UPPSALA
UNIVERSITET

Improvisations in RevPi Compact based Data Acquisition System for Point Absorbers

Balakrishnan Kannan

Masterprogram i förnybar elgenerering

Master Programme in Renewable Electricity Production

UPPSALA
UNIVERSITET

Faculty of Science and Technology

Visiting address:
Ångströmlaboratoriet
Lägerhyddsvägen 1
House 4, Level 0

Postal address:
Box 536
751 21 Uppsala

Telephone:
+46 (0)18 – 471 30 03

Telefax:
+46 (0)18 – 471 30 00

Web page:
http://www.teknik.uu.se/student-en/

Abstract

Improvisations in RevPi Compact based Data Acquisition System for Point Absorbers

Balakrishnan Kannan

Point absorbers are devices that float offshore and extract the energy from the incoming waves to convert into electrical energy. Wave buoys are such point absorbers that are used in wave energy research to measure and record important data about the wave climate in a particular region. This project report is a continuation of a previous master thesis titled 'Design and Development of a Data Acquisition and Communication System for Point Absorber Tracking' by Balakrishnan Kannan. This project is an attempt to overcome 3 important challenges encountered in the previous master thesis. The challenges are listed below:

- The RevPi Compact device requires a manual log in using a user name and password on every reboot. This is not possible when installed offshore.
- The real-time monitoring software needs a manual authentication from the RevPi Compact device on every attempt to establish a connection. This is again challenging after installation offshore.
- The Tracking application (VNC) should also be able to work with the computers connected to different internet protocols.

This project report is to document all the necessary steps carried out to overcome these challenges and the alternatives done to make the Data Acquisition (DAQ) system automatic without any manual operations needed and reliable even when operating in offshore environments.

Table of Contents

List Of Figures

1. Introduction

1.1 Background

The Lysekil test site in the west coast of Sweden has been used to carry out several different experiments using point absorber wave buoys and Wave Energy Converters (WECs). The point absorber buoys are made to float on the incoming waves, 2 to 5 kms away from the coast. The measurement buoys are used to record valuable data about the waves that strike the buoy. The data collected is usually the force acting on the buoy due to the waves and the movement of the buoy accordingly. This data, upon further analysis, will be useful in many other studies including the wave climate in that particular region.

To measure these data, two different sensors are used. One is a strain gauge transducer to measure the force acting on the buoy and the other sensor is called an Inertial Measurement Unit. These sensors are then connected to a controller Data Acquisition system (DAQ) to get the data stored on to a memory device. This data is then transmitted to an onshore computer for further analysis.

1.2 Previous design

The master thesis titled 'Design and Development of a Data Acquisition and Communication System for Point Absorber Tracking' [1] is based on the master thesis of Juliana Lüer titled 'Design and Development of a Measurement System to Track the Motion of a Point Absorber' [2]. The Arduino based data measurement system explained in [2] is replaced by a Raspberry Pi based system explained in [1]. The Raspberry Pi based controller solution is provided by KUNBUS in a device called RevPi Compact [3]. This device can work with both analog and digital sensors without any intermediate interfacing devices. One more important change adopted in [1] is the implementation of an Internet protocol for communication. The 4G internet is used to transfer the data from the buoy to the onshore computer. The Huawei 4G Internet modem [4] with Telenor internet service is used to provide a stable network inside the buoy. The RevPi Compact is connected with the Huawei modem with a Local Area Network (LAN) cable. The data is transferred by communicating with the nearest cellular tower through an antenna placed outside the buoy.

The entire system is powered by two Lithium Polymer (Li-Po) batteries of 1.5 kWh capacity (both combined) that are charged by four solar panels (15 W each) mounted on the surface of the buoy. The charging of the batteries and the load management is done by a charge controller from Victron Energy [5].

The connection of the peripheral sensors and communication devices is shown in a block diagram below (Figure 1).

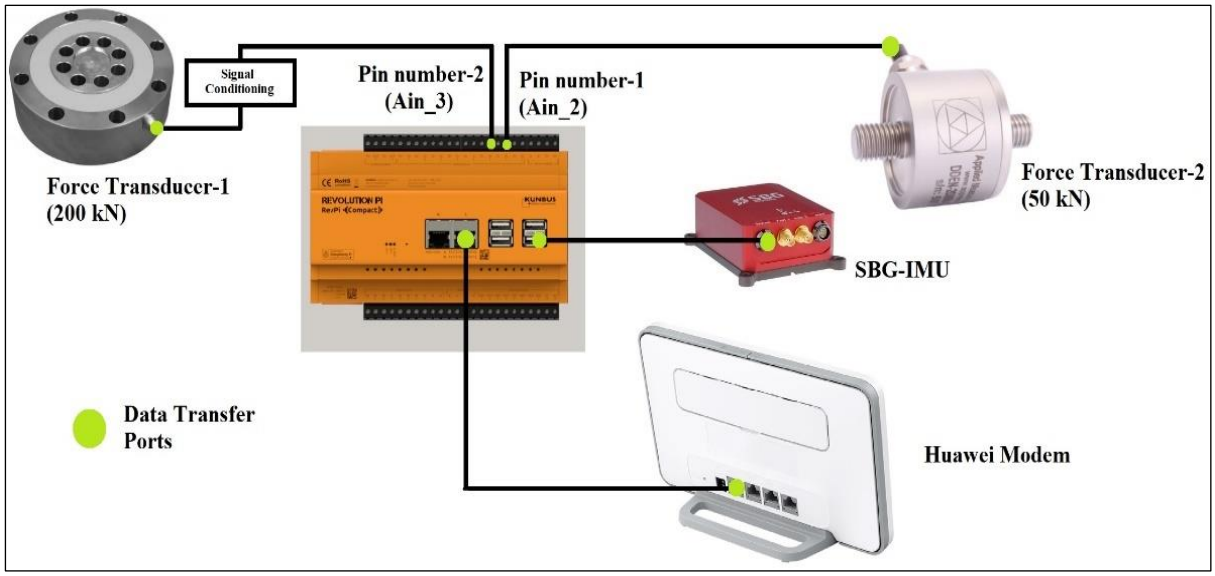

Figure 1: Interconnecting all the sensors and peripheral devices with the RevPi Compact [1].

1.3 Challenges

After all the peripherals were connected and the RevPi Compact was programmed to read the data, it was observed that there were a few more hurdles that made the device inoperable in standalone conditions in the marine environment. These challenges are mostly related to programming and settings as in any normal computer. The challenges are listed and explained below:

a. *Device Login*
   The RevPi Compact is like any other computer but operating on Raspberry Pi OS (Operating System). So, on booting the system, it runs all the boot operations and requires login Identification Data (ID) and password to authenticate. When operating offshore, it is not possible to manually enter the details every time the system reboots.

b. *Remote Access Authentication*
   The use of remote access software such as Team Viewer or VNC requires an authentication formality. In this project, the RevPi Compact is the remote device to be monitored by a computer onshore. By default, the remote access software requires manual authentication from the slave device. This declares its consent to be operated by the onshore computer and also a signal that that computer is authentic or trusted. But this manual authentication from the slave computer (RevPi Compact) cannot be done once installed offshore.

c. *Devices connected to different Local Area Networks*
The remote access software (TeamViewer & VNC) used in the previous work [1] were tested for operating in the same Local Area Network. Though it is suitable for lab testing, there is no possibility that the onshore computer and the buoy offshore will be operating on the same LAN. So, the settings are to be modified such that the systems are capable of operating on different internet connections.

2. Method

This section deals in detail with the steps to overcome the challenges explained in Section 1.3 Challenges

2.1 Bypass the login after boot

As a normal computer, the Raspberry Pi based system also uses a username and password authentication for the user to get into the system after every boot. The username and password have to be manually entered in order to authorize any login. This can be manually done onshore during the test phase. But once installed in the buoy, this process becomes a hurdle for the onshore system that tries to gain access over RevPi Compact offshore. So, a change in the internal device settings is required to bypass the boot login. Once the settings are modified, the device directly boots into the Graphical User Interface (GUI) desktop.

Step 1: The following command is executed in the shell command prompt directly on the RevPi Compact or using the Putty software from a system working on the same LAN (shown in Figure 2).

```
sudo raspi-config
```

This command opens up the configuration window of the Raspberry Pi where the device settings can be monitored and altered.

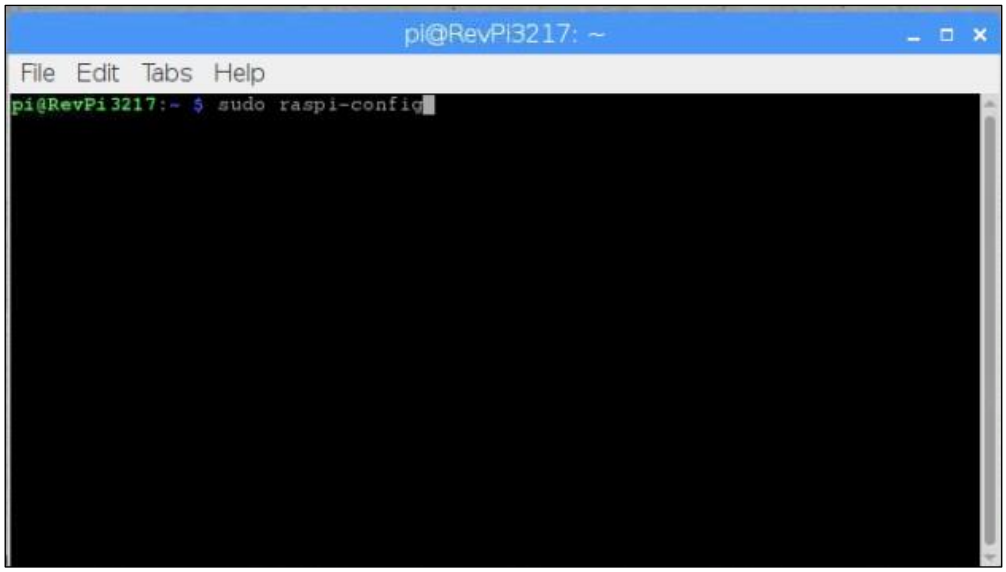

Figure 2 Command to open the configuration window in Raspberry Pi

Step 2: The configuration window opens up displaying a number of options and settings that can be viewed and altered. The third option titled 'Boot Options' is to be selected as shown in Figure 3.

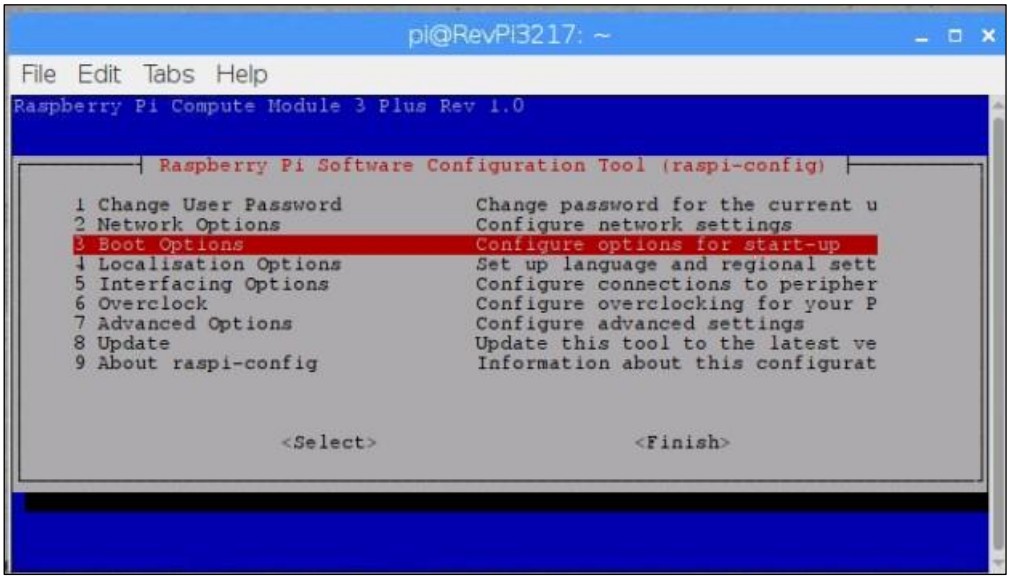

Figure 3: The Boot Option setting that has to be selected.

Step 3: The selection of the boot option leads to four sub-options. The fourth option 'B4' (shown in Figure 4) is selected to bypass the login authentication to enter into the GUI desktop.

Figure 4: The option 'B4' removes the necessity of login authentication.

Step 4: After all the above-mentioned steps are completed, the system is rebooted using the shell command sudo reboot to save the settings and to check if the system boots directly into the GUI desktop.

The RevPi Compact now boots into the desktop without a need for authentication using User-Id and Password.

2.2 One-Step Authentication for VNC remote access

The VNC remote access application is used to view, access or even take full control of a computer that is either in a different location or in the same local network with the help of the internet. The computer from which the remote system is accessed can be referred to as a Master and the remote computer can be referred to as a Slave. There are two types of VNC software applications. The 'VNC Viewer' is the application to be installed in the master computer and is used to view and take control over the slave system. The 'VNC Server' application is to be installed in the remote slave computer and is used to allow the connection from the master computer. In the VNC Viewer application, the connection with the slave can be established in two ways. The first method is to use the IP address of the slave computer is connected to the same LAN. The second method is to enter the unique name of the slave computer and search in the application. The application finds the system with this unique name. This unique name can be found on the VNC Server application in the slave computer.

Previously while the VNC Server application was used, it was not tested for operating on different internet connections. The data transfer between the computers was checked during the operation on the same internet connections through the VNC connection. To enable the system to communicate on different internet connections, either the IP address of the master can be added as a rule in step 3 (Figure 7) or use the account login method. When both the master and slave computers are on the same VNC accounts, the master computer becomes a trusted device automatically. The steps are explained in detail below.

Step 1: After downloading the software applications in both the systems and the necessary installations completed, a new profile account should be created with a username and password. This can also be done on the RealVNC website [6]. After the profile is created, the VNC Server application is opened in the RevPi Compact (slave).

The VNC Server is shown in Figure 5. The options tab is selected from the drop-down list in the top-right corner.

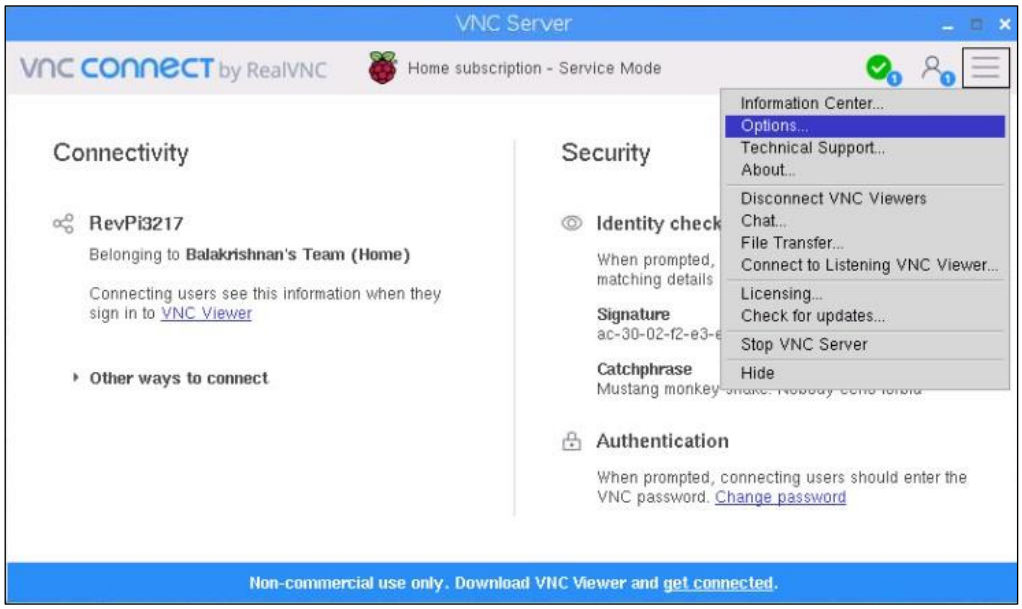

Figure 5: VNC server window with the drop-down settings.

The authentication method and encryption settings can be modified in the 'Security' tab shown in Figure 6.

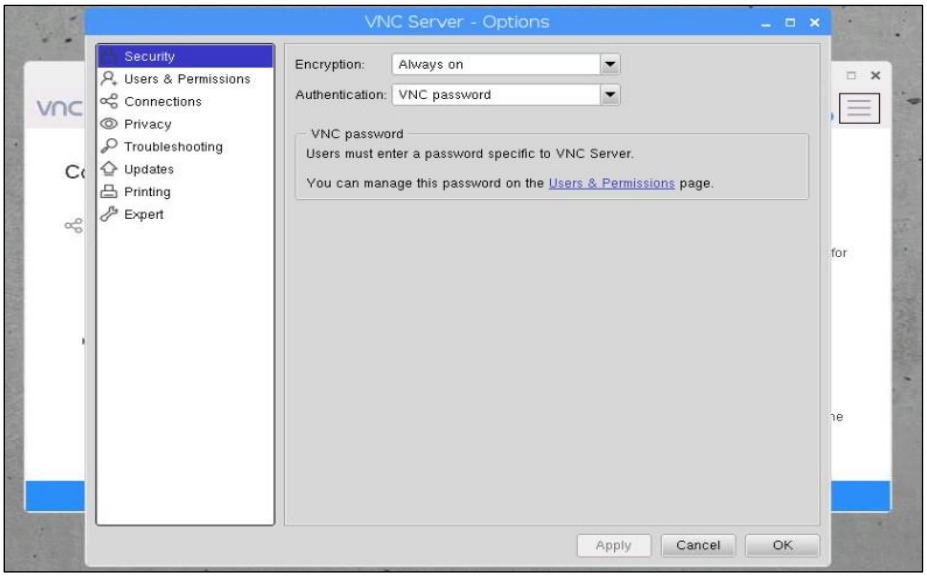

Figure 6: The encryption and authentication settings.

Step 2: From the menu listed on the left side of the Options window shown in Figure 6, the 'connections' tab is selected. The connections window opens up as shown in Figure 7. This window is important for setting rules to accept/reject the incoming connections.

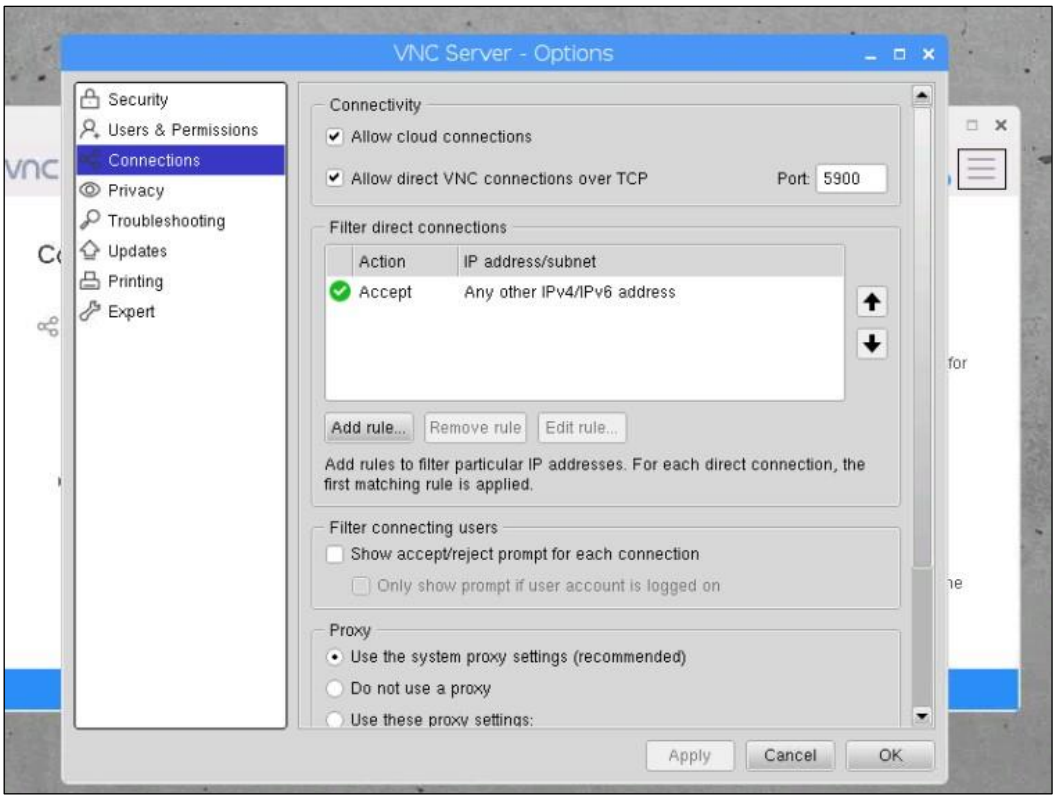

Figure 7:The connections window displaying all the options.

For disabling the manual authentication for an incoming connection from the slave device, the small box titled ‘Filter connecting users’ is used. The check box ‘Show accept/reject prompt for each connection’ is unchecked. This disables the necessity of manually authorizing the incoming connection.

After this step, it is also possible for any computer to establish a connection with the slave device and the RevPi Compact may fall prey to hackers. But the security settings altered in Step 1 (Figure 6) will act as one-way security. This means only the user that knows the password of the VNC account or the password of RevPi Compact can have access to the slave system.

3. Results and Discussion

3.1 Testing the access to the RevPi Compact

After all the necessary steps are carried out, the final part is testing if all these settings are working as expected. The two devices are connected to the internet using two different networks. This is to make sure that the remote access connection can be established even when the devices are in different geographical locations. The VNC Viewer application is opened up on the master computer. The name of the slave computer can be entered in the Search Tab shown in Figure 8. When the unique name is searched, it can be found by the search engine.

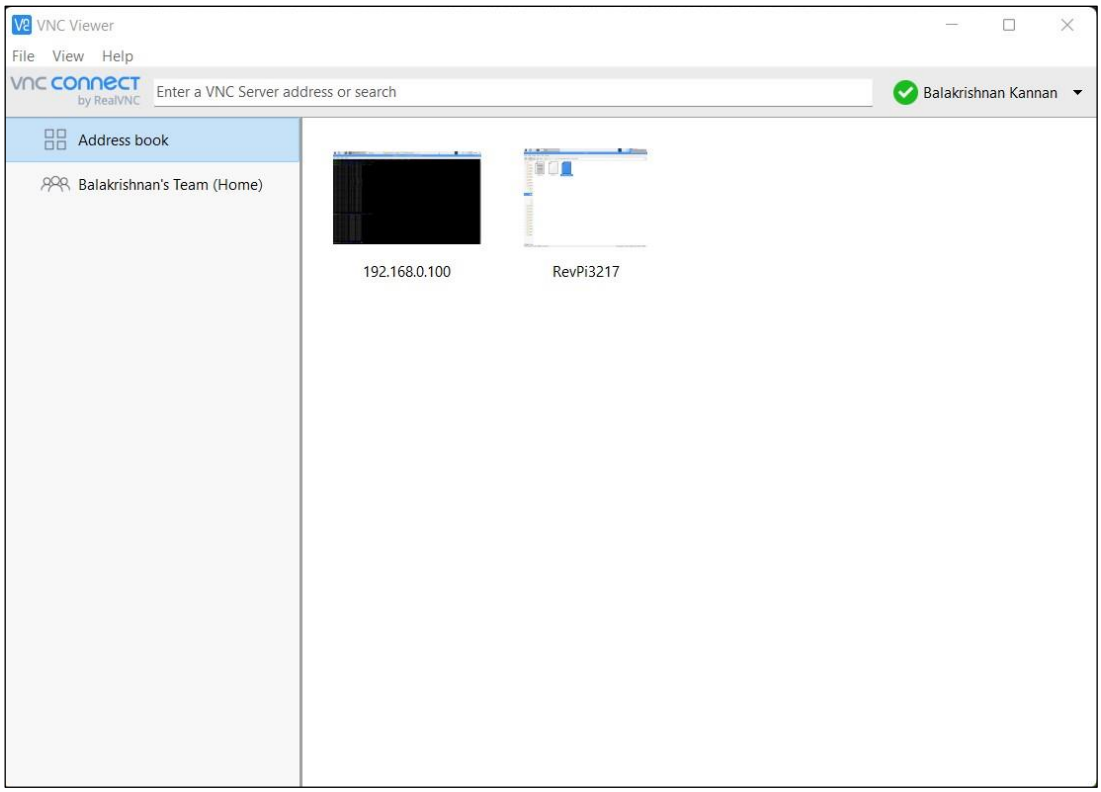

Figure 8: The VNC Viewer on the master computer, displaying a list of connected slaves, address book and search tab.

One-Way Authentication

The RevPi Compact is selected to establish a connection. The ‘Authentication’ window opens up as shown in Figure 9. In this window, the password of the RevPi Compact (user-defined) is entered and ‘OK’ is pressed. A connection request is immediately sent to the remote slave device (RevPi Compact).

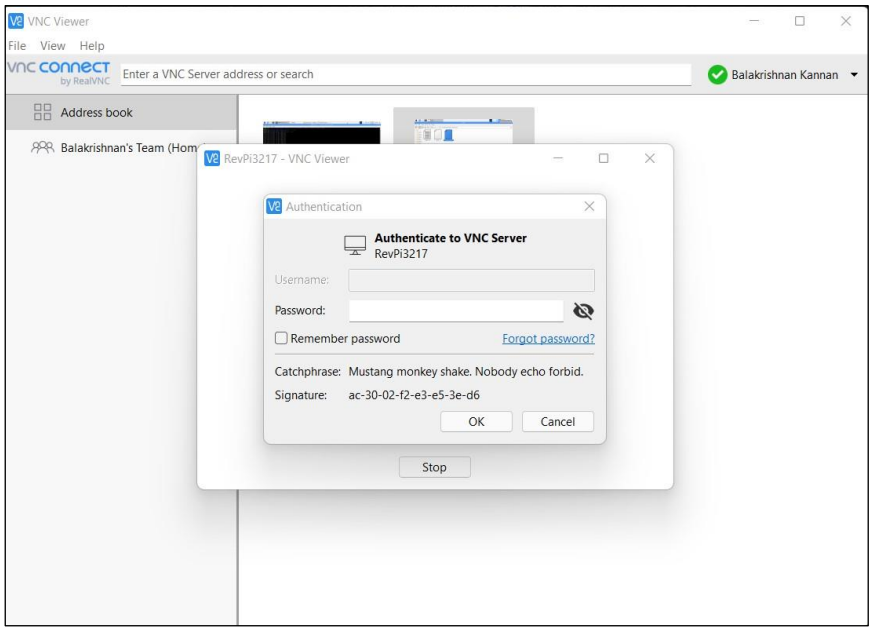

Figure 9: ‘Authentication’ window to enter the password and request access to the remote device.

The connection request and authentication take a few seconds depending upon the strength and speed of the internet connections. But once the connection is established, the system directly boots into the GUI desktop of RevPi Compact as shown in Figure 10.

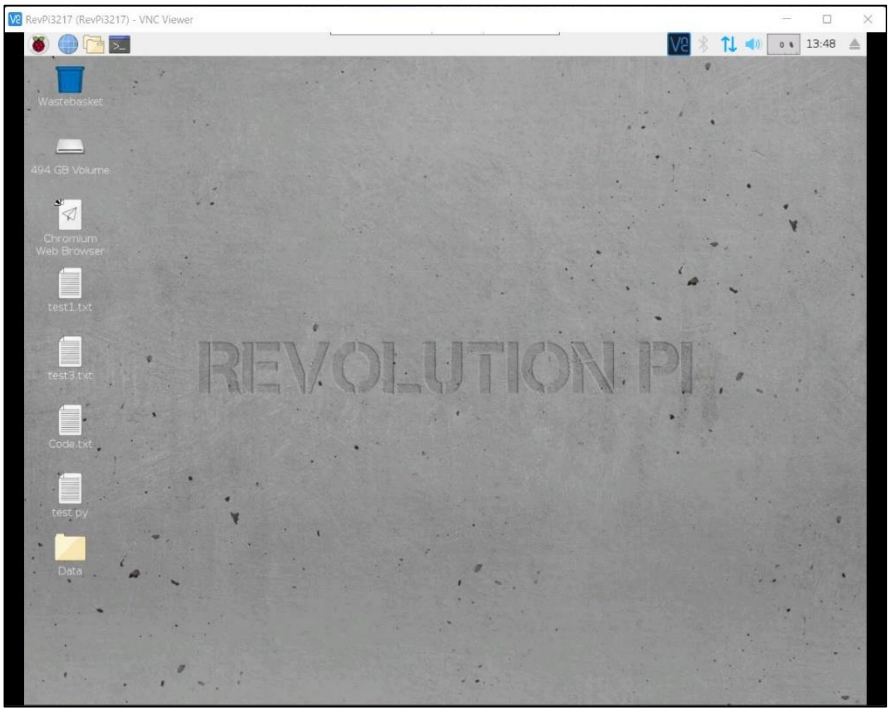

Figure 10: The GUI desktop of RevPi Compact as viewed on VNC Viewer from the master computer.

Once the desktop is visible, it is possible to take control of the entire system and all its peripheral sensors connected. The data can be transferred as files between the two systems from the 'File Transfer' option. Again, the speed of transfer depends on the size of the file, speed and strength of the internet connection.

Finally, the slave computer (RevPi Compact) is rebooted multiple times to check if the connection is reliably established the same way as expected.

4. Conclusion

The communication between a computer working offshore and a master computer onshore should be reliable and highly stable. This is because of the less manual accessibility of the offshore computer (RevPi Compact) and once installed, it should work for a brief time to measure and store useful data about the waves. A remote access software will help the onshore operator to gain full access to the offshore system and helps to control, modify, rectify or even add new functions to the existing code.

The steps explained in this report increases the reliability of the communication protocol making it easily accessible from any authentic user around the world. There is a level of security that comes with one-way password authentication, which protects and strengthens the device and the stored data. Making the device completely automatic and virtually 100% accessible opens up a gateway to make any future updates and changes without physically accessing it.

References

[1] B. Kannan, "Design and Development of a Data Acquisition and Communication System for Point Absorber Tracking," Master Thesis published at Uppsala University, Uppsala, Sweden, 2021.

[2] J. Luer, "'Design and Development of a Measurement System to Track the Motion of a Point Absorber'," Master Thesis Published at Uppsala University, Uppsala, Sweden, 2020.

[3] "Revolution Pi - RevPi Compact," KUNBUS GmBH, 2021. [Online]. Available: https://revolution.kunbus.com/revpi-compact/. [Accessed 2021].

[4] HUAWEI TECHNOLOGIES, "cdn.competec.ch," 03 May 2019. [Online]. Available: https://cdn.competec.ch/documents2/5/3/7/51921735/51921735.pdf. [Accessed April 2021].

[5] "Victron Energy," 02 May 2017. [Online]. Available: https://www.victronenergy.com/upload/documents/Manual-BlueSolar-PWM-Light-12-24V-Charge-Controller-EN-A4.pdf. [Accessed 2021].

[6] "RealVNC-Account setup and Download," RealVNC Limited, 2021. [Online]. Available: https://www.realvnc.com/en/connect/download/vnc/. [Accessed June 2021].