**Various risks imposed on smart cities cause of Internet of Things (IoT)**

* **Ethical risks**
  + This risk is any uncalled negative outcome of any unethical action taken.
* **Privacy risks**
  + This risk occurs when the control over the system containing all the confidential information is lost for a temporary or permanent period.
* **Security risks**
  + When there are minute gaps in between the security program and in the system, this leads to exploitation of the vulnerabilities and an open gateway for the cyber-attacks.
* **Technical risks**
  + Because of the poor design structure and its implementation, it leads to failure of hardware and software.

**Various threats imposed on smart cities cause of Internet of Things (IoT)**

* **Physical threats:**
  + It includes wrongfully penetrating inside the Electronic Control Unit (ECU) in order to gain access of the central locking systems.
  + Malicious attacks to leak the private information and to introduce data glitches to gain unauthorised control of the system.
* **Interception threats:**
  + Includes the replay attacks that can be occurred internally between the transition of data between the networks over the Electronic Control Unit (ECU).
* **Man-in-the-middle**
  + An attack/attacker breaches in-between the link of transmission/communication between two systems and disrupts the flow of the network.
* **Device hijacking**
  + The attacker gains the control of the system/device without the consent of the user.
  + These attacks are hard to detect as the attacker doesn’t alter the basic functionality of the device or the system.
  + In smart cities, the attacker could hijack and gain control of the smart meters to launch the ransomware attacks on the Energy Management Systems (EMS).
* **Data and identity theft:**
  + The data that is being generated by the unprotected smart city infrastructure such as parking garages, EV charging stations and surveillance feeds provide huge number of data for the attacker to attack the personal information that can lead to deployment of fraudulent transactions.
* **Distributed denial of service (DDoS)**
  + This attack floods the communication by sending several requests that results in breakdown of the system.
* **Permanent Denial of Service (PDoS):**
  + Also known as phlashing.
  + It is an attack that damages the device permanently and requires reinstallation or replacement of hardware.
* **Malicious code threat:**
  + With the increase in the usage of the windows, linux and android, malicious code can be penetrated through them in order to gain control and compromise all the connected devices such as smart vehicle network.
* **Various security threats towards IoT sensors are**
* **Confidentiality and integrity compromise:**
  + It is to be ensured that only authorized parties are permitted to have access to sensor data collect and the stored sensor data.
  + The integrity if the data is being compromised if the unauthorized parties try to gain its access.
* **Eavesdropping:**
  + If the communication link between the sensor and the centralized server is not secure it leads to loss of integrity of the data.
  + As the data is being transmitted onto the centralized server, communications can be intercepted by the attacker.
* **Data loss**
  + Due to insufficient data management of the sensors it could impact the operations of the smart city.
* **Availability compromise:**
  + In certain events of the sensor failure, a protocol should be laid to avoid negative impact of the operations of the smart city.
* **Remote exploitation**
  + The sensors that are connected to the smart city are being communicated towards the centralized server.
  + The insecure channels could be used by the attacker to perform remote exploitation.
* **The threats imposed on smart cities which are transmitted and stored in the cloud are as follows.**
* **Data leakage**
  + When the infrastructure or the resources are being moved to the cloud, the data is been handled by the third-party cloud provider.
  + As the data is handled by the third-party, it can be accessed by the third-party personnel.
* **Insecure API’s**
  + Most of the software and the applications are connected to the cloud infrastructure with the help of API’s to interact with the cloud services.
  + Hence the API’s must support secure communication with authentication, access control, encryption and activity login.
* **Malware injection**
  + The cloud provider host web application through the middleware platforms.
  + By failing to secure the web application and the server would lead the attacker to penetrate malware inside it.
* **Data locations and regulation boundaries**
  + It is difficult to manage the security of the data location.

**Countermeasures**

1. **Firmware integrity and secure boot**
   1. The secure boot utilizes cryptographic code signing techniques which ensures that the device only executes the code which is been generated by the device OEM.
   2. It helps prevents the attackers from replacing the firmware with malicious codes.
   3. It is also important that the IoT device communicate with the authorized services only to prevent replacing the firmware.
2. **Mutual authentication**
   1. When a smart city device is connected to the network it should be authenticated prior to transmitting or receiving data.
   2. This will make sure that the data is from a legitimate device and not a fraud one.
3. **Security monitoring and analysis**
   1. Security monitoring captures all the data including the end devices and connectivity traffic.
   2. The data is then analysed for any threats and security violations.
   3. Once it is detected a wide range of steps are taken to remove it from the system.
4. **Security life cycle management**
   1. This feature allows the service providers and the OEM’s to control the security aspects of the IoT device when an operation is running
   2. The rapid over the air (OTA) device key replacement during the cyber disaster recovery measures causes minimal service disruptions.
5. **Secure booting**
   1. By applying cryptographic hash algorithms, the authenticity of the program can be checked in order to resist any attack.
6. **Device authentication**
   1. Prior device authentication should be done when a device enters the network and begins transmitting or receiving the data.
7. **Hyper safe**
   1. This provides protection against all the memory pages and denies any alteration done within them.

References:

1. Ahmed, A.W., Ahmed, M.M., Khan, O.A. and Shah, M.A., 2017. A comprehensive analysis on the security threats and their countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, *8*(7), pp.489-501.
2. Radanliev, P., De Roure, D.C., Maple, C., Nurse, J.R., Nicolescu, R. and Ani, U., 2019. Cyber Risk in IoT Systems.
3. Rambus. 2020. *Smart Cities: Threats And Countermeasures - Rambus*. [online] Available at: <<https://www.rambus.com/iot/smart-cities/>> [Accessed 7 May 2020].