



- (51) **International Patent Classification:**
G06F 21/31 (2013.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/IT2016/000179
- (22) **International Filing Date:**
20 July 2016 (20.07.2016)
- (25) **Filing Language:** Italian
- (26) **Publication Language:** English
- (30) **Priority Data:**
102015000036552 21 July 2015 (21.07.2015) IT
- (71) **Applicant:** MINDED SECURITY S.R.L. [IT/IT]; Via
Duca d'Aosta, 20, 50129 Firenze (IT).
- (72) **Inventors:** FEDON, Giorgio; Via Cesare Battisti, 78,
31046 Oderzo (TV) (IT). DI PAOLA, Stefano; Via XXV
Aprile, 86, 50019 Sesto Fiorentino (FI) (IT). BRINDISI,
Gianluca; Via Nazionale, 1145 Ponte a Moriano, 55100
Lucca (LU) (IT).
- (81) **Designated States** (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,
MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM,
PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) **Designated States** (*unless otherwise indicated, for every
kind of regional protection available*): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

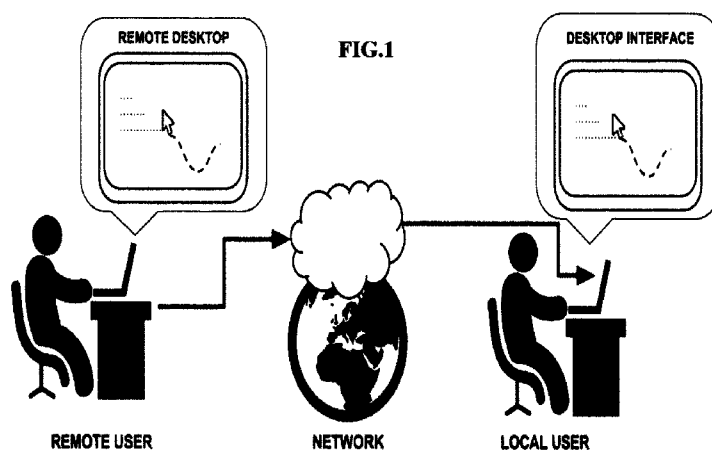
— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments (Rule 48.2(h))*

(54) **Title:** METHOD FOR DETECTING THE USE OF REMOTE SCREEN CONTROL APPLICATIONS THROUGH THE DETECTION AND PROFILING OF ANOMALIES ON THE USER INPUT INTRODUCED BY THE PROTOCOL OF SAID APPLICATIONS



(57) **Abstract:** Recently, the use of the so-called Desktop Sharing programs (RDP from Microsoft and VNC from RealVNC Ltd) has been exploited by cybercriminals as a further means to carry out identity thefts and financial frauds: by installing a malware with a component of "Remote Desktop" in a victim's system, the criminal can control its user session and interact, for example, with the banking portal of the victim on behalf thereof. To date, the operator of an on-line server is not able to establish with certainty whether a client session is native or controlled through a remote desktop system without using software components installed on the user's system. The object of the present invention is to provide a system for the detection of controlled user sessions through the Remote Desktop applications, by means of the profiling of the protocol used based on the anomalies that it produces on the user's input. These anomalies are constant and are normalized with respect to the traditional user biometric detection, and thus are a direct and measurable reflection of a remote connection in use. To simplify the implementation and usability of the system, an object is also to realize an "agent-less"-type solution, i.e., without the need for installing third-party software's on users' systems.



Method for detecting the use of Remote Screen Control applications through the detection and profiling of anomalies on the user input introduced by the protocol of said applications

Background art

5 The term “Remote Desktop” or “Desktop Sharing” refers to the ability of a computer system, by means of a special application, of opening an interactive user session on a remote computer. Such systems are commonly used to interact with a physical machine for maintenance, technical support, and remote administration purposes. The various
10 solutions on the market of “Desktop Sharing” are based on different proprietary or open-source communication protocols, of which the most popular are RDP from Microsoft and VNC from RealVNC Ltd. Recently, the use of such programs has been exploited by cybercriminals as a further means to carry out identity thefts and financial frauds: by
15 installing a malware with a component of “Remote Desktop” in a victim's system, the criminal can control its user session and interact, for example, with the banking portal of the victim on behalf thereof. It is therefore difficult for the banking portal to detect accurately whether a session is legitimate or it is remotely controlled, as the traditional
20 detection indexes such as the IP address and the characteristics of the system used are unchanged. In addition, the client side code of a web portal does not have the privileges to apply traditional remote desktop detection solutions such as those used by an anti-virus software. To try to distinguish between legitimate sessions and controlled remotely
25 sessions, the so-called anomaly detection systems have been developed,

which are based on biometric profiling of the users easily acquirable through the web portal: a user's interaction with the web page is measured in the order to create a "behavioural profile" of the same to be used later as a reference metric to detect abnormal interactions. Such systems have in the first place the disadvantage of not being deterministic, and in the second of requiring large resources to collect and process the required amount of data to be able to build the behavioural profiles of each user. Finally, the detection is not strictly connected to the use of a remote desktop but more simply the purpose is to try to distinguish the use of a same session by different individuals.

To date, the operator of an on-line server is not able to establish with certainty whether a client session is native or controlled through a remote desktop system without using software components installed on the user's system. There are user identity verification solutions (patent WO2014105994A3 of NokNok Labs, patent US20050008148 of Biocatch, patent US20140289820 of Behaviosec) characterized by the use of biometric and behavioural metrics that specifically detect the protocol characteristics while using a Remote Desktop software but, more generally, identify whether the same session is used by individuals with different biometric/behavioural profiles. Alternatively, detection systems that require third-party software components to be installed locally on the monitored system (Method and apparatus for remote desktop control identification CN 103428190 A). Compared to such systems it is desirable for a solution that does not require third-components nor a profiling history, and especially that is independent

from behavioural/biometric aspects of individual users whose alterations, detected for example by means of the above patents, may not necessarily imply a wilful misconduct.

An alternative approach to the solutions proposed consists in identifying
5 abnormal features in the sequence of inputs sent that does not depend on the user's actions but rather are introduced by the Desktop Sharing protocols.

Disclosure of the invention

10 The object of the present invention is to provide a system for the detection of controlled user sessions through the Remote Desktop applications, by means of the profiling of the protocol used based on the anomalies that it produces on the user's input. These anomalies are constant and are normalized with respect to the traditional user biometric
15 detection, and thus are a direct and measurable reflection of a remote connection in use. To simplify the implementation and usability of the system, an object is also to realize an "agent-less"-type solution, i.e., without the need for installing third-party software's on users' systems.

20 The proposed solution is to detect user input data via an application normally used by the user, for example a web browser that executes JavaScript code when the user visits a web page. This code collects the user's input telemetry, and processes it directly, or sends it asynchronously to a remote server that is able to process the received data. By processing the collected data, four metrics are extracted whose

comparison with reference profiles allows to identify which of the remote desktop protocol family is associated with the activity measured.

Brief description of the drawings

Further characteristics and advantages of the proposed technical solution will appear more evident in the following description of a preferred but not exclusive embodiment shown by way of example and not limitation in the accompanying 5 drawings, in which:

- Fig.1 shows the typical situation in which a desktop session of a system is remotely controlled through a Remote Control software.
- Fig.2 is an example implementation in which a user via a Remote Desktop application connects to a remote desktop from which the user uses the browser to access a web page. This page includes the measurement code of the detection system that measures the user input data and sends them to a processing server, where the data are processed to extract the metrics and obtain the detection result. This result, ultimately, is saved in a database for future or immediate consultation.
- Fig.3 indicates the process for measuring and analysing a user's input in order to detect the presence of a remote control. This process is carried out in five steps: measuring the user's input such as keyboard and mouse, collecting the data, processing the data and extracting the metrics, comparing the processed data with the reference models.

- The Figure 4 represents in detail the four metrics used to calculate the result of the detection.
- Fig.5 shows the periodic tuning process by which the processing system is trained by defining the protocol profiles to be used as a reference and by carrying out further classification of the data in relation to the measuring system used (version of the application used and operating system), and to allow a more precise profiling of the protocol.

Best mode for carrying out the invention

In a case of a remote session via a Remote Desktop application (Fig.1), the user input data are collected by a JavaScript code installed on a web page being monitored (Fig.2). In the case of mouse movement data, the coordinates of the pointer on the page are measured at every moment and time for each coordinate. The data thus collected are processed to extract the four major indexes: “data burst index”, “data burst density”, “sampling density”, “frequency index”. These four dimensions are further processed to derive: the estimated proximity of the observed connection, the estimated latency, and finally the profile of the Remote Desktop Protocol used. These dimensions make up the result of the detection.

The process is defined by the following steps (Fig.3): In a first phase, the times of each sampling $[Tc_n]$ are collected, along with the number $[n]$ thereof and the sequence $[\Delta time]$ of temporal distances between each

sampling. The data thus collected are processed in four successive analysis steps to produce four indexes (Fig.4), which are:

- (Fig. 4.1) “Data Burst Index” [DBI]: this metric is calculated from $[\Delta\text{time}]$ and represents the number of samples, as a percentage of total $[n]$, whose temporal distances are smaller than a given threshold $[\text{th}]$. These values are called Data Bursts [DB]
- (Fig. 4.2) “Data Burst Density” [DBD]: this index measures the percentage of total Data Bursts [DB] sent in succession.
- (Fig. 4.3) “Sampling Density” [SD]: this metric represents the density based on the sampling time except for the values driving from the inactivity or termination of user's activity, which are excluded from the calculation to filter the result from the influences of any behavioural aspects.
- (Fig. 4.4) “Frequency Index” [FI]: calculated as a given percentile $[\text{p-th}]$ of the cumulative frequency of $[\Delta\text{time}]$.

At this point, the four main metrics are further processed to produce additional parameters:

- The estimated proximity [proximity] of the connection, which is calculated by comparing $[n]$, [DBI] and [SD], and indicating whether the observed connection is “local” or “remote”. This index defines an abstraction layer in turn consists of:
- The estimated latency [latency] of the network connection, the value of which is conditioned by both the desktop sharing protocol

used and the distance in terms of network hops between the monitored user and the controller.

- The Remote Desktop Protocol profile used [ratdet].

5 These new dimensions make up the result of the detection.

The threshold values of the variables used during all processing phases can be modified, if necessary, in order to increase the accuracy of the system. Such values may be previously calculated through a “tuning” phase of the system (Fig.5) in which the produced data are measured
10 from different sample interactions (“training set”), characterized by different combinations of Remote Desktop systems and protocols. The detection indexes are normally extracted from these measurements, the detection indexes being then grouped into clusters according to different parameters of closeness. This process has the purpose of identifying the
15 threshold values producing a cluster set that leads to minimum occurrence of false positives/negatives.

For further clarity, below we show an implementation of the method using a common web page. The page in question contains a JavaScript code that is responsible for collecting the user input data, in this case the
20 telemetry of the mouse movement, and sending that data asynchronously to a remote server used for the processing phase.

As shown in Fig.2, a remote user via a Remote Desktop software interacts with the browser of the controlled system used to access the page that contains the monitoring code. The collected data are sent to the
25 remote server that performs the process explained in the previous paragraph and represented in Fig.3 to extract the dimensions that

compose the detection. The web application that contains the page to be monitored can query the processing server to obtain the analytical result and, in case of positive detection, can decide whether to take action on the user's session and, if necessary, to block or invalidate it.

5

Industrial applicability and implementation options

By way of example and not of limitation, it is observed that different sources of measured user input data can be used ("mouse", "keyboard", etc.) and that further data can be considered such as, by way
10 of example and not of limitation, the profile of the user system (browser, operating system, etc.) and the interfaces that interact by application proxy to the native user interface of a system, such as virtualizations of desktop interfaces and alternative remote control systems.

The proposed solution is effective in distinguishing whether the use
15 of a Desktop interface takes place locally or remotely. With the term local is meant a condition of proximity where the user is using devices connected physically with the computer whose operating system shows the graphical interface or Desktop interface. The proximity analysis allows to detect whether a user session is subject to a remote control
20 without having to construct a user biometric and/or behavioural profile but only through the measurement and the identification of anomalies in data transmission that depend on the remote control protocol in use. This distinction is archived by comparing the deviation of the metrics with respect to the local profile, while the identification of the specific
25 desktop sharing protocol is carried out by analysing the relationships

between the identified metrics. Another advantage of the proposed method is related to the increase of detection accuracy thanks to the increase of the connection latency, which increases proportionally with the network hops (network distance) between the controller and the controlled subject.

The proposed solution applies in particular to the risk control systems of financial transactions, such as anti-fraud systems for banking portals. In this case, it is monitored whether the user who is performing the transaction is using the own device locally. This solution also applies to the risk analysis on the use of authentication and validation systems of the navigation session and, in general, to the integration with the monitoring systems to prevent cyber attacks, where the remote control condition is a known attack vector to circumvent security defences.

CLAIMS

1. A method for detecting the use of desktop remote control applications through the detection and profiling of user's input anomalies introduced by the protocol of such applications and characterized by the following steps:

A) Collecting the user input data provided by a client code executed in the context of an application being monitored;

B) Detecting the input data such as the telemetry of the movement and the sequencing of the events produced by mouse, keyboards, or similar devices;

C) Extracting, from the sequence of the above samples, the sampling times $[T_{cn}]$, the number of samples $[n]$, and the sequence $[\Delta time]$ of time intervals between each sampling;

D) Processing the data collected and extracting four main parameters, i.e., "data burst index" $[DBI]$, "data burst density" $[DBD]$, "sampling density" $[SD]$, "frequency index" $[FI]$;

E) Identifying if the user session is controlled by a Remote Desktop Application through a connection proximity parameter $[proximity]$ obtained by measuring the distance between the vector of components $[DBI]$, $[DBD]$, $[SD]$, $[FI]$ and a reference cluster related to sessions executed in local mode;

F) Identifying the type of remote desktop protocol $[ratdet]$ by verifying the possible belonging of the vector of components $[DBI]$, $[DBD]$, $[SD]$, $[FI]$ to the reference clusters related to known remote desktop protocols;

G) Calculating the quality of the connection [latency] comparing the vector of components [DBI], [DBD], [SD], [FI] with specific thresholds of the clusters related to known protocols.

2. Method according to claim 1, wherein said "Data Burst Index" [DBI] parameter is calculated from the data sequence [Δ time] and represents the percent number of the samples of "Data Burst" [DB] type as compared to the number of total samples [n], said samples being characterized by temporal distances less than a predetermined threshold [th].

3. Method according to claim 1, wherein said "Data Burst Density" [DBD] parameter measures the percentage of the samples of [DB] type, as compared to the total, sent in the group i.e. in temporal succession.

4. Method according to claim 1, wherein said "Sampling Density" [SD] parameter represents the density in time of the samplings obtained by excluding the values attributable to behavioural nature, such as those resulting from stationing or any cessation of activity by the user.

5. Method according to claim 1, wherein said "Frequency Index" [FI] parameter is calculated as a given percentile of the cumulative frequency [Δ time].

6. Method according to claim 1, points E), F), G), wherein said reference cluster and the relevant thresholds are calculated by measuring and combining the vectors of components [DBI], [DBD], [SD], [FI] at different combinations of operating systems, applications, remote desktop protocols, and latencies known a priori.

7. Method according to claims 1 and 6, wherein said reference cluster is updated by means of a periodic tuning carried out manually or automatically using statistical inference, and validated manually.

5

10

15

20

25

30

FIG.1

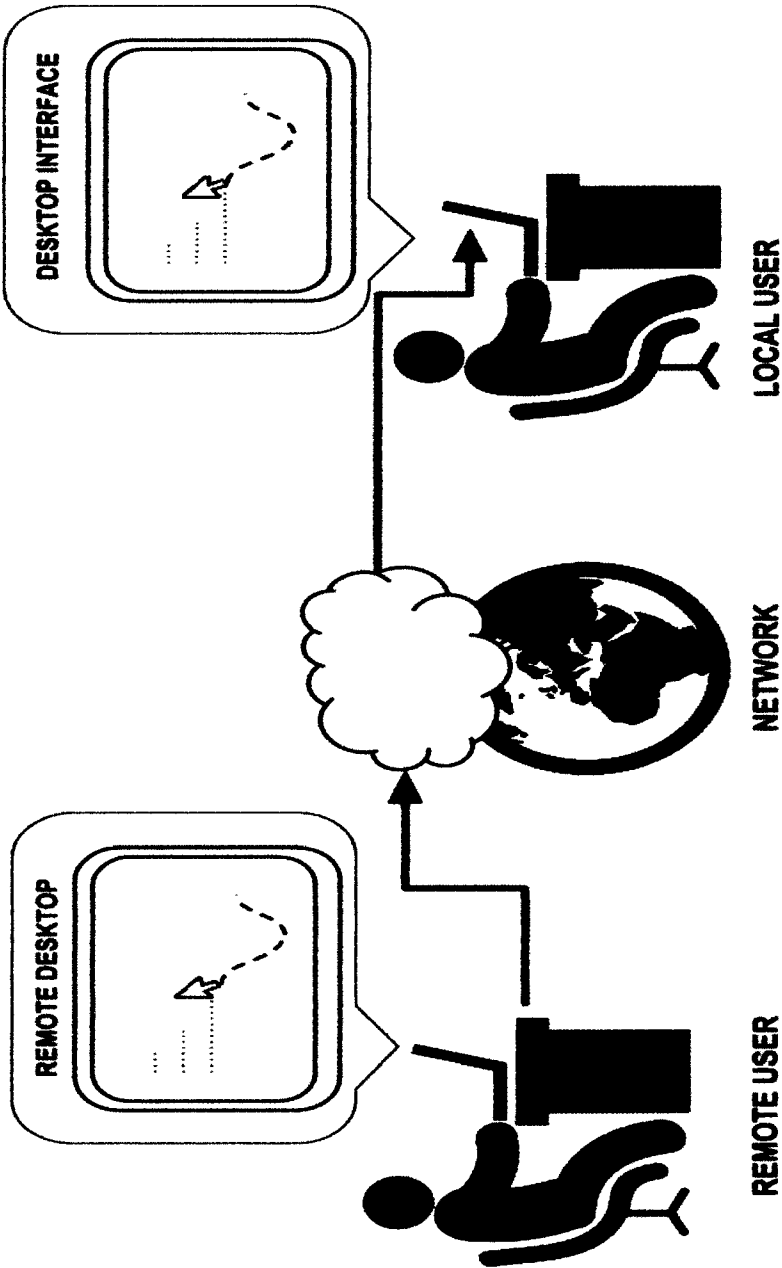


FIG.2

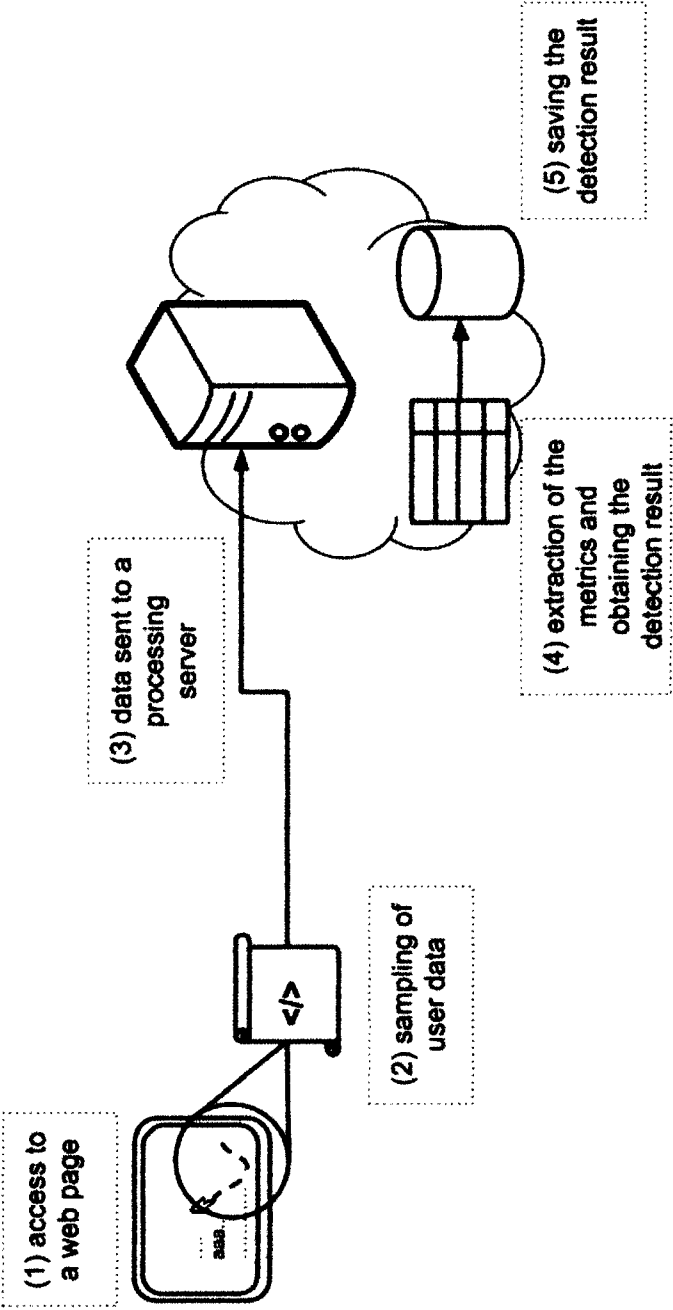


FIG.3

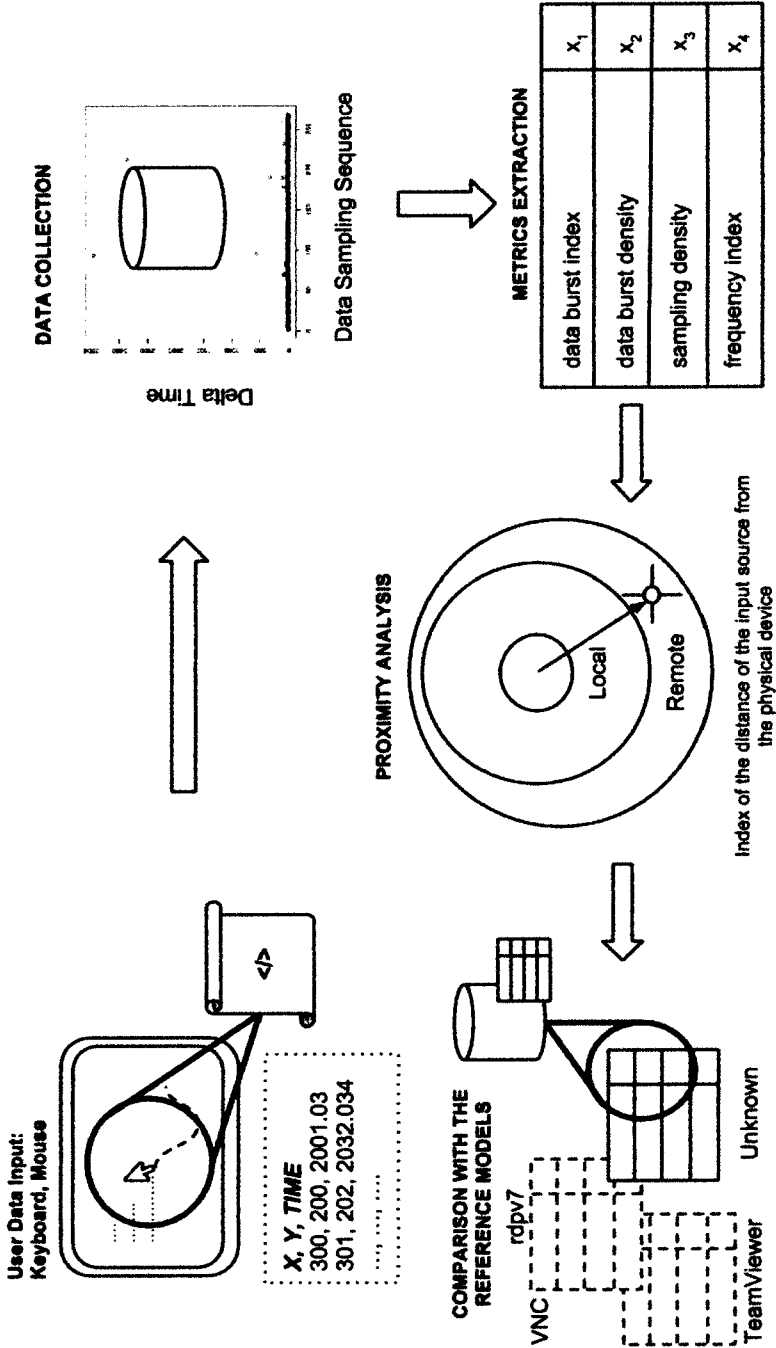


FIG.4

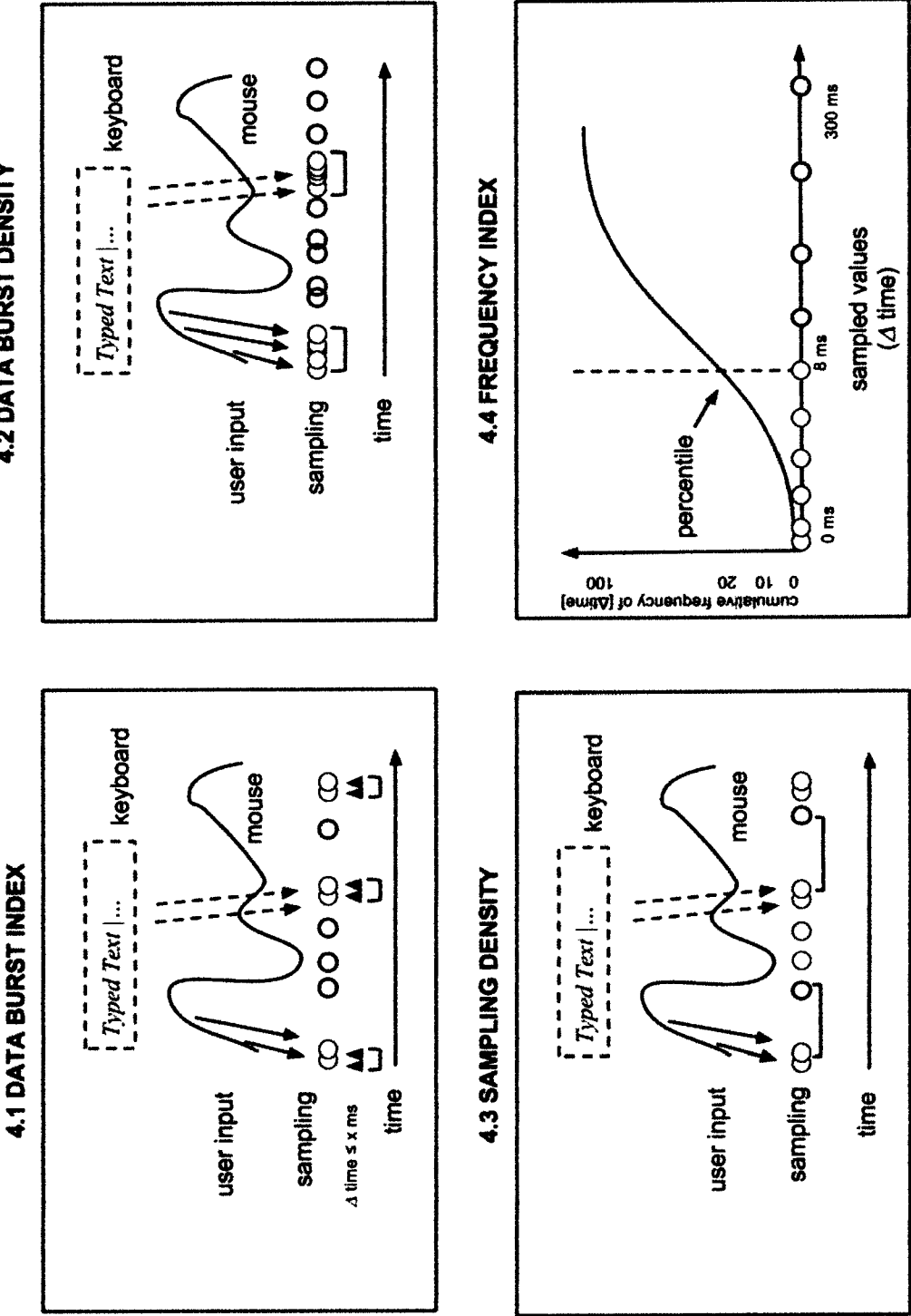
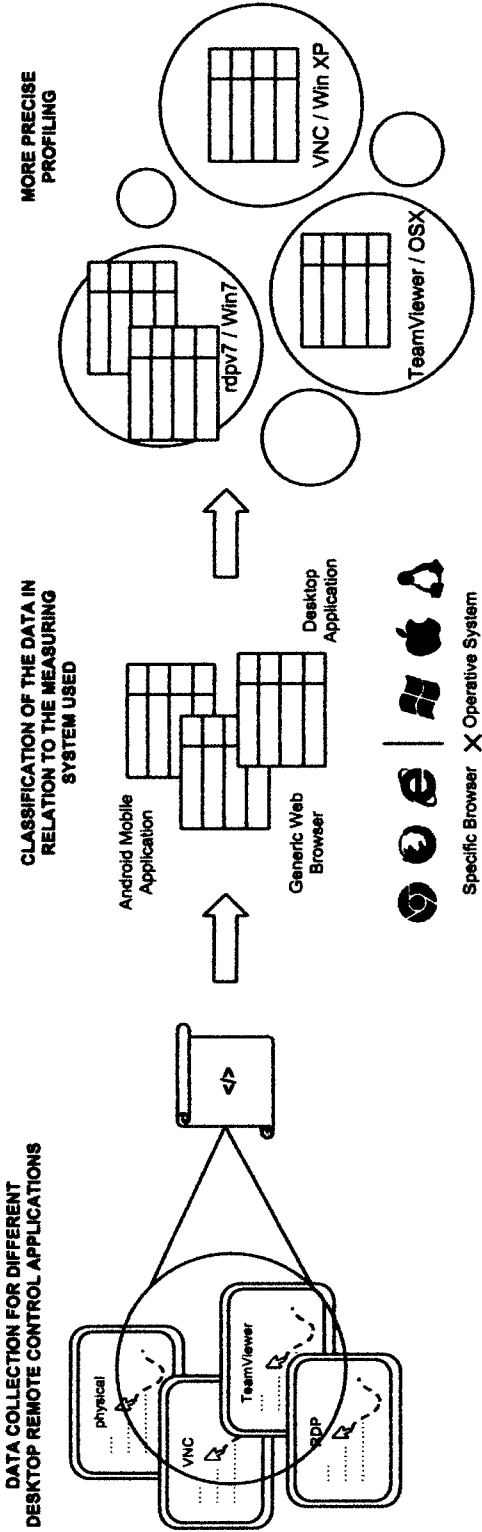


FIG.5



INTERNATIONAL SEARCH REPORT

International application No
PCT/IT2016/000179A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/31 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/317744 A1 (TURGEMAN AVI [US] ET AL) 23 October 2014 (2014-10-23) abstract paragraph [0009] - paragraph [0030] paragraph [0050] paragraph [0178] - paragraph [0181] ----- -/--	1-7



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

1 December 2016

Date of mailing of the international search report

08/12/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bertolissi, Edy

INTERNATIONAL SEARCH REPORT

International application No
PCT/IT2016/000179

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Biocatch Biocatch: "Detecting Remote Access (RAT) Attacks on Online Banking Sites", A BioCatch White Paper, 3 July 2014 (2014-07-03), XP055257988, Retrieved from the Internet: URL: http://informationsecurity.report/Resources/Whitepapers/bbb3b0fb-9ba1-4602-8cec-17dcb2381892_detecting-remote-access-attacks-on-online-banking-sites-pdf-7-w-1088.pdf f [retrieved on 2016-03-14] the whole document -----	1-7
A	ZHONGQIANG CHEN ET AL: "Catching Remote Administration Trojans (RATs)", SOFTWARE PRACTICE & EXPERIENCE, WILEY & SONS, BOGNOR REGIS, GB, vol. 38, no. 7, 1 June 2008 (2008-06-01), pages 667-703, XP007917689, ISSN: 0038-0644, DOI: 10.1002/SPE.837 [retrieved on 2007-08-09] abstract Sections 1 and 2 -----	1-7
A	CN 103 428 190 A (ALIBABA GROUP HOLDING LTD) 4 December 2013 (2013-12-04) cited in the application abstract -----	1-7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IT2016/000179

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014317744	A1	23-10-2014	NONE

CN 103428190	A	04-12-2013	NONE
