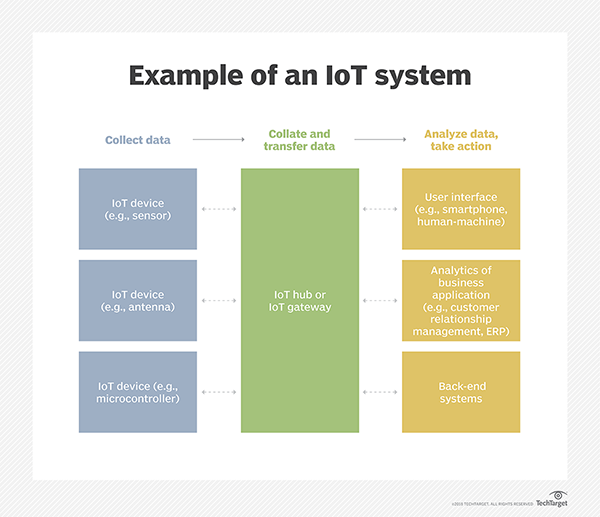
**Distributed Attack Based Detection Framework for IOT**

**Introduction to IOT-** The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers ([UIDs](https://internetofthingsagenda.techtarget.com/definition/unique-identifier-UID)) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

**How IOT Works-** An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT can also make use of artificial intelligence (AI) and machine learning to aid in making data collecting processes easier and more dynamic.



**Why IOT is important-** The internet of things helps people live and work smarter, as well as gain complete control over their lives. In addition to offering smart devices to automate homes, IoT is essential to business. IoT provides businesses with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

IoT enables companies to automate processes and reduce labor costs. It also cuts down on waste and improves service delivery, making it less expensive to manufacture and deliver goods, as well as offering transparency into customer transactions.

As such, IoT is one of the most important technologies of everyday life, and it will continue to pick up steam as more businesses realize the potential of connected devices to keep them competitive.

**IOT benefits to the organisation-**

The internet of things offers several benefits to organizations. Some benefits are industry-specific, and some are applicable across multiple industries. Some of the common benefits of IoT enable businesses to:

* monitor their overall business processes;
* improve the customer experience (CX);
* save time and money;
* enhance employee productivity;
* integrate and adapt business models;
* make better business decisions; and
* generate more revenue.

IoT encourages companies to rethink the ways they approach their businesses and gives them the tools to improve their business strategies.

Generally, IoT is most abundant in manufacturing, transportation and utility organizations, making use of sensors and other IoT devices; however, it has also found use cases for organizations within the agriculture, infrastructure and home automation industries, leading some organizations toward [digital transformation](https://searchcio.techtarget.com/definition/digital-transformation).

The ability to monitor operations surrounding infrastructure is also a factor that IoT can help with. Sensors, for example, could be used to monitor events or changes within structural buildings, bridges and other infrastructure. This brings benefits with it, such as cost saving, saved time, quality-of-life workflow changes and paperless workflow.

A home automation business can utilize IoT to monitor and manipulate mechanical and electrical systems in a building. On a broader scale, [smart cities](https://internetofthingsagenda.techtarget.com/definition/smart-city) can help citizens reduce waste and energy consumption.

IoT touches every industry, including businesses within healthcare, finance, retail and manufacturing.

**Pros and Cons of IOT-**

Some of the advantages of IoT include the following:

* ability to access information from anywhere at any time on any device;
* improved communication between connected electronic devices;
* transferring data packets over a connected network saving time and money; and
* automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

Some disadvantages of IoT include the following:

* As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.
* Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices, and collecting and managing the data from all those devices will be challenging.
* If there's a bug in the system, it's likely that every connected device will become corrupted.
* Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

**Aim of this model/project**

Alongside the development of Internet of Things (IoT), security attacks are also increasing day by day. A number of centralized attack detection mechanisms have been proposed to detect attacks in IoT, wherein an attack detection system is deployed at the central point in the network that collects data from the network and classifies it as “attack” or “normal” using a supervised machine learning algorithm. Note, however, that these mechanisms have failed to achieve significant results due to the distinct requirements of IoT devices, such as scalability, distribution, resource limitations, and low latency. Moreover, the application of supervised machine learning for classification needs a significant amount of labelled data. In this paper, we introduce a fog-based attack detection framework that relies on the fog computing paradigm and a newly proposed ELM-based Semi-supervised Fuzzy C-Means (ESFCM) method. As an extension of cloud computing, fog computing enables attack detection at the network edge and supports distributed attack detection. The ESFCM method uses a semi-supervised fuzzy c-means algorithm to handle the labelled data issue and an Extreme Learning Machine (ELM) algorithm to provide good generalization performance at a faster detection rate. The evaluation was performed on the NSL-KDD dataset, demonstrating that the proposed framework achieved better performance than the centralized attack detection framework.

This model provides design and implementation of fog-based attack detection framework for IoT, which satisﬁes the distinct requirements of IoT such as distribution, resource limitations, and lower detection time. We propose an ELM-based Semi-Supervised Fuzzy C-Means(ESFCM) method that integrates a Semi-supervised Fuzzy C-Means with the Extreme Learning Machine (ELM) classiﬁer to support efﬁcient attack detection in IoT. We evaluate the performance of the proposed framework by comparing it with the centralized cloud-based framework. To demonstrate the effectiveness of the proposed ESFCM method for attack detection in IoT, this paper compares it with traditional machine learning methods in terms of standard measures.