# पेटेंट कार्यालय
# शासकीय जर्नल

# OFFICIAL JOURNAL
# OF
# THE PATENT OFFICE

| | | |
|---|---|---|
| निर्गमन सं. 37/2022 | शुक्रवार | दिनांक: 16/09/2022 |
| ISSUE NO. 37/2022 | FRIDAY | DATE: 16/09/2022 |

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202241050947 A

(19) INDIA

(22) Date of filing of Application :06/09/2022

(43) Publication Date : 16/09/2022

(54) Title of the invention : A CERTIFICATE AUTHENTICATION SYSTEM WITH BLOCKCHAIN FOR IOT WITH 5G NETWORK

| | |
|---|---|
| (51) International classification | :B82Y0005000000, B82Y0010000000, C40B0040060000, C12Q0001682500, B01J0019000000 |
| (86) International Application No<br>Filing Date | :PCT//<br>:01/01/1900 |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>:NA |

(71)**Name of Applicant :**

**1)Dr. D. Sengeni**

Address of Applicant :Associate Professor, Electronics and Communication Engineering, CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 Cuddalore ----------- -----------

**2)Dr. Siddhartha Choubey**

**3)Dr. Sima Sahu**

**4)Dr. Shaik Fairooz**

**5)Dr. K.Jamal**

**6)Dr. Joshuva Arockia Dhanraj**

**7)Dr. M. Ravichandran**

**Name of Applicant : NA**

**Address of Applicant : NA**

(72)**Name of Inventor :**

**1)Dr. D. Sengeni**

Address of Applicant :Associate Professor, Electronics and Communication Engineering, CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 Cuddalore ----------- -----------

**2)Dr. Siddhartha Choubey**

Address of Applicant :Associate Professor, Computer Science and Engineering, Shri Shankaracharya Technical Campus, Bhilai, Durg, Chhattisgarh 490020 Durg ----------- -----------

**3)Dr. Sima Sahu**

Address of Applicant :Associate Professor, Department of ECE, Malla Reddy Engineering College, Hyderabad, Pin Code: 500100 Hyderabad ----------- -----------

**4)Dr. Shaik Fairooz**

Address of Applicant :Associate Professor, Department of ECE, Malla Reddy Engineering College, Hyderabad, Pin Code: 500100 Hyderabad ----------- -----------

**5)Dr. K.Jamal**

Address of Applicant :Professor, Department of ECE, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Pin Code: 500090 Hyderabad ----------- -----------

**6)Dr. Joshuva Arockia Dhanraj**

Address of Applicant :Assistant Professor (S.G.), Department of Mechatronics Engineering, Hindustan Institute of Technology and Science (HITS), #1, IT Expressway, Bay Range Campus, Padur, Tamil Nadu, 603103, India Padur ----------- -----------

**7)Dr. M. Ravichandran**

Address of Applicant :Professor, Department of Mechanical Engineering, K. Ramakrishnan College of Engineering, Trichy-621112, Tamil Nadu, India Trichy ----------- -----------

(57) Abstract :

The present invention discloses a certificate authentication system with blockchain for IoT with 5G network. The system is comprised of, but not limited to, an authentication method using blockchain technology to store security credentials for IoT devices in a decentralized manner, and through both an informal and a rigorous security examination utilizing the Scyther tool, the system is determined to be safe and secure. When implemented in the Ethereum test network, the smart contracts utilized in the scheme are also determined to be effective. Further, the technique is shown to have achieved lower communication latency compared to the existing protocols through experimental performance analysis. Accompanied Drawings [FIGS.1-2]

No. of Pages : 20 No. of Claims : 7

|  |  |
|---|---|
| FORM 1<br>THE PATENTS ACT 1970 (39 of 1970) and THE PATENTS RULES, 2003 **APPLICATION FOR GRANT OF PATENT**<br>(See section 7, 54 and 135 and sub-rule (1) of rule 20) | (FOR OFFICE USE ONLY) |

|  |  |  |
|---|---|---|
|  | Application No. |  |
|  | Filing date: |  |
|  | Amount of Fee paid: |  |
|  | CBR No: |  |
|  | Signature: |  |

|  |  |
|---|---|
| **1. APPLICANT'S REFERENCE / IDENTIFICATION NO. (AS ALLOTTED BY OFFICE)** |  |

**2. TYPE OF APPLICATION [Please tick (✓ ) at the appropriate category]**

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Ordinary (✓) |  | Convention ( ) |  | PCT-NP ( ) |  |
| Divisional ( ) | Patent of Addition ( ) | Divisional ( ) | Patent of Addition ( ) | Divisional ( ) | Patent of Addition ( ) |

**3A. APPLICANT(S)**

| Name In Full | Nationality | Country of Residence | Address of the Applicant |
|---|---|---|---|
| 1. Dr. D. Sengeni | INDIAN | India | Associate Professor,<br>Electronics and Communication Engineering,<br>CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 |
| 2. Dr. Siddhartha Choubey | INDIAN | India | Associate Professor,<br>Computer Science and Engineering,<br>Shri Shankaracharya Technical Campus, Bhilai, Durg, Chhattisgarh 490020 |
| 3. Dr. Sima Sahu | INDIAN | India | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College,<br>Hyderabad, |

| | | | |
|---|---|---|---|
| | | | Pin Code: 500100 |
| 4. Dr. Shaik Fairooz | INDIAN | India | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College,<br>Hyderabad,<br>Pin Code: 500100 |
| 5. Dr. K.Jamal | INDIAN | India | Professor,<br>Department of ECE,<br>Gokaraju Rangaraju Institute of Engineering and Technology,<br>Hyderabad,<br>Pin Code: 500090 |
| 6. Dr. Joshuva Arockia Dhanraj | INDIAN | India | Assistant Professor (S.G.),<br>Department of Mechatronics Engineering,<br>Hindustan Institute of Technology and Science (HITS), #1, IT Expressway, Bay Range Campus, Padur, Tamil Nadu, 603103, India |
| 7. Dr. M. Ravichandran | INDIAN | India | Professor,<br>Department of Mechanical Engineering,<br>K. Ramakrishnan College of Engineering, Trichy-621112, Tamil Nadu, India |

| | | | |
|---|---|---|---|
| Natural Person (✓ ) | Other than Natural Person | | |
| | Small Entity ( ) | Startup () | Others () |

**4. INVENTOR(S) [Please tick (✓ ) at the appropriate category]**

| | | |
|---|---|---|
| Are all the inventor(s) same as the applicant(s) named above? | Yes (✓ ) | No () |

**If “No”,** furnish the details of the inventor(s)

| Name in Full | Nationality | Country of Residence | Address of the Inventor |
|---|---|---|---|
| Same as Applicant | | | |

**5. TITLE OF THE INVENTION**

"A CERTIFICATE AUTHENTICATION SYSTEM WITH BLOCKCHAIN FOR IOT WITH 5G NETWORK"

| | | |
|---|---|---|
| **6. AUTHORISED REGISTERED PATENT AGENT(S)** | IN/PA No. | |
| | Name | |
| | Mobile No. | |

| | | |
|---|---|---|
| **7. ADDRESS FOR SERVICE OF APPLICANT IN INDIA** | Name | Dr. D. Sengeni |
| | Postal Address | Associate Professor, Electronics and Communication Engineering,<br>CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 |
| | Telephone No. | |
| | Mobile No. | 7892425885 |
| | Fax No. | |
| | E-mail ID | sengeni@ckcet.edu.in |

**~~8. IN CASE OF APPLICATION CLAIMING PRIORITY OF APPLICATION FILED IN CONVENTION~~**

**~~COUNTRY, PARTICULARS OF CONVENTION APPLICATION~~**

| ~~Country~~ | ~~Application Number~~ | ~~Filing date~~ | ~~Name of the applicant~~ | ~~Title of the invention~~ | ~~IPC (as classified in the convention country)~~ |
|---|---|---|---|---|---|
| | | | | | |

**~~9. IN CASE OF PCT NATIONAL PHASE APPLICATION, PARTICULARS OF INTERNATIONAL APPLICATION FILED UNDER PATENT CO-OPERATION TREATY (PCT)~~**

| ~~International application number~~ | ~~International filing date~~ |
|---|---|
| | |

**~~10. IN CASE OF DIVISIONAL APPLICATION FILED UNDER SECTION 16, PARTICULARS OF~~**

**~~ORIGINAL (FIRST) APPLICATION~~**

| ~~Original (first) application No.~~ | ~~Date of filing of original (first) application~~ |
|---|---|
| | |

**~~11. IN CASE OF PATENT OF ADDITION FILED UNDER SECTION 54, PARTICULARS OF MAIN~~**

**~~APPLICATION OR PATENT~~**

| ~~Main application/patent No.~~ | ~~Date of filing of main application~~ |
|---|---|

**12. DECLARATIONS**

**(i) Declaration by the inventor(s)**

(**In case the applicant is an assignee**: the inventor(s) may sign herein below or the applicant may upload the assignment or enclose the assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period).

I/We, the above named inventor(s) is/are the true & first inventor(s) for this Invention and declare that the applicant(s) herein is/are my/our assignee or legal representative.

(a) Date 06/09/2022

| (b) Name | (c) Signature |
|---|---|
| 1. Dr. D. Sengeni<br>2. Dr. Siddhartha Choubey<br>3. Dr. Sima Sahu<br>4. Dr. Shaik Fairooz<br>5. Dr. K.Jamal<br>6. Dr. Joshuva Arockia Dhanraj<br>7. Dr. M. Ravichandran | D. Sengeni Siddhartha Sima Sahu<br>K. Jamal<br>M. R |

~~**(ii) Declaration by the applicant(s) in the convention country**~~

~~**(In case the applicant in India is different than the applicant in the convention country:** the applicant in the convention country may sign herein below or applicant in India may upload the assignment from the applicant in the convention country or enclose the said assignment with this application for patent or send the assignment by post/electronic transmission duly authenticated within the prescribed period)~~

~~I/We, the applicant(s) in the convention country declare that the applicant(s) herein is/are my/our assignee or legal representative.~~

~~(a) Date~~

~~(b) Signature(s)~~

(c) ~~Name(s) of the signatory~~

**(iii) Declaration by the applicant(s)**

I/We the applicant(s) hereby declare(s) that: -

€ ~~I am/~~ We are in possession of the above-mentioned invention.

€ The ~~provisional~~/complete specification relating to the invention is filed with this application.

~~€ The invention as disclosed in the specification uses the biological material from India and the necessary permission from the competent authority shall be submitted by me/us before the grant of patent to me/us.~~

€ There is no lawful ground of objection(s) to the grant of the Patent to me/us.

- € ~~I am~~/we are the true & first inventor(s).
- ~~€ I am/we are the assignee or legal representative of true & first inventor(s).~~
- ~~€ The application or each of the applications, particulars of which are given in Paragraph-8, was the first application in convention country/countries in respect of my/our invention(s).~~
- ~~€ I/We claim the priority from the above mentioned application(s) filed in convention country/countries and state that no application for protection in respect of the invention had been made in a convention country before that date by me/us or by any person from which I/We derive the title.~~
- ~~€ My/our application in India is based on international application under Patent Cooperation Treaty (PCT) as mentioned in Paragraph-9.~~
- ~~€ The application is divided out of my /our application particulars of which is given in Paragraph-10 and pray that this application may be treated as deemed to have been filed on DD/MM/YYYY under section 16 of the Act.~~
- € ~~The said invention is an improvement in or modification of the invention particulars of which are given in Paragraph-11.~~

**13. FOLLOWING ARE THE ATTACHMENTS WITH THE APPLICATION**

(a) Form 2

| Item | Details | Fee | Remarks |
|---|---|---|---|
| Complete/ ~~Provisional~~ specification) # | No. of pages: 16 | | |
| No. of Claim(s) | No. of claims: 07<br>No. of pages: 02 | | |
| Abstract | No. of pages: 01 | | |
| No. of Drawing(s) | No. of drawings: 02<br>No. of pages: 01 | | |

# In case of a complete specification, if the applicant desires to adopt the drawings filed with his provisional specification as the drawings or part of the drawings for the complete specification under rule 13(4), the number of such pages filed with the provisional specification are
required to be mentioned here.

(b) Complete specification (in conformation with the international application)/as amended before the International Preliminary Examination Authority (IPEA), as applicable (2 copies).

(c) Sequence listing in electronic form

(d) Drawings (in conformation with the international application)/as amended before the International Preliminary Examination Authority (IPEA), as applicable (2 copies).

(e) Priority document(s) or a request to retrieve the priority document(s) from DAS (Digital Access Service) if the applicant had already requested the office of first filing to make the priority document(s) available to DAS.

(f) Translation of priority document/Specification/International Search Report/International Preliminary Report on Patentability.

(g) Statement and Undertaking on Form 3

(h) Declaration of Inventorship on Form 5

(i)Power of Authority

(j)**Total fee ₹……….in Cash/ Banker's Cheque /Bank Draft bearing No.......... Date on …………. Bank.**

I/We hereby declare that to the best of my/our knowledge, information and belief the fact and matters slated herein are correct and I/We request that a patent may be granted to me/us for the said invention.

**Dated this 6th day of September 2022**

**Signature:** D. Sengeni

Name: Dr. D. Sengeni et. al.

To,
The Controller of Patents
The Patent Office, at Chennai

Note: -

* Repeat boxes in case of more than one entry.

* To be signed by the applicant(s) or by authorized registered patent agent otherwise where mentioned.

* Tick ()/cross (x) whichever is applicable/not applicable in declaration in paragraph-12.

* Name of the inventor and applicant should be given in full, family name in the beginning.

* Strike out the portion which is/are not applicable.

* For fee: See First Schedule”;

**FORM 2**

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patent Rules, 2003

**COMPLETE SPECIFICATION**

(See section 10 and rule 13)

**TITLE OF THE INVENTION**

“A CERTIFICATE AUTHENTICATION SYSTEM WITH BLOCKCHAIN FOR IOT WITH 5G NETWORK”

We, applicant(s)

| NAME | NATIONALITY | ADDRESS |
|---|---|---|
| 1. Dr. D. Sengeni | INDIAN | Associate Professor,<br>Electronics and Communication Engineering,<br>CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 |
| 2. Dr. Siddhartha Choubey | INDIAN | Associate Professor,<br>Computer Science and Engineering,<br>Shri Shankaracharya Technical Campus, Bhilai, Durg, Chhattisgarh 490020 |
| 3. Dr. Sima Sahu | INDIAN | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College, Hyderabad,<br>Pin Code: 500100 |

|  |  |  |
|---|---|---|
| 4. Dr. Shaik Fairooz | INDIAN | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College, Hyderabad,<br>Pin Code: 500100 |
| 5. Dr. K.Jamal | INDIAN | Professor,<br>Department of ECE,<br>Gokaraju Rangaraju Institute of Engineering and Technology,<br>Hyderabad,<br>Pin Code: 500090 |
| 6. Dr. Joshuva Arockia Dhanraj | INDIAN | Assistant Professor (S.G.),<br>Department of Mechatronics Engineering,<br>Hindustan Institute of Technology and Science (HITS), #1, IT Expressway, Bay Range Campus, Padur, Tamil Nadu, 603103, India |
| 7. Dr. M. Ravichandran | INDIAN | Professor,<br>Department of Mechanical Engineering,<br>K. Ramakrishnan College of Engineering, Trichy-621112,<br>Tamil Nadu, India |

The following specification particularly describes the nature of the invention and the manner in which it is performed:

## FIELD OF THE INVENTION

[001] The present invention relates to internet of things and more particularly relates to a certificate authentication system with blockchain for IoT with 5G network.

## Background of the invention

[002] There are many services in a variety of industrial fields that can be provided in real time through the Internet, including financial services like a wire transfer or stock trading by accessing servers run by banks or securities firms, civil services like issuing copies of resident registration and other various certificates by accessing servers run by governmental bodies, and e-commerce services for purchasing goods by accessing servers for selling goods.

[003] Digital certificates are employed throughout the authentication processes that authenticate users' identities as consumers in order to use services in these diverse industrial fields.

[004] A digital certificate in this context is electronic data that a certification authority (CA) issues in order to verify a user's identity, prevent transaction denials or document forgery and falsification when using services in various industrial fields, and act as a type of digital transaction's certificate of seal impression. A digital certificate of this type typically includes information about the certificate's version, serial number, effective time, issuing organization, information about how to verify an e-signature of a user, the user's name, information about confirming their identity, etc.

[005] Additionally, the use of digital certificates is susceptible to password and certificate theft since the existing authentication mechanisms primarily involve

verifying the existence of digital certificates and the accuracy of passwords. As a result, the currently in use digital certificates suffer from issues including decreased security, expensive issuing, and usage restrictions. Therefore, a less expensive method that offers better security and usability and could displace the current digital certificates is needed.

[006] Therefore, there is a need to overcome the prior arts to provide a more enhanced solution. The present invention provides a novel approach to mitigate the conventional methods. However, the present invention relates to a certificate authentication system with blockchain for IoT with 5G network.

[007] The present invention's object is to provide an improved method and system to address the existing challenge. Alternatively, it is an object of the present invention to address the foregoing problems or at least to provide the public with a useful choice.

## Summary of the present invention

[008] A favored connectivity method for Internet of Things deployments is the 5G cellular network (IoT). One such topic is the creation of effective security frameworks for IoT device authentication. The security credentials of the devices in the home network are now maintained centrally by the authentication protocol used in 5G cellular networks. As a result, the home network must always be communicated with whenever a device needs to be authorized.

[009] However, frequent connection with the home network may cause an increase in communication latency in the IoT situation where there is widespread device deployment.

[010] The currently proposed authentication method uses blockchain technology to store security credentials for IoT devices in a decentralized manner. Through both an informal and a rigorous security examination utilizing the Scyther tool, the system is determined to be safe and secure. When implemented in the Ethereum test network, the smart contracts utilized in the scheme are also determined to be effective. The technique is shown to have achieved lower communication latency compared to the existing protocols through experimental performance analysis.

[011] Nearly all of the gadgets in use are becoming smarter and contributing to the Internet of Things (IoT) network as a result of the rapid improvements in technology. Before permitting a new IoT device to connect to the network and begin communicating, it is crucial to confirm the device's legitimacy. Access control is therefore a crucial security technique that only permits the authenticated node to join the network.

[012] A technique for access control also promotes secrecy by creating a session key for secure communication over open, widely accessible channels. In order to improve security, access control systems have recently adopted blockchain technology. IoT is the basis of, and a thorough explanation of IoT, its architecture, and applications is given there. Additionally, a variety of security problems are presented, as well as potential IoT security assaults and their defenses. more emphasis should be placed on the development of blockchain technology in IoT.

[013] Additionally, the current invention offers a thorough explanation of access control techniques. For easier understanding, the protocols are divided into three

categories: access control mechanisms using certificates, those without certificates, and blockchain technology. While describing access control systems, be sure to detail on each use case, such as smart homes, smart grids, smart healthcare, and smart agriculture. The explanation offers a broader perspective on IoT applications in addition to outlining how the access mechanism is implemented. The effectiveness of each protocol is then demonstrated by a thorough comparison of their expenses for computation and communication. We conclude by talking about ongoing research projects and difficulties in a blockchain-envisioned IoT network.

[014] Although the Internet of Things (IoT) is commonplace in both urban and rural settings, it is also infamous for having lax security. Authentication is even more crucial for IoT applications since it serves as the first line of security against various threats. In addition, there has been an increase in the necessity for cross-domain authentication due to the rising demand for cross-domain collaboration.

[015] Recent years have seen intensive study and development of certificate-based authentication techniques. However, many of these methods lack the computing, storage, and communication efficiency that the Internet of Things so desperately needs. The current state of the art calls for the creation of a trust-building lightweight authentication system based on consortium blockchains.

[016] Additionally, the number of tokens is adjusted to control the trust lifecycle. The thorough research and evaluation show that the suggested scheme is more cost-effective than competing methods in terms of storage, communication, and authentication costs while also being resistant to a number of typical assaults.

[017] Another goal of the invention is to offer an alternative to the current digital certificate that is less expensive, has greater security, and is easier to use. Another goal of the invention is to create a system for issuing authentication information, also known as an authentication information issuing system, by recording a transaction on a blockchain that includes a user's public key and (ii) a hash value of the user's identification information or its processed value.

[018] Another goal of the invention is to create a system for issuing authentication information that can direct the creation of a public key and a private key while preventing communication with a network.

## Detailed Description of the Present Invention

[019] Description of the Invention for a thorough understanding of the present invention, reference is made to the following detailed description in connection with the invention. Although the present invention is described with reference to exemplary embodiments, the present invention is not intended to be limited to the specific forms set forth herein. It is understood that various omissions and substitutions of equivalents are contemplated as circumstances may suggest or render expedient, but these are intended to cover the application or implementation without departing from the spirit or scope of the present invention.

[020] Further, it will nevertheless be understood that no limitation in the scope of the invention is thereby intended, such alterations and further modifications in the figures and such further applications of the principles of the invention as illustrated therein being contemplated as would normally occur to one skilled in the art to which the invention relates.

[021] Also, it is to be understood that the phraseology and terminology used herein are for the purpose of description and should not be regarded as limiting. Further, reference herein to “one embodiment” or “an embodiment” means that a particular feature, characteristic, or function described in connection with the embodiment is included in at least one embodiment of the invention.

[022] Furthermore, the appearances of such phrases at various places herein are not necessarily all referring to the same embodiment. The terms “a” and “an” herein do not denote a limitation of quantity, but rather denote the presence of at least one of the referenced items.

[023] In order to be illustrated more clearly in the utility model embodiment or technical scheme of the prior art, to the of required use in embodiment or description of the Prior Art be briefly described below, apparently, accompanying description in the following describes is only embodiment more of the present utility model, for those of ordinary skill in the art, do not paying under the prerequisite of creative work, can also obtain according to this accompanying description. Those of ordinary skill in the art are not making every other accompanying object obtaining under creative work prerequisite, all belong to the scope of the utility model protection.

[024] The present invention relates to internet of things and more particularly relates to a certificate authentication system with blockchain for IoT with 5G network.

[025] A favored connectivity method for Internet of Things deployments is the 5G cellular network (IoT). One such topic is the creation of effective security frameworks for IoT device authentication. The security credentials of the devices in the home network are now maintained centrally by the authentication

protocol used in 5G cellular networks. As a result, the home network must always be communicated with whenever a device needs to be authorized.

[026] However, frequent connection with the home network may cause an increase in communication latency in the IoT situation where there is widespread device deployment.

[027] The currently proposed authentication method uses blockchain technology to store security credentials for IoT devices in a decentralized manner. Through both an informal and a rigorous security examination utilizing the Scyther tool, the system is determined to be safe and secure. When implemented in the Ethereum test network, the smart contracts utilized in the scheme are also determined to be effective. The technique is shown to have achieved lower communication latency compared to the existing protocols through experimental performance analysis.

[028] Nearly all of the gadgets in use are becoming smarter and contributing to the Internet of Things (IoT) network as a result of the rapid improvements in technology. Before permitting a new IoT device to connect to the network and begin communicating, it is crucial to confirm the device's legitimacy. Access control is therefore a crucial security technique that only permits the authenticated node to join the network.

[029] A technique for access control also promotes secrecy by creating a session key for secure communication over open, widely accessible channels. In order to improve security, access control systems have recently adopted blockchain

technology. IoT is the basis of, and a thorough explanation of IoT, its architecture, and applications is given there. Additionally, a variety of security problems are presented, as well as potential IoT security assaults and their defenses. more emphasis should be placed on the development of blockchain technology in IoT.

[030] Additionally, the current invention offers a thorough explanation of access control techniques. For easier understanding, the protocols are divided into three categories: access control mechanisms using certificates, those without certificates, and blockchain technology. While describing access control systems, be sure to detail on each use case, such as smart homes, smart grids, smart healthcare, and smart agriculture. The explanation offers a broader perspective on IoT applications in addition to outlining how the access mechanism is implemented. The effectiveness of each protocol is then demonstrated by a thorough comparison of their expenses for computation and communication. We conclude by talking about ongoing research projects and difficulties in a blockchain-envisioned IoT network.

[031] Although the Internet of Things (IoT) is commonplace in both urban and rural settings, it is also infamous for having lax security. Authentication is even more crucial for IoT applications since it serves as the first line of security against various threats. In addition, there has been an increase in the necessity for cross-domain authentication due to the rising demand for cross-domain collaboration.

[032] Recent years have seen intensive study and development of certificate-based authentication techniques. However, many of these methods lack the computing, storage, and communication efficiency that the Internet of Things so desperately needs. The current state of the art calls for the creation of a trust-building lightweight authentication system based on consortium blockchains.

[033] Additionally, the amount of tokens is adjusted to control the trust lifecycle. The thorough research and evaluation show that the suggested scheme is more cost-effective than competing methods in terms of storage, communication, and authentication costs while also being resistant to a number of typical assaults.

[034] Another goal of the invention is to offer an alternative to the current digital certificate that is less expensive, has greater security, and is easier to use. Another goal of the invention is to create a system for issuing authentication information, also known as an authentication information issuing system, by recording a transaction on a blockchain that includes a user's public key and (ii) a hash value of the user's identification information or its processed value. Another goal of the invention is to create a system for issuing authentication information that can direct the creation of a public key and a private key while preventing communication with a network.

[035] This disclosure has been presented for purposes of illustration and description but is not intended to be exhaustive or limiting. Many modifications and variations will be apparent to those of ordinary skill in the art. The example embodiments have been chosen and described in order to explain principles and practical application, and to enable others of ordinary skill in the art to understand the disclosure for various embodiments with various modifications as are suited to the particular use contemplated.

[036] Above description is only the general introduction of technical solution of the embodiment of the present invention, in order to better understand the embodiment of the present invention Technological means and can be implemented in accordance with the contents of the specification, and in order to allow above and other mesh of the embodiment of the present invention, feature and advantage can be more clearly

understood, the special specific embodiment for lifting the embodiment of the present invention below.

[037] The foregoing is only preferred embodiment of the present invention, not in order to limit the present invention, all any modifications of doing within the spirit and principles in the present invention, be equal to and replace and improvement etc., within all should being included in protection scope of the present invention.

[038] What has been described above includes examples of the subject invention. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of describing the subject invention, but one of ordinary skill in the art may recognize that many further combinations and permutations of the subject invention are possible. Accordingly, the subject invention is intended to embrace all such alterations, modifications, and variations that fall within the spirit and scope of the appended claims. Furthermore, to the extent that the term “includes” is used in either the detailed description or the claims, such term is intended to be inclusive in a manner similar to the term “comprising” as “comprising” is interpreted when employed as a transitional word in a claim.

[039] The foregoing descriptions of specific exemplary embodiments of the present invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the invention to the precise forms and sequence of steps disclosed, and obviously many modifications and variations are possible considering the above teachings.

[040] The exemplary embodiments were chosen and described in order to explain certain principles of the invention and their practical application, thereby enabling

others skilled in the art to make and utilize various exemplary embodiments of the present invention, as well as various alternatives and modifications thereof.

**We Claim:**

1. A certificate authentication system with blockchain for IoT with 5G network, comprising:

   an authentication method using blockchain technology to store security credentials for IoT devices in a decentralized manner, and through both an informal and a rigorous security examination utilizing the Scyther tool, the system is determined to be safe and secure.

2. The system as claimed in claim 1, wherein when implemented in the Ethereum test network, the smart contracts utilized in the scheme are also determined to be effective.

3. The system as claimed in claim 1, wherein the technique is shown to have achieved lower communication latency compared to the existing protocols through experimental performance analysis.

4. The system as claimed in claim 1, wherein a technique for access control also promotes secrecy by creating a session key for secure communication over open, widely accessible channels.

5. The system as claimed in claim 1, wherein in order to improve security, access control systems have recently adopted blockchain technology.

6. The system as claimed in claim 1, wherein the security credentials of the devices in the home network are now maintained centrally by the authentication protocol used in 5G cellular networks.

**7.** The system as claimed in claim 1, wherein as a result, the home network must always be communicated with whenever a device needs to be authorized.

**Dated this 6th day of September 2022**

Signature: D. Sengeni

**Applicant(s)**

Dr. D. Sengeni et. al.

.

# ABSTRACT

## A CERTIFICATE AUTHENTICATION SYSTEM WITH BLOCKCHAIN FOR IOT WITH 5G NETWORK

The present invention discloses a certificate authentication system with blockchain for IoT with 5G network. The system is comprised of, but not limited to, an authentication method using blockchain technology to store security credentials for IoT devices in a decentralized manner, and through both an informal and a rigorous security examination utilizing the Scyther tool, the system is determined to be safe and secure. When implemented in the Ethereum test network, the smart contracts utilized in the scheme are also determined to be effective. Further, the technique is shown to have achieved lower communication latency compared to the existing protocols through experimental performance analysis.

Accompanied Drawings [FIGS.1-2]

**Dated this 6th day of September 2022**

Signature: D. Sengeni

**Applicant(s)**

Dr. D. Sengeni et. al.

**Applicant(s) Name:** Dr. D. Sengeni et. al.

Total No. of sheet **1**
Sheet No.**1** of **1**

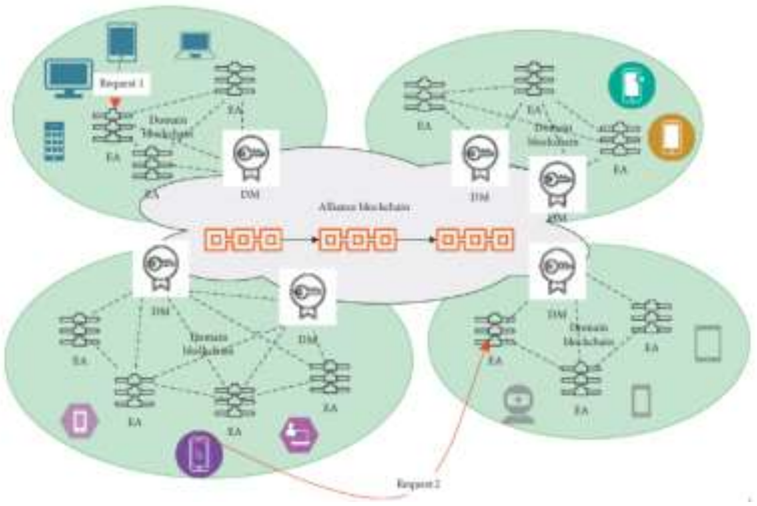

**Figure 1**

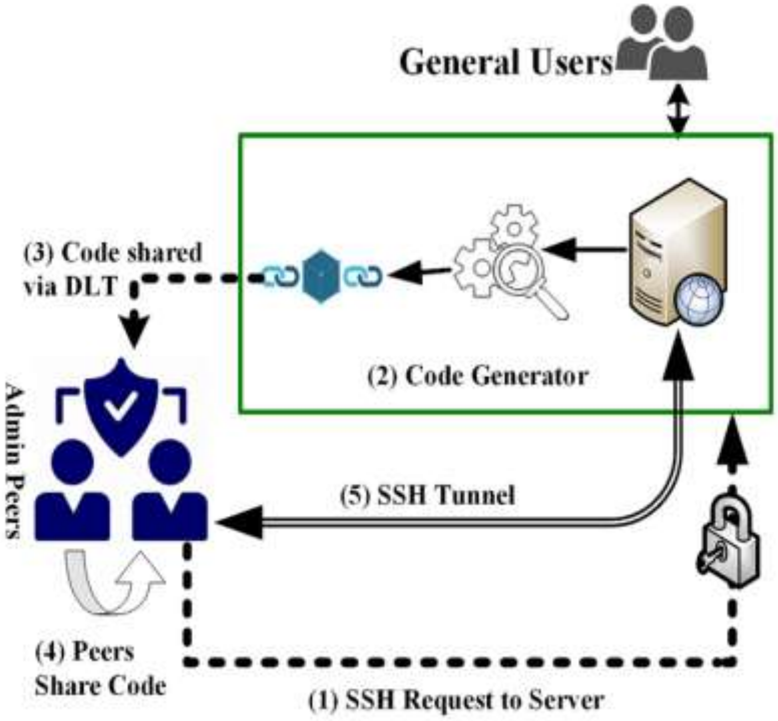

**Figure 2**

**Dated this 6th day of September 2022**

**Signature:** D. Sengeni

**Applicant(s) Name:** Dr. D. Sengeni et. al.

## FORM 3

THE PATENTS ACT,
1970 (39 of 1970)
and
THE PATENTS RULES, 2003

## STATEMENT AND UNDERTAKING UNDER SECTION 8

(See section 8; Rule 12)

| | |
|---|---|
| 1. Name of the applicant(s). | I/We Dr. D. Sengeni et. al., all are citizen of India, Address of one of the Applicant: Associate Professor, Electronics and Communication Engineering, CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003. |
| 2. Name, address and nationality of the joint applicant. | (i) that I/We have not made any application for the same/substantially the same invention outside India<br>Or<br>~~(ii) that I/We who have made this application No… dated alone/jointly with ………………………, made for the same/ substantially same invention, application(s) for patent in the other countries, the particulars of which are given below:~~ |

| Name of the Country | Date of Application | Application No. | Status of the Application | Date of Publication | Date of grant |
|---|---|---|---|---|---|
| - | - | - | - | - | - |

| | |
|---|---|
| 3. Name and address of the assignee | (iii) that the rights in the application(s) has/have been assigned to ……………… none ……………………<br>…………………………………………………………<br>………………………… that I/We undertake that upto the date of grant of the patent by the Controller, I/We would keep him informed in writing the details regarding corresponding applications for patents filed outside India within six months from the date of filing of such application.<br>**Dated this 6th day of September 2022** |

| | |
|---|---|
| 4. To be signed by the applicant or his authorized registered patent agent. | **Signature:**<br>D. Sengeni |
| 5. Name of the natural person who has signed. | Dr. D. Sengeni et. al.<br>**Name of the Applicant(s)** |
| | To<br>The Controller of Patents,<br>The Patent Office, at<br>Chennai |
| Note.- Strike out whichever is not applicable; | |

**FORM- 5**
THE PATENTS ACT, 1970
(39 of 1970)
&
The Patents Rules, 2003
DECLARATION AS TO INVENTORSHIP
[See Section 10(6) and Rule 13(6)]

1. NAME OF THE APPLICANT(S)

I/We Dr. D. Sengeni et. al., all are citizen of India, Address of one of the Applicant: Associate Professor, Electronics and Communication Engineering, CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003.

hereby declare that the true and first inventor(s) of the invention disclosed in the complete specification filed in pursuance of ~~my~~ / our application numbered ___________ dated 06/09/2022 ~~is/~~are

2. INVENTOR(S)

| (a) NAME | (b) NATIONALITY | (c) ADDRESS |
|---|---|---|
| 1. Dr. D. Sengeni | INDIAN | Associate Professor,<br>Electronics and Communication Engineering,<br>CK College of Engineering and Technology, Jayaram Nagar, Chellangkuppam, Cuddalore - 607003 |
| 2. Dr. Siddhartha Choubey | INDIAN | Associate Professor,<br>Computer Science and Engineering,<br>Shri Shankaracharya Technical Campus, Bhilai, Durg, Chhattisgarh 490020 |
| 3. Dr. Sima Sahu | INDIAN | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College, Hyderabad,<br>Pin Code: 500100 |
| 4. Dr. Shaik Fairooz | INDIAN | Associate Professor,<br>Department of ECE,<br>Malla Reddy Engineering College, Hyderabad,<br>Pin Code: 500100 |
| 5. Dr. K.Jamal | INDIAN | Professor,<br>Department of ECE,<br>Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad,<br>Pin Code: 500090 |

| | | |
|---|---|---|
| 6. Dr. Joshuva Arockia Dhanraj | INDIAN | Assistant Professor (S.G.),<br>Department of Mechatronics Engineering,<br>Hindustan Institute of Technology and Science (HITS), #1, IT Expressway, Bay Range Campus, Padur, Tamil Nadu, 603103, India |
| 7. Dr. M. Ravichandran | INDIAN | Professor,<br>Department of Mechanical Engineering,<br>K. Ramakrishnan College of Engineering, Trichy-621112, Tamil Nadu, India |

~~3. DECLARATION TO BE GIVEN WHEN THE APPLICATION IN INDIA IS FILED BY THE APPLICANT(S) IN THE CONVENTION COUNTRY: -~~

N.A.

~~We the applicant(s) in the convention country hereby declare that our right to apply for a patent in India is by way of assignment from the true and first inventor(s).~~

Dated this 6th day of September 2022

Dr. D. Sengeni et. al.
**Applicant(s)**

To,
The Controller of Patents
The Patent Office, Chennai

# FORM 9

THE PATENT ACT, 1970
(39 of 1970)
&
THE PATENTS RULES, 2003

## REQUEST FOR PUBLICATION

[See section 11A (2) rule 24A]

I/We **Dr. D. Sengeni,Dr. Siddhartha Choubey,Dr. Sima Sahu,Dr. Shaik Fairooz,Dr. K.Jamal,Dr. Joshuva Arockia Dhanraj,Dr. M. Ravichandran** hereby request for early publication of my/our [Patent Application No.] TEMP/E-1/58448/2022-CHE

Dated **06/09/2022 00:00:00** under section 11A(2) of the Act.

Dated this(Final Payment Date):------------
Signature
Name of the signatory

To,
The Controller of Patents,
The Patent Office,
At Chennai

This form is electronically generated.