IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

# Anti-Theft ATM Robbery System for Big Video Surveillance using Improved_SVM Algorithm

**R.Pradheepa[1*], V.Priya[2]**

[1,2]Dept. of Computer Science, Nehru Memorial College (Autonomous), Tiruchirapalli, India

[*]*Corresponding Author: pradeeparames2009@gmail.com*

**Available online at: www.ijcseonline.org**

***Abstract*—**Video survey framework has turned into a basic part in the security and assurance arrangement of urban areas, since Smart Monitoring cameras furnished with canny video examination procedures can screen and pre-alert anomalous practices or occasions. Nonetheless, with the extension of the reconnaissance arrange monstrous observation video information postures colossal difficulties to the examination, stockpiling and recovery in the Big Data time. This paper proposed the new enhanced SVM Algorithm is called IMROVED_SVM. This algorithm shows a novel insightful preparing and usage answer for enormous reconnaissance video information in light of the occasion recognition and disturbing messages from front-end shrewd cameras. The technique incorporates three sections: the astute pre-disturbing for strange occasions, keen stockpiling for observation video and fast recovery for confirm recordings, which completely explores the transient spatial affiliation investigation regarding the unusual occasions in various checking locales. Test comes about uncover that our proposed approach can dependably pre-alert security hazard occasions, considerably diminish storage room of recorded video and essentially accelerate the proof video recovery related with particular suspects**.**

***Keywords*— :** *Big Data, Support Vector Machine (SVM)*

## I. INTRODUCTION

**Big Data**

Big data is an all-encompassing term for any collection of data sets so large and complex that it becomes difficult to process them using traditional data processing applications. The challenges include analysis, capture, curation, search, sharing, storage, transfer, visualization, and privacy violations. The trend to larger data sets is due to the additional information derivable from analysis of a single large set of related data, as compared to separate smaller sets with the same total amount of data, allowing correlations to be found to spot business trends, prevent diseases, combat crime and so on.

Scientists regularly encounter limitations due to large data sets in many areas, including meteorology, genomics, connectomics, complex physics simulations, and biological and environmental research.The limitations also affect Internet search, finance and business informatics. Data sets grow in size in part because they are increasingly being gathered by ubiquitous information-sensing mobile devices, aerial sensory technologies (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks. The world's technological per-capita capacity to store information has roughly doubled every 40 months since the 1980s; as of 2012, every day 2.5exabytes ($2.5\times10^{18}$) of data were created.

The challenge for large enterprises is determining who should own big data initiatives that straddle the entire organization.

Big data is difficult to work with using most relational database management systems and desktop statistics and visualization packages, requiring instead "massively parallel software running on tens, hundreds, or even thousands of servers. What is considered big data varies depending on the capabilities of the organization managing the set, and on the capabilities of the applications that are traditionally used to process and analyze the data set in its domain. Big Data is a moving target; what is considered to be Big today will not be so years ahead. "For some organizations, facing hundreds of gigabytes of data for the first time may trigger a need to reconsider data management options. For others, it may take tens or hundreds of terabytes before data size becomes a significant consideration."

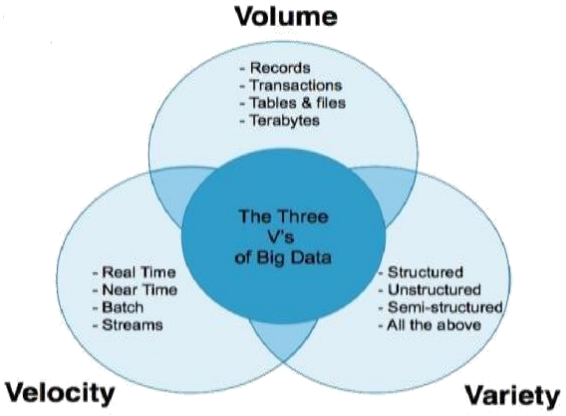
Big data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process data within a tolerable elapsed time. Big data size is a constantly moving target, as of 2012 ranging from a few dozen terabytes to many peta bytes of data. Big data is a set of techniques and technologies that require new forms of integration to uncover large hidden values from large datasets that are diverse, complex, and of a massive scale.

In a 2001 research report and related lectures, META Group now Gartner analyst Doug Laney defined data growth challenges and opportunities as being three-dimensional, i.e. increasing volume amount of data, velocity speed of data in and out, and variety range of data types and sources. Gartner, and now much of the industry, continue to use this 3Vs model for describing big data. In 2012,Gartner updated its definition as follows: Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization. Additionally, a new V Veracity is added by some organizations to describe it. If Gartner's definition (the 3Vs) is still widely used, the growing maturity of the concept fosters a more sound difference between big data and Business Intelligence, regarding data and their use:

Business Intelligence uses descriptive statistics with data with high information density to measure things, detect trends etc.;Big data uses inductive statistics and concepts from nonlinear system identification to infer laws regressions, nonlinear relationships, and causal effects from large sets of data with low information density to reveal relationships, dependencies and perform predictions of outcomes and behaviors. Big data can also be defined as Big data is a large volume unstructured data which cannot be handled by standard database management systems like DBMS, RDBMS or ORDBMS**.** Big Data Can Be Described By The Following Characteristics:

**Volume –** The quantity of data that is generated is very important in this context. It is the size of the data which determines the value and potential of the data under consideration and whether it can actually be considered as Big Data or not. The name Big Data itself contains a term which is related to size and hence the characteristic.




**Variety -** The next aspect of Big Data is its variety. This means that the category to which Big Data belongs to is also a very essential fact that needs to be known by the data analysts. This helps the people, who are closely analyzing the data and are associated with it, to effectively use the data to their advantage and thus upholding the importance of the Big Data.

**Velocity** - The term velocity in the context refers to the speed of generation of data or how fast the data is generated and processed to meet the demands and the challenges which lie ahead in the path of growth and development.

**Variability** - This is a factor which can be a problem for those who analyze the data. This refers to the inconsistency which can be shown by the data at times, thus hampering the process of being able to handle and manage the data effectively.

**Veracity -** The quality of the data being captured can vary greatly. Accuracy of analysis depends on the veracity of the source data.

**Complexity** - Data management can become a very complex process, especially when large volumes of data come from multiple sources. These data need to be linked, connected and correlated in order to be able to grasp the information that is supposed to be conveyed by these data. This situation, is therefore, termed as the complexity of Big Data. Big data analytics enables organizations to analyze a mix of structured, semi-structured and unstructured data in search of valuable business information and insights.

The existing intelligent surveillance systems can only detect and alarm single abnormal event yet without bridging the spatial and temporal association among multiple unusual events. However, it is quite not convincible to judge suspicious behavior by a single monitoring. As the case of wandering in the front of a bank, the occasional wander outside the bank may be a usual behavior for awaiting others. It only makes sense to treat the wandering as suspicion when it happens repeatedly or takes a long time. The huge amount of video acquired by the city scale monitoring network results in the rapid increasing of storage costs. IDC International Data Corporation calculated that surveillance video data accounts for 65 percent of whole data, which was far more than any other data like transaction data, medical data, entertainment and social media data. Since the massive surveillance video needs to be stored for several months or years, it leads to a large storage cost. The amount of false alarming resulted from the data explosion is beyond the limitations of manual processing. Traditional methods for obtaining evidences highly depend on the surveillance video within or near the accident site. However, when the incident passes through a wide range of space and time, it is hard to find any valuable evidences on the criminals from massive surveillance video, which hampers the efficiency of resolving

cases. The recent emerging smart monitoring cameras are able to automatically identify abnormal behaviors through the built-in intelligent algorithms, greatly boosting the performance of the surveillance system. However, the above mentioned three major challenges have not been fundamentally resolved. The essential reason is that the existing system only individually accepts alarm information front end camera and makes a limited range of alarming, without performing collaborative analysis among camera network. Besides, the detection results on unusual behaviors are not fully exploited in terms of deep utilization, paying little attention to storage and retrieval on massive video but for event alarming.

## II. LITERATURE REVIEW

Gerhard P. Hancke et al 2012 described a world where resources are scarce and urban areas consume the vast majority of these resources, it is vital to make cities greener and more sustainable. Advanced systems to improve and automate processes within a city will play a leading role in smart cities. From smart design of buildings, which capture rain water for later use, to intelligent control systems, which can monitor infrastructures autonomously, the possible improvements enabled by sensing technologies are immense. Ubiquitous sensing poses numerous challenges, which are of a technological or social nature. This paper presents an overview of the state of the art with regards to sensing in smart cities. Topics include sensing applications in smart cities, sensing platforms and technical challenges associated with these technologies. In an effort to provide a holistic view of how sensing technologies play a role in smart cities, a range of applications and technical challenges associated with these applications are discussed. As some of these applications and technologies belong to different disciplines, the material presented in this paper attempts to bridge these to provide a broad overview, which can be of help to researchers and developers in understanding how advanced sensing can play a role in smart cities.

Kranti Wanawe et al 2014 proposed phishing is becoming one of the biggest network crimes. Phishing is a current social engineering attack that results in online theft. Phishing is a form of identity theft in which a combination of social engineering and web site spoofing techniques are used to track a user into revealing confidential information with economic value. Over the past few years, we applied different methods for detecting phishing web using known as well as new features. In existing approach, Phishing sites are recognized by using blacklist based approach. The disadvantage of this approach is that non-blacklisted phishing sites are not recognized. This paper presents an efficient approach for detection of phishing a web based on features of legitimate and phishing webs. In this paper, we proposed two algorithms that are K-Means and Naïve Bayes. Using these algorithms, we are checking blacklist for detection of phishing sites as well as their behavior also.

Amaze et al 2016 invented to design and develop a video surveillance and monitoring system that will provide easy access to both live and archived images during and after an institutions examination. My motivation into this paper work is the rate at which students and staff of tertiary institutions participate and encourage examination malpractice. The paper methodology adopted for this paper work was by observation. The top-down software design was adopted for this research. Prototype development methodology was used in the development of the system and Microsoft visual studio 2010; using visual basic in the .net framework was used as the programming language. The resultant outcome of this paper was tested to make sure examination malpractice in tertiary institutions is brought to its lowest minimum, making sure all requirements are met and are working perfectly as expected, bringing all offenders and defaulters involved in examination malpractice to book.

Du Tran et al 2014 suggested sliding window-based approaches have been quite successful in detecting objects in images; it is not a trivial problem to extend them to detecting events in videos. We propose to search for spatiotemporal paths for video event detection. This new formulation can accurately detect and locate video events in cluttered and crowded scenes, and is robust to camera motions. It can also well handle the scale, shape, and intra-class variations of the event. Compared to event detection using spatiotemporal sliding windows, the spatiotemporal paths correspond to the event trajectories in the video space, thus can better handle events composed by moving objects. We prove that the proposed search algorithm can achieve the global optimal solution with the lowest complexity. Experiments are conducted on realistic video data sets with different event detection tasks, such as anomaly event detection, walking person detection, and running detection. Our proposed method is compatible with different types of video features or object detectors and robust to false and missed local detections. It significantly improves the overall detection and localization accuracy over the state-of- the-art methods.

Raghavendra1 et al 2016 improved a new scheme for detecting and localizing the abnormal crowd behavior in video sequences. The proposed method starts from the assumption that the interaction force, as estimated by the Social Force Model (SFM), is a significant feature to analyze crowd behavior. We step forward this hypothesis by optimizing this force using Particle Swarm Optimization (PSO) to perform the advection of a particle population spread randomly over the image frames. The population of particles is drifted towards the areas of the main image motion, driven by the PSO fitness function aimed at minimizing the interaction force, so as to model the most

diffused, normal, behavior of the crowd. In this way, anomalies can be detected by checking if some particles (forces) do not fit the estimated distribution, and this is done by a RANSAC-like method followed by a segmentation algorithm to finely localize the abnormal areas. A large set of experiments are carried out on public available datasets, and results show the consistent higher performances of the proposed method as compared to other state-of-the-art algorithms, proving the goodness of the proposed approach.

## III. PROPOSED METHODOLOGY

### SVM ALGORITHM

In machine learning, support vector machines (SVMs, also support vector networks) are supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall. In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.

When data are not labeled, supervised learning is not possible, and an unsupervised learning approach is required, which attempts to find natural clustering of the data to groups, and then map new data to these formed groups. The clustering algorithm which provides an improvement to the support vector machines is called support vector clustering and is often used in industrial applications either when data are not labeled or when only some data are labeled as a preprocessing for a classification pass.

Support Vector Machine (SVM) is a machine learning tool that is based on the idea of large margin data classification. The tool has strong theoretical foundation and the classification algorithms based on it give good generalization performance.

Standard implementations, though provide good classification accuracy, are slow and do not scale well. Hence they cannot be applied to large-scale data mining applications. They typically need large number of support vectors. Hence the training as well as the classification times is high. With the increasing number of different types of abnormal behaviors detected by smart monitoring cameras, set A shall be enlarged correspondently. With the expansion of abnormal behavior set A, case or events which are closely related to For an given entry E, in event set E, according to the historical case data, the frequency of associated abnormal behavior will be counted and sorted as set S1· For an given entry E, in event set E, according to exports knowledge, all the relevant unusual behaviors are enumerated by priority and labeled as set S2 Get intersection elements S=S1∩S2 End.

**SVM Algorithm:**

**Definition of event set:**

E={bank robbery, Robbery, Riot…}

**Definition of abnormal behavior set:**

A={reading invasion, Entering/Leaving the area, Wandering, Fast movement, Fighting…}

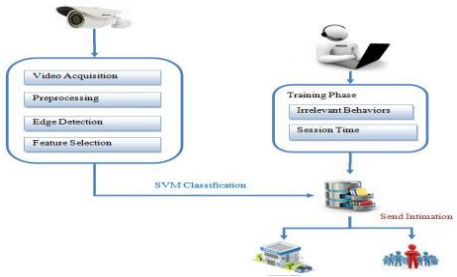



*Figure 1. SVM diagram*

**Improved_SVM algorithm:**

This paper proposed the new enhanced SVM Algorithm is called IMROVED_SVM. This algorithm shows a novel insightful preparing and usage answer for enormous reconnaissance video information in light of the occasion recognition and disturbing messages from front-end shrewd cameras.

**Improved _SVM Algorithm:**

**Input :** Input data matrix, class information
**Output:** Set of Basis vectors
**Begin**
**Repeat**
For every candidate example - examples not in current set of BVs
Include it in the model efficiently
Observe the generalization performance on the remaining points End For candidate examples
Add that point to the BVs' list that gave better test error till the stopping criterion
**End**

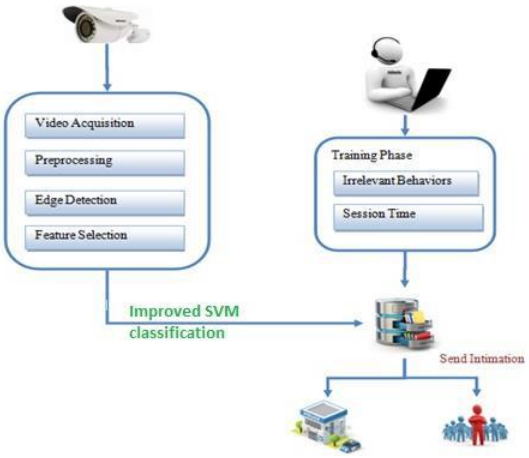



*Figure2. Improved_SVM algorithm*

In the major bank robbery cases happened previously, criminals usually cautiously observed environment around the spot for many times before robberies, so as to decide best chances for committing crimes and routes for escaping as well. The longest observation time even approached hours in a crime committed. The behavior features are very distinguished from normal activities, such as wandering in the target area seemingly to be aimless, repeatedly entering or leaving the place without doing any business

The location of committing crimes .According to the method proposed in this article, in terms of criminal's wandering, we adopt single site period analysis and person re-identification technology to judge whether there are people staying for too long, and fire alarming if the answer is yes. In the upcoming cases, by using multi-spot association analysis.

The criminal not only wandered frequently for a long time in the spot but also behaved similarly in many other places, which thus produces alarming as soon as possible due to its high spatial correlation.

According to the established abnormal behavior database, risk assessment model is constructed based on the potential security risk consequences of anomalous behaviors. Specifically, a risk weight is given for each type of behavior to form a risk weighted table. The abnormal behavior of high potential security risk will be assigned to a large weight value, and vice versa. The occurrence frequency of unusual behavior is counted, which is combined with the risk weight so as to obtain the risk value. The risk value is further mapped into five risk levels. The determination of risk weights not only depends on the potential of different unusual behaviors for instance, fighting is more serious than fast movement but also accounts for the geographical environment of monitoring sites (for instance, financial institution more important than ordinary public places). According to historical criminal cases and the opinions of experts, monitoring target types (corresponding to geographical environment) typically include important facilities (e.g., military facilities, power plants, and urban infrastructures), financial institutions and public places. In contrast, unusual behaviors are much more diversified, for example, typically, running, fighting, wandering, and gathering, and so on. Furthermore, it is acknowledged that abnormal behavior risk to the place of its occurrence, and mean-while it may also be dangerous to the surrounding targets as the criminal space is not stationary. Therefore, the risk weights of unusual behaviors should be examined from two perspectives:

Local risk weights and surrounding risk weights, which indicate the degree of hazard to in-place and around targets, respectively. For example, gathering has almost the same effect on the current locations and the surroundings, but leaving/taking baggage has little impact on the places other than the local one.

Risk value is then calculated by: R

$$R = \sum_{i=1}^{N} W_i n_i$$

Where N is the total warned number of abnormal behaviors, is the risk weight corresponding to abnormal behavior, and is the frequency of abnormal behavior N i w i n i

The risk value is mapped into five levels according to Following Eqn.

$$L = \begin{cases} A, & R \geq 50 \\ B, & 50 > R \geq 30 \\ C, & 30 > R \geq 10 \\ D, & 10 > R \geq 5 \\ E, & 0 \leq R < 5 \end{cases}$$

Where represents extremely high, represents high, represents medium, represents general, and represents no risk, respectively. A B C D E

Depending on the different security requirements of monitoring sites, a set of high-risk abnormal behaviors are constructed for each type of monitoring site. The abnormal behaviors in the set are regarded as potential threats to this type of monitoring site. The definition of high risk abnormal behaviors set is listed as follows:

$$S_I = \{\text{Invasion of the region, Cross-border invasion, Gathering}\}$$

$$S_F = \{\text{Suspicious face, Fast movement}\}$$

$$S_P = \{\text{Gathering, Fighting}\}$$

Where $S_i$ represents important facilities, $S_f$ represents financial institutions, and $S_p$ represents public places.

## IV. RESULT AND DISCUSSIONS

JFreeChart is an open source library developed in Java. It can be used within Java based applications to create a wide range of charts. JFreeChart is open source and 100% free, good accuracy and time result. graph is open source and support all method . it produce the good result. System basic configuration and Java and j-script supported

It comes with well documented APIs, which makes it quite easy to understand. It supports multiple output formats like PNG, JPEG, PDF, SVG etc. It allows extensive customizations of charts.

| Algorithm | Accuracy | Execution Time |
|---|---|---|
| I-SVM | 90-unit | 44 sec |
| KNN | 78-unit | 89 sec |
| SVM | 85-unit | 55sec |

**A Time and Accuracy comparison on playback2 using various algorithm**

Above graph show I_SVM Algorithm is compared with SVM and KNN algorithm for accuracy and time on playback2.avi.Improved_SVM better than the other algorithms. It high accuracy and low time is produced I_SVM Algorithm.

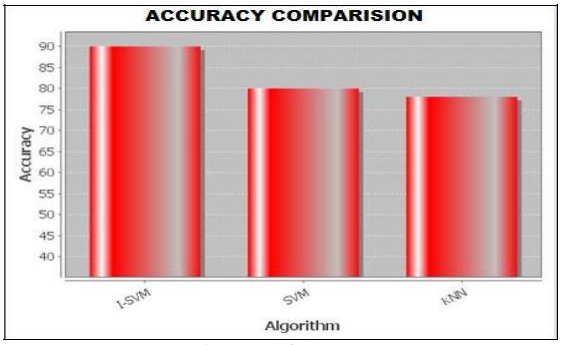



*Figure 3. Accuracy*

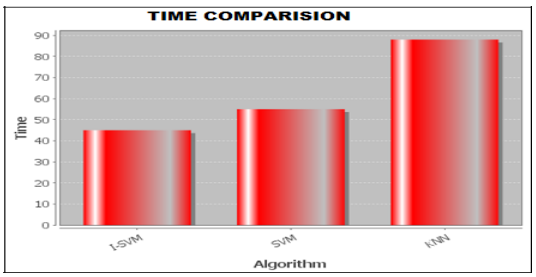



*Figure 4. Time Comparison*

It supports a wide range of chart types such as Pie Chart, Line Chart, Bar Chart, Area Chart and 3D charts.

Consider a situation where you are developing an application and you need to show the data in the form of charts, and the data itself is populated dynamically. In such case, displaying the data in the form of charts using JFreeChart programming is very simple.

In this graph is represented as comparison between SVM and KNN Algorithm on the prediction accuracy and Expectation time.

## V. CONCLUSION

Improved_SVM Algorithm is compared with SVM and KNN algorithm for accuracy and time on playback2.avi.Improved_SVM better than the other algorithms. It high accuracy and low time is produced I_SVM Algorithm. In this video surveillance system, the proposed solution contributes to make full use of detected and alarmed events by smart monitoring cameras. In contrast to the traditional video surveillance system, the proposed solution contributes to make full use of detected and alarmed events by smart monitoring cameras, which thus effectively improves the performance of intelligent surveillance system, promotes the ability to danger pre-alarming, and greatly saves the storage space for surveillance video data. Meanwhile, the surveillance video data relevant to specific cases will be scaled down, which will greatly improve the efficiency for discovering valuable investigation clues. Several practical cases demonstrate that our approach outperforms the existing solutions. An effectively improves the performance of Surveillance System in ATM.In future, to implement the surveillance system in other public places. To implement the different types of classification algorithm analyze the performance

## REFERENCES

[1] Amanze B.C , Ononiwu C.C , Nwoke B.C , Amaefule I.A *"Video Surveillance And Monitoring System For Examination Malpractice In Tertiary Institutions"* 2016

[2] Junjun Jiang, Member, IEEE, Jiayi Ma, Member, IEEE, Chen Chen, Xinwei Jiang, and Zheng Wang *" Noise Robust Face Image Super-Resolution Through Smooth Sparse Representation"* 2016

[3] Du Tran, Student Member, IEEE, Junsong Yuan, Member, IEEE, and David Forsyth, Fellow *" Video Event Detection: From Subvolume Localization to Spatiotemporal Path Search"* february 2014

[4] Ms. Kranti Wanawe 1, Ms. Supriya Awasare 2, Mrs. N. V. Puri *" An Efficient Approach to Detecting Phishing A Web Using K-Means and Naïve-Bayes Algorithms"* 2014

[5] Divya J *" Automatic Video Based Surveillance System for Abnormal Behavior Detection "* 2013.

[6] Gerhard P. Hancke 1,*, Bruno de Carvalho e Silva 1 and Gerhard P. Hancke Jr.*" The Role of Advanced Sensing in Smart Cities"* 27 December 2012

[7] R. Raghavendra1 , Alessio Del Bue1, Marco Cristani1,2, Vittorio Murino1,2 *" Abnormal Crowd Behavior Detection by Social Force Optimization"* 2012
[8] Mubarak Shah *" Automated Visual Surveillance in Realistic Scenarios"* 2014
[9] ABITEBOUL J. et al., *"Turbulent momentum transport in core tokamak plasmas and penetration of scrape-off layer flows"*, Plasma Physics and Controlled Fusion, vol. 55, no. 7, p. 074001, 2013.
[10] ACKOFF R.L*., "From data to wisdom",* Journal of Applied Systems Analysis, vol. 15, pp. 3–9, 2015.
[11] AGERON B., MARIE-LYNEGOURY, SPALANZANI A., *Knowledge Management appliqué aux problématiques de développement durable dans la Supply Chain*, Cahier de recherche n° 2010–03 E5.Version 1, CNRS, 2010.