

Internet of Everything, How to Connect?

(Mar 03, 2021)

Internet of Everything. I believe everyone is excited and has a lot of imagination when they see this term. Simply put, the Internet of Everything is to organically connect people and things through networking technologies to realize the interconnection, information interaction and resource sharing between people and people, people and things, things and things, so as to promote human civilization to a higher level, and further benefit mankind.

According to related reports, there are currently more than 50 billion IoT connected devices in the world, and with the rapid development of 5G, more things will be interconnected. It can be said that an era of Internet of Everything has arrived. The topic of this blog is a bit big. There are already many solutions for "how to connect", and these solutions are being practiced and improved. And I also like to put forward some of ideas based on my work experience and practice.

It has been 52 years since the Internet was invented, and the networking technologies and application technologies have been very mature. I think the Internet of Things or the Internet of Everything should use the Internet protocol. It's just the people and people, people and things of Internet extends to things and things and allows more things to realize the connection with people. In fact, all kinds of smart home appliances are already connected in this way.

However, the current Internet of Things connection or communication between the Internet of Things has security risks, which must be solved at the beginning, otherwise it will be a huge disaster when it becomes popular in the future! At present, there are two main problems in the communication of the Internet of Things: One is that the centralized communication method is not suitable for the Internet of Things. Currently, the communication between the things of Internet and the communication between people and things must pass through a centralized

server in the cloud, once this central service system fails or is attacked, the entire Internet of Everything will be paralyzed, which is an unacceptable result. Second, it is not feasible to use the Internet security protection solution for the Internet of Things security protection. It is not only a problem of high cost but also can be said to be unworkable. Because the things of the Internet of Things are not humans, things do not have the data processing capabilities of computers and mobile phones used by humans. This point deserves the attention of relevant security vendors.

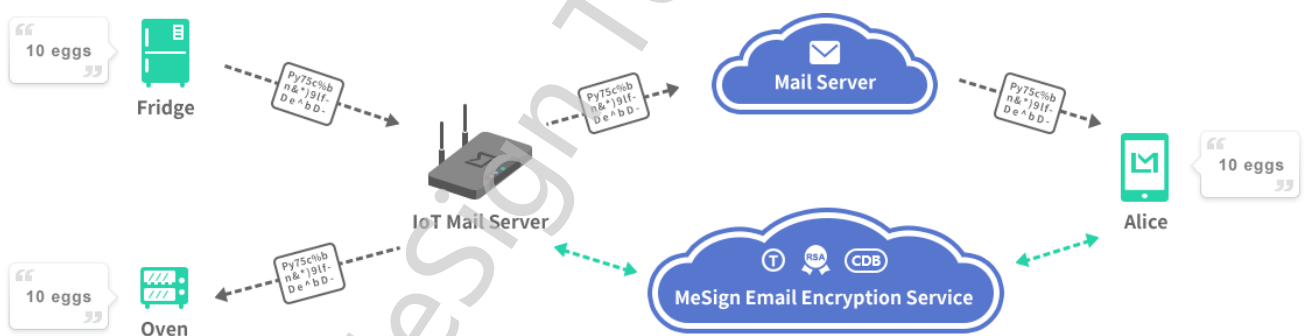
For the first problem, I proposed a decentralized Internet of Things communication solution based on the email communication protocol. Everyone knows that email is a decentralized communication system, anyone in the world can achieve reliable communication through email. All mail servers are the decentralized communication nodes around the world. There is no central node for email communication, and email is not like a highly centralized social network that people must rely on a certain service provider to achieve communication, and people cannot achieve communication unless they use the same highly centralized social service system. Obviously, the email communication system is not like this. As long as you have an email address, you can send email to another email address user regardless of which email service the other party uses.

For the Internet of Things, things can also have an email address like a person, and the Internet of Things service node provides email services for the things of this node. For example, a home router can be a service node that provides email services for all electrical appliances and things in the home. It is possible to realize global email communication between things and things, people and things, regardless of which mail server the people and things belong to. This is a decentralized and reliable communication solution between people and things, and things and things, completely solve the problem of unreliability of centralized communication methods.

For the second problem, we can implement the encrypted email communication service for the Internet of Things through digital signature and encryption technology. Every thing has a digital identity. Email digital signature is used to prove its identity, and encryption certificate is used to encrypt everything communication, to ensure that the content of communication will

not be illegally stolen and illegally tampered with, thereby protecting the security of IoT communication. In this case, the security protection of the Internet of Things is very simple. The communication receiver must validate the digital signature and decide whether to accept or reject the communication according to the security rules. That is to say, things only receive trusted communications, thus effectively resisting all attacks, without the need for additional complex security protection modules.

Of course, not only communication between things, but also communication between people and things requires people to digitally sign email with their signing certificate, so that things can automatically identify whether they should communicate with this person, so that things can truly be protected from human attacks. This is a very efficient, low-cost and reliable Internet of Everything communication security protection solution, which completely solves the vicious circle of Internet security protection that is also trapped in the current Internet of Things security protection.





The era of the Internet of Everything has come, but how to connect, I believe that we should fully learn from the already very mature Internet development ideas, copy the mature technology into the Internet of Things, but also consider the particularity of the Internet of Things, and realize that the Internet of Things different schemes should be adopted from the Internet for people. The use of encrypted email to achieve secure and reliable communication between people and things and between things and things is the lowest cost and the easiest solution to implement. Of course, for things that require high real-time performance or communication between people and things, more efficient https encrypted communication methods can also be adopted, but people and things still need to use their digital certificates to

prove their identity to achieve communication to ensure that things security of communication with things and between people and things.

----- END -----



Want to contact me to discuss this topic? Please use [MeSign App](#) ( - ) to scan the QR code and send me an encrypted email, I will reply to your encrypted email ASAP.

© 2021