

IoT enabled smarter RPA ecosystem

Description

Background

1. Technical Field :-

[0001] The present disclosure is directed to an integrated RPA solution and method for automating a business process in an enterprise. In particular the present system and method integrates IOT capabilities, Process Automation, Security and Remote monitoring and management of any be it simple or complex business process into a dedicated unified hardware solution.

2. Discussion of Related Art :-

[0002] Currently there exist in the market a number of RPA solutions which can automate repetitive and complex tasks in a business process. Most of these solutions use rules based software and still others utilize metaphorical software BOT's or combination of these that run on a generic infrastructure, typically on a desktop or a server which are not dedicated. As a paradigm shift to the traditional ways of Robotic Process automation which are purely desktop/server/cloud based software products, AntWorks proposes an IOT enabled hardware device under the trademark **Oodles** for automating the Business processes in a dedicated mode.

[0003] Oodles a portable IOT hardware platform that enables a Business Process Owner to embed any simple or complex RPA software module that can automate any elements in a workflow, infrastructure, back office process or front office routines which are labor intensive. Integrated Processing Unit is the smallest hardware unit in Oodles which has a definitive RAM, Processor, Hard Drive space and comes with a Windows OS installed to handle the BOT's created by QueenBOT, the RPA software Platform . Each Integrated Processing Unit can host multiple AntBOTS depending upon the complexity of the process for which the AntBOTS are built. Each of these Integrated Processing Units are available in different variants to suit the needs of the enterprise. Each Oodles is provisioned to accommodate a maximum of 50 such Integrated Processing Units, say 10 per each vertical side of the pentagon shaped host. AntBOTS when deployed in the Independent Units are activated by the Orchestrator named as QueenBOT™ which is also residing in the same Oodles. Once activated, the AntBOTS relentlessly continue their operation in a dedicated mode until either the process comes to an end or otherwise. Each Integrated Processing Unit can be plugged or removed in real time since every Independent Processing Unit is connected in parallel to the backbone unit of the Oodles.

[004] The end user namely the enterprise can setup the Oodles effortlessly. Oodles needs a real estate of 2 * 2 feet, requires one Electric power source and one LAN connectivity. Oodles also supports WIFI mode wherein no direct internet source cable is needed. KVM switches are provided as a part of Oodles where any display device can be

connected to Oodles and software switches are provided to switch display from one IPU to other.

Internal hardware design & specifications:-

[005] Oodles takes a pentagonal shape and the internal hardware of Oodles has a provision of 50 slots, 10 slots on each side of pentagon to hold the Integrated Processing Units. Each Integrated Processing Unit is facilitated with 2 USB port 3.0, a LAN port RJ-45 with an Ethernet controller 1211-AT, IEEE 802.3u, IEEE 802.3, a HDMI v1.4 port and a power source of 19v DC, it also comes with an Onboard storage of 128GB. The dimension of the Integrated Processing Unit is 94.5mm * 55mm * 5mm, it has also got a support for mechanical security latch

[006] As shown in the fig 1B. these Integrated Processing Units are arranged vertically and are plugged to a backbone board which is a typical PCB board. The dimension of the board is 60mm*60mm. This PCB board is facilitated with connectors to connect to the all GPIO ports of the Integrated Processing Unit. There are 5 such PCB boards provisioned one on each side of the pentagon. The PCB board runs different tracks which actually is a conductive path to connect different points in the PCB board.

[007] At the bottom of the pentagonal Oodles, a provision is given to accommodate controller that is designed to control all individual Integrated Processing Unit. In addition to this, a Network switch which in turn connects to the LAN RJ-45 of each Integrated Processing Unit, a

switchmode power supply (SMPS) accomodating 12v,125 amps is also available to regulate the power supplied to the Integrated Processing Units.

[008] Heat sink and fans are provided to dissipate the heat which is generated from the computer card out . These Integrated Processing Units are designed to run the BOT's 24 *7*365 in a dedicated mode. Appropriate heat sink mechanism is followed to avoid hung state and to ensure the longevity of the operational devices.

Glossary of Terms Used:

1. Oodles: A stack of 50 Independent Processing Units (IPU) connected and bounded together to operate as a single unit
2. Independent Processing Unit (IPU) : Individual and dedicated hardware unit which shall hosts AntBots to carry out automation assignments.
3. IoT: Network of interconnected things/devices which are embedded with sensors, software, network connectivity and necessary electronics that enables them to collect and exchange data making them responsive
4. Robotic Process Automation (RPA): Business process automation technology based on metaphorical software robots (Bots) or artificial intelligence (AI) workers
5. Bots: Software robots that are built and execute to automate processes / tasks
6. QueentBOT: Centralised Orchestrator that enables:
 - a. Remote publishing and deployment of BOTs/modules
 - b. Centralised and remote control, monitoring, orchestrating and reporting performance of AntBots and their associated Hardware.
7. AntBots: Bots built using ANTstein platform

Claims

1. IOT enabled smarter RPA ecosystem comprising the following hardware
 - (a) A configurable mini Integrated Processing Unit loaded with Windows OS to host and operate the Artificial intelligent digital workers designed and deployed by QueenBOT™
 - (b) A back bone PCB board provisioned to stack the IPU's and provide connectivity for all the GPIO pins of the Integrated Processing Unit
 - (c) A KVM switch to connect any display unit and access the Integrated Processing Units
 - (d) A heatsink and the intuitive design ensuring the dissipating of heat generated and improving the longevity of the device
 - (e) A controller unit controlling the configuration and activity of AntBOT's loaded onto the Integrated Processing Unit
 - (f) A unique networking layer to differentiate the AntBOT's deployed for automating processes.
 - (g) A hardware access layer (HAL) to access and configure all hardware ports
 - (h) An IOT layer to enable all comprehensive and sophisticated IOT protocols
 - (i) An orchestrator to engage and disengage the digital workers hosted in the IPU's
2. The IOT enabled smarter RPA ecosystem of claim 1 ensuring any confidential data and information stored is being encrypted and encapsulated. All data to and from the IPU's are protected from threats and sniffs.

3. The IOT enabled smarter RPA ecosystem of claim 1 Implements protections from Common Vulnerabilities and Exposures (CVEs) in a timely manner to protect from exploits.
4. The IOT enabled smarter RPA ecosystem of claim 1 Implements encryption for confidential information being transmitted over Internet connections with a strength of minimum AES 256 bit and / or uses TLS 1.0/ TLS 1.1.
5. The IOT enabled smarter RPA ecosystem of claim 1 Implements IDS/IPS technology
6. The IOT enabled smarter RPA ecosystem of claim 1 has any inbuilt firewall protection to block illegitimate traffic aimed
7. The IOT enabled smarter RPA ecosystem of claim 1 has Physical decapping of chip packages to optically read NVRAM contents
8. The IOT enabled smarter RPA ecosystem of claim 1 Implements protections for CVEs in a timely manner to protect from exploits.
9. The IOT enabled smarter RPA ecosystem of claim 1 has Hardware tamper protection
10. The IOT enabled smarter RPA ecosystem of claim 1 Protection against Application tampering
11. The IOT enabled smarter RPA ecosystem of claim 1 is embedded with sanitized RPA application preventing intrusion thus preventing modification or removal of sensitive data
12. The IOT enabled smarter RPA ecosystem of claim 8 is Hardened against known vulnerabilities and configuration issues
13. The IOT enabled smarter RPA ecosystem of Claim 3 has a Trusted Server certificate for the embedded software

14. The IOT enabled smarter RPA ecosystem of Claim 3 Approved Hash functions.
15. The IOT enabled smarter RPA ecosystem of Claim 3 has Approved Signature algorithms
16. The IOT enabled smarter RPA ecosystem of Claim 3 has Approved Encryption algorithms
17. The IOT enabled smarter RPA ecosystem of Claim 3 Approved Key exchange algorithms
18. The IOT enabled smarter RPA ecosystem of claim 8 Approved Pseudo Random functions (PRF) used for key derivation
19. The IOT enabled smarter RPA ecosystem of claim 8 Uses industry standard best practices for application security (e.g. OWASP)
20. The IOT enabled smarter RPA ecosystem of claim 8 has host firewall protection
21. The IOT enabled smarter RPA ecosystem of claim 1 has a multi-modal interface comprising a remote user interface.
22. The IOT enabled smarter RPA ecosystem of Claim 1, wherein the multi-modal user interface comprises at least one of the following user interfaces : a smart phone, a wall panel, a computer, and a server.
23. The IOT enabled smarter RPA ecosystem of Claim 1 wherein the multi-modal interface comprises a sensor interface.
24. The IOT enabled smarter RPA ecosystem of Claim 1 wherein the device interface comprises at least one of the following: a serial interface, an Ethernet interface, a LonWorks protocol interface, an X10 protocol interface, a wireless interface, an HTTP server, and a line of sight interface.

25. The IOT enabled smarter RPA ecosystem of Claim 1 further comprising the interaction guide library.
26. The IOT enabled smarter RPA ecosystem of Claim 1 wherein the interaction guide library stores a plurality of interaction rule objects according to a location specific indexing scheme.
27. The IOT enabled smarter RPA ecosystem of Claim 1 wherein interaction rule objects comprises device interaction rules.
28. The IOT enabled smarter RPA ecosystem of Claim 1 wherein the device interaction rules depend on observed data.
29. The IOT enabled smarter RPA ecosystem of Claim 1 enables Bluetooth, Wi-Fi, Z-Wave, ZigBee protocols
30. The IOT enabled smarter RPA ecosystem of Claim 1 wherein the network communication circuit communicates with the additional Oodles devices using a wireless network communication medium.
31. The IOT enabled smarter RPA ecosystem of Claim 1 further comprising using a cryptographic element of the Oodles to establish secure communication with at least one of the additional Oodles device.
32. A non-transitory program storage device on which are stored instructions, comprising instructions that when executed cause an Oodles device to :
 - (a) employ a provisioning state machine that includes a sequence of provisioning states including an initial state and a final state, the final state of which is an operational state
 - (b) establish, via a network communication circuit, communication with an additional Oodles device of a collection of oodles devices.

- (c) establish, prior to reaching the operational state, Oodles-specific state information in a memory and periodically communicate the Oodles-specific state information to the additional Oodles of a collection via the network communication circuit
- (d) determine IoT collection-specific state information based on the periodic and interval based communication
- (e) sequence from the initial state through the sequence of provisioning states based on a combination of the IoT collection-specific state information and the Oodles-specific state information until the Oodles and the additional Oodles are in the operational state comprising instructions that when executed cause the main Oodles device to use a mismatch between the a state of the collection of Oodles and a state of the Oodles to initiate action to move to a new state of the provisioning state machine

33. The program storage device of claim 32 wherein the instructions that when executed causes the Oodles to establish communication through a network communication circuit comprise instructions that when executed cause the Oodles to establish communication through a wireless network communication circuit.

34. The program storage device of claim 32 wherein the instructions that when executed cause the Oodles to establish communication through a network communication circuit comprise instructions that when executed cause the IoT device to establish secure communication through a network communication circuit using a cryptographic element of the Oodles.

35. The program storage device of claim 32, wherein each state in the provisioning state machine has actions associated with provisioning the Oodles.
36. A predefined method for collaborative decision making among Oodles comprising
- (a) transmitting a recommendation request message to one or more member Oodles in the group, wherein the recommendation request message indicates a planned state transition
 - (b) receiving one or more responses to the recommendation request message, wherein the one or more responses include feedback about the planned state transition from the one or more member Oodles responding to the recommendation request message
 - (c) determining whether to initiate the planned state transition based on the one or more responses to the recommendation request message.
37. The method stated in claims 36 further comprises of determining whether to initiate the planned state transition based on the one or more responses to the recommendation request message.
38. The method stated in claims 36 further comprises planning the state transition based on a local decision-making algorithm.
39. The method stated in claims 36, wherein the one or more responses to the recommendation request message include a Boolean value to indicate whether the responding member IoT devices approve or disapprove the planned state transition.

40. The method stated in claims 36, wherein the one or more responses to the recommendation request message include a fuzzy logic value to indicate a degree to which the responding member IoT devices approve or disapprove the planned state transition.
41. The method stated in claims 36, wherein the one or more member Oodles analyze a potential impact associated with the planned state transition based on a dependency tree that describes relationships among the member Oodles in the group and determine whether to approve or disapprove the planned state transition based on the potential impact.
42. The method stated in claim 41, wherein at least one member Oodles in the group ignores the recommendation request message in response to having no opinion about whether to approve or disapprove the planned state transition.
43. The method stated in claim 41, wherein at least one member Oodles in the group designates a proxy member Oodles that determines whether to approve or disapprove the planned state transition on behalf of the at least one member Oodles.
44. The method stated in claim 36, further comprises advertising a final decision indicating that the planned state transition will be initiated to the one or more member Oodles devices in the group and initiating the planned state transition subsequent to advertising the final decision.
45. The method stated in claim 36, further comprises advertising a final decision indicating that the planned state transition will not be initiated to the one or more member Oodles in the group.
46. The method recited in claim 45, further comprises receiving an unsolicited recommendation from at least one member Oodles in the

group, wherein the unsolicited recommendation indicates an operational state associated with the at least one member Oodles and deciding to not initiate the planned state transition in response to determining that the planned state transition has a potential adverse impact on the operational state associated with the at least one member Oodles that sent the unsolicited recommendation.

47. A computer-readable storage medium having computer-executable instructions for collaborative group-based decision-making recorded thereon, wherein executing the computer-executable instructions on an Oodles causes the device to

- (a) transmit a recommendation request message to one or more member Oodles in a group wherein the recommendation request message indicates a planned state transition

- (b) receive one or more responses to the recommendation request message, wherein the one or more responses include feedback about the planned state transition from the member Oodles responding to the recommendation request message

- (c) determine whether to initiate the planned state transition based on the responses to the recommendation request message

48. The IOT enabled smarter RPA ecosystem of claim 8, the discoverer module of the QueenBOT to aggregate the recorded actions of the users from discrete machines. Actions may include all actions pertaining to carry out the tasks, be it mouse click, text input or otherwise pertaining to any applications. These are sequenced, analysed and learnt by the Machine learning model which then produces process maps, propensity of automatable tasks and the coverage of automation. This powerful

unit of the QueenBOT helps the enterprise in identifying the automatable parts of the processes either in whole or as a part which then can be built and deployed in the IPU's.

49. The IOT enabled smarter RPA ecosystem of claim 8 the Bot Builder unit of the QueenBOT provides canvas to build AntBOTs by using the pre-built components which are available as a component library. The canvas facilitates drag and drop of such components without any need to write lines of programming codes.
50. The IOT enabled smarter RPA ecosystem of claim 8, the platform looks beyond basic RPA routines and accommodates various important aspects of Integrated Automation Platform. Knowledge building, correlated content mapping and suggesting intelligent routes to increase propensity of Automation. These elements of yield provides horizontal scalability and vertical scalability.
51. The IOT enabled smarter RPA ecosystem of claim 8, the platform provides comprehensive reporting and brings a host of new features for measuring, managing and enhancing the AntBOT's productivity. QueenBOT offers Multi-tenancy, Cognitive Responsiveness and Real-Time digital Workforce Management thus enhancing the Bots productivity to new level.
52. The IOT enabled smarter RPA ecosystem of claim 8 QueenBOT, the RPA software platform responds intelligently and dynamically to the changes on the target machines. It ensures continuance of work without bringing the AntBOTS down whenever known or unknown exceptions occur in the target application hosted in the target machines. Exceptions can be

classified such as UI (User Interface) changes, data layer changes, hardware failures or network downtime.

53.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT, the RPA Software Platform has Multi skilling functions wherein every AntBOT deployed in IPU's, can be used to execute any process thus not binding the AntBOTS to any particular process or to any IPU. AntBOTS are monitored in synchorouns mode and the states of each AntBOT is identified. This helps in allocation and assignment of work in real time and as a result all the AntBOTS are put to work continuously and managed automatically by QueenBOT. This humanless orchestration increases the productivity and ensuring the capacity issues be it over or under.

54.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT , the RPA Software Platform allows the Collaboration between BOTs and Humans in synchrous mode. Multiple BOTs can reside in a single IPU and perform different tasks and processes simultaneously

55.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT, the RPA software Platform enable the AntBOTs residing in IPU's to self-heal from any failures in the overall infrastructure such as network, database or failure of any IPU. The The orchestrator alerts the user and logs in such event and resurrects AntBOTSS residing in another IPU and based on the state of the AntBOT, work is assigned and coninued. This helps in automnated recovery of the process due to hardware failure and serves as BCP.

56.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT, the RPA software offers inbuilt Credential vault to facilitate Data in motion and data at rest, which are stored and transmitted within the platform are encrypted to the highest standards. The In-built credential vault secures your process data in addition to connectors to third party security applications like CyberArk.

57.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT, the RPA software provides actionable metrics and supports AI enabled decision making routines, which includes hidden patterns, accurate predictions or forecasts which are not rule based but descriptive.

58.The IOT enabled smarter RPA ecosystem of claim 8, QueenBOT, the RPA software Platform, has a centralized dashboard to manage and monitor the performance of AntBOTS.