Maratha Vidya Prasarak Samaj's
Karmaveer Adv. Baburao Ganapatrao Thakare College Of Engineering
Nashik-13.
(NAAC ACCREDITED INSTITUTE WITH 'A' GRADE)

DEPARTMENT OF ELECTRONICS &TELECOMMUNICATION ENGG.

Departmental TeChronicle

Month: -April 2021

Vol. - 03, Issue – 01

Department Vision:-

To be recognized as an excellent department offering competent technical education to create competent electronics & telecommunication engineers for the benefit of the common masses.

Department Mission:-

Committed to serve the needs of society through innovative teaching learning processes, promoting industry- institute interaction to provide competent and cultured electronics and telecommunication engineers.

Greeting,

Department of Electronics and Telecommunication Engineering is unveiling technical newsletter, "TeChronicle" Vol-3, Issue-1 on the occasion of birth anniversary of Late **Dr. V. N. Pawar**, on **4th April 2021**. This issue is exploring various aspects and challenges of Internet of Thing, Popularly Known as IoT.

IOT and Agriculture

[Mr. A. P. Meshram]

Today no one is unaware of the world IoT; with the active use of IoT anything can be smart. It can work with the help of predictive analysis and machine learning and a combination of both increasing the efficiency of any system, specific word, and areas. IoT has different application areas, you name it you can use IoT like smart home, waste management, health care, environment, safe driving, smart cities the list is unending, I would like to take your attention towards the agriculture sector. There are lot many things that are left unnoticed.

Precision agriculture is nowadays an advancing area in the agriculture sector, Precision Agriculture (PA) helps to boost production and necessarily keep it in line with the population explosion happening all over the world. Survey says - it is expected that by 2050, the global population will reach about 9.6 billion, and food production must effectively double from current levels to feed every mouth. As per the Agricultural Census of 2010–11, the total number of operational holdings (individual farmers) was estimated as 138.35 million and the total operated area was 159.59 million hectares. The average size of the holding has been estimated as 1.15 hectare. It simply meant one farmer is having 1.15 hectares of land to grow the crops. The solution for this is the only advancement in technology. IoT can best fit for enhancing food production and yields.

PA - the technique of optimizing existing inputs and fertilizers, tillage tools, fields, and crops, for improved control and measurement of farm yields has the potential of playing a key role in meeting the incremental food demands of the growing population worldwide.

The IoT may be incorporated to predict and use the fertilizers to be used by knowing and estimating the soil properties, nutrients requirement of crops, real-time monitoring the health of a crop by knowing the different characteristics of plants like chlorophyll measures, leaf area, and other different parameters. Here in every stage, IoT can be used.

Tillage has been inseparable from crop production

and is the very first task at the beginning of an agricultural season. High yields are associated with well-cultivated soil, providing a proper environment for seeds to germinate and roots to grow. Besides, tillage can help to control weeds, disrupt pest lifecycles, incorporate nutrients into the soil, and manage crop residues. Tillage affects soil workability and thereby eventually impacts all other field operations: the amount of necessary water for irrigation, the amount of pesticide, as well as the necessary supplement of nutrients. Here also effective use of IoT may be incorporated.
There are lot many areas where the IoT may help farmers to have the best from existing land.
For the average farmer, setting up the necessary IoT architecture and sensor network for his/her field(s) can be a big task. Getting farmers thoroughly acquainted with the concept of smart farming, and the tools/devices involved in it is of the utmost importance.

Reference :

- https://www.nationalgeographic.com/foodfeatures/feeding-9-billion/
- https://apollo-h2020.eu/why-you-need-to-improve-your-tillage-practices/

Internet of Things: The Future of Technology

[Vaaideehi N. Sonavani, T.E. E & TC]

IoT devices contain various sensors and microprocessors that act on the data collected by sensors through machine learning. Machine learning is when the machine learns similarly to humans by collecting the data present in their surroundings, this is what makes the IoT devices smarter.
As we all know, technology is advancing day by day, with this, the future of IoT seems very promising as it already impacts our lives, homes, and works place. Due to the latest advancements in artificial intelligence and big data analytics, our homes will be slowly filling with more and more IOT i.e. smart devices. Not only our homes but also our cities can be designed to tackle traffic congestion, parking issues or even making our lifestyle greener. For example, access to real-time traffic maps will assist the residents in selecting an appropriate route to save time and effort. In the future, IoT technology will have a lot of opportunities of connecting all sorts of multiple devices and collecting many different types of data, and learn from it.
With this being said, it is visible that IoT will lead us to a better lifestyle, improved security, augmented development, and proper traffic management.

IoT Security Challenges

[Sonal Shirsath. T.E. E & TC]

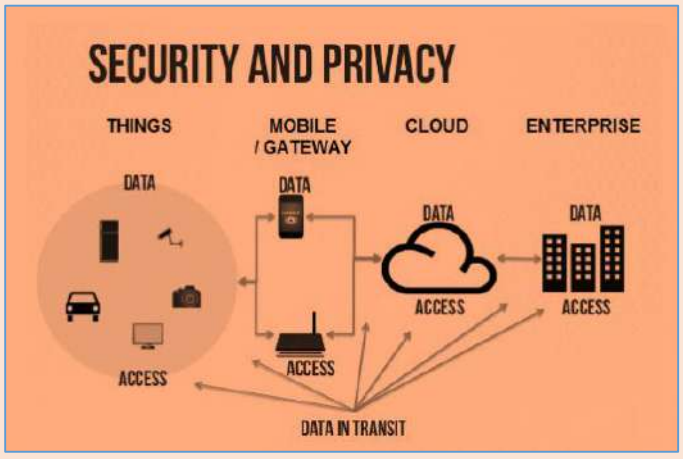
Today 2.9 billion people or 40% of the world's population are online. By 2020, at least 40 billion more devices will become smart via embedded processors. It will influence most consumer and business sectors, impact education, healthcare, and safety. However, it certainly will also pose a challenge from a security point of view. Not only will the devices themselves become more complex, but also the interaction between devices, the networks, and the variance in topology will grow. The impact of such Internet of Things (IoT) on our society will be extraordinary. Finally, with increasing amounts of data and assets at stake, the incentive for attackers will increase. The costs of cyber-attacks in such a setting are estimated to reach about 2 trillion USD by 2020. Today, the IoT is just beginning to emerge. Unfortunately, when looking at its security, there is lots of room for improvement. Security, and security risk awareness, insufficiently present in today's consumer and developer mind set, are only a starting point. Once the requirement for strong security is widely accepted, there will be still the economical question of who is going to pay for security and its maintenance. Without enforcing certain standards utilizing third-party evaluation this problem is expected to be hard to get under control.

Security and Privacy

IoT devices are connected to your desktop or laptop. Lack of security increases the risk of your information leaking while the data is collected and transmitted to IoT devices. IoT devices are connected with a consumer network. This network is also connected with the other system. So, if the IoT device contains any security vulnerability, it can be harmful to the consumer's network. This vulnerability can attack other systems and damaged them.

> *"The Internet of Things (IoT) devoid of comprehensive security management is tantamount to the Internet of Threats. Apply open collaborative innovation, systems thinking & zero-trust security models to design IoT ecosystems that generate and capture value in value chains of the Internet of Things."* **—-** *Stephane Nappo*

Sometimes unauthorized people might exploit the security vulnerabilities to create risks to physical safety. In IoT, devices are inter-connected with various hardware and software, so there are obvious changes of sensitive information leaking through unauthorized manipulation. All the devices are transmitting the user's personal information such as name, address, date of birth, health care information, credit card details, and much more without encryption. Though there are security and privacy concerns with IoT, it adds value to our lives by allowing us to manage our daily routine tasks remotely and automatically, and more importantly, it is a game-changer for industries.



Cryptography

The Internet of Things (IoT) is starting to get a bad reputation – every day it seems like we hear of another way insecure IoT devices were compromised. One of the only ways that the IoT can become more secure is through the proper use of cryptography and not the home-spun, bring your type of cryptography.

Encrypted Communication Protocols

The single biggest area of use of cryptography in the IoT is in securing the communication channels. IoT-centric communication protocols like MQTT and AMQP allow developers to use transport layer security (TLS) to ensure all data sent over the network is unreadable to outside parties. TLS is a rightful heir to the better-known standard knowing as Secure Socket Layers (SSL), which was the long-time standard for web encryption (see HTTPS) but is now considered insecure. TLS ensures that data between two entities is not readable nor prone to manipulation by third parties.

In addition to encrypting the main data connections, it's also important to encrypt any available secondary communication channels such as those use for maintenance or customer features. For instance, if an IoT device comes with a web portal for use by consumers (think of a web interface for a printer) that should also come encrypted by default. If not, anyone on the same network could intercept usernames, passwords or use session data to impersonate those logged in to control these devices. For the same reason, insecure maintenance interfaces like telnet should be shuttered in favour of secure approaches like Secure Shell (SSH).

Hashed Passwords with Salts

There is a well-known adage that states that the most secure systems are those with nothing to steal. Storing hashed passwords is one way to accomplish this. A hash is a cryptographic function that will take any input and create a unique, irreversible, yet consistent set of bits.

Good hash algorithms are nearly impossible to reverse. In other words, once a password is hashed, you shouldn't be able to reverse the hash to determine what the password was. However, the hash can still be used to validate submitted passwords because the same input to a hashing function will return the same output or hash. Some examples of hashing functions are MD5 (popular but no longer considered secure), SHA-256, and Blowfish.

Private Key Authentication

Private Key cryptography is asymmetric encryption that provides two keys, one public and one private. If data is encrypted with the private key, it can only be decrypted with the public key and vice versa. Keeping the private key private then allows a single machine to securely communicate with the outside world or authenticate with remote machines. This bit of cryptographic functionality is particularly well suited for a couple of aspects of IoT infrastructure. The first is the authentication of a single machine that joins an IoT network. For example, an end node may need to connect to a central MQTT broker to publish data upstream. Using private key authentication gives each machine a secret and unique identifier when joining the network (eliminating the oft-used insecure global credential approach) and due to their length are virtually impossible to brute force (which is where a machine is programmed to guess values).
The second area where private keys can help in IoT is in the verification of messages between devices. A hash or other integrity-checking algorithm would be computed on a message (such as a firmware image) and then encrypted with a private key and appended to the message. Then that check is decrypted by the message receiver with the public key, which proves that it could only have been generated by the holder of the private key.
Finally, the result of the integrity-check is validated to ensure the message was not compromised or altered in transit. This sort of electronic signature can be useful in situations where a secure communication channel is unavailable.

Signed Firmware and Secure Boot

The electronic signature approach described in the previous section is also something that can be used for secure boot and the signing of firmware images. This so-called signature ensures that an authorized user or machine has put its stamp of approval on the firmware before it is executed. It makes it much harder for a malicious individual to create rogue firmware and hijack a machine – they wouldn't be able to sign the code they've created.
Secure boot is the feature that utilizes this, ensuring that any code that is set to run on a device is appropriately signed. The very first bits of code a device will run after it is booted includes functionality to compute and verify the electronic signature. Furthermore, the use of a private key infrastructure (PKI) with secure boot gives maintainers a pathway to remediation if the secret key used to sign code is compromised.

Resource-Constrained Devices

This is all well and good, you might think, but if you work in IoT for any length of time, you will come across situations where you are using resource-constrained devices at the edge. These devices have restricted power, processing, memory and can give developers some big technical hurdles. Unfortunately, modern cryptography can be a resource hog and so the question naturally arises: How do we build devices that are safe and secure while also meeting the constraints placed on them?
Don't dismay! Smart compromises can be made in these environments. For instance, if data integrity is important but not necessarily the secrecy of the data, then full-encryption of data streams can be forgone for a simpler scheme where a hash is computed with a shared, secret salt – a poor man's electronic signature, you might say.
This would allow the receiving system to validate the data and ensure, with some confidence, that the data was generated by authorized machines. It's less than ideal but might be an acceptable risk in some environments. This is just one example, but the idea is that with some creativity and a good working knowledge of cryptography, you can effectively balance these risks and security within IoT systems.

Reference

- https://dl.acm.org/doi/abs/10.1145/2995289.2995298
- https://medium.com/@arindey/internet-of-things-iot-security-privacy-applications-trends-

Website: www.kbtcoe.org
Email Id: techronicle.etc@gmail.com