CHAPTER 7

# Factor-based Authentications Techniques in Machine-to-Machine Communication

*Shafi Ullah, Raja Zahilah Raja Mohd Radzi, and Rashidah Kadir*

## 7.1 INTRODUCTION

Authentication is an extremely important feature of security in Machine-to-Machine (M2M) communication networks. Machines communicate with each other autonomously to perform their respective tasks and share crucial data. Devices authenticate each other before sending and receiving data. Thus, both sending and receiving devices must be trusted. There are several types of topologies used to interconnect remote M2M communication devices. Apart from group and local-based authentication, several other techniques have been proposed in securing Machine Type Communication (MTC) device communication with efficiency by adding additional unique parameters including encryption, pre-shared unique identity keys, two factors such as user and device by using encrypted keys, three-factor such as user to device and device to gateway, device signatures and implementing secure hash-functions.

Each parameter addresses a particular environment and topological structure of a Wireless Sensor Network (WSN). Such authentication schemes are basically used for specific business applications that require specific networks with specific user-controlled privileges. Figure 7.1 shows a generic M2M communication network while Figure 7.2 shows a taxonomy of authentication in the M2M communication network.

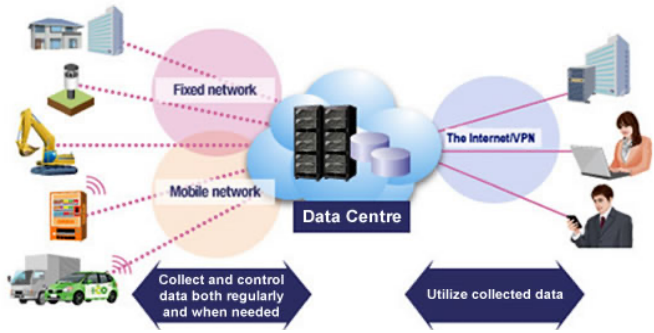


**Figure 7.1** Generic M2M communication networks

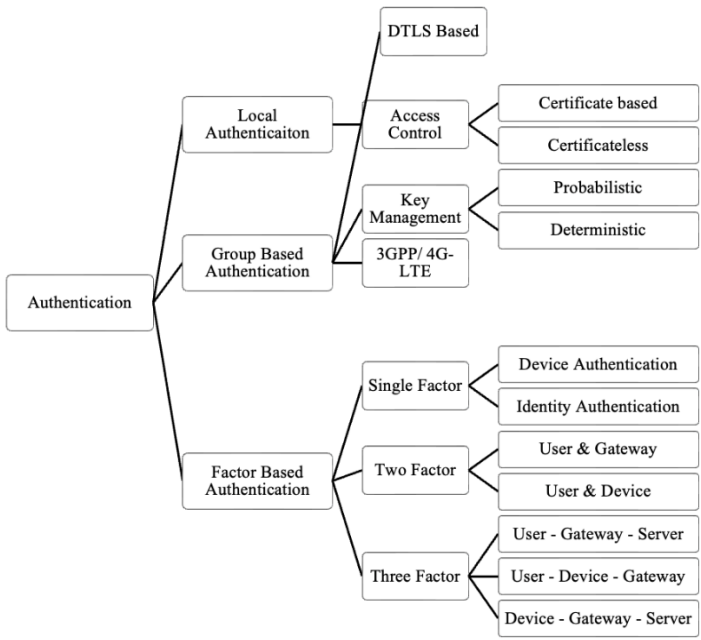


**Figure 7.2** Taxonomy of authentication in M2M communication network

## 7.2 RELATED WORK IN FACTOR-BASED AUTHENTICATION

Table 7.1 shows a summary of hybrid and factor-based authentication schemes which are analysed through features presented in (Das, 2009) offered a dual-factor user verification method for WSN by securing secret key risking, mimicking, and Dos attacks. Whereas Vaidya et al. (2010) pointed out that such a scheme had a few security flaws by not offering users to alter passwords and mutual authorization among gateway, sensor, and end node. Vaidya et al. (2010) brought up a strategy that proposed an improved method. However, the method was defenceless against malicious insider and password-guessing attacks. Additionally, Hsieh & Leu (2014) proposed a scheme that can counter such attacks by merging keys and eXclusive OR (XOR) the results. However, the scheme could not resist insider attacks and disconnected secret key speculating attacks. Devi et al. (2015) devised simple architecture for mutual authentication by prioritizing lower computational and lesser memory consumption.

The scheme met targeted performance criteria but lacked databased related security measures. Qui and Ma (2016) proposed an improved Authentication and Key Agreement (AKA) scheme that is significantly intended for M2M correspondences in IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) systems. To overcome the insufficiencies referenced in AKAES (Authentication and Key Agreeing Encrypted System), a combination of cryptography is utilized for secure authentication and shared keys with the thought of resource constraints at 6LoWPAN utilising MTC devices. A handover ticket is produced for a mobile device (6LR) to accomplish quick authentication when performing handovers. Therefore, a full authentication process may be performed once the ticket is terminated.

In addition, the proposition has a remarkable element to give security backing to both static and portable devices in