analyzed, both SDDs and users data will be focused to extract the evidence of an SSD fraud. The Data Fusion process will be operated by using a generalization of the Bayesian theory, such as the Dempster-Shafer theory of Evidence (Dempster, 1968). Figure 3 shows the high level architecture that aims at develop a multi sensor decision supports system which by the data gathered by multiple data sources (i.e. Social Networks data, SDD raw data, third party services...), will provide a measure of likelihood of an ongoing Direct Debit fraud.

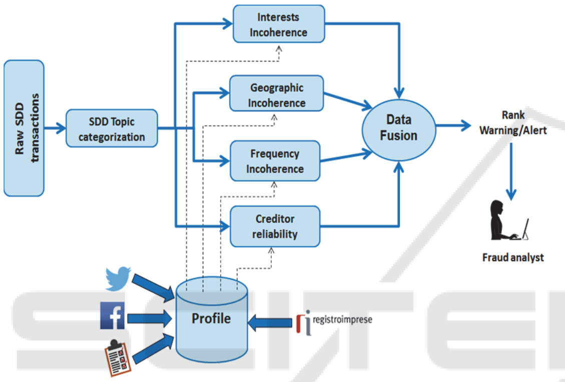

Figure 3: Decision Supports System Global Architecture.

The above architecture consists of the main following blocks:

- **SDD Topic categorization**

It is the module responsible of the classification of each incoming SDD to a topic of interest. It operates on raw SDD data and performs a data filtering step to extract the Creditor information. This data will be used as input for third party services (i.e. Registro delle Imprese and Agenzia delle Entrate websites) to retrieve the working sector, such as the topic, of the Creditor.

- **Profile**

It is a centralized database that stores in real-time the profile of each Debtor and in the specific his/her personal data, banking account information, addresses and interests. For the definition of the Debtor's interests, once obtained the user's authorization, tools that perform machine learning, text analysis and natural language processing have been used. These receive a text in input - e.g. Facebook posts, tweets, hashtags - and execute an automatic classification in categories. Also, the profile contains a table with the information related to the Creditors (i.e. venues and working sector) which the Debtor has made business.

- **Detection Criteria**

The Detection Criteria allow to evaluate the deviation between the context of the SDD operation and the ideal profile of the Debtor. From a careful analysis of the attack patterns described at previous section and, observing the typologies of services involved, the preconditions and the modus operandi of cyber criminals, the following criteria have been defined:

1) Geographic Incoherence

The "Geographic Incoherence" criterion is applicable to the SDDs that involving the fruition of "location-bound" services. This criterion measures the coherence between the known Debtor's addresses (i.e. residence address, job address and other addresses communicated from Debtor to the bank) and the location of use of the service. One parameter to take into account for evaluating a location of service as plausible is the distance in kilometre from the Debtor's addresses. The criterion integrates the Google Maps Geocoding API (Google, 2016) to converting addresses in geographic coordinates and calculating the distance between two geographic points.

2) Interests Incoherence

The "Interests Incoherence" criterion can be used to recognize suspicious SDDs both for "location-bound" and "location-unbound" services. It aims at measuring the match between the topic of the transaction and the Debtor's interests. The criterion, through the exploitation of Dempster-Shafer theory and using Sentiment analysis techniques, evaluates the evidence that Debtor's interest is close to topic of service.

3) Creditor Reliability

The "Creditor Reliability" criterion, by the use of third party services (i.e. Registro delle Imprese and Agenzia delle Entrate websites), allows to identify if a company is real or not. Of course, for a company does not inscribed to the "Registro delle Imprese", the criterion will raise an alert.

4) Frequency Incoherence

A direct debit is a service typically used to perform recursive payments. That means observing of an account should highlight periodicity of payments of the same nature. The presence of spurious payments or a suspect increasing of the number of transactions, could be index of malicious operations.

Each one of the described criteria produces as outcome an indicator that summarizes the evidence of an ongoing fraud as defined by the Basic Probability Assignment (BPA) of Dempster-Shafer theory. All the BPAs will be in turn focused using the Dempster's rule of combination. In this way, more criteria can be combined for the same transaction to increase the fraud detection rate and reduce the false alarms. For instance, in an attempting of "Location-bound Service Fraud" the isolated use of the "Geographic Incoherence" criterion could conduct to evaluate a transaction as genuine. Adding also the "Interests Incoherence" criterion, and evaluated that the Debtor is totally unclosed to the transaction's topic, a warning will be raised.

Table 1: Application of Detection Criteria.

Misuse Cases vs Detection Criteria	Geo. Incoh.	Interests Incoh.	Freq. Incoh.	Credit. Reliab.
Misuse Case 1	×	✓	✓	×
Misuse Case 2	✓	✓	✓	×
Misuse Case 3	✓	✓	✓	✓
Misuse Case 4	×	✓	✓	✓

Table 1 shows how the proposed Detection Criteria can be used to recognize the misuse cases described at Sec.5.

7 CONCLUSIONS

In this paper we discussed of the new SEPA Direct Debit standard adopted by the European Union to transfer funds within its economic area. From an in depth study of the Direct Debit process, many safety risks for user's money emerged. In this context, only a strong understanding of the fraud strategies can indicate the best countermeasures. Our work, starting from real SDDs data, presented an analysis of emerging attack patterns against Direct Debit transactions, it has categorized them in misuse cases and defined four Detection Criteria. The classification is been conducted in order to ensure a high detection rate and a low occurrence of false-positives. Our goal is to develop a tool that recognizes possible ongoing attacks through real time analysis (Ficco, 2011) (Romano, 2010) and the continuous monitoring of the SDDs data flow (Cicotti, 2015) (Cicotti, 2012). Such a tool will provide a support service, by means of the Software as a Service (SaaS) paradigm (Ficco M, 2012) (Ficco, 2012), to the fraud analyst. The tool will be also provided with a powerful Human Machine Interface (HMI) specifically designed to support Big Data analytics for fraud detection (Coppolino, 2015).

ACKNOWLEDGEMENTS

The research leading to these results has received funding from European Commission within the context of Seventh Framework Programme (FP7/2007-2013) for research, technological development and demonstration under Grant Agreement No. 619606 (Ultra-Scalable and Ultra-Efficient Integrated and Visual Big Data Analytics, LeanBigData Project). It has been also partially supported by the "Embedded Systems in critical domains" POR Project (CUP B25B09000100007) funded by the Campania region in the context of the POR Campania FSE 2007-2013, Asse IV and Asse V and by the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research.

REFERENCES

Allison, S. e. a., 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, pp. 19-29.

BEUC, 2011. Establishing technical requirements for credit transfers and direct debits in euro. (Online) Available at: http://www.beuc.eu/publications/ 2011-00202-01-e.pdf [Accessed 24 October 2015].

Blash, E. e. a., 2013. Revisting theJDL model for information exploitation. In: *Information Fusion, 16th International Conference on.*, IEEE.

CI, 2015. Creditor Identifier Overview. (Online) Available at: http://www.europeanpaymentscouncil .eu/index.cfm/ [Accessed 23 October 2015].

Cicotti, G. C. L. a. a., 2012. QoS monitoring in a cloud services environment: the SRT-15 approach. In: *Euro-Par 2011: Parallel Processing Workshops*. Springer Berlin Heidelberg, pp. 15-24.

Cicotti, G. e. a., 2015. How to monitor QoS in cloud infrastructures: the QoSMONaaS approach., *International Journal of Computational Science and Engineering*, 11(1), pp. 29-45.

Coppolino, L. e. a., 2015. Use of the Dempster-Shafer Theory for Fraud Detection: The Mobile Money Transfer Case Study. *Intelligent Distributed Computing VIII. Springer,* p. 465–474..

Coppolino, L. e. a., 2015. Effective Visualization of a Big Data Banking Application. In: *Intelligent Interactive Multimedia Systems and Services,* Springer, pp. 57-68.

D'Antonio, e. a., 2015. Use of the Dempster–Shafer theory to detect account takeovers in mobile money transfer services. *Journal of Ambient Intelligence and Humanized Computing, DOI:10.1007/s12 652–015–0276–9.,* p. 1–10.

Dempster, A., 1968. A generalization of bayesian inference. *Journal of the Royal Statistical Society,* Volume Series B (Methodological), pp. 205-247.

Duman, E. a. O. M. H., 2011. Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications,* 38(10).

EPC, 2002. *Euroland: Our Single Euro Payment Area!*. (Online) Available at: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/euroland-our-single-payment-area/sepa-whitepaper-05 20021pdf/ (Accessed 15 January 2016).

Ficco, M. e. a., 2011. An event correlation approach for fault diagnosis in SCADA infrastruc-tures. In: *Proceedings of the 13th European Workshop on Dependable Computing.* s.l.:ACM, pp. 15-20.

Ficco, M. and Rak, M., 2012. Intrusion tolerance as a service: a SLA-based solution. Porto, Portugal, *2nd Int. Conf. on Cloud Computing and Services Science (CLOSER 2012)*.

Ficco, M. and Rak. M., 2012. Intrusion tolerance in cloud applications: the mosaic approach. Palermo, Italy, *6th Int. Conf. on Complex, Intelligent, and Software Intensive Systems (CISIS 2012)*.

FINEXTRA, 2010. Direct debit fraud at an all-time high; Bacs challenges figures. (Online) Available at: http://www.finextra.com/news/fullstory. aspx?news itemid=22028 [Accessed 11 January 2016].

Finklea, M., 2010. Identity theft: Trends and issues. DIANE Publishing.

Google inc., Google Maps Geocoding API. (Online) Available at: https://developers.google.com/maps/documentation/geocoding/intro [Accessed 18 January 2016].

Goswell, S., 2006. Iso 20022: The implications for payments processing and requirements for its successful use. *Journal of Payments Strategy & Systems,* 1(1), pp. 42-50.

List, 2015. Epc List of SEPA Scheme Countries. [Online] Available at: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-list-of-sepa-scheme-countries/epc409-09-epc-list-of-sepa-scheme-countries-v21-june-2015pdf/ [Accessed 22 October 2015].

Pardede, M. e. a., 2013. E-fraud, Taxonomy on Methods of Attacks, Prevention, Detection, Investigation, Prosecution and Restitution.

Patidar, R. e. a., 2011. Credit Card Fraud Detection Using Neural Network. *International Journal of Soft Computing and Engineering (IJSCE) ISSN,* p. 2231–2307.

Project, 2014. Ultra-Scalable and Ultra-Efficient Integrated and Visual Big Data Analytics. (Online) Available at: http://leanbigdata.eu/ [Accessed 12 January 2016].

Raj, S e. a., 2011. Analysis on credit card fraud detection methods. *Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on.,* pp. 152-156.

Romano, L. e. a., 2010. An intrusion detection system for critical information infrastructures using wireless sensor network technologies. In: *Critical Infrastructure (CRIS), 2010* 5th International Conference on., IEEE, pp. 1-8.