Name : رحمة محمد محمد محمود

ID : 309

G:3

Sec:14

✓Internet of things system 5 webpage

1- Home

```
  <div id="home">
        <p>
            The main concept of a network of smart devices was discussed as e
arly as 1982, with a modified Coca-Cola
            vending machine at Carnegie Mellon University becoming the first
ARPANET-connected appliance,
            able to report its inventory and whether newly loaded drinks were
 cold or not.
            Mark Weiser's 1991 paper on ubiquitous computing, "The Computer o
f the 21st Century", as well as academic
            venues such as UbiComp and PerCom produced the contemporary visio
n of the IOT.
            The concept of the "Internet of Things" and the term itself, firs
t appeared in a speech by Peter T. Lewis,
            to the Congressional Black Caucus Foundation 15th Annual Legislat
ive Weekend in Washington, D.C, published
            in September 1985.
        </p>
    </div>
```

2- Organizational

```
 <div id="Organizational">
```

```
        <p>
            The Internet of Medical Things (IoMT) is an application of the Io
T for medical and health related purposes,
            data collection and analysis for research, and monitoring.[38][39
][40][41][42] The IoMT has been referenced
            as "Smart Healthcare",[43] as the technology for creating a digit
ized healthcare system, connecting
            available medical resources and healthcare services.
            IoT devices can be used to enable remote health monitoring and em
ergency notification systems. These health
            monitoring devices can range from blood pressure and heart rate m
onitors to advanced devices capable of
            monitoring specialized implants, such as pacemakers, Fitbit elect
ronic wristbands, or advanced hearing aids.
            Some hospitals have begun implementing "smart beds" that can dete
ct when they are occupied and when a
            patient is attempting to get up. It can also adjust itself to ens
ure appropriate pressure and support is
            applied to the patient without the manual interaction of nurses.[
            IoT devices "can save the United States more than $300 billion in
 annual healthcare expenditures by
            increasing revenue and decreasing cost."[47] Moreover, the use of
 mobile devices to support medical
            follow-up led to the creation of 'm-
health', used analyzed health statistics.
        </p>
        <!-- img  -->
        <img src="https://encrypted-
tbn0.gstatic.com/images?q=tbn:ANd9GcRfthmmYnPURGXuAfXgTPr0uG8q0hAn5Wg5Bg&usqp
=CAU">
    </div>
```

3- Classification

```
<div id="classification">
        <table>
            <caption>classification internet of things</caption>
            <tr>
                <th> iot Health care </th>
            </tr>
            <tr>
                <th>Architecture</th>
```

```
                <td>hierarchial and whole model reflection of the sytem throu
gh softwore organiztion</td>

            </tr>
            <tr>
                <th scope="row"> topology </th>
                <td>application sceniors ,uses phases , phiscal configration
</td>
            </tr>
            <tr>
                <th> platform</th>
                <td>framework , library and environment</td>
            </tr>
        </table>
    </div>
```

4- Security

```
 <div id="Security">
        <p>
            Security is the biggest concern in adopting Internet of things te
chnology,[196] with concerns that rapid
            development is happening without appropriate consideration of the
 profound security challenges involved[197]
            and the regulatory changes that might be necessary.[198][199]

            Most of the technical security concerns are similar to those of c
onventional servers, workstations and
            smartphones.[200] These concerns include using weak authenticatio
n, forgetting to change default
            credentials, unencrypted messages sent between devices, SQL injec
tions, Man-in-the-middle attacks, and poor
            handling of security updates.[201][202] However, many IoT devices
 have severe operational limitations on the
            computational power available to them. These constraints often ma
ke them unable to directly use basic
            security measures such as implementing firewalls or using strong
cryptosystems to encrypt their
            communications with other devices[203] - and the low price and co
nsumer focus of many devices makes a robust
            security patching system uncommon.[204]
```

```
            Internet of Things devices also have access to new areas of data,
 and can often control physical
            devices,[205] so that even by 2014 it was possible to say that ma
ny Internet-connected appliances could
            already "spy on people in their own homes" including televisions,
 kitchen appliances,[206] cameras, and
            thermostats.[207] Computer-
controlled devices in automobiles such as brakes, engine, locks, hood and tru
nk
            releases, horn, heat, and dashboard have been shown to be vulnera
ble to attackers who have access to the
            on-
board network. In some cases, vehicle computer systems are Internet-
connected, allowing them to be
            exploited remotely.[208] By 2008 security researchers had shown t
he ability to remotely control pacemakers
            without authority. Later hackers demonstrated remote control of i
nsulin pumps[209] and implantable
            cardioverter defibrillators.
        </p>
    </div>
```

- 4 web pages

```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>internet of things</title>
</head>

<body>
    <p>internet of things</p>
    <!-- list of anchor -->
    <ul>
        <li>home</li>
        <li>Organizational</li>
        <li>classification</li>
        <li>Infrastructure</li>
        <li>Security</li>
    </ul>
```

```
    <div id="home">
        <p>
            The main concept of a network of smart devices was discussed as early
 as 1982, with a modified Coca-Cola
            vending machine at Carnegie Mellon University becoming the first ARPA
NET-connected appliance,
            able to report its inventory and whether newly loaded drinks were col
d or not.
            Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of th
e 21st Century", as well as academic
            venues such as UbiComp and PerCom produced the contemporary vision of
 the IOT.
            The concept of the "Internet of Things" and the term itself, first ap
peared in a speech by Peter T. Lewis,
            to the Congressional Black Caucus Foundation 15th Annual Legislative
Weekend in Washington, D.C, published
            in September 1985.
        </p>
    </div>
    <div id="Organizational">

        <p>
            The Internet of Medical Things (IoMT) is an application of the IoT fo
r medical and health related purposes,
            data collection and analysis for research, and monitoring.[38][39][40
][41][42] The IoMT has been referenced
            as "Smart Healthcare",[43] as the technology for creating a digitized
 healthcare system, connecting
            available medical resources and healthcare services.
            IoT devices can be used to enable remote health monitoring and emerge
ncy notification systems. These health
            monitoring devices can range from blood pressure and heart rate monit
ors to advanced devices capable of
            monitoring specialized implants, such as pacemakers, Fitbit electroni
c wristbands, or advanced hearing aids.
            Some hospitals have begun implementing "smart beds" that can detect w
hen they are occupied and when a
            patient is attempting to get up. It can also adjust itself to ensure
appropriate pressure and support is
            applied to the patient without the manual interaction of nurses.[
            IoT devices "can save the United States more than $300 billion in ann
ual healthcare expenditures by
            increasing revenue and decreasing cost."[47] Moreover, the use of mob
ile devices to support medical
```

```
            follow-up led to the creation of 'm-
health', used analyzed health statistics.
        </p>
        <!-- img  -->
        <img src="https://encrypted-
tbn0.gstatic.com/images?q=tbn:ANd9GcRfthmmYnPURGXuAfXgTPr0uG8q0hAn5Wg5Bg&usqp=CAU
">
    </div>
    <!-- table -->
    <div id="classification">
        <table>
            <caption>classification internet of things</caption>
            <tr>
                <th> iot Health care </th>
            </tr>
            <tr>
                <th>Architecture</th>
                <td>hierarchial and whole model reflection of the sytem through s
oftwore organiztion</td>

            </tr>
            <tr>
                <th scope="row"> topology </th>
                <td>application sceniors ,uses phases , phiscal configration </td
>
            </tr>
            <tr>
                <th> platform</th>
                <td>framework , library and environment</td>
            </tr>
        </table>
    </div>
    <div id="Infrastructure">
        <p>
            Monitoring and controlling operations of sustainable urban and rural
infrastructures like bridges, railway
            tracks and on- and offshore wind-
farms is a key application of the IoT.[64] The IoT infrastructure can be
            used for monitoring any events or changes in structural conditions th
at can compromise safety and increase
            risk. The IoT can benefit the construction industry by cost-
saving, time reduction, better quality workday,
            paperless workflow and increase in productivity. It can help in takin
g faster decisions and save money with
```

```
            Real-
Time Data Analytics. It can also be used for scheduling repair and maintenance ac
tivities in an
            efficient manner, by coordinating tasks between different service pro
viders and users of these
            facilities.[46] IoT devices can also be used to control critical infr
astructure like bridges to provide
            access to ships. Usage of IoT devices for monitoring and operating in
frastructure is likely to improve
            incident management and emergency response coordination, and quality
of service, up-times and reduce costs
            of operation in all infrastructure related areas.[71] Even areas such
 as waste management can benefit[72]
            from automation and optimization that could be brought in by the IoT.

        </p>
    </div>
    <div id="Security">
        <p>
            Security is the biggest concern in adopting Internet of things techno
logy,[196] with concerns that rapid
            development is happening without appropriate consideration of the pro
found security challenges involved[197]
            and the regulatory changes that might be necessary.[198][199]

            Most of the technical security concerns are similar to those of conve
ntional servers, workstations and
            smartphones.[200] These concerns include using weak authentication, f
orgetting to change default
            credentials, unencrypted messages sent between devices, SQL injection
s, Man-in-the-middle attacks, and poor
            handling of security updates.[201][202] However, many IoT devices hav
e severe operational limitations on the
            computational power available to them. These constraints often make t
hem unable to directly use basic
            security measures such as implementing firewalls or using strong cryp
tosystems to encrypt their
            communications with other devices[203] - and the low price and consum
er focus of many devices makes a robust
            security patching system uncommon.[204]

            Internet of Things devices also have access to new areas of data, and
 can often control physical
            devices,[205] so that even by 2014 it was possible to say that many I
nternet-connected appliances could
```

```
            already "spy on people in their own homes" including televisions, kit
chen appliances,[206] cameras, and
            thermostats.[207] Computer-
controlled devices in automobiles such as brakes, engine, locks, hood and trunk
            releases, horn, heat, and dashboard have been shown to be vulnerable
to attackers who have access to the
            on-
board network. In some cases, vehicle computer systems are Internet-
connected, allowing them to be
            exploited remotely.[208] By 2008 security researchers had shown the a
bility to remotely control pacemakers
            without authority. Later hackers demonstrated remote control of insul
in pumps[209] and implantable
            cardioverter defibrillators.
        </p>
    </div>
</body>

</html>
```