

SYSTEM AND METHOD FOR AUTHENTICATING COMMUNICATION WITH A MARITIME VESSEL VIA A CENTRALIZED PLATFORM

FIELD OF INVENTION

[0001] Embodiments of a present invention relate to authentication of communication with maritime vessels, and more particularly, to a system and method for authenticating the communication with a maritime vessel via a centralized platform.

BACKGROUND

[0002] As the world's population continues to grow, particularly in developing countries, low-cost and efficient maritime transport has an essential role to play in the growth and sustainable development. Shipping helps ensure that the benefits of trade and commerce are more evenly spread. At the same time communication with the ships is also important. Currently, the ships use the Very Small Aperture Terminal Internet Service provider (VSAT ISP) facility for communication. This only provides a physical layer communication. There is a plurality of approaches to provide secured messaging communication.

[0003] One such approach includes a platform using authentication such as Password, which is easy to hack. Therefore, a modern approach includes a platform using 2-Factor Authentication (2FA). The 2FA works on the principle of "What you know" and "What you have". "What you know" is typically a Password. For the second factor (What you have), many applications use One-time Password (OTP) sent on Mobile or e-Mail. Sending OTP on mobile is fraught with issues arising due to network coverage. A smarter approach is to provide an Authentication platform using Time-based One-Time Passcode (TOTP), normally installed on Mobile devices, which is a one-time effort. Such an approach includes an Authentication platform that provides unique passcode for each individual device which also changes based on time. However, mobile devices are mostly tied to an individual and not to an entity such as a Marine Vessel. For Marine Vessels, e-Mail of vessel bound computing devices are unique, and hence such a 2FA platform needs to be installed on Vessel bound computers.

[0004] Hence, there is a need for an improved system and method for authenticating communication with a maritime vessel via a centralized platform which addresses the aforementioned issues.

BRIEF DESCRIPTION

[0005] In accordance with one embodiment of the disclosure, a system for authenticating communication with a maritime vessel via a centralized platform is provided. The system includes one or more processors. The system also includes a vessel registration subsystem operable by the one or more processors. The vessel registration subsystem is configured to receive one or more vessel related parameters from an authorized user via a vessel device, wherein the vessel device on the maritime vessel is connected to a router, wherein the one or more vessel related parameters include one of a unique International Maritime Organization number of the maritime vessel, a unique vessel E-mail Identifier, Internet Protocol address of the router, or a combination thereof. The vessel registration subsystem is also configured to compare the unique International Maritime Organization number of the maritime vessel with an International Maritime Organization number linked to the Internet Protocol address received to generate a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router's service provider database. Further, the vessel registration subsystem is also configured to generate a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result. Furthermore, the vessel registration subsystem is also configured to register the maritime vessel on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel. Further, the system also includes an authentication subsystem operable by the one or more processors. The authentication subsystem is configured to generate a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel on the centralized platform. Further, the authentication subsystem is also configured to transmit the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device and the corresponding one or more destined devices for authenticating the communication of the

corresponding one or more destined devices with the vessel device on the maritime vessel.

[0006] In accordance with another embodiment, a method for authenticating communication with a maritime vessel via a centralized platform is provided. The method includes receiving one or more vessel related parameters from an authorized user via a vessel device, wherein the vessel device on the maritime vessel is connected to a router, wherein the one or more vessel related parameters include one of a unique International Maritime Organization number of the maritime vessel, a unique vessel E-mail Identifier, Internet Protocol address of the router, or a combination thereof. The method also includes comparing the unique International Maritime Organization number of the maritime vessel with an International Maritime Organization number linked to the Internet Protocol address received for generating a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router's service provider database. Further, the method also includes generating a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result. Further, the method also includes registering the maritime vessel on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel. Furthermore, the method also includes generating a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel on the centralized platform. Furthermore, the method also includes transmitting the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device and the corresponding one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device on the maritime vessel.

[0007] To further clarify the advantages and features of the present disclosure, a more particular description of the disclosure will follow by reference to specific embodiments thereof, which are illustrated in the appended figures. It is to be appreciated that these figures depict only typical embodiments of the disclosure and

are therefore not to be considered limiting in scope. The disclosure will be described and explained with additional specificity and detail with the appended figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The disclosure will be described and explained with additional specificity and detail with the accompanying figures in which:

[0008] FIG. 1 is a block diagram representation of a system for authenticating communication with a maritime vessel via a centralized platform in accordance with an embodiment of the present disclosure;

[0009] FIG. 2 is a block diagram representation of an exemplary embodiment of the system for authenticating communication with the maritime vessel via the centralized platform of FIG. 1 in accordance with an embodiment of the present disclosure;

[0010] FIG. 3 is a block diagram of an authenticating computer or an authenticating server in accordance with an embodiment of the present disclosure; and

[0011] FIG. 4 is a flow chart representing steps involved in a method for authenticating communication with a maritime vessel via a centralized platform in accordance with an embodiment of the present disclosure.

[0012] Further, those skilled in the art will appreciate that elements in the figures are illustrated for simplicity and may not have necessarily been drawn to scale. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the figures by conventional symbols, and the figures may show only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the figures with details that will be readily apparent to those skilled in the art having the benefit of the description herein.

DETAILED DESCRIPTION

[0013] For the purpose of promoting an understanding of the principles of the disclosure, reference will now be made to the embodiment illustrated in the figures

and specific language will be used to describe them. It will nevertheless be understood that no limitation of the scope of the disclosure is thereby intended. Such alterations and further modifications in the illustrated system, and such further applications of the principles of the disclosure as would normally occur to those skilled in the art are to be construed as being within the scope of the present disclosure.

[0014] The terms "comprises", "comprising", or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a process or method that comprises a list of steps does not include only those steps but may include other steps not expressly listed or inherent to such a process or method. Similarly, one or more devices or sub-systems or elements or structures or components preceded by "comprises... a" does not, without more constraints, preclude the existence of other devices, sub-systems, elements, structures, components, additional devices, additional sub-systems, additional elements, additional structures or additional components. Appearances of the phrase "in an embodiment", "in another embodiment" and similar language throughout this specification may, but not necessarily do, all refer to the same embodiment.

[0015] Unless otherwise defined, all technical and scientific terms used herein have the same meaning as commonly understood by those skilled in the art to which this disclosure belongs. The system, methods, and examples provided herein are only illustrative and not intended to be limiting.

[0016] In the following specification and the claims, reference will be made to a number of terms, which shall be defined to have the following meanings. The singular forms "a", "an", and "the" include plural references unless the context clearly dictates otherwise.

[0017] Embodiments of the present disclosure relate to a system for authenticating communication with a maritime vessel via a centralized platform. As used herein, the term "maritime vessel" is defined as a component or structure intended for exposure to a marine environment or anything that can float and can be steered/moved, either by own means or by other means. The maritime vessel may include a ship, a floating platform, boats, barges, and the like. Maritime vessels are used by great industries for multiple applications and hence communication among the maritime vessels and

between the maritime vessel and other devices may be important for multiple reasons. Further, maintaining the authenticity of such communication is also important. Thus, the system as described hereafter in FIG. 1 is the system for authenticating communication with the maritime vessel via the centralized platform.

[0018] FIG. 1 is a block diagram representation of the system 10 for authenticating communication with a maritime vessel 20 via a centralized platform in accordance with an embodiment of the present disclosure. The system 10 includes one or more processors 30. Basically, to authenticate the communication with the maritime vessel 20 using the system 10, the corresponding maritime vessel 20 may have to be registered on the centralized platform. Thus, the system 10 also includes a vessel registration subsystem 40 operable by the one or more processors 30. The vessel registration subsystem 40 is configured to receive one or more vessel related parameters from an authorized user via a vessel device 50.

[0019] Further, the one or more vessel related parameters include one of a unique International Maritime Organization (IMO) number of the maritime vessel 20, a unique vessel E-mail Identifier (ID), Internet Protocol (IP) address of the router, and the like, or a combination thereof. Moreover, in one embodiment, the one or more vessel related parameters may be stored in a database (as shown in FIG. 2) of the system 10. In one exemplary embodiment, the database may include one of a local database and a cloud database. As used herein, the term “International Maritime Organization Number” is defined as a unique identifier for ships and it consists of the three letters "IMO" followed by the seven-digit number assigned to all ships by (Information Handling Service) IHS Fairplay constructed, assigned under the International Convention for the Safety of Life at Sea and it remains unchanged through a vessel's lifetime and is linked to its hull, regardless of any changes of names, flags, or owners. Also, in one embodiment, the authorized user of the maritime vessel 20 may be provided with a unique vessel e-mail ID which may be used for communication by the corresponding authorized user. In one exemplary embodiment, the authorized user may include a vessel captain. Thus, in an embodiment, even if the vessel captain changes, the unique vessel e-mail ID may remain the same as the corresponding unique vessel e-mail ID belongs to the corresponding maritime vessel 20.

[0020] Further, the vessel device 50 on the maritime vessel 20 is connected to a router 60. In one embodiment, the vessel device 50 may include a computing device on the maritime vessel 20. In such embodiment, the computing device may include a desktop computer. In another embodiment, the vessel device 50 may include any device which may be feasible to be used on the maritime vessel 20. In one exemplary embodiment, router 60 may be configured to establish a communication link using a Very Small Aperture Terminal Internet Service provider (VSAT ISP). As used herein, the term “Very Small Aperture Terminal” is defined as a satellite communications system that serves home and business users. A VSAT end user needs a box that interfaces between the user's computer and an outside antenna with a transceiver. The transceiver receives or sends a signal to a satellite transponder in the sky. Moreover, the VSAT ISP may be a service provider who provides a service of the VSAT to the corresponding maritime vessel 20 to establish the communication link with the vessel device 50 on the maritime vessel 20 via the router 60.

[0021] In one exemplary embodiment, the router 60 may include a satellite route. As used herein, the term “satellite router” is defined as an Indoor Unit (IDU) that contains a modulator and a demodulator and is one of the essential components of a VSAT. Thus, in one embodiment, the IP address of the router 60 may also be received by the vessel registration subsystem 40, for the vessel registration subsystem 40 to verify that the IP address received is linked with the unique IMO number received of the maritime vessel 20 as the router 60 having the corresponding IP address is linked to the vessel device 50 on the corresponding maritime vessel 20.

[0022] Thus, the vessel registration subsystem 40 is also configured to compare the unique IMO number of the maritime vessel 20 with an IMO number linked to the IP address received to generate a validation result for validating the IP address received, wherein the IMO number linked to the IP address received is stored in a router's service provider database. In one exemplary embodiment, the IMO number linked to the IP address received may be extracted from the router's service provider database, and then the corresponding IMO number extracted may be compared with the unique IMO number of the maritime vessel 20. In another exemplary embodiment, the unique IMO number of the maritime vessel 20 and the IP address received may be transmitted to the router's service provider, wherein the router's service provider may extract the

IMO number linked to the IP address received and then compare with the unique IMO number received.

[0023] Further, in one embodiment, the validation result may include a positive validation result when the unique IMO number of the maritime vessel 20 matches with the IMO number linked to the IP address received. In another embodiment, validation result may include a negative validation result when the unique IMO number of the maritime vessel 20 mismatches with the IMO number linked to the IP address received.

[0024] In one exemplary embodiment, the system 10 may also include a notification subsystem (as shown in FIG. 2) operable by the one or more processors 30. The notification subsystem may be operatively coupled to the vessel registration subsystem 40. The notification subsystem may be configured to generate a notification for the authorized user via the vessel device 50 when the validation result generated may include the negative validation result. In one exemplary embodiment, the notification generated may be in one or more forms such as a text message, an audible notification, a pop up on a user interface on the vessel device 50, or the like.

[0025] Further, the vessel registration subsystem 40 is also configured to generate a unique vessel identity based on the one or more vessel related parameters received upon generating the positive validation result. Furthermore, the vessel registration subsystem 40 is also configured to register the maritime vessel 20 on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel 20. In one embodiment, the unique vessel identity assigned to the maritime vessel 20 may also be stored in the database.

[0026] Further, whenever the vessel device 50 of the maritime vessel 20 may receive a communication request, the communication may have to be authenticated before initiating the corresponding communication. In one embodiment, the communication request may include a text message, an E-mail, a voice note, a web link, or the like. Thus, the system 10 also includes an authentication subsystem 70 operable by the one or more processors 30. The authentication subsystem 70 is operatively coupled to the vessel registration subsystem 40. The authentication subsystem 70 is configured to generate a time-based one-time password (TOTP) after

every pre-defined time interval using a password generation technique upon registering the maritime vessel 20 on the centralized platform.

[0027] In one embodiment, the TOTP may include a string of one of one or more characters, one or more numbers, and the like, or a combination thereof. In one embodiment, a size of the string may include about six to about seven. Further, in one exemplary embodiment, the pre-defined time interval after which the TOTP may be generated periodically may include about 30 seconds. In one embodiment, the TOTP may be generated in the vessel device 50 upon registering the maritime vessel 20 on the centralized platform via the vessel device 50.

[0028] Later, in one embodiment, the TOTP generated may have to be shared with one or more destined devices from which the communication request was received for authenticating the communication between the vessel device 50 and the corresponding one or more destined devices. Thus, the authentication subsystem 70 is also configured to transmit the TOTP generated to at least one of one or more destined devices every time the communication link is established between the vessel device 50 and the corresponding one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device 50 on the maritime vessel 20. In one exemplary embodiment, the one or more destined devices may include a computing device on one of the one or more destined maritime vessels, land, and the like, or a combination thereof. In one embodiment, the computing device may include a desktop computer.

[0029] Also, in one embodiment, the TOTP may be unique and related to the corresponding maritime vessel 20. In one embodiment, the time-based one-time password may be generated based on the one or more vessel related parameters and hence may be unique and related to the corresponding maritime vessel 20. In one embodiment, the password generation technique may include the implementation of a set of instructions related to RFC 6238. As used herein, the “RFC 6238” is defined as an extension of the Hashed Message Authentication Code (HMAC)-based One-time Password algorithm (HOTP), it has been adopted as Internet Engineering Task Force (IETF) standard RFC 6238. The time-based one-time password (TOTP) is the cornerstone of Initiative for Open Authentication (OATH) and is used in a number of two-factor authentication (2FA) systems.

[0030] FIG. 2 is a block diagram representation of an exemplary embodiment of the system 10 for authenticating communication with the maritime vessel 20 via a centralized platform of FIG. 1 in accordance with an embodiment of the present disclosure. The system 10 includes the one or more processors 30. Suppose a ship 'A' 80 is traveling from a first location to a second location carrying one or more goods, wherein the one or more goods may have to be transported to the second location via sea. As used herein, the ship 'A' 80 is substantially similar to the maritime vessel 20 in FIG. 1. The ship 'A' 80 is registered on the centralized platform via the vessel registration subsystem 40 of the system 10 by a ship captain 90 of the ship 'A' 80 for the ship 'A' 80 to be able to use the system 10. While registration, the one or more ship related parameters received by the vessel registration subsystem 40 may be stored in the database 100 of the system 10.

[0031] Further, the router 60 is linked to a first computing device 110 of the ship 'A' 80, to enable the first computing device 110 to establish the communication link with one or more second computing devices 120 on one of one or more other ships, land, the first location, the second location, and the like, or a combination thereof. As used herein the first computing device 110 and the one or more second computing devices 120 are substantially similar to the vessel device 50 and the one or more destined devices in FIG. 1 respectively.

[0032] Moreover, the IP address of the router 60 may have to be validated while registration which is done upon comparing the unique IMO number of the ship 'A' 80 with the IMO number linked to the IP address transmitted to the VSAT ISP 130. Here, the IMO number linked to the IP address received by the VSAT ISP 130 is stored in the service provider's database 140. If the validation result generated includes the negative validation result then a notification is generated for the ship captain 90 via the notification subsystem 145 of the system 10. Suppose the validation result generated includes the positive validation result. Therefore, the ship 'A' 80 gets registered on the centralized platform.

[0033] Further, suppose the ship 'A' 80 has missed carrying some the one or more goods from the first location. Later, authorities 150 at the first location load a boat 'X' with the one or more goods which were missed by the ship 'A' 80 and send the boat 'X' towards the direction of the ship 'A' 80, so that the ship 'A' 80 which maybe now

in the middle of its way, might receive the one or more goods from the boat 'X' before reaching to the second location. Now, this has to be communicated to the ship 'A' 80, so that the ship captain 90 of the ship 'A' 80 might take one or more actions such as reduce the traveling speed of the ship 'A' 80, waits, or the like. Thus, the authorities 150 via the one or more second computing devices 120 at the first location send an E-mail to the first computing device 110 of the ship 'A' 80, wherein the E-mail includes information about missing of the one or more goods and information about the boat 'X' which is on its way to drop the one or more goods to the ship 'A' 80 which were missed.

[0034] Basically, upon registering the ship 'A' 80 on the centralized platform, the system 10 keeps on generating the TOTP after every 30 seconds via the authentication subsystem 70 of the system 10. The TOTP is generated based on the one or more ship related parameters of the ship 'A' 80. Further, upon receiving the E-mail from the one or more second computing devices 120, the communication may have to be authenticated by the ship captain 90. Thus, the ship captain 90 enters the TOTP generated before opening the E-mail received, and hence the TOTP gets transmitted to the corresponding one or more second computing devices 120 via the authentication subsystem 70, thereby authenticating the communication as the TOTP generated at that time is unique and related to the ship 'A' 80. Further, upon authenticating, the ship captain 90 reads the E-mail received and take the corresponding one or more actions.

[0035] FIG. 3 is a block diagram of an authenticating computer or an authenticating server 160 in accordance with an embodiment of the present disclosure. The authenticating server 160 includes processor(s) 170, and a memory 180 coupled to a bus 190. As used herein, the processor(s) 170 and the memory 180 are substantially similar to the system 10 of FIG. 1. Here, the memory 180 is located in a local storage device.

[0036] The processor(s) 170, as used herein, means any type of computational circuit, such as, but not limited to, a microprocessor, a microcontroller, a complex instruction set computing microprocessor, a reduced instruction set computing microprocessor, a very long instruction word microprocessor, an explicitly parallel

instruction computing microprocessor, a digital signal processor, or any other type of processing circuit, or a combination thereof.

[0037] Computer memory elements may include any suitable memory device(s) for storing data and executable program, such as read only memory, random access memory, erasable programmable read only memory, electrically erasable programmable read only memory, hard drive, removable media drive for handling memory cards and the like. Embodiments of the present subject matter may be implemented in conjunction with program modules, including functions, procedures, data structures, and application programs, for performing tasks, or defining abstract data types or low-level hardware contexts. Executable program stored on any of the above-mentioned storage media may be executable by the processor(s) 170.

[0038] The memory 180 includes a plurality of subsystems stored in the form of executable program which instructs the processor(s) 170 to perform method steps illustrated in FIG. 3. The memory 180 has following subsystems: a vessel registration subsystem 40 and an authentication subsystem 70.

[0039] The vessel registration subsystem 40 is configured to receive one or more vessel related parameters from an authorized user via a vessel device 50, wherein the vessel device 50 on the maritime vessel 20 is connected to a router 60, wherein the one or more vessel related parameters include one of a unique International Maritime Organization number of the maritime vessel 20, a unique vessel E-mail Identifier, Internet Protocol address of the router 60, or a combination thereof.

[0040] The vessel registration subsystem 40 is also configured to compare the unique International Maritime Organization number of the maritime vessel 20 with an International Maritime Organization number linked to the Internet Protocol address received to generate a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router 60's service provider database.

[0041] The vessel registration subsystem 40 is also configured to generate a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result. The vessel registration subsystem 40 is

also configured to register the maritime vessel 20 on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel 20.

[0042] The authentication subsystem 70 is configured to generate a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel 20 on the centralized platform. The authentication subsystem 70 is also configured to transmit the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device 50 and the corresponding one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device 50 on the maritime vessel 20.

[0043] FIG. 4 is a flow chart representing steps involved in a method 200 for authenticating communication with a maritime vessel via a centralized platform in accordance with an embodiment of the present disclosure. The method 200 includes receiving one or more vessel related parameters from an authorized user via a vessel device, wherein the vessel device on the maritime vessel is connected to a router, wherein the one or more vessel related parameters include one of a unique International Maritime Organization number of the maritime vessel, a unique vessel E-mail Identifier, Internet Protocol address of the router, or a combination thereof in step 210. In one embodiment, receiving the one or more vessel related parameters includes receiving the one or more vessel related parameters by a vessel registration subsystem 40.

[0044] The method 200 also includes comparing the unique International Maritime Organization number of the maritime vessel with an International Maritime Organization number linked to the Internet Protocol address received for generating a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router's service provider database in step 220. In one embodiment, comparing the unique International Maritime Organization number of the maritime vessel with the International Maritime Organization number linked to the Internet Protocol address includes comparing the unique International Maritime Organization number of the maritime vessel with the International Maritime

Organization number linked to the Internet Protocol address by the vessel registration subsystem 40.

[0045] In one exemplary embodiment, generating the validation result includes generating the positive validation result when the unique International Maritime Organization number of the maritime vessel matches with the International Maritime Organization number linked to the Internet Protocol address received. In another embodiment, generating the validation result includes generating a negative validation result when the unique International Maritime Organization number of the maritime vessel mismatches with the International Maritime Organization number linked to the Internet Protocol address received.

[0046] Furthermore, the method 200 includes generating a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result in step 230. In one embodiment, generating the unique vessel identity includes generating the unique vessel identity by the vessel registration subsystem 40.

[0047] Furthermore, the method 200 also includes registering the maritime vessel on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel in step 240. In one embodiment, registering the maritime vessel on the centralized platform includes registering the maritime vessel on the centralized platform by the vessel registration subsystem 40.

[0048] Furthermore, the method 200 also includes generating a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel on the centralized platform in step 250. In one embodiment, generating the time-based one-time password includes generating the time-based one-time password by an authentication subsystem 70.

[0049] In one exemplary embodiment, generating the time-based one-time password includes generating the time-based one-time password which is unique and related to the corresponding maritime vessel.

[0050] Furthermore, the method 200 also includes transmitting the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device and the corresponding

one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device on the maritime vessel in step 260. In one embodiment, transmitting the time-based one-time password generated to at least one of the one or more destined devices includes transmitting the time-based one-time password generated to at least one of the one or more destined devices by the authentication subsystem 70.

[0051] Various embodiments of the present disclosure enable secured communication with the maritime vessel as the communication is authenticated via the centralized platform. Also, the validation of the IP address of the router connected to the vessel device during registration ensures that the system is installed in the vessel device of the maritime vessel and nowhere else. Moreover, the TOTP generated for authentication is based on the one or more vessel related parameters which make the TOTP generated unique, thereby making the system unique, more secure, and more efficient.

[0052] While specific language has been used to describe the disclosure, any limitations arising on account of the same are not intended. As would be apparent to a person skilled in the art, various working modifications may be made to the method in order to implement the inventive concept as taught herein.

[0053] The figures and the foregoing description give examples of embodiments. Those skilled in the art will appreciate that one or more of the described elements may well be combined into a single functional element. Alternatively, certain elements may be split into multiple functional elements. Elements from one embodiment may be added to another embodiment. For example, order of processes described herein may be changed and are not limited to the manner described herein. Moreover, the actions of any flow diagram need not be implemented in the order shown; nor do all of the acts need to be necessarily performed. Also, those acts that are not dependent on other acts may be performed in parallel with the other acts. The scope of embodiments is by no means limited by these specific examples.

WHAT IS CLAIMED IS:

1. A system for authenticating communication with a maritime vessel via a centralized platform, wherein the system comprises:

one or more processors;

a vessel registration subsystem operable by the one or more processors, wherein the vessel registration subsystem is configured to:

receive one or more vessel related parameters from an authorized user via a vessel device, wherein the vessel device on the maritime vessel is connected to a router, wherein the one or more vessel related parameters comprise one of a unique International Maritime Organization number of the maritime vessel, a unique vessel E-mail Identifier, Internet Protocol address of the router, or a combination thereof;

compare the unique International Maritime Organization number of the maritime vessel with an International Maritime Organization number linked to the Internet Protocol address received to generate a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router's service provider database;

generate a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result; and

register the maritime vessel on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel; and

an authentication subsystem operable by the one or more processors, wherein the authentication subsystem is configured to:

generate a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel on the centralized platform; and

transmit the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device and the corresponding one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device on the maritime vessel.

2. The system according to claim 1, wherein the router is configured to establish the communication link between the vessel device and the one or more destined devices.
3. The system according to claim 2, wherein the router is configured to establish the communication link using a Very Small Aperture Terminal Internet Service provider.
4. The system according to claim 1, wherein the router comprises a satellite router.
5. The system according to claim 1, wherein the vessel device comprises a computing device on the maritime vessel.
6. The system according to claim 1, wherein the validation result comprises the positive validation result when the unique International Maritime Organization number of the maritime vessel matches with the International Maritime Organization number linked to the Internet Protocol address received.
7. The system according to claim 1, wherein the validation result comprises a negative validation result when the unique International Maritime Organization number of the maritime vessel mismatches with the International Maritime Organization number linked to the Internet Protocol address received.
8. The system according to claim 1, wherein the time-based one-time password is unique and related to the corresponding maritime vessel.
9. A method for authenticating communication with a maritime vessel via a centralized platform, wherein the method comprises:

receiving, by a vessel registration subsystem, one or more vessel related parameters from an authorized user via a vessel device, wherein the vessel device on the maritime vessel is connected to a router, wherein the one or more vessel related parameters comprise one of a unique International Maritime Organization number of the maritime vessel, a unique vessel E-mail Identifier, Internet Protocol address of the router, or a combination thereof;

comparing, by the vessel registration subsystem, the unique International Maritime Organization number of the maritime vessel with an International Maritime Organization number linked to the Internet Protocol address received for generating a validation result for validating the Internet Protocol address received, wherein the International Maritime Organization number linked to the Internet Protocol address received is stored in a router's service provider database;

generating, by the vessel registration subsystem, a unique vessel identity based on the one or more vessel related parameters received upon generating a positive validation result;

registering, by the vessel registration subsystem, the maritime vessel on the centralized platform upon assigning the unique vessel identity to the corresponding maritime vessel;

generating, by an authentication subsystem, a time-based one-time password after every pre-defined time interval using a password generation technique upon registering the maritime vessel on the centralized platform; and

transmitting, by the authentication subsystem, the time-based one-time password generated to at least one of one or more destined devices every time a communication link is established between the vessel device and the corresponding one or more destined devices for authenticating the communication of the corresponding one or more destined devices with the vessel device on the maritime vessel.

10. The method according to claim 9, wherein generating the validation result comprises generating the positive validation result when the unique International Maritime Organization number of the maritime vessel matches with the

International Maritime Organization number linked to the Internet Protocol address received.

11. The method according to claim 9, wherein generating the validation result comprises generating a negative validation result when the unique International Maritime Organization number of the maritime vessel mismatches with the International Maritime Organization number linked to the Internet Protocol address received.

12. The method according to claim 9, wherein generating the time-based one-time password comprises generating the time-based one-time password which is unique and related to the corresponding maritime vessel.