**Motivation:**

1. Emerging developments in the field of IOt.
2. To improve security, authentication and trust between many iot devices and any internet host.
3. Trustworthy communication between users, services, and internet providers.
4. Try to remove vulnerabilities especially on the malicious attacks of the devices
5. Framework that considers integrity, privacy and the authenticity in the IoT devices.
6. Analysing access control applicability in IoT systems.

**Introduction:**

The Internet of Things (IoT) is the network of physical objects embedded with electronics, software, sensors, and network connectivity which enables these objects to collect and exchange data. IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems and resulting in improved efficiency, accuracy and economic benefit.

Internet of things concept based on people connected to anything anywhere where it merges the physical world with the information. In IoT there has a variety of computing devices which differ in size, operating systems and its inference within the technologies. Devices have major limitations in capabilities and ranges starting with Radio frequency identifications (RFID) tags to embedded devices, PDAs and sensor nodes. Providing a secure communication between objects is one of the important factors for a successful operation in IoT. Authentication and Access control are important and critical functionality in context of IoT. To achieve security and privacy, we should implement access control methods which cover both authentication and authorization.

In the IoT, Access control lets only authorized users to access a resource such as a file, IoT device, sensor or URL. All modern operating systems limit access to the file system based on the user. For instance, the super user has wider access to files and system resources than regular users. Access control is needed to make sure that only trusted parties can update device software, access sensor data or command the actuators to perform an operation. Access control enables companies to share IoT device data selectively with technology vendors to allow both predictive maintenance and protection of the sensitive data.

**Definition:**

IoT eases the connection of many devices and entities with each other and shares information, services, and many other things that can be sensitive and private. That’s why a sufficient model and framework of access models were demanded. An intensive research about access control approaches in the IoT field has been done. Some of the main approaches used in the field to secure devices, users, communication and data transmitted were found. The following are some of those approaches:

**Role-based Access Control (RBAC):**

RBAC depends on the concept of Role in which an administrator is the only one who is granted to assign the permissions to the Roles. Assign the Roles to certain users. No user can delegate some of the access granted to another user. The user can delegate all or none of the Role to another user, even the admin can’t change any permission given to a user. The association between the user and the role should be removed and another one built with another role holding the new permissions. This seems to be not applicable on the case when user needs to delegate some of his permissions or roles to another trusted user for a limited period of time. On the other hand, the administration is centralized so that you should have access to credentials and profiles on every device you own. It seems incredible when talking about a whole home and many appliances connected. The RBAC has another disadvantage on the IoT word. It can’t handle millions or even billions of devices and each one has a role to access, and many users to administrate. All the above gives an indicator that there is a demand to have an access control method applicable on the IoT.

**Problem Statements:**

1. Huge number of devices available.( The Internet of Things (IoT) is creating a revolution in the number of connected devices. Cisco reported that there were 25 billion IoT devices in 2015 and modest estimation that this number will almost double by 2020.)
2. The emergent IoT devices as a technology are creating a huge security rift between users and usability, sacrificing usability for security created a number of major issues.
3. The size of the data generated from IoT makes big data problems pale in comparison not to mention IoT devices need a real-time response.
4. IoT devices are classified under Bring Your Own Device (BYOD) that blows any organization security boundary and make them a target for espionage or tracking.
5. Incorporating secure access and control for IoT devices ranging from edge nodes devices to application level (business intelligence reporting tools) is a challenge because it has to account for several hardware and application levels.
6. Role-based Access Control (RBAC) RBAC depends on the concept of Role, in which an administrator is the only one who is granted to assign the permissions to the Roles. Additionally, assign the Roles to certain users. No user can delegate some of the access granted to another user. The user can delegate all or none of the Role to another user, even the admin can’t change any permission given to a user. The association between the user and the role should be removed and another one built with another role holding the new permissions [15]. This seems to be not applicable on the case when user needs to delegate some of his permissions or roles to another trusted user for a limited period of time. On the other hand, the administration is centralized so that you should have access to credentials and profiles on every device you own. It seems incredible when talking about a whole home and many appliances connected. The RBAC has another disadvantage on the IoT word. It can’t handle millions or even billions of devices and each one has a role to access, and many users to administrate. All the above gives an indicator that there is a demand to have an access control method applicable on the IoT [16].
7. With the IoT constraints and low-security mechanisms applied, the malicious attacks could exploit the sensor vulnerability to provide wrong data where it can lead to wrong interpretation and actuation to the users