**Unit-4**

**SECURE RESOURCE MANAGEMENT:**

**Introduction:**

The Internet of Things (IoT) is a set of connected smart device and sensors over the Internet. These devices are connected using the wired/wireless network technologies to communicate and transfer data from one node to another. The things in IoT infrastructure network are sensors, smart devices, sensor data, software agents and human beings. These networked independent devices make local network and connected to the global network to share information with others in real time to realize that the Things are connected into the real world and connect all devices. In cyber-physical ecosystem, each edge-node is supposed to an IoT device which can dynamically cooperate with other devices in the network to execute one or more user’s tasks allocated to the system network. Resources like processing power, storage, network bandwidth, RAM are usually limited in these IoT network, though these infrastructures and computing resources are provided by the Cloud service providers. IoT devices produce huge amount of real-time data from the sensors. Cloud storage is used for storing these real-time data on different local networked data centers, which upload these data to the global networked data centers to allow access for all globally situated smart devices. In this paper, the author studied various resource allocation techniques for Cloud-based IoT system. Classification of these techniques have been done based on parameters like QoS, context, cost, energy consumption and SLA. Furthermore, the author also discussed various parameters of resource allocation techniques of IoT system

**Basic Concepts of IoT, Cloud and Resource Management:**

Internet of things offers numerous advantages and services to the users. Therefore, to use them correctly, some elements are needed. The IoT elements will be discussed in this section

**Identifiers:**

Within the network, it offers an explicit identity for each object. In identification, two processes exist naming and addressing. The naming relates to the object’s title 3 whereas the addressing explains address of an object. These two processes are very different even though two or more objects could have the same name, but they are always different and unique. There are several approaches accessible which expedite the naming of objects in the network, such as ubiquitous codes (uCode) and electronic product codes (EPCs). Using IPv6, each object has a unique address. First, IPv4 was used to allocate the address, but due to a huge amount of IoT devices, it was unable to address the need. IPv6 is therefore used because it uses a 128-bit addressing system.

**Sensing Devices:**

This involves acquiring information from the environment and transferring it to a local, remote or Cloud-based database as an instance of the IoT sensor. We can identify intelligent devices, portable sensors or actuators. The collected information is transmitted to the storage medium. Numerous detection devices to collect data on objects such as RFID tags, actuators, portable sensors, smart sensors, etc.

**Communications Devices:**

To achieve smart services, IoT communication techniques communicate heterogeneous artifacts. One of the main goals of Internet of things is Communication in which various devices connect and communicate with each other. In the communication layer, devices can transfer and deliver messages, documents and other information. There are many methods which facilitate communication.

**Compute Devices:**

The computation of the data collected by the objects is achieved using sensors. It is used to develop processing in IoT applications. Raspberry Pi, Arduino, and Gadgeteer are utilized for hardware platforms, whereas the operating system plays a significant role in the processing of software platforms.

**Services IoT:**

Applications provide four types of service. The first service that is associated with an identity. It is used to acquire the identity of the objects which sent the request. The aggregate of information is another service aimed at collecting all the data about the objects. The aggregation service also performs the processing. The third service refers to co-operative service that makes decisions-based on the information gathered and transfer suitable rejoinders to the devices. The last service is the pervasive service, which is used to replace devices immediately without rigidity in terms of time and place.

**Semantics:**

They are the IoT’s concern to facilitate the consumers who perform their tasks. To fulfill its responsibilities, it is the most important component of IoT. It performs as the IoT’s brain. It accepts all the information and makes the appropriate decisions to send responses to the devices.

**SECURE IOT DATABASE**

* **Limit connectivity and access:** The fewer IoT devices that are connected to the Internet, the fewer endpoints you have on the surface of your network. You should also control which connected devices are able to download and share on the Internet so no device has more access points than it needs to perform its job.
* **Keep software and passwords updated:** Whenever there’s an opportunity to update the software on your IoT devices, install it right away. Unfortunately, most IoT manufacturers don’t release security updates, so it’s up to you to implement as much password security as you can. If possible, you should add multi factor authentication to your devices.
* **Implement firewalls:** Firewalls are one of the best ways to protect your network in case of an attempted IoT breach. Be sure to identify any weak points in your network and deploy firewalls to protect your devices.
* **Encrypt IoT data:** [SSL (Secure Sockets Layer) encryption](https://www.turn-keytechnologies.com/blog/article/iot-security-is-an-enterprise-problem-heres-how-ssl-encryption-can-help/) ensures that the data sent between two systems can’t be intercepted, read, or modified by any bad actors. By encrypting the transactions that occur across IoT networks, organizations can make it more difficult for cyber criminals to compromise their devices.

**Why is IoT security so important?**

From increasing the safety of roads, cars, and homes, to fundamentally improving the way we manufacture and consume products, [IoT solutions](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot) provide valuable data and insights that will enhance the way we work and live.

Success depends on ensuring the integrity and confidentiality of IoT solutions and data while mitigating cybersecurity risks. So, what should we know about IoT security?

**Build trust in IoT connected devices:**

* The benefits of IoT are undeniable, and yet, high-profile attacks, combined with uncertainty about security best practices and their associated costs, are keeping many businesses from adopting the technology.
* Besides, end-users are wary of the consequences of IoT security breaches.
* Recent research indicates that 90% of consumers lack confidence in IoT device security.

**Understanding IoT security risks:**

* Machines and objects in virtually any industry can be connected and configured to send data over cellular networks to cloud applications and backends.
* The digital security risk is present at every step along the IoT journey, and there is a bunch of hackers that would take advantage of a system's vulnerability.
* Unfortunately, diverse data types and computing power among IoT devices mean there's **no**'**one size fits all'** cybersecurity solution that can protect any IoT deployment.
* The first step for any IoT business is to undergo a thorough security risk assessment that examines vulnerabilities in devices and network systems and user and customer backend systems.
* Risk must be mitigated for the entire IoT lifecycle of the deployment, especially as it scales and expands geographically.



## More resources on securing the IoT:

* Explore our infographics on [The IoT circle of trust](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/documents/iot-lifecycle).
* Discover the three keys to a successful[IoT security strategy](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security/key-principles).
* [IoT security issues](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats) and challenges (2021)
* End-to-end [cybersecurity for critical IoT infrastructures](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/iot-security/trusted-key-manager)
* [Using connected cars to go greener](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/connected-cars/to-go-greener)
* Download our [IoT security whitepaper](https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/documents/iot-security)

## Security product

## IoT Security Products:

 The list of products below is based purely on reviews (sorted from most to least). There is no paid placement and analyst opinions do not influence their rankings. Here is our [Promise to Buyers](https://www.trustradius.com/static/promise-to-buyers) to ensure information on our site is reliable, useful, and worthy of your trust.

## What are IoT Security Solutions?

 IoT security solutions (or embedded security software) secure edge devices and machines (e.g. industrial control systems, ATM machines, retail devices, etc.) through a variety of techniques including encryption or cryptographic keys, securing APIs and USB connections, and by performing scans and analytics. Comprehensive IoT security should provide multiple aspects of IoT device protection. Complete solutions should give administrators visibility into IoT networks and devices. They should also be able to secure communications to and from IoT devices, often including data encryption. They should also be able to actively monitor devices to identify and respond to attacks. Network-wide solutions should also allow for device segmentation, to mitigate the impact of an attack should it occur.

One challenge of IoT security is the sheer range of devices and use cases within the IoT ecosystem. IoT devices can range from quality of life improvements, like smart coffee-makers, to mission-critical monitoring devices embedded in energy grids. Understanding the spectrum, and severity, of the IoT environments in question is crucial to identifying which solutions are best suited to securing it. Many vendors provide IoT-specific security solutions, which are designed to cover any of the more common IoT configurations. Other vendors, particularly those in endpoint or network security, have added IoT support to existing offerings.

In addition to point solutions, IoT security can be aggregated across several different types of security tech, including:

* Firewalls
* Network access controllers
* Agent-based or agentless endpoint protection
* Network monitoring
* IoT management systems

IoT security tools that are not part of a larger management or security suite should also be able to integrate with these systems. IoT devices are known to generate a massive amount of data. Other systems in the business should be set up to intake and process this data accordingly.

**IoT Security Risks:**

IoT devices are still a largely emerging and evolving market. As such, there are many possibilities for the technology. There are also far fewer regulations and security standards to help protect IoT devices. Left unchecked, this can pose serious risks to businesses.

There are myriad risks for B2B and B2C businesses alike. Businesses’ consumers’ data can be highly sensitive and vulnerable in IoT devices, such as home security cameras, home mapping data, or medical tracking data from wearable devices. Failure to secure these devices can irrevocably harm consumer trust and lead to legal repercussions.

B2B organizations also face risks from insecure IoT environments. IoT vulnerabilities can jeopardize, among others:

* Physical infrastructure monitoring systems
* Remote firmware updates, patching, and management
* Legal repercussions from insecure data management

In either case, IoT attacks can lead to data losses, malicious device takeovers, or devices can be used to enter other parts of the network.

### IoT Security Solutions Comparison:

 Consider these factors when comparing IoT security solutions:

* Solution Type: Do you need a specific point solution for specialized IoT environments? Or do you need to add IoT support to the business’s existing security stack, such as firewalls, endpoint security, etc. with support for IoT devices? Some more common IoT device configurations can be readily supported by broader security suites. For more edge-case situations, a point solution may be more effective.
* Use Case: What IoT devices and environments are currently in use? Are there mission-critical environments that need protection, or sensitive dataflows that should be encrypted? Or are the IoT devices mostly a risk factor for intrusion elsewhere on the network? Products will come with different feature strengths. Clarity on your own use case will help guide which solution is the best fit.

### Understand IoT interoperability and its three types:

 IoT interoperability is the capacity for multiple components within an IoT deployment to effectively communicate, share data and perform together to achieve a shared outcome. Organizations must be able to transmit and understand data throughout all the connections from devices to the cloud.

"Interoperability in an IoT context refers to the ability to transport meaningful, actionable information between systems. Information can refer to many things, so it's important to understand that IoT is a vast [system of systems](https://www.techtarget.com/searchapparchitecture/definition/system-of-systems-SoS), where connections and data exchange can occur between literally billions of devices and systems," said Shawn Chandler, CTO at GridCure and a senior member of the professional association IEEE.

**IoT deployments have three interoperability needs:**

* **Technical interoperability.** The deployment has the ability to use a physical communications infrastructure to transport bits of data.
* **Syntactic interoperability.** A shared syntax or common information model structures the data and establishes a protocol to share the information as specific typed data.
* [**Semantic**](https://www.techtarget.com/searchdatamanagement/definition/semantic-technology) IoT deployments require the ability to establish the meaning of the data

### Interoperability challenges inhibit opportunities for additional IoT advantages:

 The current inability of connected devices to effectively communicate immediately when deployed has [stymied the adoption of connected devices](https://internetofthingsagenda.techtarget.com/feature/Top-challenges-of-IoT-adoption-in-the-enterprise), increased costs and limited the value of many IoT uses. Addressing interoperability requirements in IoT deployments can be complex and costly, which can derail or slow IoT projects.

The lack of automatic, widespread interoperability doesn't only slow the consumer or home IoT markets, but it slows progress in civic and commercial IoT deployments. Smart city projects can require hundreds or thousands of devices in numerous categories to work in concert to get the technology's full advantages. Industrial IoT investments with different device requirements and physical barriers could also necessitate the use of multiple communication protocols.

### Interoperability standards bridge IoT device communication:

 Many within the IoT community, including manufacturers and engineers who design connected ecosystems for use, work together to develop standards that address interoperability challenges. Multiple standards organizations have rallied around the cause, but there's no dominant common standard that's applicable in every IoT use case.

"There are so many competing government organizations, standards bodies, industry coalitions, corporations, academic institutions and even individual contributors making contributions in this space, with significant variance by industry and even location sometimes in the same industry," Chandler said.

However, some standards are more widely used than others. Key communication standards, such as IP, have formed in the technical and syntactic interoperability layers over the last 30 years.

MQTT, the open source networking protocol that transports messages between devices, has served as a lingua franca -- a common or bridge language -- for the wide range of IoT components that can use it to exchange information, Glover said.

Meanwhile, experts said the industry is beginning to coalesce around the notion that devices should simply work together -- with the idea that IoT interoperability will resemble plug-and-play technology -- and the industry will come together around the use of mature standards such as [Open Connectivity Foundations IoT specification](https://www.businesswire.com/news/home/20181127005035/en/Open-Connectivity-Foundation-Specification-Achieves-Recognition-by-International-Standards-and-Conformity-Committees-Driving-Secure-Interoperability-Across-the-Internet-of-Things-Worldwide) that defines how devices can interoperate securely between each other and the cloud.

**Managing Authorization**

**Authorization:**

 Authorization is the process of granting permissions to an authenticated identity. You grant permissions in AWS IoT Core using AWS IoT Core and IAM policies. This topic covers AWS IoT Core policies. For more information about IAM policies, see [Identity and access management for AWS IoT](https://docs.aws.amazon.com/iot/latest/developerguide/security-iam.html) and [How AWS IoT works with IAM](https://docs.aws.amazon.com/iot/latest/developerguide/security_iam_service-with-iam.html).

AWS IoT Core policies determine what an authenticated identity can do. An authenticated identity is used by devices, mobile applications, web applications, and desktop applications. An authenticated identity can even be a user typing AWS IoT Core CLI commands. An identity can execute AWS IoT Core operations only if it has a policy that grants it permission for those operations.

Both AWS IoT Core policies and IAM policies are used with AWS IoT Core to control the operations an identity can perform. The policy type you use depends on the type of identity you are using to authenticate with AWS IoT Core.

**AWS IoT Core operations are divided into two groups:**

* Control plane API allows you to perform administrative tasks like creating or updating certificates, things, rules, and so on.
* Data plane API allows you send data to and receive data from AWS IoT Core.

The type of policy you use depends on whether you are using control plane or data plane API.

The following table shows the identity types, the protocols they use, and the policy types that can be used for authorization.

AWS IoT Core policies are attached to X.509 certificates or Amazon Cognito identities. IAM policies are attached to an IAM user, group, or role. If you use the AWS IoT console or the AWS IoT Core CLI to attach the policy (to a certificate or Amazon Cognito Identity), you use an AWS IoT Core policy. Otherwise, you use an IAM policy.

Policy-based authorization is a powerful tool. It gives you complete control over what a device, user, or application can do in AWS IoT Core. For example, consider a device connecting to AWS IoT Core with a certificate. You can allow the device to access all MQTT topics, or you can restrict its access to a single topic. In another example, consider a user typing CLI commands at the command line. By using a policy, you can allow or deny access to any command or AWS IoT Core resource for the user. You can also control an application's access to AWS IoT Core resources.

Changes made to a policy can take a few minutes to become effective because of how AWS IoT caches the policy documents. That is, it may take a few minutes to access a resource that has recently been granted access, and a resource may be accessible for several minutes after its access has been revoked.

Top of Form