My system cia is the most compulsory security

Business, Management

My survey was based on the security and privacy issues of Internet-of-Things.

It’s not an easy job to define a standard security principle and to suggest the countermeasures of security attacks and threats. Different scholars research in their own way to identify the issues and provide solution. A glimpse of their research is provided below. 1.

IoT Security Principles Ioannis Andrea et al. 3 believes that the system needs to be robust to prevent data-related attacks and must provide data security and privacy. As per their view, a secured IoT system needs to provide confidentiality, integrity, and availability (CIA). And it can be achieved through the authentication, access control, data encryption etc. Also, they emphasize that an IoT system must have trust between each layer, security, and privacy in each layer as well as the trust between the user and IoT system. Rwan Mahmoud et al.

4 mentioned that for a strong and secured IoT system CIA is the most compulsory security goals. Along with this typical security goals, they also put weight on availability, security policy, heterogeneity, key management system. Hui Suo et al. 9 discuss the individual security requirements for each architectural layer of IoT system. As per their research, in perceptual layer authentication of access is the first security measure followed by confidentiality by encrypting the data. For data encryption, lightweight cryptographic algorithm and protocol are preferred. As they believe to apply the security mechanism is quite difficult in the network layer.

For that they refer identity authentication between nodes is required to maintain confidentiality and integrity. Also, they highlight on to prevent the DDoS attack. For cloud computing and secure multiparty computation strong encryption algorithm and protocol, strong system security technology and antivirus suggest by them. To solve the security problem in the application layer, either authentication or strong key management across the heterogeneous network or user's privacy protection can be used.

Monika Bhalla et al. 2 also referred the CIA requirements for a secure system but they mainly emphasis on the security of wireless sensor networks instead of whole IoT system. 2. IoT Security Attacks and Threats Andrea et al. 3 classified the IoT attacks in four distinct classes: physical, network, software and encryption attacks. Physical attacks are mainly focused on the hardware components of an IoT system. To make such threats attacker need to be physically close or reside within the system.

Whereas for the network attack, an attacker need not be closed on the system. It mainly manipulates the network system through RFID spoofing, RFID cloning, Denial-of-service attack etc. to damage IoT network. Software attack makes the security vulnerabilities of IoT system. It exploits the system attacking by trojan horse, worm, spyware or any other malicious activities. Encryption attack first breaks the encryption scheme of the system and then attacks the system.

Man-in-the-middle attack, cryptoanalysis attack etc. are varieties of encryption attack. Xu Xingmei et al. 6 discuss security issue in each layer of IoT system face.

In the perception layer, the main threat is the RFID and WSN security. Many types of attack can happen in this layer such as replication attack, channel blocking attack, flooding attack etc. Consequently, in the network layer, the common security attacks are the DDOS attack, middleman attack, heterogeneous network attack etc. Finally, in the application layer, the security challenge is to maintain the privacy of information by prohibiting illegal access to the database, prevent information leakage from system etc. Weizhe Zhang et al. 5 also explains different type of threats for the different architectural layer of IoT. Even though, In the perceptual layer, the node resource is limited, a versatile network topology and distributed organized structure is present.

But still, it has some security threats like brute force attack, routing attack, clone node etc. The main security concern of network layer is DoS attack, data attack or session attack. Whereas in application layer security attack can be done by privacy leak, malicious activities or social engineering. 3.

IoT Security Countermeasures Hui Suo et al. 9 provides the procedures to keep the IoT system secure based on a layer basis. They define IoT has four layers and strongly recommend that to keep the system secure its essential to maintain individual security procedure for each layer. Andrea et al. 3 also suggest the security approaches on a layer basis.

Both have a strong emphasis on secure authentication, data encryption, cryptographic algorithms to prevent the system from threat and attacks in each layer. Hui Suo 9 believes with AES and RSA algorithm Diffie-Hellman and SHA cryptographic algorithm is also effective for security and integrity of the system. Whereas Andrea 3 only mention about AES and RSA for application layers security. Apart from that, they suggest security software and firewall prevent unauthorized access. Weizhe Zhang 5proposed their own security architecture to secure IoT system. They propose a two-dimensional security architecture in which the security is based on environment: perceptual layer, network security layer, a middleware layer, and application layer. And then divided by the function on each layer consists of identity security, data security, control safety and safety behavior.

Rwan. M et al. 4 proposed the security countermeasures with an emphasis on secure authentication, establishing trust, federated architecture and finally security awareness. For secure data exchange and to protect data from theft they also referred for cryptographic algorithm and techniques.

They proposed an abstract session layer as an additional layer to manage connection protocol and communication between heterogeneous devices. So that, IoT can manage to open, closing and handling a session between two devices. Currently, IoT mainly focuses on authentication and access control protocol but with the rapid growth of technology they want to incorporate the new networking protocol IPv6 and 5G with it. Monica. B et al.

2 mainly research on the security of WSN and proposed security protocols for the wireless sensor network. They referred to the
security protocol, encryption protocol and give special important on ZigBee which is a higher-level communication protocol.