Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02672-x

ORIGINAL RESEARCH

A review on lightweight cryptography for Internet-of-Things based applications

Vidya Rao[1] · **K. V. Prema**[1]

Received: 25 April 2020 / Accepted: 3 November 2020

Abstract
The Internet-of-Things (IoT) is a combination of an intelligent infrastructure combined with various self-organizing devices. These devices are used to monitor the environment and help to exchange sensitive data over the Internet without much human interference. Such a huge network of unmanned devices are subjected to various security and privacy concern. As these devices are battery powered and have low inbuilt resources, it is important to enable secure and resource-constrained security solutions to secure the devices. Thereby, to address the security and privacy of these devices and the data, the authentication plays an important role along with data integrity. Through this paper, we have analyzed the various lightweight solution and their security threats under the authentication and data integrity of the IoT applications. From the study, it can be seen that the major security concern of these protocols is to perform with less computation and resist to attacks like man-in-the-middle, replay attacks, denial of service attacks, forgery and chosen-ciphertext attacks. Also, this review provides an insight into using the Microsoft threat modeling tool used for IoT based applications.

Keywords Authentication · Data integrity · Lightweight cryptography · Internet-of-Things · Security analysis · Threat modeling

1 Introduction

Internet-of-Things (IoT) is a paradigm that connects various physical devices to the Internet using different wireless technologies. In the past few decades IoT (smart environment) has taken a large share in the development of technology (Jing et al. 2014; Da Xu et al. 2014). Foremost, imagine a day when you are returning home after a busy schedule and you enter your house to see that your coffee is ready before even you sit on your couch or imagine your mobile automatically provides you the information about empty parking place in a shopping mall and navigates you towards it or your plants know when they need water and so on. Such an interactive environment can be developed with the help of IoT. These IoT devices are termed as 'objects' that include a TV remote to water pump system or from a car key to driver-less cars and much more. The objects are embedded with various types of sensors that can sense the environment, process the data and communicate the data to various destinations using the Internet.

An attempt to transform machine-to-machine communication to Internet-of-Things (IoT) has brought the greatest revolution in the current human era. The vision of IoT is to create a heterogeneous network of millions of connected objects that securely communicate using the Internet (Jing et al. 2014; Vermesan and Friess 2014). The IoT is a vast network of networks consisting of physical and virtual interconnected entities with unique addressing schemes; they interact with each other to provide certain customized or generic services. IoT has become an essential part of the socio-economical growth of the country as it has various domain-specific applications in diverse areas. Some of the applications are health care, surveillance, transport, security, manufacturing, environmental monitoring, food processing, as in Fig. 1. These applications are integrated with technologies like autonomic networking, decision making, machine-to-machine communication, cloud computing, big

✉ Vidya Rao
vidyarao1988@yahoo.com

K. V. Prema
prema.kv@manipal.edu

[1] Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka 576104, India

Published online: 21 November 2020

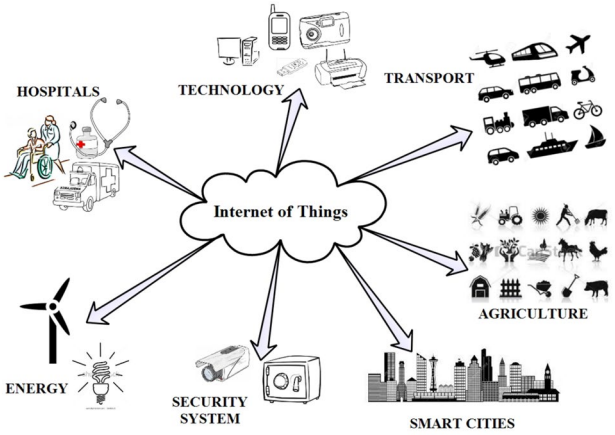

Fig. 1 Applications of Internet-of-Things

data analytic, confidentiality protection, security and many more (Zeinab and Elmustafa 2017).

As these IoT devices are poorly secured, they can serve as means of entry points for cyberattacks by allowing various malicious individuals to re-program a device and cause malfunctioning (Abomhara and Køien 2014). Some of the most common attacks are denial-of-service (DoS) attacks, distributed DoS (DDoS), node compromise attacks, identity and forgery attacks, man-in-the-middle attacks, replay attacks, chosen cipher-text attacks (CCA), remote recording attacks and many more. Thereby, it becomes essential to provide security and privacy at the devices level (Abomhara and Kien 2015). So to develop a safer IoT solution, it is required to consider security requirements like confidentiality, integrity and authentication (CIA) (Hafsa Tahir and Junaid 2016).

These devices communicate among themselves and with the users over the publicly available Internet network. As these devices posses low memory, low power, low processing capabilities, it is feasible to design lighter yet stronger cryptographic solutions. The most commonly used lightweight cryptographic algorithm can be classified into symmetric and asymmetric algorithms. For example, advance encryption standard (AES), high security and lightweight (HIGHT), the tiny encryption algorithm (TEA), PRESENT and RC5 are symmetric cryptography. But for the IoT devices, generation and distribution of symmetric keys are the major tasks that include: (1) embedding the key onto the device during manufacturing, (2) provide security model to protect the hardware from being tampered, (3) issue of keys during operation, (4) selection of better cryptographic primitives. Therefore for scarce environment, having lightweight public-key cryptography (PKC) ensures stronger cryptography by consuming fewer resources. Also, PKC enables a strong authentication over data and maintains the confidentiality of the user's private data. Some of the PKC algorithms

Table 1 Key size and security level comparison

RSA Key size (bits)	ECC key size (bits)	Security level (bits)	Protection
1024	160	73	Short term
1536	192	89	Between short term and long term
2048	224	103	Between legacy standard level and medium
4096	256	128	Long term

are, Rivest–Shamir–Adleman (RSA) (Stallings 2006; McAndrew 2016a), digital signature algorithm (DSA) (Zheng 1997; Roy and Karforma 2012), elliptic curve cryptography (ECC), ECC using Diffie–Helman Algorithm (ECDHA) and ECC using Digital Signature Algorithm (ECDSA) (Lenstra and Verheul 2001).

Among these algorithms, ECC is considered a light weighted cryptographic solution for various resource-constrained devices. Many organizations like National Institute of Standards and Technology (NIST), IEEE, Internet Engineering Task Force (IETF), International Telecommunications Union and American Bankers Association (ABA) are working on the mathematics related to elliptic curve to provide the highest level of network security. The organization X9 under ABA has proposed the standards ANSI X9.62 and ANSI X9.63 for ECDSA and ECDH, respectively. IEEE has published P1363, which describes the implementation of elliptic curve operations. Also, NIST has provided different types of elliptic curves that can be used for ECDSA (Lauter 2004). From Table 1, we can see that ECC has a longer protection period with a key size of 128-bit, which is equivalent to the 4096-bits key-size of RSA (ECRYPT 2012). Also, with smaller key-size, the time taken to generate the signature is faster than that of RSA, as described in Table 2 (Jansma and Arrendondo 2004). Hence ECC is more suitable for devices with the lesser inbuilt resource.

The paper is organized as followed: Sect. 2 provides the motivation towards securing IoT. Section 3 provides a standard protocol stack of IoT. Some of the applications of IoT are briefed under Sect. 4. Various security concerns, requirements and threats are explained in Sect. 5. Section 6 explains various existing lightweight data integrity scheme, followed by Sect. 7 with various authentication scheme for IoT and Sect. 8 explains lightweight hash functions. Later, Sect. 9 provides different security analysis and Sect. 10 describes threat modeling of IoT infrastructure. Finally, Sect. 12 provides the conclusion of the study.

Table 2 Comparison of ECC with RSA

Algorithm	Key-size (bits)	Key-Gen time (ms)	Sig-Gen time (ms)	Sig-Verifi time (ms)
ECC	163	0.08	0.15	0.23
	233	0.18	0.34	0.51
	283	0.27	0.59	0.86
	409	0.64	1.18	1.80
	571	1.44	3.07	4.53
RSA	1024	0.16	0.01	0.01
	2240	7.47	0.15	0.01
	3072	9.89	0.21	0.01
	7680	133.90	1.53	0.01
	15360	676.06	9.20	0.03

2 Motivation towards securing the Internet-of-Things environment

During infancy, IoT faced a lot of issues related to architectural design, context-aware computing, manufacturing and interoperability, device lifetime, robustness, security and privacy. Among, which data security and privacy of the user information plays an vital role in IoT. The three basic functionalities of IoT are: connecting, sharing and managing the devices and the data. In short, IoT enables a person to be connected to anyone around the world at any time using any device connected to the Internet. We know that IoT comprises of trillions of devices with various technologies like cameras, biometric devices, physical and chemical sensors, it is important to design a standard secured communication module that can withstand the scalability and security challenges faced by IoT devices and applications (Abomhara and Kien 2015).

The major domain of the applications that IoT has taken share are; smart home, health-care, transportation and power management (Al-Fuqaha et al. 2015). According to the World Economic Forum, there are about 91.2% of people depend on IoT devices. They use smart devices to control their home appliances, to keep track of their health habits, to distribute power to various areas and also to control the traffic of aircraft or urban vehicles. Thereby, the security and privacy issues that occur during the analysis of large data communicating over the Internet has created opportunities to intruders to invade through the network by accessing the devices (Da Xu et al. 2014; Abomhara and Køien 2014; Peng et al. 2013). It also opens a way for a hacker to forge the user's identity and imitate as a genuine user leading to attacks like eavesdropping, masquerade and replay attacks.

Hence the manufacturing industries need to develop their devices that can easily communicate with other devices and exchange data over the Internet with the concern of devices' privacy and maintain security of the collected data. The manufacturers should also consider the limitations regarding resources like the energy of the devices, memory capacity, processing time, the freshness of data, network throughput, network delay, etc. Among these issues, manufactures should ensure the privacy of the user as many wearable devices that help people to track objects or other persons store sensitive information. Which can be easily exploited by intruders and disturb the network. Hence it would be a priority to ensure the design of a secure and privacy enabled model (Abomhara and Køien 2014).

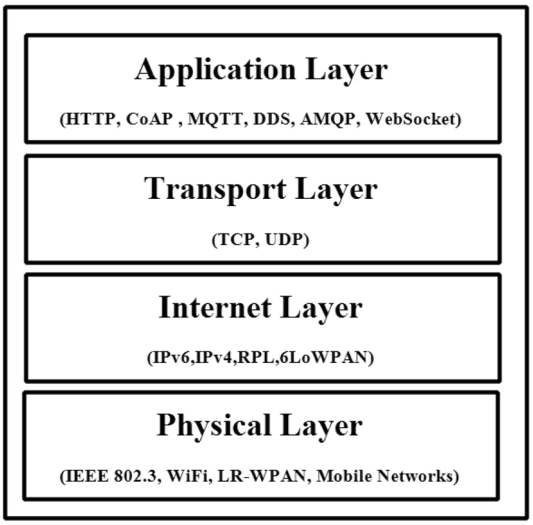

Fig. 2 IETF IoT protocol stack

3 IoT protocol stack

Currently, the Internet architecture is based on IP-based protocols that enable ubiquitous connection of wireless resource-constrained IoT applications (Li and Xiong 2013). International Engineering Task Force (IETF) has proposed a four-layer protocol stack that describes the various protocols used at each layer, as in Fig. 2.

The first layers is *Physical layer* that concentrates on the connection between devices and data flow between them. Some of the physical layer protocols are IEEE 802.3, 802.11-WiFi, 802.16-WiMax, 802.15.4-LR-WPAN, 2G,3G, 4G mobile network and Long Term Evolution (LTE) network (Jing et al. 2014). Then it is *Internet layer* that performs host identification and packet routing. IETF has proposed Routing over the Lossy and Low-Power network (RoLL) group that focuses on the standardization of the IPv6 routing protocol for the Lossy and Low-Power network (LLN). Some of the protocols used are IPv4 (Li et al. 2014), 6LoWPAN (Babar et al. 2011) and RPL (He and Zeadally 2015).

Next layer is *Transport layer* that is concerned with end-to-end message transfer. The message transfer can be either by handshaking using TCP or without a handshake like UDP. The transport layer involves segmentation, congestion control, error control and flows control (Zhao 2014; Zhang and Qi 2014) presented in the IETF standards for Transmission Control Protocol (TCP) and User Datagram Protocol(UDP) protocols. Lastly, the *Application layer* interfaces with all the lower layers by establishing a secure connection among them. This layer uses port numbering for application addressing and most commonly used are Port 80 for Hyper Text Transmission Protocol (HTTP) and Port 22 for Secure Shell Protocol (SSH). These port helps in establishing a process-to-process connection. IETF CoRE working group have initiated a resource-constrained protocol called Constrained Application Protocol (CoAP) (Farash and Sabzinejad 2014). Each resource corresponds to a universal resource identifier (URI) that helps the resource to operate statelessly using GET, PUT, POST, DELETE and so on. Other than CoAP, the application layer uses Hypertext Transfer Protocol (HTTP), which uses the request-response model and URI to identify the resources. Message Queuing Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DSS) and Advanced Message Queuing Protocol (AMQP) is commonly used application layer protocol (Mahmoud et al. 2015). Some of the commonly used protocols are explained bellow:

CoAP: Constrained Application Protocol (CoAP) is an application layer protocol that defined on Representational State Transfer (REST) protocol above HTTP protocol functionalities. REST used Request-Response model as shown in Fig. 3, where a client-request-message is sent to the server and the server prepares a response and returns the response to the client. This communication is similar to the client/server model. REST is a stateless communication model and each request-reply messages are independent of each other. Unlike REST, CoAP uses a connectionless protocol like UDP for message exchange and has customized HTTP functionalities for resource-constrained devices of IoT (Lenstra and Verheul 2001). CoAP uses methods like create, retrieve, update, and delete. Hence CoAP is divided into two sub-layers, called *messaging sub-layer* and *request/response sublayer*. The messaging sub-layer checks for duplication and asynchronous nature of the interactions. The request-response sub-layer performs REST communication. CoAP uses four types of messages: configurable, non-configurable, acknowledgment and reset. The reliability of CoAP is checked based on the configurable and non-configurable messages.

MQTT: Message Queue Telemetry Transport (MQTT) is a messaging protocol used in IoT based applications that were introduced by IBM at OASIS labs (Meier 2005). MQTT works based on a publish-subscribe communication model as in Fig. 4. It involves three entities, namely: the publisher, the broker and the consumer. Publishers are the sources of data; brokers maintain information about the topics sent by publishers and consumers are the one who subscribes the topic managed by the broker. Here, the publisher is not aware of consumers and the broker independently provides information to consumer's requests. MQTT is built over TCP protocol and has applications in healthcare monitoring, energy meter, Facebook notifications etc,.

XMPP: Extensible Messaging and Presence Protocol (XMPP) (Jing et al. 2014) is an instant messaging (IM) standard by IETF. XMPP is used basically for multi-party chatting, voice-video calling. This was initially developed by Jabber open-source community to aid and spam-free, secured and decentralized protocol for IM services. XMPP uses XMP stanza to connect either between client-to-server. Each stanza represents a piece of code that has three parts: message, presence and ID. Where the message stanza speaks about the source and destination address, the presence stanza shows update status and identity (ID) stanza pairs message with the respective receiver and sender.

HTTP: World Wide Web (WWW) founded an application layer protocol called Hypertext Transfer Protocol (HTTP) (Jing et al. 2014) that could interface with lower-layer protocols. HTTP works under a request-response communication

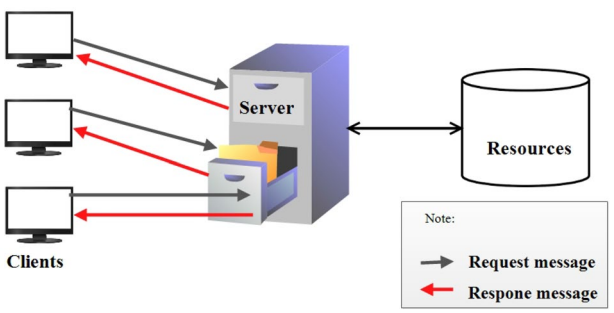

Fig. 3 Request-reply method

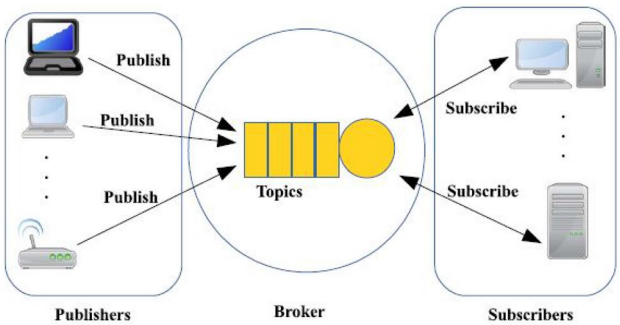

Fig. 4 Publish-subscribe method

model and uses commands like GET, POST, PUT, DELETE, HEAD, TRACE, OPTIONS, etc. Even HTTP is a stateless protocol and each request is independent of the other request. HTTP uses universal resource identification (URI) to identify HTTP resources.

6LoWPAN: IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is a low-cost network communication protocol developed under IETF to allow resource-constrained applications to function efficiently. 6LoWPAN possess characteristics like smaller packet size, star and mesh topology, a large number of devices can be connected dynamically. But as they are designed for resource-constrained devices, during their sleep schedule, they are inactive. The limited packet size and variable addressing has created a need to have an adaptation layer that fits IPv6 packets to IEEE 802.15.4 specifications. This standard provides header compression and fragmentation to meet the maximum transmission unit (MTU) of 1280 bytes from a link.

4 Domain specific applications

IoT poses a diverse set of applications in various domains that include cities, environment, energy systems, retail, manufacturing, health and logistics (Vermesan and Friess 2014). This versatility has created opportunities for hardware manufacturers, application developers and the Internet Service Providers (ISP). Gartner has estimated that by the end of 2020, the cost spent on IoT hardware will reach almost to $3 trillion with the expected data flow of about 45% more than current. Beyond these predictions, the applications of IoT in health care has taken a share of about 40% and follow the manufacturing industry with 33%. The smart grid technology (Chung et al. 2016; Zhao et al. 2014) posses 7% of total market share. Agriculture, urban infrastructure, security and resource extraction has taken 4% each. Lastly, IoT application in vehicle and retail takes a share of 3% and 1%, respectively as in Fig. 5. With such a progression of applications, we can see some of the domain-specific applications (Hafsa Tahir and Junaid 2016).

4.1 Home automation

A smart home has become popular for two reasons. Firstly, the involvement of a wireless sensor network in sensing and actuating has made life more comfortable. Secondly, safeguarding home and house-hold things have become easier (Mahmoud et al. 2015). In the smart home, we can see applications like smart lighting, smart appliance, home intrusion detection, smoke/gas detector etc. In such applications, many sensors and actuators are attached to each device inside the home and are controlled by the user through the Internet using smartphones or web pages (Jing et al. 2014).

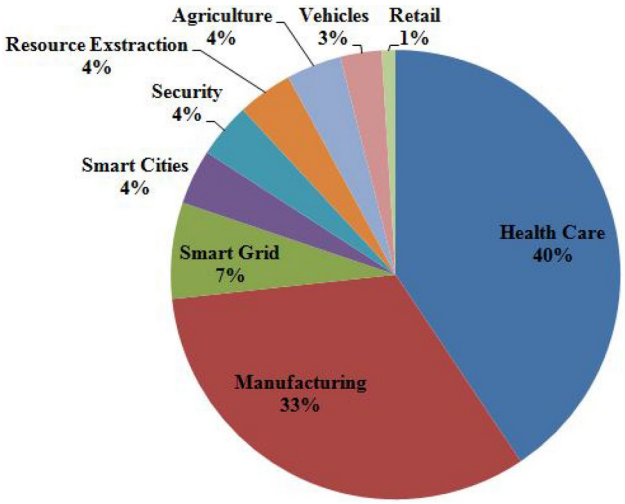

Fig. 5 Graphical representation of IoT applications share

4.2 Smart cities

Similar to smart-homes, every country is installing its cities with intelligent and self-adaptive smart systems that are coupled with sensors, actuation units and Internet-based cloud services (Jing et al. 2014). We can see smart city applications in smart street lighting that help in automatic operation of street light based on light intensity (Tan et al. 2016). Likewise, smart parking is another application that helps drivers to park their car efficiently by saving time in searching for an empty parking slot. Smart sensors are also used in understanding the road quality and structural health monitoring by implanting sensors on the road and building to get a regular interval of information of road and building stress data (Tan et al. 2016). Lastly, IoT is used in surveillance and emergency response in case of any environmental disaster with-in the city (Camtepe and Yener 2004).

4.3 Environment and agriculture

Monitoring weather conditions is an important task to analyze the temperature, humidity, air particles, etc., in the atmosphere. IoT has taken its place in environmental monitoring by developing weather monitoring systems like AirPi. AirPi is capable of monitoring temperature, humidity, smoke, UV level, carbon dioxide(CO_2), carbon monoxide (CO), nitrogen dioxide NO_2 and air pressure. Other than weather monitoring stations, IoT used in air pollution monitoring where harmful gases like CO_2, CO, NO_2 and NO are monitored and the results are presented to the administrator (Mahmoud et al. 2015; Le et al. 2009). IoT is also used in noise pollution monitoring, Forest fire detection and river flood detection. Monitoring weather conditions and air quality helps in improving agricultural production. Smart

irrigation and greenhouse crop production are major two agriculture-based IoT applications along with soil quality monitored for pesticide content in the soil (Jing et al. 2014).

4.4 Smart grid

A smart grid is an information and communication technology that collects and analyzes real-time electrical power data (Chung et al. 2016). Through this analysis, the power will be distributed efficiently across the region. Generation of electricity, consumption, storage, distribution and health information of the device are the major functions of the smart grid. IoT based smart meters can capture real-time power consumption and can be controlled remotely. The data collected by these smart meters are analyzed using cloud-based applications that provide real-time response and management strategies.

4.5 Manufacturing industry

IoT has created ample opportunity for the manufacturing industry to manage there work and machines. Sensors are installed on machines and these sensors can diagnose any change the machine behavior and report to the operator to take further precautionary/corrective measures. IoT is also used in logistics to route the product towards the destination, object tracking and shipment monitoring.

4.6 Health care

A personal health-care system (PHS) is a smart wearable device that helps anyone to track their daily activities. The technologies like NFCs, RFIDs, other sensors are mounted on hardware that can be worn by the user. These sensors shall track their activities and report to a smartphone coupled to the devices. Such devices help in heartbeat monitoring, walking rate, user location tracking, user sleep schedule monitoring and many more. These data are saved to cloud-based applications that can be accessed by the physician and helps them to keep track of user's activities (McGrath and Scanaill 2013).

5 Security concern of smart devices

IoT can also be defined as the interconnection of "*factual-and-virtual*" objects placed across the globe that are attracting the attentions of both "*makers-and-hackers*". IoT infrastructure can be divided into five different phases as mentioned in (Hu 2016) by Jeyenthi, as shown in Fig. 6. The first phase is termed as *data collecting phase* that is the primary interface between the physical environment and sensors. There can be either static objects like body sensors

PHASES	ATTACKS
Data Perception	Data Leakage, Data Authentication, Data Loss
Storage	Data Availability, Modification of Message, DOS, Attack on Integrity, Data Fabrication
Processing	Attack on Authentication
Transmission	Channel Security Attack, Session Hijacking, Routing Protocol Attack, Flooding
End-to-end Delivery	Man Induced or Machine Failure, Maker or Hacker

Fig. 6 IoT phases and possible attacks

or RFIDs or dynamic objects like sensors and chips on vehicles. The second phase is *storage phase* which deals with IoT devices having low self-storage capability and thereby provides a server or cloud-based storage. Next is *intelligent processing phase* that deals with the analysis of stored data and later on, appropriate services are provided to the users. IoT devices can be queried and controlled remotely using the results obtained after the processing of data. The fourth phase is *data transmission* that performs the processing of data communication between all the above phases. Finally, *delivery phase* has the activity of delivering the processed data to all the objects in time without being altered or hacked.

Among the five phases, the data perception phase is subjected to more attacks like data leakage, data authentication and data loss as the devices are easily available to users and hackers. Similarly, in the storage phase, we can see an attack on availability, modification of message, Denial of service (DOS) attack, attack on integrity, data fabrication. Attacks on authentication are seen at the processing phase and Channel security attack, session hijack, routing protocol attack, flooding are seen during the transmission phase. Lastly, at the delivery phase, man and machine-made attacks are found, as in the Fig. 6.

Likewise, there are various attacks based on layers of IoT, as shown in Fig. 7 (Ahemd et al. 2017; Ammar et al. 2018). *Sensing/Perception/Physical Layer* is made up of sensors, RFIDs, NFCs, ZigBee, Bluetooth and other intelligent hardware devices. These devices are exposed to more external attacks like node compromise attack, fake node injection, access control, RF interference on RFIDs. The second layer is *Internet Layer* and is subjected to attacks like address compromise attacks, routing information attack, RFID spoofing, sinkhole attack. The next layer is *Transport Layer* that experiences attacks like Denial-of-Service (DoS), masquerade, Distributed DoS (DDoS), Man-In-The-Middle (MITM) attack, session hijacking. And finally, the *Application Layer* experiences attacks like a phishing attack, viruses, worms, malicious scripting, revealing of sensitive

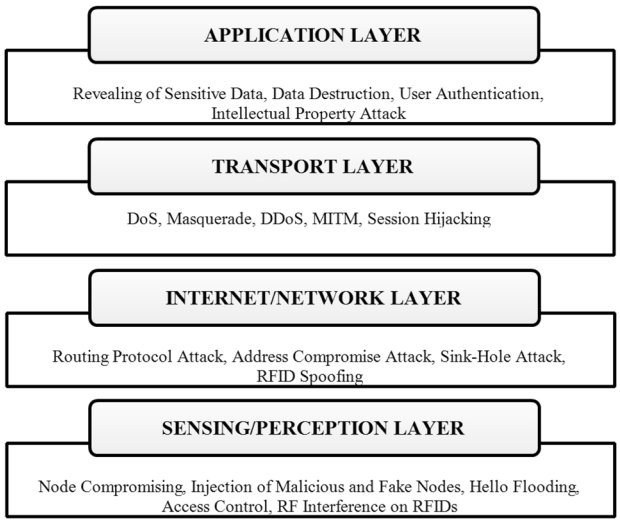

Fig. 7 IoT layers based attacks

data, user authentication, software vulnerability, intellectual property.

5.1 Security mechanisms in IoT

The security measures of IoT vary from conventional network security. For example, the installation of the IoT environment is unique when compared to other Internet-enabled applications. IoT deployment depends on Low power Lossy Network (LLN), where the devices are having low power, limited memory and are highly dynamic. These LLNs also experience a high amount of data losses due to the impersonation of nodes (Alaba et al. 2017). Each layer of IoT encounters various attacks as mentioned in the previous section. The various attacks on IoT layers have countermeasures like authentication, data integrity checks, secure booting, IPSec security channel and secure physical design to keep malicious users out of the IoT network. Later at the network layer, it is essential to provide data privacy to prevent illegal access to network components. And also by using Secure Routing protocols for LLNs (S-RPL) (Glissa et al. 2016) routing information attack can be prevented. At the transport layer, transport layer security (TLS) and secure socket layer (SSL) are used to avoid attacks (Styger). User authentications, access control lists, firewalls, anti-virus methods, risk management, are used to avoid attacks on the application layer (Zolanvari and Jain 2015).

5.2 Security threats, attacks and impact on IoT

Devices within the IoT communicate personalized data of many users like health information, bank details, passwords, location information and many more. These devices are subjected to *securirty threats* like (a) malicious node in the network, (b) defective manufacturer and (c) external adversary (Atamli and Martin 2014). These threats lead to security attacks that can be initiated either by nature or humans. The natural-threats may include earthquakes, floods, fire, and hurricanes that cause severe damage to the computer system. And it is hard to safeguard against natural calamities, and thereby it is advisable to collect a backup of data through a contingency plan to reduce the damage. Accordingly, the *security attacks* caused by the human can be classified as below (Abomhara and Kien 2015; Atamli and Martin 2014):

5.2.1 Information level attacks

All IoT devices are enabled with sensors that record the data from the physical environment and communicate the information over the Internet. As the Internet is an open domain, attackers can easily damage the information under the following categories (Conti et al. 2016; Stallings 2006; McAndrew 2016a):

- Denial-of-service (DOS): DOS is an attack over the network component that makes it be unavailable for an intended user.
- Masquerade: An intruder behaves as an intended user and tries to talk with the network component.
- Modification-of-message: An intruder can alter or delete or fake a message sent by a legitimate user.
- Man-In-The-Middle (MITM): MITM is a kind of attack wherein a malicious user takes control of the communication channel between two or more endpoints.
- Message replay attack: A malicious node stores the message without the knowledge of intended users and the malicious node transmits an altered message to the receiver.

5.2.2 Adversary location attack

An intruder can be present in any part of the IoT ecosystem. He can either be within or outside the IoT environment like (Nawir et al. 2016):

- Internal attack: An attack caused by the components within border of auntentication. Also called an insider attack where the intruder tries to inject malicious code towards the IoT components being a part of the network.
- External attack: An attack caused by an advisory that is located outside the IoT environment from a remote place.

5.2.3 Access level attack

Access level attacks are broadly classified into active and passive attacks (Nawir et al. 2016). In the *passive attack*, an attacker can read the packet that is transmitted, but he/she cannot alter the packets like eavesdropping and Traffic Analysis. On contradictory, in *active attack*, the attacker sees the data and alter the content of the data and transmits the altered data back to the network.

5.2.4 Host-based attack

Many devices in an IoT system are made up of different manufacturers (Nawir et al. 2016). These devices are subjected to user compromise attack, software compromise attack and hardware compromise attack. This is because the manufacturer can hold the devices' information which can be misused by him. Hence the production of such poorly secured goods results in compromising user privacy. At the same time, any manufacturer can attack his competitor through its devices.

Atamli and Martin (2014) have analyzed the impact of the above attacks on the IoT applications like power management, smart car and the smart health-care system. Through their study, they have projected that there is a need for security and privacy considerations at the level of (a) actuators, (b) sensors, (c) RFID tags and (d) the Internet/network. Attack on actuators in power management applications can lead to financial loss due to excessive power consumption. Similarly, in smart cars, these compromised actuators may control the brake system causing human casualty. Also, in the health-care system, these compromised actuators can inject the wrong dosage of medicine to a patient who is remotely monitored by the doctor. Likewise, a compromised sensor can fake the data that may lead to the wrong diagnosis of a patient. At the same time, these compromised nodes can reveal the personal information of the patient or the data related to a user's home through the power management system.

5.3 Security requirements

Smart network is composed of a large number of network components, which can be either of people-to-people (P2P), people-to-machine(P2M), or machine-to-machine (M2M), the concern of security is more. When two objects of such diverse network initiate to communicate over the public channel, the attackers can eavesdrop, replay, or alter the message. So some of the security requirements that the network security algorithms should possess are (Luhach et al. 2016; Babar et al. 2011):

SR1 *Confidentiality*, states that the data is kept secret from the unintended users. i.e., the data forwarded by the sender should be received by the intended receiver. Even if intruders hack the network, he/she must not be able to derive the actual data that has been communicated.

SR2 *Data integrity* is a process in which the data sent by a sender should reach the receiver unaltered. In other words, intruder should not be able to scramble/modify the data.

SR3 *User privacy* is required as IoT involves activities related to human beings and with the knowledge of their personalized information, hence providing security to such sensitive information demands more security concern.

SR4 *Non-repudiation* is a scenario wherein either sender or receiver deny to participate in the communication.

SR5 *Authentication* is a task of validating and verifying the user.

SR6 *Authorization* is a process that enables the authentic user to access the resources.

SR7 *Availability* ensures that the network must be operational in all types of circumstances. The network services must be available to all legitimate users even if the network is hacked by intruders.

SR8 *Access control* instruct the communication end point to be authenticated, i.e., the entities accessing the network should possess the authentication to access the network.

6 Lightweight integrity schemes

ECC was introduced in early 1985 by Miller (1985). They defined that the hardness of ECC security depends on the discrete logarithmic problem defined on the elliptic curve E_q. Later, Gura et al. (2004) experimented ECC and RSA on an 8-bit CPU to compare their performance and found that the use of ECC for a lower bit processor provides the same level of security as that of RSA. Later during 2013, Wenger (2013) developed an ECC based access control scheme over a prime field on 16-bits MSP430 micro-controller whereby the results confirmed the feasibility of ECC for resource-constrained devices.

ECCs are often implemented by using a static public elliptic curve that are shared among all the users in the network. In (SEC 2000) the recommended elliptic curve domain parameters are provided for the Weierstrass curve equation $y^2 = x^3 + ax + b$ that is followed by various researchers (Silverman 2009). Liu and Ning (2008) and Wenger (2013) have proposed software and hardware architecture for resource-constrained embedded devices. Their work has shown the feasibility of ECC on

the embedded system. But the use of a fixed elliptic curve can be challenged on intensive crypt-analysis. Wang and Cheng (2017) made a study on using a fixed prime field to build a crypto-system for applications developed for different processors varying from 8- to 256-bits.

To address the usage of the static curve in ECC, Wang et al. (2018) proposed a dynamic elliptic curve based on Internet-of-Vehicular (IoV) network. Their work showed good computational efficiency and security for a smaller key size. But storing the elliptic curves as a plain text in embedded systems would lead to security concerns. To address the data integrity issue of Java card-based application, Gayoso Martínez et al. (2011) initiated the use of ECC based encryption algorithm called an elliptic curve integrated encryption scheme (ECIES) and concluded that ECIES based encryption is best among encryption schemes for resource-constrained devices.

Lin et al. (2018) proposed a two-tier device-based authentication protocol for primary user emulation attack (PUEA) for IoT applications. Their work used a spectrum management method to guard against common types of security threats. They have proposed that the work can be extended to movable objects based on the detection performance to increase the reliability of the protocol. Tiwari and Kim (2018) have used Deoxyribonucleic acid (DNA) and ECC to provide double folded security for mobile and cloud-based applications. They have used Kobliz's algorithm to choose the elliptic curve and compared the results with RSA based schemes.

Uninterrupted and accurate functioning of IoT devices in smart city applications is a crucial task. Such applications have major challenges to ensure the authenticity of devices so as to make better decisions. Hence to balance the performance between efficiency and communication cost, Li et al. (2017) have designed a lightweight mutual authentication protocol based on public-key encryption scheme for smart city applications. They have evaluated their work on a Contiki OS and CC2538 evaluation model. The encryption process was performed offline and then the ciphertext was subjected to an authentication process that was done online. This online and offline process of the digital signature consumed more time and created overhead on the node's resources. Parrilla et al. (2018) had designed a compact crypto co-processor for FPGA based IoT devices. This co-processor uses elliptic curve cryptography (ECC) with advance encryption standard (AES) and group keys. The proposed processor ensures the security of wireless sensor networks independent of the communications protocols used. The crypto-processor is named as ECC163AES128 as it can handle symmetric cipher with 128-bits and ECC cryptography over GF(2163) binary filed. The developed crypto-processor provides the security of heterogeneous local Wireless Sensor Networks composed of IoT devices, independently of communication protocols.

A simple block-cipher-based message authentication encryption scheme is proposed by Mazumder et al. (2017). The system takes variable message size as input along with the initial vector (IV). The use of nonce and associated data is replaced with the concept of IV to reduce the overhead incurred due to nonce. A block-cipher based compression function is used with the OFB model of encryption as the system encrypts variable size of data, padding of the message is removed, which reduces communication overhead. But the entire work is studied under serial communication of the participants, which is not feasible for IoT based applications where each device can communicate parallel to each other or/and the base station.

Shivraj et al. (2015) have proposed a one-time password authentication scheme based on ECC for IoT. They have handled the end-to-end authentication of devices and their application. As these end devices have dynamic topology and non-standardized framework has led the security concern of IoT devices and applications; hence a two-layered authentication is proposed. They have used lightweight identity based elliptic curve cryptography with Lamports OTP algorithm with smaller key size and limited infrastructures. When compared with existing schemes like Hashable OTP (HOPT), Time based OPT (TOTP), Bicakai OTP (BOTP) methods, their proposed scheme reduced the storage overhead on the devices as past keys were not being stored.

For the vehicular network, providing PKI based security is difficult. Tan et al. (2016) has proposed a secure authentication key management protocol that maintains a list of keys bonded to the entitys identities. These entities can either placed on road-side or vehicles. SA-KMP used 3D-matrix based key agreement scheme with symmetric encryption. The use of symmetric encryption has reduced the high computational cost and the performance is analyzed in terms of transmission and storage overhead, network latency and key generation time. They have used ProVerif tool to prove the method under Dolev and Yao mode to check the system against DOS, collision attack and wide range of malicious attacks. Through numerical analysis, the SA-KMP scheme has shown good efficiency and scalability than the existing certificate-based PKI schemes.

To handle the overhead that occurred due to runtime, firmware size, communication and energy consumption on an ARM-based device, Mössinger et al. (2016) has proposed ECC based signature scheme. They have considered Secp192r curve parameters with 192-bits key length. The work provides proof against message integrity via cryptography that is greater than the cost of encryption. They have found that the amount of sending unsigned messages created two-third of overhead that the cryptographic operation against the signed message. The work was simulated using

Contiki OS through which they have shown the performance of additional 200 ms of the runtime.

The most commonly used communication medium in healthcare is RFID. Basically, RFID based security scheme uses either a hash function or symmetric key encryption. Zhao has analyzed the method proposed by Liao and Hsiao and found that the private keys stored, are easily hacked. Hence to overcome the private key compromise attack, an authentication protocol for Healthcare Environments Using Elliptic Curve Cryptosystem is proposed by Zhao (2014). Through security analysis, the proposed scheme has shown better performance than Liao and Hsiaos method. Le et al. (2009) has presented a public key-based access control mechanism using ECC. The work is compared with HBQ and symmetric key encryption and uses online KDC. Through the result analysis, its been proven that their work has shown resistance to a drawback of the HBQ scheme. But the use of online KDC has led to the issue of network breakdown in case the Internet goes down.

For automatic control application (AAC), Li et al. (2014) has provided an attribute-based encryption (ABE) key management to develop a privacy-preserving protocol (P3). The P3 protocol is based on ciphertext policy attribute-based encryption (CP-ABE) and Rivest Shamir and Aldman (RSA) public-key encryption algorithm. Their work used a key revocation scheme to generate a periodic batch rekeying strategy that is apt for resource-limited smart meters. The ABE revocations reduce the vulnerability window, authorize the legal activities of smart meters and cover the privacy for both the control server end and appliance end. An effective multifactor authentication method is proposed by Ahmed and Ahmed (2019) that uses combiner hash functions. Their work achieves collision resistance, pseudo-randomness and one-way properties of hash functions. But they lack in providing complete encryption and decryption solution for IoT applications.

Pan et al. (2017) has proposed an ECC based server called GUESS, which is implemented under the key size of 256-b on a Linux platform. GUESS is used for a heavily loaded application like e-commerce and other online transaction required authentication. Also, GUESS supports various categories of ECC schemes like DSA, key agreement and encryption. In the near future, the GUESS server is checked for side-channel attacks. To protect the patient data, Farash and Sabzinejad (2014) developed HiDE to provide a hierarchical clustered based framework that as a backbone cluster with several area clusters. Under this setup, there is an area cluster having a secure access point (SAP) that collects the data and aggregates to the root SAP located in the backbone cluster. HiDE is used to establish a secure session between each pair of cluster head and cluster members. Hence HiDE has maintained the confidentiality of sensitive medical data with low computational overhead.

A review of ECIES is done by Bernstein et al. (2013). The ECIES use both symmetric and asymmetric cryptography that provides double-level security. The analysis is done on the Java Card and the performance evaluation has concluded that encryption using ECIES is best. Based on card shuffling-logic, a data confidentiality algorithm is designed using ECC by Rahaman (2017). The use of random card shuffling has exhibited double encryption and increased the security of the scheme. In this work, they have removed the mapping process of every alphabet to corresponding ASCII values of the plain text to be paired up. The algorithm can encrypt or decrypt any ASCII value-based input. The use of ECC has proved that the algorithm is suitable for resource-constrained devices.

The integration of IoT and cloud has taken a major share in the communication industry. As the IoT infrastructure needs to combine with cloud, the existing infrastructures exhibit difficulty in ensuring distributed computing. A Internet Protocol/Multiprotocol label switching (IP/MPLS) based security framework using ECC is proposed by Bai et al. (2015). Their framework ensures the protection against security risks like confidentiality, integrity and authentication and privacy is used. The model has eliminated ambiguity and has shown that a smart card-based application for the evaluation process has shown that in the future, there can be one smart card per citizen that can be used anywhere, anytime. The multifactor authentication and message encryption have ensured the CIA requirements.

To an IP-based communication technology of smart grid applications, Mahmood et al. (2016) have proposed a lightweight authentication scheme. They have used RSA and AES algorithm to develop a hybrid Diffie-Hellman based lightweight authentication scheme. Li et al. (2018) have presented a study on ciphertext-only fault analysis (CFA) on light encryption device (LED). The analysis is done for LEDs like square Euclidean imbalance (SEI), the goodness of fit (GF), the goodness of fit-square Euclidean imbalance (GF-SEI), maximum likelihood (ML), hamming weight (HW) and maximum a posteriori (MAP) distinguishers. Their CFA method took about 152 ciphertexts and 304 ciphertexts to recover the 64-bit and 128-bit secret keys of LED, respectively. Through this study, they were able to analyze the threat of CFA over IoT.

A stateful based forwarding stores the routing information on forwarding state table. Such storages create overhead on the devices and also is susceptible to "varietal" Denial-of-Service expected to occur due to complicated forwarding state operations. Liu et al. (2019a) have proposed an enhanced distributed low-rate attack mitigation (eDLAM) mechanism. eDLAM stores a lightweight malicious request table (MRT), which is very small and removed the burden over the resource-constrained device that incurred during the forwarding state table. Wang et al. (2019) has designed

a secure, lightweight entity authentication scheme for hardware primitive called SLATE. SLATE is a challenge-response based verification system that has shown efficiency against the exiting lightweight ciphers. SLATE is resistant to logic obfuscation and Boolean satisfiability (SAT) attacks under theoretical information analysis.

7 Lightweight authentication schemes

For smart dust based resource-constrained devices, Lee et al. (2016) have designed an energy-efficient authentication scheme. Their scheme ensures lightweight mutual verification and key exchange mechanism. They have used a simple hash calculation and certificate framework to support devices with limited hardware resources. For the existing security configurations of IEEE 802.11x, (Kim et al. 2017) designed an authentication and key management scheme (AKM) for IEEE 802.11ah based IoT communication. The design was able to delegate the burden of AKM processes to a station-side authentication server (SAS). The IoT devices delegated the burden of AKM to SAS and had to just verify the authenticity with an access point (AP) using basic encryption and decryption. Such delegation showed better performance by reducing the authentication workload of the access network.

For applications involving a long period of time like healthcare, industrial automation system and public facilities management, Kim et al. (2016a) have proposed a session key establishment based scheme for a clustered sensor network by using ECDH key exchange and hash chain. It showed resistance against session key attack, node impersonation attack, reply attack and node capture attack. It showed the main advantage of storing the past and future session keys in a repository. But on the real-time work model, these processes consumed device memory space and created overhead on the device. Similarly, for a health care based IoT application Chen et al. (2017) has provided a solution to secure the patient's privacy. The devices placed over the patient's body undergo many physiological movements and are subjected to collect a lot of data. Hence when a doctor wants to access this data through remote login, the patient has to authenticate the doctor. To enable the privacy of user identity, Yuwen et al., have designed a scheme where a gateway knows the shared keys and these keys are shared using ECDHA to maintain key secrecy.

Chung et al. (2015) have proposed a novel anonymous authentication scheme that uses the virtual identification for the IoT devices by ensuring anonymity and authentication. By keeping the uniqueness and virtual identities, they are providing untraceability of devices. This scheme has helped them to withstand replay attack, forgery and impersonation attacks; they are using common and specific keys that make the system more complicated. Even if the common key is leaked or forged, it is difficult to find the specific key. Hence by using collision-free one-way hashing and XOR operations, they are able to provide considerable fast computation.

For an RFID based application, John and Thampi (2016) have implemented mutual authentication using hybrid ECC (HECC). The hardness of the proposed method was in solving the hyper-elliptic discrete logarithm problem (HCDLP) that provides security over eavesdropping from breaking into the cryptosystem. They have used a D-Quark hashing algorithm. HECC is used to exchange the symmetric keys between the communicating parties. Pereira et al. (2016) has evaluated the proposed method using AVR low-power micro-controller ATmega-128l controller and have shown the proposed method is suitable for resource-constrained devices. The proposed Hash-based signature scheme has shown resistance against pre-image resistance due to the adoption of randomized hashing using a particular nonce.

Wazid et al. (2018) have designed a secure authentication scheme for hierarchical IoT networks (HIoTN). HIoTN is made up of different nodes, gateway nodes, cluster head node and sensing nodes arranged in a hierarchical manner. For such a network, they have proposed a three-factor remote user authentication scheme for HIoTNs called user authentication key management protocol (UAKMP). UAKMP uses the smart card, password and personal biometric entities to provide three-tier user authentication. Even though UAKMP is proved to provide security against known attacks through simulation, they were unable to show the same performance on a real-time based scenario with resource-constrained devices.

Le et al. (2009) discussed the issues of mutual authentication problems in mission-critical applications related to WSN. They present an ENergy-efficient Access control scheme Based on ECC (ENABLE). The performance of ENABLE is compared with HBQ[Enable-4] and symmetric key based schemes on SENSE simulator under AODV protocol that showed ENABLE provided better scalability with lesser memory requirement and no key predistribution. As they have used online KDC, if the Internet goes down, providing access control would be difficult.

In a cognitive IoT architecture, there are security concerns over the radios, hence Lin et al. (2018) have proposed two-tier device-based authentication schemes. This setup has helped them to explore the tradeoff between the detection of malicious node and spectrum management. But by developing a joint spectrum allocation and topology control, their system could be extended to real-time sensing through which they could reduce the end-to-end delay and control the network access. Using an iterative MerkleDamgard (MD) hash function, a lightweight signing and verification method was proposed for IoT applications.

Based on the challenge-response phase of physically unclonable functions (PUF) of IoT devices, Aman et al. (2017a) have proposed a mutual authentication scheme for communication between a device and server and between two devices. The challenge-response method was also used for session key establishment. Even though their system showed improvement in their performance, the latency of authentication was more due to the number of messages exchanged between the entities were increasing with every session created. For the WSN environment, Lavanya and Natarajan (2017) proposed a lightweight authentication scheme using mBLAKE2b as hashing method for ECDSA based authentication scheme. Their method was studied for performance parameters like energy consumption, throughput, latency, packet delivery ratio and signature verification using the NS-2 simulator. The security of the method was evaluated using the SCYTHER tool. Through the result analysis, they have shown a better performance of the authentication process when compared with traditional authentication schemes.

The standard methods to provide user authentication are password, tokens or biometrics. But these methods also possess security issues. Hence, Srinivas et al. (2017) has introduced a new method called biohashing. Biohashing eliminates false acceptance rates without an increase in the occurrence of false rejection rates. This scheme supports user-friendly password reset and dynamic node addition. Under BAN-logic, their scheme has shown mutual authentication between the nodes and also, under the AVISPA tool, they were able to test for man-in-the-middle(MITM) attack and replay attack. But their scheme possessed limitations in lack of dynamic identities for large growing IoT networks. Based on a one-time-password (OTP) based security scheme, Shivraj et al. (2015) have proposed a security scheme to ensure end-to-end authentication between various IoT devices. They have used a lightweight identity-based ECC scheme and Lamport's OTP algorithm. With the argument of having a two-factor authentication scheme, their experimental proof has shown significantly better performance than existing standby OTP algorithms. But they are unable to provide the same efficiency for a widely spread IoT network as generating OTP simultaneously for many devices is infeasible.

Kumar et al. (2016) have proposed the ECC-based Access Control Protocol (ACP) solution to prevent malicious nodes from eavesdropping the network and also to protect the node privacy. During the comparative study of their scheme, the time taken by ACP in computing point multiplication is much lesser when compared with existing protocols and energy consumed during the multiplication is also less. They have concluded that their method is feasible for access control and privacy of the node. But they have failed to address the data integrity of the wireless sensor network-based application. But providing integrity on sensed data is the major concern of a secured IoT system. To overcome the shortcoming of Mun et al. scheme, Zhao et al. (2014) has proposed a unique anonymous authentication scheme for global mobility network (GMN). BAN logic is used to validate the authentication of the scheme. The scheme does not use time-stamp; hence clock synchronization problem is overruled. The scheme ensures authentication and establishes a session key when the user is in the home network. The efficiency of the scheme has proven for low-power and limited resourced mobile devices.

To address the issues related to scalability and resilience to the node compromise attack, hop-by-hop message authentication, and source privacy is proposed by Le et al. (2009). As the polynomial based scheme has the issue of when a number of message transmission is larger than the threshold, the message can be easily cracked by the hacker. Thereby, the ECC based authentication method is proposed that ensures message source privacy. They have presented an unconditional secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified Elgamal signature (MES) scheme on ECC. The scheme authenticates every intended node and ensures to identify the corrupted message and sources. To setup a secure communication channel between sensor nodes and the Internet host, a heterogeneous online-offline signcryption method is proposed by Li and Xiong (2013). The work has shown resistance against adaptive chosen ciphertext attack under Bilinear Diffie Helman Scheme and unforgeability against the chosen message attack. The online phase does lighter computations using the message and in the offline phase, the heavy computations are done in the absence of a message. The work has fulfilled CIA and non-repudiation properties.

Lee et al. (2016) have suggested lightweight mutual verification and key exchange method for smart dust applications of wireless sensor networks based on the IoT environment. In their work, they have used the group signature scheme where each sensor node elects a middle node (MN) and transmits the data collected in the one-hop communication model. In the course of the MN election, the node having more existing resources is selected and complex calculations are performed in MN. During authentication and smart device registration, gateways verify the smart nodes through CA. The security and energy verification of the method is performed through functional evaluation. But their work showed drawbacks while updating the group keys of subminiature devices as they are resource deficit in nature.

Lu et al. (2017) proposed a heterogeneous data aggregation scheme called lightweight privacy-preserving data aggregation (LPDA) scheme. LPDA is implemented using the Chinese Remainder Theorem, homographic Paillier encryption scheme and one-way hashing techniques.

Their scheme was successful in identifying false data and aggregate hybrid IoT devices data. The proposed scheme is not evaluated for the security of the adversary model. In health-care based IoT applications, wearable sensors transmit the data to the server that helps the doctors to obtain information using Telecare Medical Information System (TMIS). As these data transmission between patients and doctors needs continuous authentication, a secure authentication and prescription safety (SAPS) protocol is developed by Mahmood et al. (2017). A secure three-party key establishment scheme is developed to provide security between doctor and patient during the prescription of medicine. The process begins when the patient registers with the trusted server and obtains the validation before establishing the session key. The SAPS protocol is analyzed for security using Rubin Logic and exhibited properties like verification, user anonymity and untraceability of the patient in TMIS.

The use of a chaotic map with ECC based cryptosystem has helped to enhance the security of authentication. During recent research, the existing research has shown lacking security concerns. To improve the security of authentication protocol for resource-constrained devices, Kang et al. (2016) have proposed a Markov Chain based authentication that has shown more security efficiency than the existing. The work is in comparison with Djellali et al. (Djellali et al. 2015) which uses Markov Chain for ubiquitous devices. The work is extended to scalable and changeable networks like the multi-server environment and the cloud services system. They have proved a theorem of not saving the verification table, which leads to passed verification drawbacks in the registration phase. Internet Engineering Task Force (IETF) has proposed a standard communication protocol called Internet Protocol version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) for enabling the communication of machine-to-machine communication. Qiu and Ma (2016) has proposed a hybrid scheme called enhanced mutual authentication and key establishment scheme (EMAKES) for such 6LoWPAN networks. They were able to show resistance towards replay attacks, man-in-the-middle attack, impersonation attack and Sybil attack using Protocol Composition Logic (PCL).

To address the security and privacy issues under smart grid applications, Afianti et al. (2019) has proposed a novel method using a dynamic cipher puzzle (DCP) called multi-DCP (M-DCP). M-DCP uses RC5 encryption with the elliptic curve digital signature algorithm (ECDSA) to ensure the integrity and authenticity of the user. Also, the DCP hash function was modified with Merkle Hash Tree and chain based hash table. But performing double hashing during the time of new node addition gave computational overhead on the devices and such a setup would be infeasible for real-time evaluation.

To provide energy efficient authentication for IoT devices, Aman et al. (2017b) has proposed a lightweight mutual authentication protocol that uses Physically Unclonable Functions (PUFs). The protocol is evaluated for two different scenarios, firstly, communication between the device and the server and secondly, communication between the devices. Their protocols work on a challenge-response mechanism using PUFs and stores the secret values of each IoT device with the server. Such storing reduces the performance of the device as it has to constantly request the server for the secret values before initiating the communication with other clients.

In the heterogeneous environment, the attacker is prone to impersonate legitimate users. To solve the impersonate attack, a lightweight anonymous authentication and key agreement scheme are proposed by Liu et al. (2019b). Their proposed method can toggle between the public key infrastructure (PKI) and certificateless cryptography. Through security analysis, the method can resist replay and DOS attacks and has shown good scalability. A certificate revocation scheme (CRS) is proposed by Mahmoud et al. (2015) for smart grid-based applications under the vehicle network (Automatic Metering Infrastructure-AMI). The method uses certificate revocation in pseudonymous public-key infrastructure (PPKI) -here a large number of certificate public and private keys are assigned to nodes. The work showed efficiency for vehicle grid application. But not suitable for other IoT applications.

As the user and the smart devices communicate over the insecure communication channel, the sensitive data that is traveling across the channel are subjected to security and privacy concerns. To avoid such issues, Shuai et al. (2019) has proposed an anonymous authentication system using ECC for smart home applications. Their scheme avoided the storage of verification tables for the authentication process and used a random number method to resist replay attack and resist clock synchronization problems. They have performed security analysis using the random oracle model and BAN logic. Also, the verification of the method is verified using ProVerif tool, under which they were able to show secrecy of the session key and achieve mutual authentication successfully. To enable direct device-to-device communication, Dang et al. (2020) have proposed a ECC based lightweight authentication scheme. Their scheme provides secure data transmission between cloud server to devices and also between devices too. The protocol is formally evaluated using BAN-logic and shown the resistivity against common security attacks.

8 Lightweight hash functions

Federal Information Processing Standards (FIPS) proposed hash function that took variable data size as input and produced a fixed size of output (McAndrew 2016b). The

cryptographic hash function generates a condensed representation of the message. These hash functions have two major properties like, one-way hash function and collision resistance. The one-way hash property, it is defined as, if *H(m)* is known by the adversary, it should be impossible to extract the message "*m*". Collision resistance is a property where no two hash values should be same i.e., $H(m) \neq H(m')$. Because of these properties, hash function are used in various applications like message authentication, digital signatures, one-way password file, intrusion detection, virus detection applications (Center 2018).

The commonly used hash functions are message digest (MD5) and secure hash functions (SHA). During 1993 National Institute of Standard and Technology (NIST) published SHA under FIPS-180-4 specification. FIPS-180-4 has seven variants of SHA-1 and SHA-2 family has algorithms of SHA-224, SHA-256, SHA-384, SHA-512, SHA2-224, SHA2-256 and SHA2-512 (Center 2018). Later in 2012 at SHA competition, FIPS proposed the need of an alternative for SHA-2 as SHA-3: Standard Permutation-based Hash and Extendable-output Functions (FIPS-202). SHA3 has four fixed-length hash algorithms as SHA3-224, SHA3-256, SHA3-384, and SHA3-512 (NIST 2018; Dworkin 2015).

At the Cryptographic Hash Algorithm Competition along with SHA3, BLAKE was also among the top five finalists proposed by Jean Philippe Aumasson, Luca Henzen, Willi Meier and Raphael C (Aumasson et al. 2008; Hao 2014). Even though BLAKE was not selected as SHA3 finalist, it has its own high-security margins and good performance. Ever science BLAKE is proposed it has attracted considerable applications in resource-constrained device security. BLAKE is built on a widely known hash structure called HAsh Iterative FrAmework (HAIFA) that has round iterations schemes, local wide-pipe internal organization and a compression function under modified Salsa20 stream cipher. BLAKE-256 produces 256 bits hash digest working on 512 bits state with 32 bits size of internal word (Hao 2014). Core BLAKE block transformation combines 16 words of input to 16 working variables and it has 14 or 16 rounds with four steps based on BLAKE-256 or BLAKE-512, respectively.

During the course of research, BLAKE showed a better performance with respect to speed and space complexity. This was proved on Qualcomm's krait micro-architecture, during which SHA3-256 took about 20% longer than SHA-256 and SHA3-512 took twice the time of SHA-512. But for the same platform, BLAKE-512 outperformed SHA-512 by showing 1.41 times faster than SHA-512 and BLAKE-256 showed 1.70 times faster than SHA-256. BLAKE-512 performed 5.76 cycles per byte, which is approximately 579 KB per second against 411 KB of SHA-512 on a CPU clocked at 3.5 GHz (Aumasson et al. 2013). Later, Preneel (Preneel 2010) observed that BLAKE's security and efficiency could be ruled out with an extensive crypt-analysis. Thus he pointed the need for improved BLAKE and hence proposed a new version as BLAKE2 that used 32% less RAM when compared to BLAKE and has less overhead with minimized padding. To provide user authentication using a password, tokens, or biometrics has raised an issue regarding password or token being stolen or forgotten. To handle such conditions, Srinivas et al. (2017) has proposed a new biohashing based authentication and key agreement scheme to eliminate the false accept rate. They have simulated the work using AVISPA tool and shown resistance against MITM and replay attack. Their work uses the BAN logic to ensure mutual authentication. The work supports dynamic node addition and user-friendly password change.

9 Security analysis of lightweight cryptography

A statistical analysis of different ECC based authentication and key exchange protocols are subjected to security analysis and threat modeling by Roy and Khatwani (2017). They have provided the vulnerability of ECC based cryptosystem under attacks like MITM, clogging attack and database. Hence is it essential to add additional defense layers to guarantee the security against the suspected attacks. An ECC based Lightweight authentication protocol with key agreement protocol is proposed for smart-card based IoT applications by Reddy et al. (2016). Their protocol involves a one-way hash function, message authentication code and exclusive OR operations. The work is resistance against replay attack, clock synchronization problem, smart card stolen attack, insider attack, user impersonation attack. It also provides forwards secrecy, two factor authentication and mutual authentication. RFID based automated patient medication system has taken a major share in the health care industry. Zhang and Qi (2014) has presented an ECC based authentication system. Through the theoretical proof, their work has shown resistance against tag-information privacy, tag-anonymity, backward-traceability and forward-traceability, tag impersonation attack, spoofing attack and DOS attack. A hybrid elliptic curve based multi-message signcryption is designed by Rahman et al. (2018). The work is evaluated for security requirements like replay attack, integrity, authentication, non-repudiation, public verifiability, forward secrecy and unforgeability, using AVISPA tool.

The combination of cloud-based services with IoT has raised to the limitations regarding low-latency and high mobility of the application. To handle the latency and mobility limitations, a fog based environment is deployed remotely that are susceptible to security attacks. Hence for a health care based Fog-IoT, an authentication scheme is proposed by Jia et al. (2018). The three-party bilinear key-agreement protocol is proposed that is resistive against

MITM, replay attack, known-session key attack, and intractability. The WSN applications of IoT are designed to use a pair-wise key, which is used for the long term in the process of communication. As these pair-wise keys have a long lifetime when being hacked, the data can be altered, and the privacy of the user can be questioned. To reduce such an impact on the device, a session key based key exchange is developed by Kim et al. (2016b). In this work, an elliptic curve Diffie–Helman (EDHA) based session key exchange is proposed for clustered based sensor networks. To provide the authentication for the participanting entities, the hash-chain is used between the gateway and the cluster head. Through the proposed method, the number of communicating messages is reduced and has provided security against MITM attacks, session key attacks, replay attacks, node impersonation attacks and node capture attacks.

A multi-factor remote login based authentication method is proposed by Dhillon and Kalra (2017). This method is a combination of three different authentication mechanisms like password-based, biometric and smart devices. The biometric-based authentication has complied with Discrete cosine transform (DCT) and Principal component analysis (PCA) based hashing function. Under formal and informal security analysis, the proposed three-factor authentication has shown resistance to attacks like password guessing attack, password change attack, parallel session attack, denial of service attack, stolen smart device attack, and impersonation attack. Annor-Asante and Pranggono (2018) has designed a real-time test-bed that is created using the Arduino Uno and Xbee module to check the resistance of smart grid application against Distributed Denial-of-Service (DDoS). They have developed cyber-security software with SCADA and PLC programming for the evaluation of cyber-security research.

As the Wireless Body Area Network (WBAN) based application carries sensitive data of the patient and any incorrect data of the sensor reading into the server, it can lead to severe wrong diagnostic by the doctor. Thereby, Wu et al. (2016) have proposed an anonymous authentication scheme that provided mutual authentication and privacy preservation along with session key generation for data encryption. Their work is in comparison with existing Wang and Zhang (2015), which showed a drawback in providing an impersonation attack between adversary or a legal client and another legal client. But the authentication proposed by Libing Wu et al. has not shown the resistance towards eavesdropping and chosen-ciphertext attacks.

An inter-device authentication and session key sharing scheme is proposed by Park and Kang (2016). To overcome the drawbacks of the key distribution center (KDC) sharing the session keys to all the participants, they have made each participant generate their own session keys. Thereby each device involving the network communication shall share their session keys to the KDC prior to communication. Their scheme is resistant towards attacks like replay attack, MITM attack and wiretapped secret-key attack. But the scheme lack the security of the session key, which sharing with the KDC, i.e., if the session key KIR is compromised, the whole device could be hacked. In a large-scale system communicating over LTE, the network is skeptical about data security and user privacy. For such an environment, Saxena et al. (2016) have proposed an authentication and key agreement (AKA) protocol. They have used sequence numbers for each authentication package instead of MAC verification information and shown resistance against chosen message attack, key secrecy and theft, MITM attack, replay attack and impersonation attack.

In machine-type communication devices (MTCDs), the communication is based on LTE/LTE-A network, the MTCDs access the network simultaneously and each MTCD has to be independently authenticated with the network base station. During such a simultaneous process, there maybe be congestion and signal overhead on the network. To avoid these issues, Fu et al. (2016) has presented a group authentication mechanism that reduces signal overhead and provides robust privacy-preserving for each MTCD along with anonymity, unlinkability and traceability. Their method is evaluated using ProVerif tool and the method has shown resistance against DoS attacks, MITM and impersonation attacks. In multi-server based mutual authentication schemes, the user must log in separately for each service and remember the login credentials like multiple identities and passwords. Such an environment is inclined to password guessing attacks, MITM, eavesdropping, replay attacks. To avoid such attacks, Tomar and Dhar (2019) has designed a multi-control server environment that uses the user's biometric and password to authenticate them. The ECC is used to strengthen security. Through informal security analysis using Burrow–Adabi–Needham (BAN) logic and fuzzy extractor, their work has shown resistance against DOS attacks, MITM attacks, replay attacks and stolen smart card attacks.

To a wearable devices based application, Kumar et al. (2019) has proposed an ECC based authentication scheme. They have verified their work using ProVerif tool and shown resistance against known attacks. As the user and the smart devices communicate over the insecure communication channel, the sensitive data that is traveling across the channel are subjected to security and privacy concerns. To avoid such issues, Shuai et al. (2019) has proposed an anonymous authentication system using ECC for smart home applications. Their scheme avoided the storage of verification tables for the authentication process and used a random number method to resist replay attack and resist clock synchronization problems. They have performed security analysis using the random oracle model and BAN logic. Also, the

verification of the method is verified using ProVerif tool, under which they were able to show secrecy of the session key and achieve mutual authentication successfully.

To overcome the reusing of existing protocol for IoT based applications, a CoAP based bootstrapping method is designed and implemented by Garcia-Carrillo and Marin-Lopez (2016). The Extensible Authentication Protocol (EAP) and Authentication Authorization and Accounting (AAA) technologies are used to ensure flexibility, scalability and accountability. They have compared the proposed design by implementing it under Contiki and PANATIKI tools and have analyzed the work under memory footprint, data processing time, message length, bootstrapping time and energy consumption. They are unable to check the proposed method under real-time Low Power Wide Area Network, which has smaller message sizes and also security over post-bootstrapping is not shown.

For the authentication of mobile-based communication Li (2012) had proposed a scheme with roaming services and user anonymity. However, an attacker could intercept the identity of a mobile user's home agent, Chain et al. (2016) have proposed an elliptic curve-based wireless roaming anonymous login method that resolves the issues of Li's scheme. They have used Burrows–Abadi–Needham (BAN) logic for analyzing the security of their authentication scheme.

For smart meter based application, Garg et al. (2019) has proposed a mutual authentication based key exchange mechanism using ECC. They have performed formal security analysis and proved the resistance against DoS attacks, replay attacks, impersonation attacks. With mutual authentication, the forward secrecy is also maintained. Further, the security analysis is studied under two different categories. Primarily, a study of existing authentication scheme under theoretical proof is analyzed and later, a various real-time testbed for performing attacks on a Raspberry Pi-based network is briefed.

9.1 Theoretical security analysis

Over the past three decades, many security protocols, frameworks, and technologies have been developed to evaluate real-life security solutions for various networks and domains. Matsuo et al. (2010) have proposed a framework that includes protocol design and protocol certification. They have studied various formal verification methods under three different categories; the first study is done under the capacity of the method used, second is based on various skills needed by the designer to evaluate, and lastly, a question-answer based security requirements. Using the inductive approach provided by Paulson (1998) has further sub-classified their work under model checking and theorem proving. The model checking is a form of algorithm verification, and in theorem checking, proofs are established using higher-order logic. Also, they have mentioned about few model checking tools like AVISPA, CryptoVerif, ProVerif and SCYTHER as the second option for formal method analysis.

Rubin and Honeyman (1993) have used Meadow's classification (Meadows 1992) of analysis to categorized the verification model into four types. Type-I uses specific language and tools that are not designed for cryptographic protocols. Type-II helps to develop a system that can be used by a designer to develop and investigate different scenarios/cases. Type-III use knowledge and belief strategy to analyze the model logically. Lastly, Type-IV uses algebraic terms and equations to rewrite the cryptographic system. Zhu (2003) has developed a scheme that provides the security of ECC against the adaptive chosen message attack (ACMA). He has used decisional Diffie–Hellman assumption to prove the ACMA.

Nam et al. (2014) have extended Bellare, Pointcheval and Rogaway (BPR) (Bellare et al. 2000) to evaluate the user anonymity property and two-factor security. They showed that their model could capture insider attacks, an offline dictionary attack with security properties like authentication, perfect forward secrecy, known-key security, session key and resistance against insider attack. The security properties were proved using elliptic curve computation Diffie–Hellman (ECCDH) assumptions. Chen et al. (2015) have proposed a two-way user authentication and secure session key agreement scheme based on a self-certified public key system. Through their formal security analysis, the proposed scheme showed resistance towards attacks like impersonation, known-key security, masquerading, forward and backward secrecy, MITM and replay attack.

9.2 Real-time security analysis

Featuring the rapid growth of smart cities, Al Barghuthi et al. (2017) has made a study of how the increase in the population of smart cities shall add to an increase in the security breach and damage the business by 2050. Thus, they have proposed Kali Linux based vulnerability assessment and penetration testing solution using low-cost Raspberry Pi-3 devices. Through their results, it has been concluded that Raspberry Pi 3 can be used as a machine to check the vulnerability check similar to any traditional PC or laptop-based Kali Linux machine.

To replace the expensive and resource-intense devices used for industrial vulnerability and assessment tests, Hu et al. (2016) has proposed an automated vulnerability assessment using OpenVAS and Raspberry Pi-3 device. They have detailed methods for analyzing the vulnerability assessment of distributed architecture. They have made the study on variables like CPU temperature, CPU usage and CPU memory of the device at the time of vulnerability assessment.

Visoottiviseth et al. (2017) have developed a GUI based penetration testing tool called PENTOS used for IoT devices. PENTOS runs on Kali Linux and is specifically designed for the ethical hacking of wireless communication like WiFi and Bluetooth. PENTOS enables the analysis of password attack, web attack and wireless attack that ensure to gain access privilege of the various algorithms. They also have explained the Open Web Application Security Project (OWASP) specified ten vulnerabilities of IoT applications. Finally, they have given the recommendations for the secure deployment of the IoT environment.

Denis et al. (2016) have performed various penetration testing using tools available on Kali Linux. They were able to set up a private network and generate attack reports and visualize the reports using Kali Linux tools. The attacks they performed were hacking phones, MITM attack, smartphone penetration testing, spying, hacking phones Bluetooth, hacking WPA protected and then hacked the remote PC using IP and open ports.

Liang et al. (2016) have experimented on different methods of doing DOS attack using Raspberry Pi based Kali Linux. They have provided an attack framework and compared various DOS attacks on their framework. They have used Hping3 with random IP, SYN flood with sproofed IP and TCP connect flood tools. The comparison was made under the parameters like CPU utilization, memory utility, time for the success of an attack and packet loss rate. Murray (2017) has proposed a forwarded looking approach for a secure eHealth solution called HealthShare. That could share data among various organizations that were hosting the patient's data over the cloud. He has provided detailed steps as to conduction of MITM and DOS attack using tools like Ettercap, Pexpect, manual SET, threads using the timer and Nmap timer and Scapy.

10 Threat modeling for smart applications

Threat model (TM) is a process of identifying the potential threats, enumerating and prioritizing the threats and providing countermeasures to mitigate the threats. TM can be applied to any platform of a working process like software, application, networks, IoT devices or business processes. (Shostack 2014) has summarized the reason to incorporate the threat model in software development life cycle (SDLC) as (1) to find the bugs at the earliest, (2) understanding the security requirements, and (3) engineering and delivering a better product. Basically, TM includes components like Target-of-Evaluation(ToE) (a design or model of environment that need to be analyzed), a list of assumptions that can be threat on ToE, a list of potential threats on ToE, possible countermeasures towards the identified threats and verification of Success (VoS), that validates the threat model.

Before modeling a threat, there are four questions to be answered and they are:

1 What are we building?
   - A detailed data flow diagram (DFD) is designed by specifying various roles and responsibilities of each participants.
2 What can go wrong?
   - The various possible threats are analyzed using methods available in STRIDE, PASTA, STRIKE or VAST.
3 What are we going to do about that?
   - Potential mitigation strategies against the threats are framed.
4 Did we do a good job?
   - Once the mitigation are applied, the system is validated for the stability and security against the threats.

10.1 Microsoft secure development lifecycle (microsoft SDL)

Microsoft SDL was introduced in 2008 to ensure security and privacy considerations throughout all the phases of the development process. This helped developers to build highly secure software, addressing security compliance requirements and reduce development costs. The core of Microsoft SDL is threat modeling. The threat modeling helps in shaping the application design and meet the security objectives of the company by reducing the risk severity. The five major steps of threat modeling involves (Fig. 8):

1 Defining security requirements: To understand the ecosystem of the device, i.e., analysis of the ToE by framing various use-cases. In this process, the external and internal assets are identified.
2 Creating an application diagram: Here, a detailed data flow diagram of the proposed ToE is framed with appro-

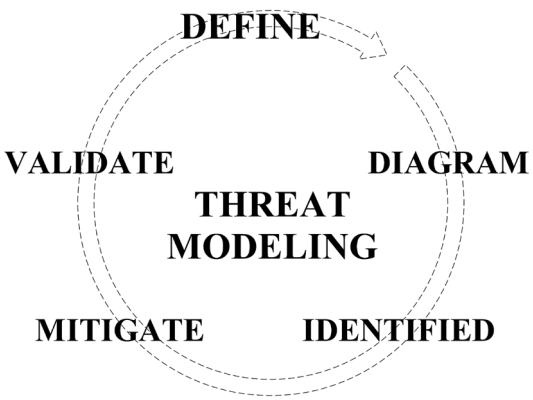

Fig. 8 Microsoft secure development life-cycle (SDL) using TMT

priate trust boundaries and security requirements for each participant.

3 Identifying the threats: Microsoft TMT follows STRIDE based threat modeling where the threats are identified. Potential adversaries are identified under four categories called remote software attacker, network attacker, malicious insider attacker and advance hardware attacker.

4 Mitigate the threats: For the threat identified, relevant countermeasures are established.

5 Validating that threats have been mitigated: Finally, the verification of a threat model against the mitigation is performed to check the stability of the proposed system.

10.2 STRIDE framework methodology

It is essential to develop a secure design for any software application or system. Failing to do so may cost about 30 times higher than estimated cost (Verheyden 2018). Hence threat modeling plays a vital role is the software development lifecycle. Among various threat modeling methods like STRIDE, PASTA, VAST and STRIKE, STRIDE has taken a major share among the industrial development process (Bodeau et al. 2018; Meghanathan et al. 2010). Microsoft develops STRIDE as a part of its security development lifecycle. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege (Khan et al. 2017). The security properties and attack type associated with STRIDE are summarized in Table 3 (Verheyden 2018).

10.3 Overview of threat modeling tool (TMT)

Microsoft TMT is used to analyze the design of a system or an application in order to check for security risks and provide a solution for the threat found. Figure 9 displays the initial page of TMT when launched. This page has two section, and the top section is used to create the threat model of the user's choice using the templates provided by Microsoft. The below section helps the user to customized his own template on the default Microsoft SDL template.

When the threat model section is selected with the appropriate template, a new window is open, which can be seen in Fig. 10. By using *Drawing* area, a Data Flow Diagram (DFD) can be built using the options available in *Stencil* sub-window located at the right corner of the window. This view is called as *Design View*. Every DFD must contain at least each one of process, data flow direction, data storage, internal inter-actors and trust boundaries from the stencil sub-window.

Once the DFD is framed, the threats can be analyzed using *Analysis View* tab as shown in Fig. 11. Under this page, we can observe the threats that are identified by the SDL template and also possible mitigation strategies are displayed for the users conveniences based on the default template definition. The user can scroll down the page to see the threats and its severity level. When scrolled down, at the *status* box the message would be *Not started*, which means the threat needs to be attended. Once the threat is handled, it can be changed to *mitigated*.

Figure 12 displays an HTM page of threat analysis report generated by the TMT tool. It displays the summary of the

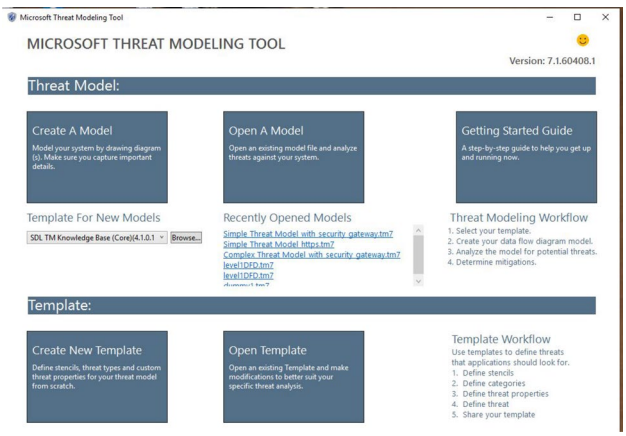

Fig. 9 Microsoft TMT initial screen

Table 3 STRIDE threat model with associated security properties

Threat	Security property	Definition
Spoofing	Authentication	Unauthorized access
		Using another user identity
Tampering	Integrity	Unauthorized information changes
		Malicious modification
Repudiation	Non-repudiation	Denying to perform action
Information disclosure	Confidentiality	Unprivileged users gain access and compromises the system
Denial of service	Availability	Deny services to valid users
		Threats to system availability and reliability
Elevation of privilege	Authorization	Exposure of information to individuals not suppose to access

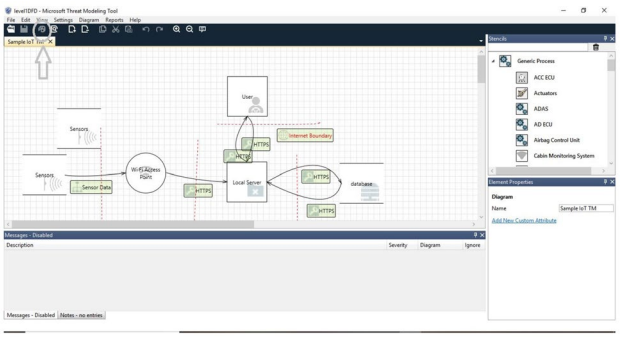

Fig. 10 Microsoft TMT design view

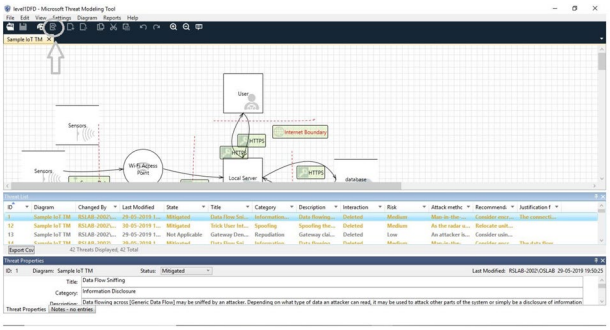

Fig. 11 Microsoft TMT analysis view

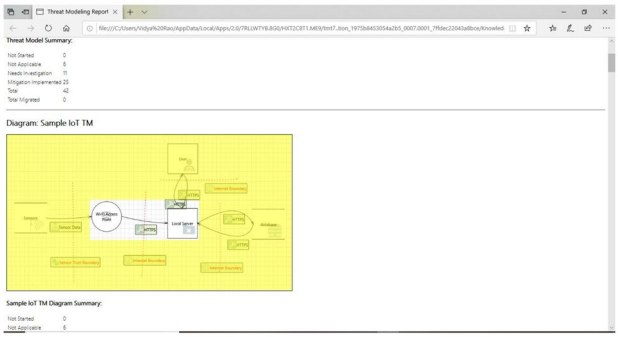

Fig. 12 Microsoft TMT sample .htm report page

threats modeled with a detailed description of each participant and possible threats on the system with the severity level of each threat.

11 Research gaps

Based on the review, following research gaps are identified.

- Smart environment involving the Internet-of-Things (IoT) solutions are vulnerable to data and privacy breaches. As the IoT applications are deployed on resource-constrained devices, it is essential to design lightweight cryptographic solutions. In this chapter, an overview of existing lightweight authentication and data integrity techniques are discussed.
- These current lightweight cryptographic solutions majorly use hashing methods like message digest (MD5) or variants of SHA hash functions. These existing hash functions have complex rotational and XOR operations that consume more resources on the device. An improved hash function is introduced as a part of the proposed work to reduce the resource consumption of the embedded devices.
- The study has shown the various lightweight scheme are based on elliptic curve cryptography (ECC) and these ECC schemes use single and static elliptic curve parameters for signature generation. These elliptic curve parameters are stored on embedded devices that are vulnerable to node compromise attacks. To enhance the security of every embedded device, we have proposed secure storage at the node level. Also, to provide data security, a dual elliptic curve based authentication and data integrity schemes are proposed. From the literature, it is observed that various cryptographic schemes are evaluated using simulation tools and security of these schemes are analyzed using various verification tools. The proposed work is evaluated both under theoretical study and experimental environment for various real-time attacks.
- In IoT, the communications are between devices and the server, or among the devices over the publically available Internet infrastructure. Such communication involves the frequent distribution of security keys from the key distribution center (KDC) and issues of certificates for every device across the Internet become a tedious job as there are thousands of devices being added and removed from the network. Thereby, the use of standard KDC or key management servers is difficult among the growing IoT applications.
- From the review, we have seen that various ECDSA and ECIES based cryptographic solutions have been using single or static elliptic curve parameters which are stored on the device and also, these devices are easily accessible to the user who can be hackers too. Imbibing secret keys or cryptographic parameters on the device shall lead to node compromise attacks. Hence, securely storing the default key values on the devices plays an important research perspective to be addressed.
- Providing authentication and data integrity using the same algorithm has shown more computation and consumes a lot of devices power. Also, from the review, it is observed that the same public and private values are being used for both authentication and data integrity methods. But such a setup can easily be broken by the

attacker if anyone set of keys is obtained using various attacks like MITM attacks, chosen cipher-text attacks, replay attacks. Such a scenario calls for the use of a different set of PKC keys for different levels of security.

- From the review, it has been seen that the security evaluation of the schemes are either done using a theoretical method or using simulation tools like AVISPA, ProVerif etc. But a real-time security evaluation is not done. Thereby, a thorough theoretical and experimental security analysis is needed. The mapping of experimental and theoretical security analysis helps to evaluate the proposed security scheme for the real-time scalable network.

12 Conclusion

Machine-to-machine communication plays a vital role in both wired and wireless environments of IoT. In IoT, the devices are equipped with sensing and smaller computational capabilities that are driven by energy constraints. These devices communicate among each other over publically available communication. Thereby, these communications are susceptible to various attacks. The major issue with such devices it maintains the privacy of users and data to be transmitted unaltered. Hence, it is essential to maintain authentication and data integrity. As these devices use a battery and have work for a longer period of time, it is important to design cryptographic solutions that are lightweight and secure. This study provides various authentication and data integrity based schemes that are suitable for resource-constrained devices of IoT. Also, the study describes the Microsoft threat modeling tool (TMT) that can be used as a part of any secure development life cycle (SDLC) of IoT based applications.

Compliance with ethical standards

Conflict of interest First author, Vidya Rao declares that she has no conflict of interest. Prema K.V., the second author, declares that she has no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

Abomhara M, Kien G (2015) Cyber security and the Internet-of-Things: vulnerabilities, threats, intruders and attacks. J Cyber Secur 4:65–88

Abomhara M, Køien GM (2014) Security and privacy in the Internet-of-Things: Current status and open issues, pp 1–8

Afianti F, Suryani T et al (2019) Lightweight and dos resistant multiuser authentication in wireless sensor networks for smart grid environments. IEEE Access 7:67107–67122

Ahemd MM, Shah MA, Wahid A (2017) IoT security: a layered approach for attacks and defenses. In: Communication technologies (ComTech), 2017 international conference on, IEEE, pp 104–110

Ahmed AA, Ahmed WA (2019) An effective multifactor authentication mechanism based on combiners of hash function over internet of things. Sensors 19(17):3663

Al Barghuthi NB, Saleh M, Alsuwaidi S, Alhammadi S (2017) Evaluation of portable penetration testing on smart cities applications using raspberry pi III. In: 2017 fourth HCT information technology trends (ITT), IEEE, pp 67–72

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376

Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of Things security: a survey. J Netw Comput Appl 88:10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Aman MN, Chua KC, Sikdar B (2017a) Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet Things J 4(5):1327–1340

Aman MN, Chua KC, Sikdar B (2017b) Mutual authentication in IOT systems using physical unclonable functions. IEEE Internet Things J 4(5):1327–1340

Ammar M, Russello G, Crispo B (2018) Internet of Things: a survey on the security of IoT frameworks. J Inf Secur Appl 38:8–27. https://doi.org/10.1016/j.jisa.2017.11.002

Annor-Asante M, Pranggono B (2018) Development of smart grid testbed with low-cost hardware and software for cybersecurity research and education. Wirel Personal Commun 101(3):1357–1377

Atamli AW, Martin A (2014) Threat-based security analysis for the internet of things. Secure Internet of Things (SIoT). International workshop on, IEEE, pp 35–43

Aumasson JP, Henzen L, Meier W, Phan RCW (2008) SHA-3 proposal BLAKE. Submission to NIST. https://doi.org/10.1093/gmo/9781561592630.article.o904247

Aumasson JP, Neves S, Wilcox-OHearn Z, Winnerlein C (2013) BLAKE2: simpler, smaller, fast as MD5. In: International conference on applied cryptography and network security. Springer, pp 119–135. https://doi.org/10.1007/978-3-642-38980-1_8

Babar S, Stango A, Prasad N, Sen J, Prasad R (2011) Proposed embedded security framework for Internet-of-Things. In: Wireless communication, vehicular technology, information theory and aerospace and electronic systems technology (Wireless VITAE), 2011 2nd international conference, IEEE, pp 1–5

Bai TDP, Rabara SA, Jerald AV (2015) Elliptic curve cryptography based security framework for Internet of Things and cloud computing. In: Conference on recent advances on computer engineering by WSEAS, pp 65–73. https://doi.org/10.1109/wccct.2016.20

Bellare M, Pointcheval D, Rogaway P (2000) Authenticated key exchange secure against dictionary attacks. In: International conference on the theory and applications of cryptographic techniques. Springer, pp 139–155

Bernstein DJ, Lange T, et al (2013) Safecurves: choosing safe curves for elliptic-curve cryptography. http://safecurvescrypto

Bodeau D, McCollum C, Fox D (2018) Cyber threat modeling: survey, assessment, and representative framework. The Mitre Corporation, HSSEDI, Bedford

Camtepe SA, Yener B (2004) Combinatorial design of key distribution mechanisms for wireless sensor networks. In: European symposium on research in computer security. Springer, pp 293–308

Center CSR (2018) Hash functions. https://csrc.nist.gov/Projects/Hash-Functions

Chain K, Kuo WC, Cheng JC (2016) A novel mobile communications authentication scheme with roaming service and user anonymity. Appl Sci 6(12):393

Chen H, Ge L, Xie L (2015) A user authentication scheme based on elliptic curves cryptography for wireless ad hoc networks. Sensors 15(7):17057–17075

Chen Y, Martínez JF, Castillejo P (2017) López L (2017) A privacy protection user authentication and key agreement scheme tailored for the Internet of Things environment: PriAuth. Wirel Commun Mob Comput

Chung Y, Choi S, Won D (2015) Anonymous authentication scheme for intercommunication in the Internet of Things environments. Int J Distrib Sens Netw 11(11):305785

Chung Y, Choi S, Lee Y, Park N, Won D (2016) An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in Wireless Sensor Networks. Multidiscip Digit Publ Inst Sens 16(10):1653

Conti M, Dragoni N, Lesyk V (2016) A survey of Man In The Middle attacks. IEEE Commun Surv Tutor 18(3):2027–2051

Da Xu L, He W, Li S (2014) Internet of Things in industries: a survey. IEEE Trans Ind Inf 10(4):2233–2243

Dang TK, Pham CD, Nguyen TL (2020) A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities. Sustain Cities Soc 20:102097

Denis M, Zena C, Hayajneh T (2016) Penetration testing: concepts, attack methods, and defense strategies. In: 2016 IEEE long island systems, applications and technology conference (LISAT), IEEE, pp 1–6

Dhillon PK, Kalra S (2017) Secure multi-factor remote user authentication scheme for internet of things environments. Int J Commun Syst 30(16):e3323

Djellali B, Belarbi K, Chouarfia A, Lorenz P (2015) User authentication scheme preserving anonymity for ubiquitous devices. Security and Communication Networks 8(17):3131–3141

Dworkin MJ (2015) Sha-3 standard: permutation-based hash and extendable-output functions. Tech. rep. https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions

ECRYPT I (2012) Yearly report on algorithms and keysizes. ECRYPT II Network of Excellence (NoE), funded within the Information Societies Technology (IST) Programme of the European Commissions Seventh Framework Programme (FP7)

Farash Sabzinejad M (2014) Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. J Supercomput 70(2):987–1001

Fu A, Song J, Li S, Zhang G, Zhang Y (2016) A privacy-preserving group authentication protocol for machine-type communication in lte/lte-a networks. Secur Commun Netw 9(13):2002–2014

Garcia-Carrillo D, Marin-Lopez R (2016) Lightweight coap-based bootstrapping service for the internet of things. Sensors 16(3):358

Garg S, Kaur K, Kaddoum G, Rodrigues JJ, Guizani M (2019) Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Trans Ind Inform 20:20

Gayoso Martínez V, Hernández Álvarez F, Hernández Encinas L, Sánchez Ávila C (2011) Analysis of ECIES and other cryptosystems based on elliptic curves. Machine Intelligence Research Labs. https://www.researchgate.net/publication/255970196

Glissa G, Rachedi A, Meddeb A (2016) (2016) A secure routing protocol based on RPL for Internet of Things. Global communications conference (GLOBECOM). IEEE, IEEE, pp 1–7

Gura N, Patel A, Wander A, Eberle H, Shantz SC (2004) Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In: International workshop on cryptographic hardware and embedded systems. Springer, pp 119–132. https://doi.org/10.1007/978-3-540-28632-5_9

Hafsa Tahir AK, Junaid M (2016) Internet-of-Things (IoT): an overview of applications and security issues regarding implementation. Int J Multidiscip Sci Eng 7(1):14–22

Hao Y (2014) The boomerang attacks on Blake and Blake2. In: International conference on information security and cryptology. Springer, pp 286–310

He D, Zeadally S (2015) An analysis of RFID authentication schemes for Internet-of-Things in healthcare environment using elliptic curve cryptography. IEEE Internet Things J 2(1):72–83

Hu F (2016) Security and privacy in Internet of Things (IoTs): models, algorithms, and implementations. CRC Press, London. https://doi.org/10.1201/b19516

Hu Y, Sulek D, Carella A, Cox J, Frame A, Cipriano K (2016) Employing miniaturized computers for distributed vulnerability assessment. In: 2016 11th international conference for internet technology and secured transactions (ICITST), IEEE, pp 57–61

Jansma N, Arrendondo B (2004) Performance comparison of elliptic curve and RSA digital signatures. nicj net/files

Jia X, He D, Kumar N, Choo KKR (2018) Authenticated key agreement scheme for fog-driven IoT healthcare system. Wirel Netw. https://doi.org/10.1007/s11276-018-1759-3

Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D (2014) Security of the Internet of Things: perspectives and challenges. Springer Wirel Netw 20(8):2481–2501

John AL, Thampi SM (2016) Mutual authentication based on HECC for RFID implant systems. In: International symposium on security in computing and communication. Springer, pp 18–29

Kang D, Jung J, Mun J, Lee D, Choi Y, Won D (2016) Efficient and robust user authentication scheme that achieve user anonymity with a Markov chain. Secur Commun Netw 9(11):1462–1476

Khan R, McLaughlin K, Laverty D, Sezer S (2017) Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE pes innovative smart grid technologies conference Europe (ISGT-Europe), IEEE, pp 1–6

Kim J, Moon J, Jung J, Won D (2016a) Security analysis and improvements of session key establishment for clustered sensor networks. J Sens 20:20

Kim J, Moon J, Jung J, Won D (2016b) Security analysis and improvements of session key establishment for clustered sensor networks. J Sens 20:20

Kim KW, Han YH, Min SG (2017) An authentication and key management mechanism for resource constrained devices in IEEE 802.11-based IoT access networks. Sensors 17(10):2170

Kumar P, Gurtov A, Iinatti J, Sain M, Ha PH (2016) Access control protocol with node privacy in Wireless Sensor Networks. IEEE Sens J 16(22):8142–8150

Kumar D, Grover HS et al (2019) A secure authentication protocol for wearable devices environment using ECC. J Inf Secur Appl 47:8–15

Lauter K (2004) The advantages of elliptic curve cryptography for wireless security. IEEE Wirel Commun 11(1):62–67

Lavanya M, Natarajan V (2017) LWDSA: light-weight digital signature algorithm for wireless sensor networks. Sādhanā 42(10):1629–1643. https://doi.org/10.1007/s12046-017-0718-5

Le XH, Lee S, Butun I, Khalid M, Sankar R, Kim M, Han M, Lee YK, Lee H (2009) An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. J Commun Netw 11(6):599–606

Lee J, Sung Y, Park JH (2016) Lightweight sensor authentication scheme for energy efficiency in ubiquitous computing environments. Sensors 16(12):2044

Lenstra AK, Verheul ER (2001) Selecting cryptographic key sizes. Springer J Cryptol 14(4):255–293

Li CT (2012) A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications. Inf Technol Control 41(1):69–76

Li F, Xiong P (2013) Practical secure communication for integrating wireless sensor networks into the Internet-of-Things. IEEE Sens J 13(10):3677–3684

Li D, Aung Z, Williams J, Sanchez A (2014) P3: privacy preservation protocol for automatic appliance control application in smart grid. IEEE Internet Things J 1(5):414–429

Li N, Liu D, Nepal S (2017) Lightweight mutual authentication for IoT and its applications. IEEE Trans Sustain Comput 2(4):359–370

Li W, Liao L, Gu D, Li C, Ge C, Guo Z, Liu Y, Liu Z (2018) Ciphertext-only fault analysis on the led lightweight cryptosystem in the internet of things. IEEE Trans Depend Secure Comput 16(3):454–461

Liang L, Zheng K, Sheng Q, Huang X (2016) A denial of service attack method for an IOT system. In: 2016 8th international conference on information technology in medicine and education (ITME), IEEE, pp 360–364

Lin SC, Wen CY, Sethares WA (2018) Two-tier device-based authentication protocol against PUEA attacks for IoT applications. IEEE Trans Signal Inf Process Netw 4(1):33–47. https://doi.org/10.1109/TSIPN.2017.2723761

Liu A, Ning P (2008) TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 7th international conference on Information processing in sensor networks, IEEE Computer Society, pp 245–256. https://doi.org/10.1109/ipsn.2008.47

Liu G, Quan W, Cheng N, Zhang H, Yu S (2019a) Efficient ddos attacks mitigation for stateful forwarding in internet of things. J Netw Comput Appl 130:1–13

Liu J, Ren A, Zhang L, Sun R, Du X, Guizani M (2019b) A novel secure authentication scheme for heterogeneous internet of thing. CoRR abs/1902.03562

Lu R, Heung K, Lashkari AH, Ghorbani AA (2017) A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access 5:3302–3312

Luhach AK et al (2016) Analysis of lightweight cryptographic solutions for Internet-of-Things. Indian J Sci Technol 9:28

Mahmood K, Chaudhry SA, Naqvi H, Shon T, Ahmad HF (2016) A lightweight message authentication scheme for smart grid communications in power sector. Comput Electr Eng 52:114–124

Mahmood Z, Ning H, Ullah A, Yao X (2017) Secure authentication and prescription safety protocol for telecare health services using ubiquitous iot. Appl Sci 7(10):1069

Mahmoud MM, Mišić J, Akkaya K, Shen X (2015) Investigating public-key certificate revocation in smart grid. IEEE Internet Things J 2(6):490–503

Matsuo S, Miyazaki K, Otsuka A, Basin D (2010) How to evaluate the security of real-life cryptographic protocols? In: International conference on financial cryptography and data security. Springer, pp 182–194

Mazumder R, Miyaji A, Su C (2017) A simple authentication encryption scheme. Concurr Comput Pract Exp 29(16):e4058

McAndrew A (2016a) Introduction to cryptography with open-source software

McAndrew A (2016b) Introduction to cryptography with open-source software. CRC Press, New York. https://doi.org/10.1201/9781439825716

McGrath MJ, Scanaill CN (2013) Sensor technologies: healthcare. Apress, wellness and environmental applications

Meadows C (1992) Applying formal methods to the analysis of a key management protocol. J Comput Secur 1(1):5–35

Meghanathan N, Boumerdassi S, Chaki N, Nagamalai D (2010) Recent trends in network security and applications: third international conference, CNSA 2010, Chennai, India, July 23–25, 2010 Proceedings, vol 89. Springer, Berlin

Meier AV (2005) The Elgamal cryptosystem. http://wwwmayr.in.tum.de/konferenzen/Jass05 /courses /1/papers/meier/paper.pdf

Miller VS (1985) Use of elliptic curves in cryptography. In: Conference on the theory and application of cryptographic techniques. Springer, pp 417–426. https://doi.org/10.1007/3-540-39799-X_31

Mössinger M, Petschkuhn B, Bauer J, Staudemeyer RC, Wójcik M, Pöhls HC (2016) Towards quantifying the cost of a secure IoT: overhead and energy consumption of ECC signatures on an arm-based device. In: World of wireless, mobile and multimedia networks (WoWMoM), 2016 IEEE 17th international symposium on A, IEEE, pp 1–6

Murray R (2017) A raspberry pi attacking guide

Nam J, Kim M, Paik J, Lee Y, Won D (2014) A provably-secure ECC-based authentication scheme for wireless sensor networks. Sensors 14(11):21023–21044

Nawir M, Amir A, Yaakob N, Lynn OB (2016) Internet of things (IoT): taxonomy of security attacks. In: Electronic design (ICED), 2016 3rd international conference on, IEEE, pp 321–326

NIST (2018) SHA-3 standardization. https://csrc.nist.gov/projects/hash-functions/sha-3-standardization

Pan W, Zheng F, Zhao Y, Zhu WT, Jing J (2017) An efficient elliptic curve cryptography signature server with GPU acceleration. IEEE Trans Inf Forensics Secur 12(1):111–122

Park N, Kang N (2016) Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors 16(1):20

Parrilla L, Castillo E, López-Ramos JA, Álvarez-Bermejo JA, García A, Morales DP (2018) Unified compact ECC-AES co-processor with group-key support for IoT devices in wireless sensor networks. Sensors 18(1):251

Paulson LC (1998) The inductive approach to verifying cryptographic protocols. J Comput Secur 6(1–2):85–128

Peng L, Ru-chuan W, Xiao-yu S, Long C (2013) Privacy protection based on key-changed mutual authentication protocol in Internet-of-Things. China conference wireless sensor networks, pp 345–355

Pereira GC, Puodzius C, Barreto PS (2016) Shorter hash-based signatures. J Syst Softw 116:95–100

Preneel B (2010) The first 30 years of cryptographic hash functions and the NIST SHA-3 competition. Cryptographers track at the RSA conference. Springer, Berlib, pp 1–14. https://doi.org/10.1007/978-3-642-11925-5_1

Qiu Y, Ma M (2016) A mutual authentication and key establishment scheme for m2m communication in 6lowpan networks. IEEE Trans Ind Inf 12(6):2074–2085

Rahaman O (2017) Data and information security in modern world by using elliptic curve cryptography. Comput Sci Eng 7(2):29–44

Rahman AU, Ullah I, Naeem M, Anwar R, ul Amin N, Khattak H, Ullah S (2018) A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve. Int J Adv Comput Sci Appl 9(5):160–167. https://doi.org/10.14569/ijacsa.2018.090520,

Reddy AG, Yoon EJ, Das AK, Yoo KY (2016) Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. IET Inf Secur 10(5):272–282

Roy A, Karforma S (2012) A survey on digital signatures and its applications. J Comput Inf Technol 3(1):45–69

Roy S, Khatwani C (2017) Cryptanalysis and improvement of ECC based authentication and key exchanging protocols. Cryptography 1(1):9

Rubin AD, Honeyman P (1993) Formal methods for the analysis of authentication protocols. Tech. rep, Center for Information Technology Integration

Saxena N, Grijalva S, Chaudhari NS (2016) Authentication protocol for an IoT-enabled LTE network. ACM Trans Internet Technol 16(4):1–20

SEC S (2000) Sec 2: recommended elliptic curve domain parameters. Standards for Efficient Cryptography Group, Certicom Corp. https://www.secg.org/SEC2-Ver-1.0.pdf

Shivraj V, Rajan M, Singh M, Balamuralidhar P (2015) One time password authentication scheme based on elliptic curves for Internet-of-Things (IoT). IEEE, pp 1–6

Shostack A (2014) Threat modeling: designing for security. Wiley, Oxford

Shuai M, Yu N, Wang H, Xiong L (2019) Anonymous authentication scheme for smart home environment with provable security. Comput Secur 86:132–146

Silverman JH (2009) The arithmetic of elliptic curves, vol 106. Springer. https://doi.org/10.1007/978-0-387-09494-6. https://link.springer.com/book/10.1007/978-0-387-09494-6

Srinivas J, Mukhopadhyay S, Mishra D (2017) Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Netw 54:147–169. https://doi.org/10.1016/j.adhoc.2016.11.002

Stallings W (2006) Cryptography and network security: principles and practices. Pearson Education India, New York

Styger E IoT security and the transport security layer. https://dzone.com/articles/iot-and-the-transport-security-layer

Tan H, Ma M, Labiod H, Boudguiga A, Zhang J, Chong PHJ (2016) A secure and authenticated key management protocol (SAKMP) for vehicular networks. IEEE Trans Veh Technol 65(12):9570–9584

Tiwari HD, Kim JH (2018) Novel method for DNA-based elliptic curve cryptography for IoT devices. ETRI J 40(3):396–409. https://doi.org/10.4218/etrij.2017-0220

Tomar A, Dhar J (2019) An ECC based secure authentication and key exchange scheme in multi-server environment. Wirel Pers Commun 107(1):351–372

Verheyden L (2018) Effectiveness of threat modelling tools. Master Thesis. https://lib.ugent.be/fulltxt/RUG01/002/508/960/ RUG01-002508960_2018_0001_AC.pdf

Vermesan O, Friess P (2014) Internet of things-from research and innovation to market deployment, vol 29. River Publishers, Aalborg

Visoottiviseth V, Akarasiriwong P, Chaiyasart S, Chotivatunyu S (2017) PENTOS: penetration testing tool for internet of thing devices. In: TENCON 2017-2017 IEEE Region 10 conference, IEEE, pp 2279–2284

Wang C, Zhang Y (2015) New authentication scheme for wireless body area networks using the bilinear pairing. J Med Syst 39(11):136

Wang J, Cheng LM (2017) Dynamic scalable ECC scheme and its application to encryption workflow design. In: Proceedings of the international conference on security and management (SAM), pp 261–262. https://csce.ucmss.com/cr/books/2017/LFS /CSREA2017/SAM9760.pdf

Wang J, Li J, Wang H, Zhang LY, Cheng LM, Lin Q (2018) Dynamic scalable elliptic curve cryptographic scheme and its application to in-vehicle security. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2018.2869872.https://ieeexplore.ieee.org/document/8463502

Wang WC, Yona Y, Wu Y, Diggavi SN, Gupta P (2019) Slate: a secure lightweight entity authentication hardware primitive. IEEE Trans Inf Forensics Secur 15:276–285

Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M (2018) Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet Things J 5(1):269–282

Wenger E (2013) Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography. In: International conference on applied cryptography and network security. Springer, pp 290–306. https://doi.org/10.1007/978-3-642-38980-1_18

Wu L, Zhang Y, Li L, Shen J (2016) Efficient and anonymous authentication scheme for wireless body area networks. J Med Syst 40(6):134

Zeinab KAM, Elmustafa SAA (2017) Internet of Things applications, challenges and related future technologies. World Sci News 2(67):126–148

Zhang Z, Qi Q (2014) An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. J Med Syst 38(5):47

Zhao D, Peng H, Li L, Yang Y (2014) A secure and effective anonymous authentication scheme for roaming service in global mobility networks. Wirel Pers Commun 78(1):247–269

Zhao Z (2014) A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. J Med Syst 38(5):46

Zheng Y (1997) Digital signcryption or how to achieve cost (signature and encryption) cost (signature) plus cost (encryption). In: Springer annual international cryptology conference. Springer, pp 165–179

Zhu H (2003) A practical elliptic curve public key encryption scheme provably secure against adaptive chosen-message attack. IACR Cryptol ePrint Arch 2003:87

Zolanvari M, Jain R (2015) IoT security: a survey