RUCAPILLAN IP

TRUE IP PARTNER

# FTO SEARCH

**CONFIDENTIAL**

***Prepared for:***

***Blockchain 5.0 Ltd,***
***Tallinn, Estonia***

**June 15, 2022**

## Table of Contents

## 1. Objective

The objective is to conduct a freedom to operate search in all jurisdictions and identify patent references relevant to the concept of **zero vulnerability computing (ZVC).**

## 2. Summary/ Key-features

The following are the key-concept of the Zero Vulnerability Computing (ZVC).

**ICOS (In-Computer Offline Storage)** is easier to comprehend as it`s as simple as its acronym In the state-of-the-art the architecture of a computer mandates a provision for non-volatile memory for storage of user data. Consequently, when a computer is connected to the network the user data stored in the memory also remains exposed to the risks associated with the network. Currently there is no way to keep the data off network risks if the computer remains connected to the network. Neither can a computer be of any use without personal storage. ICOS creates a user-controlled personal offline storage within the computer itself.

**Supra OS (SOS)** challenges another core fundamental rule that legacy computing systems follow: "No computer can be built without granting installation and operation permissions to 3rd party applications." Such permissions are often exploited by the bad actors by creating malware as attack vectors that attack computer thus creating an attack surface. An attack surface is essentially the entire external-facing area of a computing environment. It contains all of the vulnerabilities or attack vectors; a hacker could use to gain access to a computing system. The “attack surface” is simply the total digital resources that are exposed to threats across the enterprise. It may be exploited at hardware, firmware, at Operating System (OS) level (primary attack surface) or even via application layer (secondary attack surface). SOS obliterates the attack surface by blocking all 3rd party permissions that allow 3rd party applications to run over the computer. However, such banning of all writing / installation permissions is compensated by allowing such 3rd party applications to run from a remote server.

**ZVC on solid-state software on a Chip (3SoC):** ZVC can be directly implemented on the non-volatile NAND flash memory without having to piggyback on any legacy firmware or OS. A Zero Vulnerability Computing (ZVC) system wherein all software layers between human computer interface (HCI) and firmware running on computer hardware are merged into single layered solid-state software on a Chip (3SoC) that declines all third-party permissions thus obliterates any attack surface that introduces vulnerabilities inherent with the conventional computing systems.

**In-Computer Offline Storage (ICOS) Device with Toggle Switch and Charging Port)** design is one of its kind, which is utilized for installation and execution of program application. No data or program is stored in the In-Computer Offline Storage (Icos) Device. The In-Computer Offline Storage (Icos) Device comprises a toggle switch with a charging port.

Prior art assumes that it is impossible to build computers without 3rd party write permissions to install applications. In the age of 5G that assumption is outdated and misplaced. There's no conceivable application that cannot run from a remote server. Once these nuances are understood, we can comprehend how the existing complexities in designing computers can be eliminated and how real solid-state computers of future generation can be built with no or minimal moving parts (software).

Thus ZVC challenges both prior art rules of computer design by disclosing ICOS and SOS and achieving Zero Vulnerability Computing.

| S. No | Application Number | Title | Priority Date |
|---|---|---|---|
| **1** | US63/202,188 | Zero Vulnerability Computing (ZVC) For The Next Generation Internet Devices | 05/31/2021 |
| **2** | US29/788,593 | USB Device With Toggle Switch | 06/30/2021 |
| **3** | US63/228,122 | In-Computer Offline Storage (ICOS) To Achieve Zero Vulnerability Computing (ZVC) | 05/31/2021 |
| **4** | US63/351,924 | Solid State Software On A Chip (3SOC) For Building Quantum Resistant Web 3.0 Computing Devices | 06/15/2022 |
| **5** | US29/842,535 | In-Computer Offline Storage (ICOS) Device With Toggle Switch And Charging Port) - Design | 06/15/2022 |

## 3. List of References

Table 1 shows the patent references which are relevant to the subject invention.

Table 2 shows the non-patent references which are relevant to the subject invention.

### Table 1 – Patent References

| S. No | Publication Number | Title |
|---|---|---|
| 1 | CN112416656A | Data offline storage method for station application server |
| 2 | US20200213385A1 | Offline mobile data storage system and method |
| 3 | CN103530388A | A cloud storage system to improve the performance of data processing method |
| 4 | CN104112455B | A data storage and read-write device, method and system based on offline disk library |
| 5 | US20200334372A1 | Offline data storage device |
| 6 | CN102664823A | Receive data off-line in the instant communication method, client terminal and system |
| 7 | WO2020000765A1 | Off-line data storage method and apparatus, computer device and storage medium |
| 8 | CN109284244A | An off-line data synchronous storage system |
| 9 | CN112115495A | An off-line cloud data storage method, system, computer device and storage medium |
| 10 | CN111290717A | A Bluetooth communication based on offline data storage device |
| 11 | US20130333021A1 | Preventing malicious software from utilizing access rights |
| 12 | US20130086670A1 | Providing third party authentication in an on-demand service environment |

## 4. Scope/Search Analysis

1. Various search techniques such as Nested Boolean search, Phrase Searching, Synonyms and Truncation searching, Patent class search, citation searching etc. are used.
2. The search was also conducted based on the Title, Assignee and Inventors of the subject invention and competitor, if provided.

### Keywords

| | | | | |
|---|---|---|---|---|
| Supra | OS | Operating System | Layer | Vulnerability |
| Protect | Attack | Surface | Protective | Zero |
| Nil | Reduced | Minimum | Computing | Device |
| `Computer | System | ICOS | In-computer Offline Storage | Cloud |
| Offline Storage | Switch | RAM | Memory | No Access |
| 3rd Party | External | Applications | Software | Permissions |
| Access | Malware | Firmware | Writing | Reading |

## 5. Patent & Non-patent Databases

Google Patents, USPTO, Espacenet and Derwant Innovation

**Search period:** Till October 7, 2021.

# 6. Patent References

## 6.1 Patent Reference 1: CN112416656A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN112416656A |
| Title | Data offline storage method for station application server |
| Abstract | *The invention claims a data off-line storage method for station application server, the method uses off-line data storage mode, the terminal software sends the operation line, scheduling command data for processing, storing in the local file and double-machine synchronous backup. Compared with the existing technology, the invention has the advantages that the station does not install database to realize local storage of data.* |
| Publication Date | 2021-02-26 |
| Application Date | 2020-12-08 |
| Priority Date | 2020-12-08 |
| Assignee | Casco Signal Co. Ltd. |
| Inventors | Wu, Xiang \| Lu, Ying-Tao \| Cao, Ya-Hui \| Chen, Zhen-Jie \| Wang, Ya-Fei \| Ke, Jian \| Chen, Hai-Huan \| Zhang, Peng |
| INPAOC Family Members | CN112416656A |
| Independent Claims | 1. A data off-line storage method for station application server, wherein the method uses the off-line data storage mode, the operation line sent by the terminal software, the scheduling command data is processed, and stored in the local file and the double-machine synchronous backup is executed. |
| Reviewer`s Comments | *This patent essentially discloses client-server architecture for sporadic access of remotely saved offline data by client computer. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.2 Patent Reference 2: US20200213385A1

Click to return to the list of references

| | |
|---|---|
| Publication Number | US20200213385A1 |
| Title | Offline mobile data storage system and method |
| Abstract | *A system and method is provided for the quick and efficient transfer of large amounts of data to mobile devices from enterprise asset management software residing on a primary server, via an intermediary server in a seamless and streamlined fashion, making the downloaded data available accessible by users of the mobile devices ahead of time, anywhere and at any time in an offline (disconnected) or online (Internet connected) mode.* |
| Publication Date | 2020-07-02 |
| Application Date | 2020-03-09 |
| Priority Date | 2018-02-09 |
| Assignee | InterPro Solutions LLC, |
| Inventors | Lee, Jack \| O'Connell, Eric James |
| INPAOC Family Members | US20200213385A1 \| US10587675B2 \| US20190253476A1 |
| Independent Claims | *1. A system for interacting with at least one external client server that is accessible via a wireless network, comprising: at least one external client server having raw client data stored thereon, an intermediate server connected between the at least one external client server and a plurality of clients, the intermediate server configured to perform functions associated with executing client data requests directed to the at least one external client server, including: a) configuring a database schema configuration (DBSC) file unique to each client during a pre-configuration stage, wherein the DBSC file informs the intermediate server regarding what tables to build to accommodate the client data received from the at least one external client server prior to forwarding the data to the plurality of clients in response to client data requests, b) converting client data retrieved from the at least one external client server into one or more SQLite compatible tables, stored as a SQLite file as part of each client's uniquely configured DBSC configuration file, c) encrypting the SQLite file, and d) downloading the encrypted SQLite file for eventual storage in an SQLite database on the client's mobile devices.*<br>*7. A database schema configuration (DBSC) file uniquely assigned to each client during a pre-configuration stage, the DBSC file configured at an intermediate server detailing all aspects of one or more SQLite compatible* |

| | |
|---|---|
| | *tables to be transferred to client mobile devices, including all tables, indexes and data retrieval actions that define the communications between a client's external client server and the intermediate server to request and retrieve information.*<br>*10. A dynamic load balancing unit employed at a computing device in a network, comprising: an application server responder unit, employed at one or more external client servers and configured to access relevant data provided by the one or more external client servers, wherein said relevant data includes details about the one or more external client servers such as the amount of requests in the queue, the number of responses to requests performed during a given period of time, a load balancer, for performing load balancing among the one or more external client servers, based on a capacity measure, and a performance facilitator unit, configured for facilitating load balancing at the relevant one or more external client servers according to their assigned priorities, such that a client server with the highest priority is assigned a user request before other client servers.*<br>*15. A method invoked by a configurable intermediate server for downloading raw XML data from a client's external client server and restructuring the raw XML data into a more readable and usable structure, the method comprising: invoking a first functional module to read a database schema configuration (DBSC) file for a particular client by utilizing input streams received from said client's external client server, invoking a second functional module to parse the database schema configuration (DBSC) file to retrieve indexes, unique columns and data retrieval actions, to yield a parsed DBSC configuration file for a particular client and creating a JAVA Object from the parsed DBSC configuration file. invoking a third functional module to establish a connection with said client's external client server to retrieve raw client data and utilize the JAVA Object to execute the start of data retrieval actions from the client's external client server, invoking a fourth functional module to retrieve said raw data from said client's external client server, and invoking a fifth functional module to process the retrieved raw data into an SQLite database using an SQLite embedded database engine.* |
| Reviewer`s Comments | *This patent discloses a system for interacting with external client server that is accessible by wireless network, comprises external client server that stores raw client data, and intermediate server that is connected between external client server and clients. The clients can access data in offline and in online mode. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

### 6.3 Patent Reference 3: CN103530388A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN103530388A |
| Title | A cloud storage system to improve the performance of data processing method |
| Abstract | *The invention relates to the field of cloud storage, and claims a cloud storage system to improve the performance of data processing method, comprising a metadata management system, an online data storage system, near-line data storage system, off-line data storage system and a client end, wherein the only transmission of control signals between the metadata management system and the client end, it does not transmits the stored data stream, client end between the online data storage system for storing the data stream transmission. through data migration of different devices in the cloud storage system, so that devices of different configuration can be effectively used, improving utilization rate of the whole cloud storage system, through data blocking, increasing concurrency of data so as to improve IOPS and bandwidth, the read/write time, improve the performance, using the cloud storage system device, based on the hardware access is completely realized, implementing, implementing problem is smaller by the software. also can be popularized and used on large data platform.* |
| Publication Date | 2014-01-22 |
| Application Date | 2013-10-22 |
| Priority Date | 2013-10-22 |
| Assignee | Inspur Electronic Information Industry Co. Ltd. |
| Inventors | Liu, Gang |
| INPAOC Family Members | CN103530388A |
| Independent Claims | 1. A cloud storage system to improve the performance of data processing method, comprising a metadata management system, an online data storage system, near-line data storage system, off-line data storage system and client end, wherein only for the transmission of the control signal between the metadata management system and the client end, it does not transmits the stored data stream, client end between the online data storage system for storing the data stream transmission, wherein online data storage system efficiency. cost is high for storage system access frequent active data, near-line data storage system efficiency, moderate cost, some active difference in |

| | |
|---|---|
| | main storage, access to a hotspot data, offline data storage system has low cost, low access efficiency is mainly used for system archiving and backup, inactive storing the hotspot data. |
| Reviewer`s Comments | This patent describes a cloud storage system performance data processing method comprising a metadata management system, an online data storage system, near-line data storage system, off-line data storage system and a client end. *in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.4 Patent Reference 4: CN104112455B

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN104112455B |
| Title | A data storage and read-write device, method and system based on offline disk library |
| Abstract | *The invention claims a disc library based on off-line data storage and read/write device, method and system, the device comprises: a plurality of offline disk base, a disc library body configuration of each offline disk base with several disc cartridge; each disc is provided with several CD box for storing CD, the offline disk library for storing the compact disk data under the condition of not power off disk library device operation, mobile access to each of said plurality of offline disk library for the corresponding off-disc library, and the storing and reading of data. The invention can finish the automatic loading of the optical disc, concurrent read and write, automatic detection, automatic printing function.* |
| Publication Date | 2017-03-15 |
| Application Date | 2014-05-04 |
| Priority Date | 2014-05-04 |
| Assignee | Suzhou Netzon Information Storage Technology Co. Ltd. |
| Inventors | Zhu, Ming |
| INPAOC Family Members | CN104112455B \| CN104112455A |
| Independent Claims | 1. CD container (1) configured with a plurality of disk library (2) 1. A disc library based on off-line data storage and read/write device, wherein said device comprises multiple offline disk base, each of the offline disk base in. each said disc (1) is provided with several CD box (12) for storing the optical disk (8), the offline disk library for storing the compact disk data under the condition of not power off CD jukebox operating device, can be moved to access each of said plurality of offline disc library, is the corresponding offline disc library, and finishing the storing and reading and writing of data.<br>13. A disc library based on off-line data storage and reading and writing method, wherein it comprises the following steps: S1. building a disk library by multiple offline data storage centre, and initializing the device in the disc (8) in the compact disc driver (52) and scanning the information of an optical disc (8) in database S2. When recording data, each time recording comprises recording and verifying step, then scanning the immediate information of the |

| | |
|---|---|
| | disc recorded data are updated in the database, power storage, S3. The step S2 of the database, which realizes the searching function, locating to the corresponding file of CD position, S4. access target disk (8) is located off-line disk base, it is electrified, and disk, S5. the target disc (8) in the compact disc driver (52), to read and write the target CD (8); S6. the target disc (8) back off disk base, and off to finish the storing and reading of offline data.<br>15. A disc library based on off-line data storage and read-write system, wherein comprises the following modules: an initialization module constructed by multiple offline CD jukebox data storage centre, and initializing the device, data recording module. the offline disc into the compact disc driver (52) and scanning the data of CD database, disc information updating module, recording data, each time recording comprises recording and verifying step, then scanning the recorded data disk for updating information in the database; compact disc retrieval module, according to the database, can realize the searching function, and locating the searching file corresponding to the position on the disc, disc grabbing module, access target disk (8) is located off-line disk base, to disc grabbing; the electrified and write module, the target disk (8) in the compact disc driver (52), reading and writing the target disk (8), disk reset module, the target disc (8) back off disk base, and off. |
| Reviewer`s Comments | *This patent describes an Offline compact disk library data storage reading and writing device, which has compact disk library provided with multiple compact disk cartridge chambers, where library is electrified for storing, reading and writing data in compact disk. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.5 Patent Reference 5: US20200334372A1

Click to return to the list of references

| | |
|---|---|
| Publication Number | US20200334372A1 |
| Title | Offline data storage device |
| Abstract | *Systems, devices, and/or computer-implemented methods for secure offline data storage are provided herein. More particularly, a system is provided that permits access to a data storage device when offline from various components of the system. Furthermore, the disclosed system may permit the re-setting of authentication passwords/PINs for the data storage devices, even when such data storage devices are offline from other components of the system.* |
| Publication Date | 2020-10-22 |
| Application Date | 2020-04-20 |
| Priority Date | 2019-04-19 |
| Assignee | DataLocker Inc. |
| Inventors | Kim, Jay W. \| Kim, David \| Sananikone, Kean |
| INPAOC Family Members | US20200334372A1 |
| Independent Claims | 1. A data storage device comprising: a secure memory configured to securely store data; a processor; and a communications port configured to connect said data storage device with a host device, wherein said data storage device is configured to connect with a remote device over a communications network, wherein said data storage device is associated with an offline occurrence value indicative of a number of occurrences that said data storage device is permitted to connect in data communication with the host device while said data storage device is offline and unable to connect with the remote device over the communications network, wherein said data storage device is configured to determine, based on the offline occurrence value, whether said data storage device is permitted to connect in data communication with the host device, wherein said data storage device is configured to modify the offline occurrence value upon each occurrence of said data storage device being in data communication with the host device. \|<br>8. A computer-implemented method for authorizing a data storage device to be in data communication with a host device, said method comprising the steps of: providing the data storage device, wherein the data storage device is configured to connect with a remote device over a communications |

| | |
|---|---|
| | network, wherein the data storage device is associated with an offline occurrence value indicative of a number of occurrences that the data storage device is permitted to connect in data communication with the host device while the data storage device is unable to connect with the remote device over the communications network; coupling the data storage device with the host device; receiving a password via the data storage device; determining, based on the offline occurrence value, whether the data storage device is permitted to connect in data communication with the host device; authorizing the data storage device to be in data communication with the host device, and modifying the offline occurrence value.<br>16. A data storage device for securely storing data, said data storage device comprising: a secure memory configured to securely store data; a processor; a key input configured to receive information from a user; and a communications port configured to connect said data storage device with a host device, wherein said data storage device is configured to store a password reset code on said data storage device; receive the password reset code via the key input; validate the password reset code received via the key input; deactivate the password reset code for use with said data storage device; receive an updated password for said data storage device via the key input; and provide access to the secure memory of said data storage device based on the validation of the password reset code.<br>24. A computer-implemented method for changing a password for a data storage device when the data storage device is offline and disconnected from a remote device, said method comprising the steps of: storing a password reset code on the data storage device; receiving the password reset code via a key input of the data storage device; validating the password reset code received via the key input; deactivating the password reset code for use with the data storage device; receiving an updated password for the data storage device via the key input; and providing access to a secure memory area of the data storage device. |
| Reviewer`s Comments | *This patent describes a device for securely storing data, has data storage device that determines whether data storage device is permitted to connect in data communication with host device based on offline occurrence value, and data storage device modifies value. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

### 6.6 Patent Reference 6: CN102664823A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN102664823A |
| Title | Receive data off-line in the instant communication method, client terminal and system |
| Abstract | *The invention claims an instant communication data received off-line method, client terminal and system, belonging to computer network technology field. the method comprises the following steps: step 1, receiver client collects from the sender client terminal for transmitting data message and triggers to generate dialog window to the data receiving, step 2, through receiver client collects receiver off-line receives trigger operation for the data, storing the data to be received to a third-party storage structure, step 3, sending for reminding the data receiving situation of the data content to the sender client terminal. Using the invention can by triggering operation of the receiver user, the sending party online transmission of the received data file into off-line, and according to the receiving condition of the data file the reminding information immediately to the sender to meet user needs, improve the use experience of the user.* |
| Publication Date | 2012-09-12 |
| Application Date | 2012-04-17 |
| Priority Date | 2012-04-17 |
| Assignee | Shanghai Liangming Technologe Development Co. Ltd., |
| Inventors | Ma, Yu-Chen \| Zhou, Peng \| Zhou, Peng-Yan |
| INPAOC Family Members | CN102664823A |
| Independent Claims | 1. A receive data off-line in the instant communication method, wherein the method comprises the following steps: step I, receiver client collects from the sender client terminal for transmitting data message and triggers to generate dialog window to the data receiving; step 2, through receiver client collecting receiver for offline received triggering operation of the data, storing the data to be received to a third-party storage structure, step 3, sending for reminding the data receiving situation of the data content to the sender client terminal. \|<br>10. A data off-line in the instant communication receiving client end, wherein the client end comprises the following structure, off-line receive selection module, collects the data transmission message for receiver client. trigger generates a dialog window to the data receiving, off-line receive triggering |

module, for through receiver client collecting receiver for offline received triggering operation of the data, storing the data to be received to a third-party storage structure, data reception feedback module. used for reminding the data receiving situation of the data content is sent to the client of the sending party.

11. A receive data off-line in the instant communication system, comprising a sender client, a recipient client and the third party storage structure, wherein said receiver client, comprising, offline receiving selection module for receiver client collects from the sender client terminal for transmitting data message and triggers to generate dialog window to the data receiving, off-line receive triggering module, for triggering operation for offline receiving of data through receiver client collecting receiver, storing the data to be received to a third party storage structure, data reception feedback module is used for reminding the data receiving situation of the data content is sent to the client of the sending party, the third party storage structure, which comprises: third party data interface module, used for data connection between the sending party client terminal, receiving from a sender client end uploading data content, offline data storage module used for storing received by third party data interface module, the sender client transmits data content.

12. A receive data off-line in the instant communication system, comprising a sender client, receiver client terminal and a system server, wherein the receiver client, comprising, offline receiving selection module for receiver client collects from the sender client terminal for transmitting data message and triggers to generate dialog window to the data receiving, off-line receive triggering module, for triggering operation for offline receiving of data through receiver client collecting receiver, storing the data to be received to the system server, the system server, comprising a data interface module, used for data connection between the system server and the sender client terminal, receiving from a sender client terminal uploading the file data; sender system server storing structure for storing received by the data interface module, the sender client transmits data content server feedback module is used for reminding the data receiving situation of the data content is sent to the client of the sending party.

13. A receive data off-line in the instant communication system, comprising a sender client, receiver client terminal and a system server, wherein the receiver client, comprising, offline receiving selection module for receiver client collects from the sender client terminal for transmitting data message and triggers to generate dialog window to the data receiving, off-line receive triggering module, for triggering operation for offline receiving of data through

| | |
|---|---|
| | receiver client collecting receiver, storing the data to be received to the system server, the system server, comprising a data interface module, used for data connection between the system server and the sender client terminal, receiving from a sender client terminal uploading the file data; sender system server storage structure corresponding to sender identification number, for storing transmitted data from content of client transmission, offline data storage module, for storing the off-line data structure to the sender system server for storing the collecting receiver after receiving triggering operation the data is transmitted to receiver system server storing structure; receiver system server storing structure, the user corresponding to the identification number, for storing data content of the receiver, server feedback module is used for reminding the data receiving situation of the data content is sent to the client of the sending party. |
| Reviewer`s Comments | *This patent describes an Off-line data receiving method involves sending data by sender client to remind receiving condition of data content. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.7 Patent Reference 7: WO2020000765A1

Click to return to the list of references

| | |
|---|---|
| Publication Number | WO2020000765A1 |
| Title | Off-line data storage method and apparatus, computer device and storage medium |
| Abstract | *Disclosed are an off-line data storage method and apparatus, a computer device and a storage medium. The method comprises: if acknowledgment information, which indicates that a user successfully logs in to a cloud server for the first time and is sent by the cloud server, is received, creating a secure disk space in a local disk (S101); receiving directory index information sent by the cloud server for the user to obtain directory selection information by means of selection, and sending the directory selection information to the cloud server (S102); receiving data information by means of an HTTPS encryption transmission protocol (S103); and storing the data information in the secure disk space, and encrypting the stored data information according to identifier information bound with the logged-in user and a download timestamp of the data information (S104).* |
| Publication Date | 2020-01-02 |
| Application Date | 2018-10-10 |
| Priority Date | 2018-06-29 |
| Assignee | Ping An Technology (Shenzhen) Co. Ltd. |
| Inventors | LI, Yang |
| INPAOC Family Members | WO2020000765A1 \| CN108900510A |
| Independent Claims | 1. An off-line data storage method, comprising the following steps: if receiving the user sent by the cloud server firstly and successfully login confirming information of the cloud server, creating a secure disk space virtualization in the local disk; receiving the directory index information sent by the cloud server and to display for the user to select directory obtaining the user from the directory index information contained in the selected category selection information obtained, and acquired by the category selection information is sent to the cloud server, establishing a data transmission connection with the cloud server via HTTPS encryption transmission protocol. to receive with the category selection information included in the data information list; the data information storing the received to secure disk space and bound according to the login user identifier information and data information downloading |

timestamp to encrypt the data information has been stored. | 6. An off-line data storage device, comprising: a secure disk space creating unit, used for if receives the user sent by the cloud server firstly and successfully login confirming information of the cloud server, creating a secure disk space virtualization in the local disk; directory index information selection unit, a content directory for receiving index information sent by the cloud server and to display for selection by the user, obtaining the user from the directory index information contained in the selected directories obtained selection information, and sends the obtained by the category selection information to the cloud server; storing encrypted unit data transmission unit, used for establishing the data transmission with the cloud server via HTTPS encryption transmission protocol connection, to receive the data information list with the list selection information comprises, for the data information storing the received to secure disk space and bound according to the login user identifier information and data information downloading timestamp to encrypt the data information has been stored.

11. A computer device, comprising a memory, a processor and computer program stored on the memory and running on the processor, wherein the processor executes the computer program to realize the following steps: if receiving the user sent by the cloud server firstly and successfully login confirming information of the cloud server, creating a secure disk space virtualization in the local disk, receiving the directory index information sent by the cloud server and to display for the user to select directory obtaining the user from the directory index information contained in the selected category selection information, and selecting the directory information obtained is sent to the cloud server, establishing data transmission with the cloud server via HTTPS encryption transmission protocol connection, to receive the data information list and included in the category selection information, the data information storage to the received secure disk space and bound according to the login user identifier information and data information downloading timestamp to encrypt the data information has been stored.

16. A storage medium, wherein the storage medium stores a computer program, the computer program when executed by a processor, cause the processor to perform the following operations: if receiving the user sent by the cloud server firstly and successfully login confirming information of the cloud server, creating a secure disk space virtualization in the local disk, receiving the directory index information sent by the cloud server and to display for the user to select directory obtaining the user from the directory index information contained in the selected category selection information, and selecting the directory information obtained is sent to the cloud server,

| | |
|---|---|
| | establishing data transmission with the cloud server via HTTPS encryption transmission protocol connection, to receive the data information list and included in the category selection information, the data information storage to the received secure disk space and bound according to the login user identifier information and data information downloading timestamp to encrypt the data information has been stored. |
| Reviewer`s Comments | *This patent describes a method for storing off-line data, involves creating secure disk space virtualization in local disk, storing received data information in safe disk space, and encrypting stored data information according to user identifier information. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.8 Patent Reference 8: CN109284244A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN109284244A |
| Title | An off-line data synchronous storage system |
| Abstract | *The invention relates to offline storage technical field, specifically an off-line data synchronous memory system, comprising an upper computer, a lower computer, a USB, wherein the GPIO port of lower computer connecting dial switch, the dial switch of the lower machine to 1. CPU read to the corresponding GPIO WAN, the lower computer of the inserted USB becomes a slave, and USB host to use the USB MSC protocol; the lower machine, dial switch of the lower machine to 0, the inserted USB becomes a host. USB becomes a slave, using USB HID protocol. Compared with the existing technology, the invention realizes the synchronous transmission of USB data, namely the flexible USB slave mode changing transmission data; and processing the data in the USB, is convenient to observe the binary data into a decimal or hexadecimal.* |
| Publication Date | 2019-01-29 |
| Application Date | 2018-01-24 |
| Priority Date | 2018-01-24 |
| Assignee | Shanghai Unitoon Information Technology Co. Ltd. |
| Inventors | Zhang, Wen-Xia \| Dong, Bin \| Ma, Na \| Li, Tao \| Li, Zhi |
| INPAOC Family Members | CN109284244A |
| Independent Claims | 1. A synchronizing offline data storage system, comprising an upper computer, a lower computer, a USB, the upper computer adopts PC device; the lower computer at least comprising a processing software of the MCU processor; the MCU processor of the lower computer is provided with a CPU, a storage unit, a GPIO port, the storage unit comprises a code space, data space, register to be transmitted, the PC device and MCU processing is respectively set with USB interface, wherein further comprising a dial switch connected with the GPIO port of the lower computer of the dial switch of the lower machine to 1, CPU read to the corresponding GPIO WAN, the lower computer of the inserted USB becomes a slave, and USB host to use the USB MSC protocol; the lower machine, a toggle switch of the lower machine to 0, make plugged into a USB host, a USB slave, using USB HID protocol, so the toggle state of the lower computer to change the subordinate |

| | |
|---|---|
| | relationship between the lower machine and the inserted USB. realizing the data transmission, and when the upper computer connected with the USB, according to the USB HID protocol, the host computer receives the USB data, to make the data meet the reading requirement, the data in the USB process, the binary data into the required hexadecimal or decimal. |
| Reviewer`s Comments | *This patent describes a system for synchronous offline data storage, has data that is processed in universal serial bus (USB), and binary data is converted to desired hexadecimal or decimal. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

### 6.9 Patent Reference 9: CN112115495A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN112115495A |
| Title | An off-line cloud data storage method, system, computer device and storage medium |
| Abstract | *The invention claims an off-line cloud data storage method and system; a computer device and a storage medium, relating to the cloud storage technology, comprising if detecting the data storage instruction sent by any trusted terminal in the user trusted area, obtaining the data to be stored corresponding to the data storage instruction, and obtaining the target storage space corresponding to the data storage instruction; the data to be stored is synchronously written into the local data area; the data to be stored is asynchronously written into the encrypted data area; if detecting the cloud data synchronization instruction sent by any trusted terminal in the trusted area of the user, obtaining the target synchronization space corresponding to the cloud data synchronization instruction; obtaining each encrypted data and the corresponding data head in another encrypted data area, and synchronizing each encrypted data and the corresponding data head in another encrypted data area to cloud server realizing the data storage in the user trusted area of the data encryption terminal, the user data privacy is safe and controllable, improving the data security.* |
| Publication Date | 2020-12-22 |
| Application Date | 2020-09-25 |
| Priority Date | 2020-09-25 |
| Assignee | Ping'an International Smart City Technology Co. Ltd. |
| Inventors | Dong, Guo-Chao |
| INPAOC Family Members | CN112115495A |
| Independent Claims | 1. An offline cloud data storage method, applied to the data encryption terminal in the user trusted area, wherein it comprises: if detecting the data storage instruction sent by any trusted terminal in the trusted area of the user, obtaining the data to be stored corresponding to the data storage instruction, and obtaining the target storage space corresponding to the data storage instruction; wherein the target storage space comprises a local data area and an encrypted data area; synchronously writing the data to be stored in the local data area; asynchronous writing the data to be stored into the encrypted |

| | |
|---|---|
| | data area; wherein the local data area comprises a working space for storing the un-encrypted data, and an encryption space for storing the encrypted data; if detecting the cloud data synchronization instruction sent by any trusted terminal in the trusted area of the user, obtaining the target synchronization space corresponding to the cloud data synchronization instruction; wherein the target synchronization space comprises another local data area and another encryption data area; the other local data area comprises another working space for storing the un-encrypted data, and another encryption space for storing the encrypted data; and obtaining each encrypted data and the corresponding data head in the other encrypted data area, and synchronizing each encrypted data and the corresponding data head in the other encrypted data area to the cloud server<br>7. An offline cloud data storage method, applied to the trusted terminal in the trusted area of the user, wherein it comprises: if detecting the terminal data synchronization instruction sent by the other trusted terminal in the same user trusted area with the trusted terminal, receiving the data in another trusted terminal local data area sent by the other trusted terminal and the data in the other trusted terminal encryption data area; combining the data in the local data area of the other trusted terminal and the data in the encrypted data area of another trusted terminal and the data in the trusted terminal; obtaining the combined dedudereby result; and sending the combined de-weight result to the other trusted terminal. |
| Reviewer`s Comments | *This patent describes a data encryption terminal offline cloud data storing method, involves obtaining each encrypted data and data head in encrypted data area, and synchronizing each encrypted data and data head in another encrypted data area to cloud server. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

### 6.10 Patent Reference 10: CN111290717A

Click to return to the list of references

| | |
|---|---|
| Publication Number | CN111290717A |
| Title | A Bluetooth communication based on offline data storage device |
| Abstract | *The invention claims a Bluetooth communication based on offline data storage device, comprising a Bluetooth radio frequency processing unit, a processor, a Flash memory unit, an SD card storage unit, the mononuclear processor is respectively connected with the Flash memory unit through SPI interface, an SD card storage unit, said Flash memory unit, an SD card storage unit respectively comprises an A area, B area, so as to realize dual-backup, the core processor is connected with the Bluetooth antenna through the Bluetooth radio frequency processing unit; further comprising a power management module is a storage device to supply power. The invention uses the built-in Flash memory and an external SD card double memory mode, ensuring equipment is damaged, capable of recovering data through SD card, data will not be lost. The invention on the flash and SD storage medium to divide the storage space into the AB region, for redundancy backup, realizes the multi-backup of data, ensuring the reliability of data storage.* |
| Publication Date | 2020-06-16 |
| Application Date | 2020-03-13 |
| Priority Date | 2020-03-13 |
| Assignee | Hc-o Inc., |
| Inventors | Li, Ang \| Zhang, Tian-Kui |
| INPAOC Family Members | CN111290717A |
| Independent Claims | 1. A Bluetooth communication based on offline data storage device, wherein it comprises a Bluetooth radio frequency processing unit, a processor, a Flash memory unit, an SD card storage unit, the mononuclear processor is respectively connected with the Flash memory unit through SPI interface, an SD card storage unit, said Flash memory unit, an SD card storage unit respectively comprises an A area, B area, so as to realize dual-backup, the core processor is connected with the Bluetooth antenna through the Bluetooth radio frequency processing unit; further comprising a power management module is a storage device to supply power. |
| Reviewer`s | *The patent describes an offline data storage device based on Bluetooth communication comprises single-core processor connected to Flash storage* |

|  |  |
|---|---|
| Comments | *unit and SD card storage unit through SPI interface and power management module to supply power to storage device. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

### 6.11 Patent Reference 11: US20130333021A1

Click to return to the list of references

| | |
|---|---|
| Publication Number | US20130333021A1 |
| Title | Preventing malicious software from utilizing access rights |
| Abstract | *In a first embodiment of the present invention, a method for enabling a device to block malicious software is provided, comprising: creating a super-user account as a new account for an operating system running on a device; and altering security rights of the operating system so that all accounts other than the super-user account of the operating system running on the device have only read access to key sections of the operating system.* |
| Publication Date | 2013-12-12 |
| Application Date | 2012-06-08 |
| Priority Date | 2012-06-08 |
| Assignee | Forty1 Technologies Inc. \| Sellers Christopher L. \| Ullman Benjamin Kyrk |
| Inventors | SELLERS, Christopher L. \| ULLMAN, Benjamin Kyrk |
| INPAOC Family Members | US20130333021A1 |
| Independent Claims | 1. A method for enabling a device to block malicious software, comprising: creating a super-user account as a new account for an operating system running on a device; and altering security rights of the operating system so that all accounts other than the super-user account of the operating system running on the device have only read access to key sections of the operating system.<br>11. A method for enabling blocking malicious software, comprising: receiving a command to open a file; prompting the user as to how to run the command, wherein the prompting includes asking the user to select “high-risk” or “low-risk”; and when the user selects “high-risk,” running the command in a guest mode, where the command is not allowed to access any part of the operating system.<br>13. A computer system comprising: a processor; an operating system, wherein the operating system contains key sections and non-key sections; a user account module, wherein the user account module is configured to: create a super-user account as a new account for the operating system; and alter security rights of the operating system so that all accounts other than the super-user account of the operating system running on the device have only read access to the key sections of the operating system. \| 15 . A program |

| | |
|---|---|
| | storage device readable by a machine tangibly embodying a program of instructions executable by the machine to perform a method for enabling a device to block malicious software, the method comprising: creating a super-user account as a new account for an operating system running on a device; and altering security rights of the operating system so that all accounts other than the super-user account of the operating system running on the device have only read access to key sections of the operating system.<br>16. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine to perform a method for enabling blocking malicious software, the method comprising: receiving a command to open a file; prompting the user as to how to run the command, wherein the prompting includes asking the user to select “high-risk” or “low-risk”; and when the user selects “high-risk,” running the command in a guest mode, where the command is not allowed to access any part of the operating system. |
| Reviewer`s Comments | *This patent describes a method for blocking malicious software by device, involves altering security rights of operating system and removal of administrator group members right to take ownership of key operating system sections, and super-user account is created. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.* |

## 6.12 Patent Reference 12: US20130086670A1

Click to return to the list of references

| | |
|---|---|
| Publication Number | US20130086670A1 |
| Title | Providing third party authentication in an on-demand service environment |
| Abstract | *A method for logging a user into an online host system begins by receiving a login request from a web browser application of a client device, wherein the login request identifies the online host system. The method continues by initiating a single sign-on routine that involves an online third party system and by obtaining third party user data from the online third party system, wherein the obtained third party user data is associated with the user and is maintained by the online third party system. Host system records maintained by the online host system are modified in accordance with the obtained third party user data. Thereafter, the user is automatically logged into the online host system.* |
| Publication Date | 2013-04-04 |
| Application Date | 2012-10-02 |
| Priority Date | 2011-10-04 |
| Assignee | Salesforce.com Inc |
| Inventors | Vangpat, Alan \| Rao, Prathima \| Mortimore, Charles |
| INPAOC Family Members | US20130086670A1 \| US8844013B2 |
| Independent Claims | 1. A method for logging a user into an online host system, the method comprising: receiving a login request from a web browser application of a client device, wherein the login request identifies the online host system; in response to receiving the login request, initiating a single sign-on routine that involves an online third party system; thereafter, obtaining third party user data from the online third party system, wherein the obtained third party user data is associated with the user and is maintained by the online third party system; modifying, in accordance with the obtained third party user data, host system records maintained by the online host system; and thereafter, automatically logging the user into the online host system.<br>10. A non-transitory computer-readable storage medium with executable instructions stored thereon, wherein the executable instructions instruct a processor to perform a method comprising: receiving a login request to log a user into an online host system; in response to receiving the login request, |

<table>
<tr><td></td><td>sending a token request to an online third party system; in response to sending the token request, receiving an authentication token from the online third party system; using the received authentication token to obtain third party user data from the online third party system, wherein the obtained third party user data is associated with the user and is maintained by the online third party system; determining that the obtained third party user data is not mapped to any existing user of the online host system; and in response to the determining, creating a new user profile for the online host system, the new user profile being linked to the user. | 16. A method for logging a user into an online host system, the method comprising: receiving a login request from a web browser application of a client device, wherein the login request identifies the online host system; in response to receiving the login request, redirecting the web browser application to an online third party system; thereafter, receiving a callback from the web browser application; in response to receiving the callback, obtaining third party user data from the online third party system, wherein the obtained third party user data is associated with the user and is maintained by the online third party system; when the obtained third party user data is mapped to an existing user of the online host system, identifying an existing host system record associated with the existing user and updating the identified existing host system record in accordance with the obtained third party user data; when the obtained third party user data is not mapped to any existing user of the online host system, creating a new user profile for the user, creating a new host system record associated with the new user profile, and populating the new host system record with at least some of the obtained third party user data; and thereafter, automatically logging the user into the online host system.</td></tr>
<tr><td>Reviewer`s Comments</td><td><i>This patent describes a method for logging user into online host system by receiving login request from web browser application of client device, involves modifying host system records maintained by host system in accordance with obtained third party user data. However, in contrast the novelty of ZVC architecture in contrast lies in creating switchable offline storage within the client computer itself.</i></td></tr>
</table>

## 7. Conclusion

The search was conducted on patent databases such as Google Patents and Thomson Innovation. The Zero Vulnerability Computing (ZVC) innovation corporates two key concepts, the combination of which render computer secure against almost all known vulnerability exploitations known to prior art. The IP of these ZVC components, viz. supra operating system (SOS), In-Computer Offline Storage (ICOS), USB with a toggle switch, Solid State Software On A Chip (3soc) and In-Computer Offline Storage (ICOS) Device With Toggle Switch And Charging Port are individually protected by their corresponding patent applications. We did not come across any strong prior-art reference that discloses a similar arrangement and method for utilizing an SOS, ICOS and Solid State Software On A Chip (3soc) for protecting the computer system from foreign or malicious attacks as described in the invention disclosure/ provisional applications.

The prior-art references cited in the report discloses various other systems and methods which are trying to achieve the similar outcome. However, the references fail to disclose a similar system and method as described in the pending provisional patent applications. Therefore, the ZVC invention has high chances of patent being granted without any infringement, and should the invention be commercialized it is highly unlikely that ZVC will fringe anyone else's patent in force in any jurisdiction globally.

## 8. Disclaimer

This report has been prepared by Raman Deep Singh of Rucapillan IP and contains analysis and recommendations based on the understanding of the subject matter by researcher. The analysis and recommendations are purely technical suggestions and should not be constitute as legal opinions under any circumstances. Client alone reserves the right to make a final decision on the subject matter as disclosed. Further, Raman Deep Singh may have used one or more third-party databases while preparing this report, and cannot warrant the accuracy of the information obtained from third-party databases.

Ramandeep Singh

Name: Raman Deep Singh
Title: Director, Rucapillan IP