Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 28, 2020, accepted August 26, 2020, date of publication September 8, 2020, date of current version September 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022661

Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey

VISHAL SHARMA[1], (Member, IEEE), ILSUN YOU[2], (Senior Member, IEEE), KARL ANDERSSON[3], (Senior Member, IEEE), FRANCESCO PALMIERI[4], MUBASHIR HUSAIN REHMANI[5], (Senior Member, IEEE), AND JAEDEOK LIM[6]

[1]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, U.K.
[2]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[3]Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 93187 Skellefteå, Sweden
[4]Department of Computer Science, University of Salerno, 84084 Fisciano, Italy
[5]Department of Computer Science, Cork Institute of Technology (CIT), Cork 021, T12 P928 Ireland
[6]Information Security Research Division, Electronics and Telecommunications Research Institute (ETRI), Gwangju 500-480, South Korea

Corresponding author: Ilsun You (ilsunu@gmail.com)

This work was supported in part by the Institute for Information & Communications Technology Planning & Evaluation (IITP) Grant funded by the Korean Government [Ministry of Science and Information and communications Technology, (MSIT)] (Development of context adaptive security autonomous enforcement technology to prevent spread of Internet of Things (IoT) infrastructure attacks) under Grant 2018-0-00231, and in part by the Soonchunhyang University Research Fund.

ABSTRACT With an enormous range of applications, the Internet of Things (IoT) has magnetized industries and academicians from everywhere. IoT facilitates operations through ubiquitous connectivity by providing Internet access to all the devices with computing capabilities. With the evolution of wireless infrastructure, the focus from simple IoT has been shifted to smart, connected and mobile IoT (M-IoT) devices and platforms, which can enable low-complexity, low-cost and efficient computing through sensors, machines, and even crowdsourcing. All these devices can be grouped under a common term of M-IoT. Even though the positive impact on applications has been tremendous, security, privacy and trust are still the major concerns for such networks and insufficient enforcement of these requirements introduces non-negligible threats to M-IoT devices and platforms. Thus, it is important to understand the range of solutions which are available for providing a secure, privacy-compliant, and trustworthy mechanism for M-IoT. There is no direct survey available, which focuses on security, privacy, trust, secure protocols, physical layer security and handover protections in M-IoT. This paper covers such requisites and presents comparisons of state-the-art solutions for IoT which are applicable to security, privacy, and trust in smart and connected M-IoT networks. Apart from these, various challenges, applications, advantages, technologies, standards, open issues, and roadmap for security, privacy and trust are also discussed in this paper.

INDEX TERMS Security, privacy, trust, protocols, IoT, M-IoT, survey and analysis.

I. INTRODUCTION

Mobile-Internet of Things (M-IoT) offers vendors a utility for providing smart services to their users by forming a highly sustainable, secure and cost-effective network [1]–[3]. The smart M-IoT paves a way for incorporating a large set of services like healthcare, business monitoring, strategic planning, public safety communications, weather forecasting, navigation, reconnaissance, and data acquisition [4]–[6]. Security and efficiency of these services are the main objectives of organizations aiming at the spread of smart M-IoT. M-IoT focuses on user-specific commercialization, where users pay as per their active applications while offering them with flexible and dynamic procedures for the selection of a service [7]–[9]. In order to enhance the security, utility and lifetime of services, most of the established business enterprises are looking forward to procuring long-range and low power solutions for connecting billions of devices to their core networks without much dependence on the existing infrastructure. Such an ideology allows for easier management and configuration of M-IoT networks and associated devices. Solutions like Low Power Wide Area Network (LPWAN), Long Range Wide Area Network (LoRaWAN) and Narrow Band-IoT (NB-IoT) are

The associate editor coordinating the review of this manuscript and approving it for publication was Chunhua Su.

efficient in deploying M-IoT networks [10]–[13]. However, at the moment, both the technologies are rival to each other and their applicability and use cases are subject to the decisions of deploying companies and the regulations of the countries involved in their development. With better reach and ease of deployment over existing cellular setup, NB-IoT and Long Term Evolution for Machines (LTE-M) are under consideration as their unification will enhance the types of applications for M-IoT by adopting service strategies similar to mobile networks [14], [15].

The major interests of some leading organizations have been towards the establishment of a different spectrum which is also obtained as a dedicated range from their allocated space or frequency band. Technologies like Software-Defined Networking (SDN) and Network-Function Virtualization (NFV) provide an altogether different way for deploying these networks in a secure way [16]–[20]. With a centralized controller, a common node helps to monitor the network, whereas network slicing through NFV will help to distribute the implementation and management of SDNs. M-IoT can operate as a separate slice, and a local or global controller can manage the related activities. Procedures like secondary authentication and group authentication can be seen as potential solutions for ensuring security in smart M-IoT. However, the effective implementation of rules and policies at the control layer due to the configuration complexity and artefacts requires intelligent solutions that can be assured by using certain aspects of optimization, machine learning or artificial intelligence.

In smart M-IoT, security refers to the protection of the infrastructure from potentially hazardous components and users, which may exploit the network with vulnerabilities, based on the known/unknown cyber-attacks. For privacy, it deals with the preservation of lawfulness in sharing the information about-and-between the involved devices. Since smart M-IoT will be dealing with a lot of connected components, maintenance of isolation in traffic patterns and establishing anonymity of users becomes an utmost requirement. Trust refers to the faithfulness in the identification of devices for communication. It further involves the reputation-building between the devices and the infrastructure leading a way to make the network secure while preserving its privacy.

Current market trends have shown that despite several solutions for establishing M-IoT communications, the end to end security will be one of the major concerns for the mobile operators. Identification of new cyber threats, which consist of zero-day attacks, is another major requirement of the security industry [21], [22]. It is estimated that M-IoT will hit the market by 2025 with maximum revenue being generated from the security, privacy and trust-based services. Even the major role players will be a low power long-range communication models, which can be evaluated around 15+ billion dollars at the same time [23]. Thus, it is required that the existing state-of-the-art must be followed and evaluated on the basis of performance metrics and parameters that enhance the security, privacy, and trust in M-IoT.

A. ADVANTAGES AND APPLICATIONS OF SMART M-IoT

Smart M-IoT focuses on the applications which help in regulating the daily works of their users. Smart M-IoT provides a different set of applications is largely diversified areas such as a smart factory, smart city, smart home, smart grid [24]–[27], healthcare, personal care, emergencies [28], as shown in Fig. 1. With smart M-IoT, it becomes easier for both users as well as business organization to accommodate and host services through intelligent architecture with effective security. In terms of market trends, business houses are looking at a huge monetary advantage from smart M-IoT networks and applications. Including these, other advantages and applications of smart M-IoT are as follows:

FIGURE 1. An overview of M-IoT applications.

- Formation of the contextual network through intelligent and rapid data acquisition and processing.
- Self-configuring capacity and support for a large set of devices through a common interface.
- Support for human to device and device to device communication with lower overheads and low-complexity.
- Information management, processing, and validation and data flow management across a wide range of the network.
- Support for real-world applications such as driverless cars, urban-surveillance, smart retailing, industrial Internet, and even provisioning of application base for Augmented Reality (AR)/Virtual Reality(VR) services.
- Low-cost deployment and development of personal applications as well as private networks and clouds.
- Requires low-frequent maintenance and can be operated through distant mode. On-site evaluations

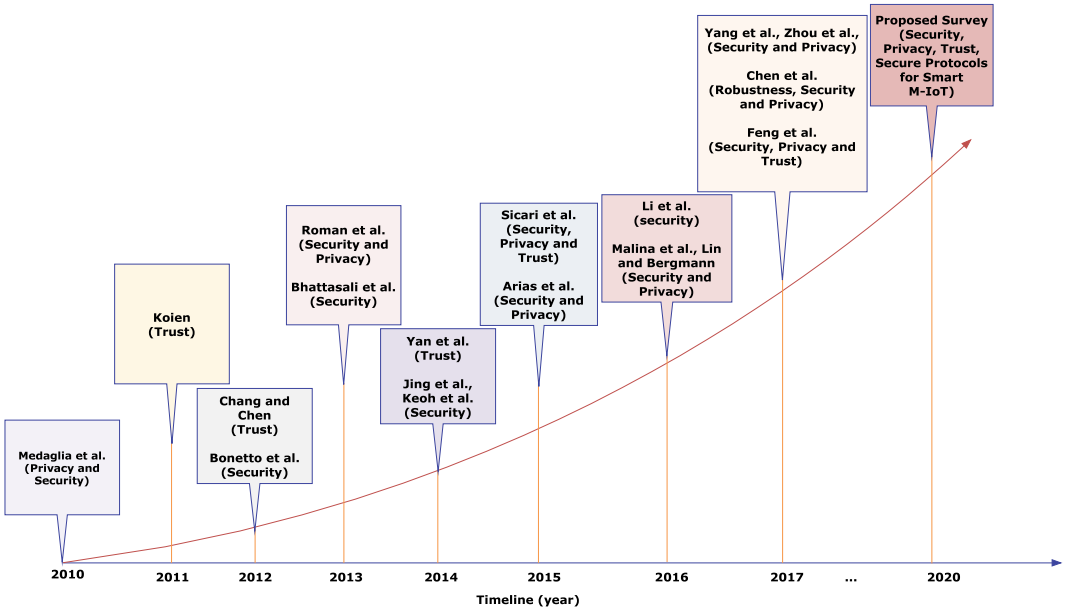


FIGURE 2. A road map of different studies on security, privacy and trust in IoT and M-IoT.

may be subject to special requirements and upgrades.

- Supports crowdsourcing as well as edge-computing models by forming an on-demand network in case of public safety communications.
- Industrial automation and personalized control formations through light-weight and low-complex Integrated Development Environments (IDEs). Further, M-IoT also helps in tracking the traffic-flows by incorporating transmissions over dynamic nodes, such as drones, smart cars, autonomous bicycles and rail networks.

B. UTILITIES, CONTRIBUTIONS AND STRUCTURE OF THIS SURVEY

This survey covers a majority of the content related to security, privacy, trust-management and protocols for smart M-IoT networks. The content presented in this article is competent compared to the existing surveys and is different in terms of comparative study, which will help its readers follow the parameters and ideology of existing works. Further, this survey can be used by the researchers at any level; especially new researchers can gain a lot from the comparisons and the roadmap sections. Academicians can follow this article to teach new trends related to the security of M-IoT and its advancements. This work can help industry researchers to follow what has been done and what can be carried further while deploying applications related to M-IoT. The open challenges presented in the lateral part of this article will help to define problem statements and can be used as a rationale for continuing research on security, privacy and trust aspects of M-IoT.

This is a comprehensive survey that collectively covers security, privacy, and trust for smart M-IoT, which otherwise are presented as individual topics in the existing surveys. The tabular studies provide a single source to understand the novelty and reach of existing state-of-the-art solutions for smart M-IoT as per the understanding of the authors. The roadmap and comparisons with the related survey articles along with key contents to follow for enhancing the knowledge of this subject are given in Section II. Section III presents characteristics, challenges, technologies and standards, an overview of security, privacy and trust along with their methodologies for evaluation. Section IV gives details on secure frameworks for smart M-IoT, Section V discusses the security-aware protocols, Section VI presents privacy preservation approaches, Section VII gives details on trust management approaches, Section VIII discusses physical layer security and Section IX gives details on the handover security for smart M-IoT networks. Research Challenges, open issues, and future directions are presented in Section X. Finally, Section XI concludes this article. The details of abbreviations and key terms used throughout the paper are presented in Table 1.

II. ROADMAP AND COMPARISON WITH RELATED SURVEY ARTICLES

Fig. 2 helps to follow the roadmap of different surveys presented over the period of time that can be used for selecting an appropriate approach for justifying the requirements of M-IoT networks in terms of security, privacy, and trust. In addition to this, Table 2 provides comparative evaluations and reachability of existing studies which are closely related to the survey presented in this article. There are limited works that focus on the details of M-IoT. Only a few of them have written in parts about such requirements and technologies for supporting communications in smart M-IoT. Despite the limited literature in this direction, some of the key and broad surveys have been selected which provides sufficient material

TABLE 1. Abbreviations and key terms.

Abbreviation	Full Form	Abbreviation	Full Form
ACL2	A Computational Logic for Applicative Common Lisp	NFV	Network Function Virtualization
AP	Access Point	OMA-DM	Open Mobile Alliance-Device Management
AMQP	Advanced Message Queuing Protocol	PKI	Public Key Infrastructure
AR/VR	Augmented Reality/Virtual Reality	PWD	Password
AKA	Authentication and Key Agreement	P2MP	Peer to Multi Peers
AKA'	Authentication and Key Agreement Prime	P2P	Peer to Peer
AS	Authentication Server	PSK	Pre-Shared Key
AAA	Authentication, Authorization, and Accounting	PANA	Protocol for Carrying Authentication for Network Access
AVISPA	Automated Validation of Internet Security Protocols and Applications	PMIPv6	Proxy Mobile IPv6
BAN	Burrows–Abadi–Needham	QoE	Quality of Experience
CSI	Channel State Information	QoS	Quality of Service
CoAP	Constrained Application Protocol	RPMA	Random Phase Multiple Access
CPS	Cyber-Physical Systems	RSSI	Received Signal Strength Indicator
DoS	Denial of Service	RADIUS	Remote Access Dial In User Service
D2D	Device to Device	RPL	Routing Protocol for Low Power and Lossy Networks
DDoS	Distributed Denial of Service	RFID	Radio-frequency identification
DNS-SD	Domain Name Server-Service Discovery	SFTP	Secure File Transfer Protocol
EKE	Encrypted Key Exchange	SPAM	Secure Password Authentication Mechanism
EAP	Extensible Authentication Protocol	SSL	Secure Sockets Layer
GTC	Generic Token Card	SPFP	Security Protocol for Fast PMIPv6
GSM	Global System for Mobile Communications	SOA	Service Oriented Architecture
HOTA	Handover Optimized Ticket-based Authentication	SIP	Session Initiation Protocol
HTTPS	Hypertext Transfer Protocol Secure	SIR	Signal-to-Interference Ratio
IP	Internet Protocol	SINR	Signal-to-Interference-plus-Noise Ratio
6LoWPAN	IPv6 and Low-power Wireless Personal Area Network	SDN	Software Defined Network
LoRaWAN	Long Range Wide Area Network	SQL	Structured Query Language
LEAP	Lightweight Extensible Authentication Protocol	TR-069	Technical Report -069
LTE-A	Long Term Evolution- Advanced	TA	Ticket-based authentication
LTE-M	Long Term Evolution for Machines	TCP	Transmission Control Protocol
LPWAN	Low Power Wide Area Network	TLS	Transport Layer Security
M2M	Machine to Machine	TTLS	Tunneled Transport Layer Security
MD	Message Digest	UNB-IoT	Ultra Narrow Band Internet of Things
MQTT	Message Queuing Telemetry Transport	UDP	User Datagram Protocol
M-IoT	Mobile Internet of Things	WEIGHTLESS-N	Weightless-Narrow band
MIMO	Multi-Input Multi-Output	WEIGHTLESS-P	Weightless-Private/Platanus Technology
NB-IoT	Narrow Band Internet of Things	WEIGHTLESS-W	Weightless-Whitespace
NFC	Near-Field Communication	WIMAX	Worldwide Interoperability for Microwave Access

TABLE 2. Comparison with related survey articles.

Article	Focus	Smart M-IoT	Security	Privacy	Trust	Classifications	Protocol Security	Handover Security	Framework Security
Medaglia et al. [29]	IoT	No	Yes	Yes	No	No	No	No	No
Køien et al. [30]	IoT	No	Yes	No	Yes	No	No	No	No
Bonetto et al. [31]	IoT	No	Yes	No	No	No	Yes	No	No
Chang and Chen [32]	IoT	No	No	No	Yes	No	No	No	No
Bhattasali et al. [33]	IoT	No	Yes	No	No	No	No	No	No
Roman et al. [34]	IoT	No	Yes	Yes	No	Yes	No	No	No
Yan et al. [35]	IoT	No	No	No	Yes	Yes	No	No	No
Jing et al. [36]	IoT	No	Yes	Yes	Yes	Yes	Yes	No	No
Sicari et al. [37]	IoT	Yes	Yes	Yes	Yes	No	No	No	No
Arias et al. [38]	IoT	Yes	Yes	Yes	No	No	No	No	No
Malina et al. [39]	IoT	No	Yes	Yes	No	Yes	Yes	No	No
Li et al. [40]	IoT	No	Yes	Yes	Yes	Yes	No	No	No
Zhou et al. [41]	IoT	No	Yes	Yes	No	No	No	No	No
Yang et al. [42]	IoT	No	Yes	Yes	No	Yes	Yes	No	No
Chen et al. [43]	IoT	No	Yes	Yes	No	Yes	Yes	No	Yes
Feng et al. [44]	MC	No	Yes	Yes	Yes	Yes	No	No	Yes
Yang et al. [45]	IoT	Yes	Yes	No	No	No	Yes	No	No
Our Survey	M-IoT	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

to be followed for covering the aspects related to security, privacy, and trust. From the comparisons, it is evident that the closely related survey is the one provided by Feng *et al.* [44], but it covers major portions related to Mobile Crowdsourcing (MC), which is not so tightly related to the requirements of smart M-IoT. The other studies in [29]–[36], [39]–[43] do not

focus on major considerations which are mandatory to form a highly secure, private and trustworthy M-IoT networks. Sicari *et al.* [37], Arias *et al.* [38] and Yang *et al.* [45] have discussed the concepts related to M-IoT, but do not cover enough details on the security, privacy and trust management in smart M-IoT. In addition to these, there are no comparative strategies provided for discussing the protocol and framework security in any of these surveys, which is a major limitation. Further, handoffs are the major part of mobile-oriented networks, which are not evaluated in the existing studies. Thus, the necessity of such a study, in-depth evaluations and conceptual-reachability of the proposed survey will help researchers to gain insight into the requirements of secure communications in smart and connected M-IoT. In addition, Table 3 presents some of the other key contributions, which can be followed for understanding the present standings in the security of M-IoT devices and its applications.

TABLE 3. Some key contributions to follow for security, privacy and trust in smart M-IoT.

Approach	Author	Ideology
TRIFECTA	Sen et al. [46]	Security, Energy efficiency, and Communication capacity
Jamming mitigation	Tang et al. [47]	Hierarchical security game
SEGB-AKA	Parne et al. [48]	AKA protocol-based solution
SNAuth protocol	Dao et al. [49]	Peer-aware communications
Low-cost security for IoT	Mangia et al. [50]	Rakeness-based compressed sensing
Enhanced attestation and security	Wang et al. [51]	Security-enhanced attestation and policy-based measurement mechanism
Traffic-aware patching	Cheng et al. [7]	Patching with limited resources and time constraints
Secure game theoretic approach	Sedjelmaci et al. [52]	Anomaly detection technique
Security access protocol	Giuliano et al. [53]	Secure key renewal
Lightweight masked AES	Yu et al. [54]	Dynamic differential logic
Secure NFC-based approach	Ulz et al. [55]	RSSI based trilateration algorithm
Security situation awareness	Xu et al. [56]	Semantic ontology and user-defined rules
Privacy protector	Luo et al. [57]	Slepian-wolf-coding-based secret sharing

III. SMART MOBILE IoT NETWORKS AND ITS SECURITY: AN OVERVIEW

This section presents the characteristics and challenges of smart M-IoT. The details are presented on the different types of technology enablers, standards, and general stacks for implementing such a network.

A. CHARACTERISTICS OF SMART MOBILE IoT NETWORKS

Smart M-IoT focuses on reliable and sustainable connectivity between the devices on the move, as shown in Fig. 3. Smart M-IoT focuses on the establishment of a trust relationship between the devices through an enhanced reputation-cycling. Dependence on Machine to Machine (M2M) communication [58], Device to Device (D2D) marking, in-built-service sharing, and energy conservation are the key characteristics of M-IoT. With the devices operating in a battery constrained environment, M-IoT characterizes on the utilization of technologies that offer a wide range but at low battery consumption. The characteristics of smart M-IoT can be summarized as follows:

- M-IoT includes devices with low power, but operable up to a wide range with lower complexity and lesser resource consumptions.
- Supports ultra-dense communication with a unique feature of reliability despite such a huge number of devices operating simultaneously.
- M-IoT may be subjected to frequent handovers and may be involved in inter- or intra-handovers depending on their network design and deployment.
- Licensed and shared spectrum usability with a primary focus on services similar to short messages. Most of the applications do not require any retraining, and configurations are automatically loaded as a part of the application program.
- Smart M-IoT applications and services are vendor-specific. However, the licensing of narrow bands can be governed by small-scale network organizations with core setups at the big business houses.
- M-IoT operations are dependent on the synergy among the mobile operators and rely heavily on the trust-relationship for their security and distributions.
- One-tap facilities for all the services, where a user just has to install and load a required feature for experiencing the applications that focus on consumer-electronics, healthcare of smart home automation.
- M-IoT needs media-independent support for most of the applications as some of the entities may be operating on 3G, while others may have 4G/LTE or even the upcoming 5G accessibility through mmWave functionalities.
- Virtualization and privatization of services are the other main characteristics of M-IoT. Virtualization has further been leveraged through the properties of network slicing, which is one of the solutions for distributed security.
- Support for immediate acquisition, decision and action are the major features of smart M-IoT. Management of the information and building contextual relationships are the other unique characteristics of smart M-IoT.

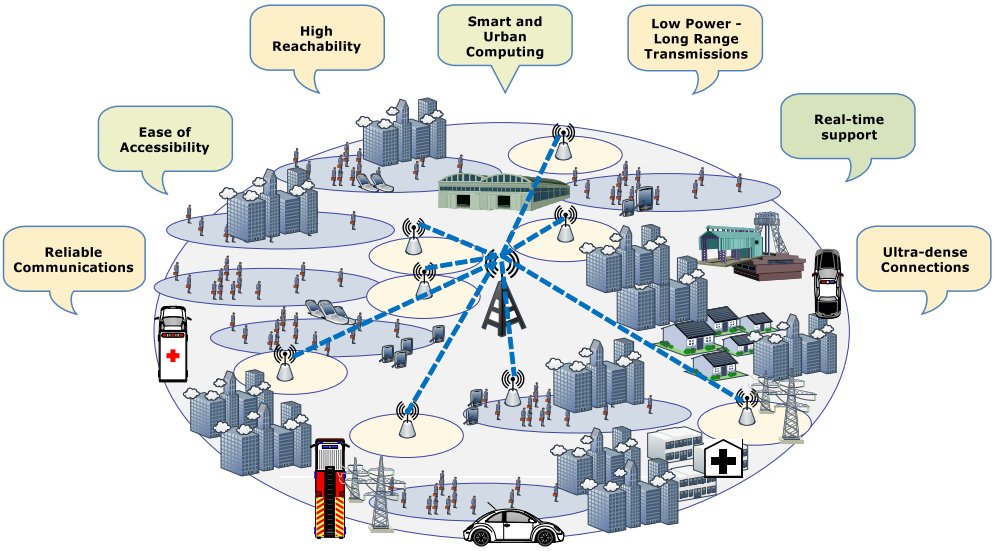


FIGURE 3. An exemplary illustration of M-IoT scenario and trends in modern day networks. The figure shows crucial aspects and properties to be satisfied for the efficient implementation of M-IoT on the backbone of cellular infrastructure.

B. CHALLENGES OF SMART M-IoT

Despite a huge set of advantages, there are some crucial challenges associated with the fully-functional usability of smart M-IoT applications. These include,

- Complexity of design: M-IoT faces a major challenge because of design complexity for both its applications as well as network. The applications must be low-complex and must not require extra knowledge for operations by its users. Further, with the requirements of ease of use, M-IoT may cause an excessive burden on the developers for designing an easy to follow and deploy environment.
- Interaction policies: Smart M-IoT is governed by the rules through which applications interact with each other for facilitating the services to its users. However, the difference in the configuration and operable technology makes it difficult for using common interaction policies for all M-IoT devices. Thus, the formation of rules and generation of interaction policies through consensuses are extremely tedious in M-IoT.
- Security: Independent of technology, security has always been a concern for all types of IoT applications. Prevention against known and unknown attacks and mitigation of zero-day possibilities are the key requirements for security solutions which aim at regulating M-IoT applications [61]. Security solutions must be light-weight and should be able to handle the trade-offs with the performance of a device or the network. Apart from general security, these networks are also subject to crucial requirements of handover security, which can be obtained through existing authentication mechanisms while focusing either on pre-authentication or post-authentication mechanisms depending on the needs and requirements of an application. Management of insider threats and policing are other requirements of security solutions [62]–[65].
- Privacy: With most of the applications personalized in M-IoT, leakage of a users' information may pose a huge threat to the entire network and can destroy an individual's belongings. With billions of devices in place, data privacy may be a reason for huge performance overheads in these networks. Thus, it is inevitably important to support data privacy which is otherwise a key challenge for smart M-IoT.
- Trust: Security and privacy are established through trust-relationships between the service providers and the users. Trust validations and support for common-reputation systems that can guarantee a low-overhead based mechanism for trust-maintenance are a huge challenge for smart M-IoT networks.
- Low-complexity protocols: Different applications need different protocols to communicate, which raises concerns about compatibility issues in terms of protocol selection and arriving at a general agreement during the sharing of context between the cross-platform applications. Thus, designing of low-complex protocols with high compatibility and ease of upgrading are the key challenges to handle in smart M-IoT applications.
- Lifetime: Since the devices in M-IoT are operable through batteries, it is required that the applications, as well as network architectural support functions, should not cause an excessive computational burden on the devices which may deplete their resources leading to a network shutdown. Thus, enhancement of life, capacity and coverage should be managed in smart M-IoT networks.

TABLE 4. Types of attacks in M-IoT.

Type	Attack	Motive	Vulnerability
Passive	Interception	Information disclose	Insufficient authentication and validation
	Release of message	Information disclose	Insufficient authentication and validation
	Traffic analysis	Information disclose	Lack of encryption
	Sniffing	Information disclose	Insufficient security validation
	Keyloggers	Information disclose	Misconfiguration and design flaws
Active	DoS	Information distort and destruct	Buffer overflow, Race condition
	DDoS	Information distort and destruct	Buffer overflow, Race condition
	Distributed DoS with Reflectors	Information distort and destruct	Buffer overflow, Race condition
	Replay attack	Information discovery	Incorrect permissions, User and sever compromise
	Masquerading	Information discovery	Insufficient security validation
	SQL injection	Information discovery	Incorrect permissions
	Man in the middle	Information disclose and discovery	Misconfiguration and design flaws, Insufficient security validation
	Modification	Information disclose and disrupt	Misconfiguration and design flaws, Insufficient security validation

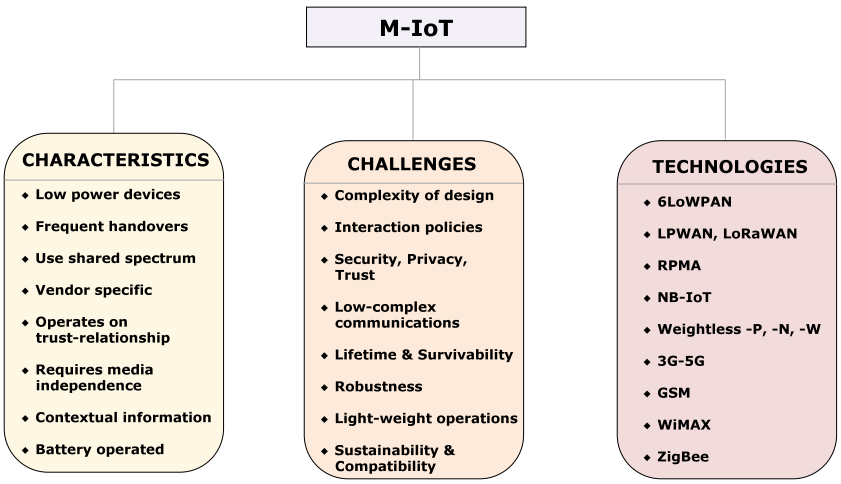


FIGURE 4. M-IoT Overview: General characteristics of M-IoT networks, challenges in implementation, and technologies available for successful deployment of M-IoT.

Apart from these issues, some of the key attacks in M-IoT, against which effective countermeasures are required, are listed in Table 4 and the summaries of characteristics, challenges and technologies are shown in Fig. 4.

C. M-IoT TECHNOLOGIES, STANDARDS, AND STACKS

There are a plethora of articles that have discussed various technologies, standards, and stacks which are applicable to M-IoT. However, to make this article self-contained, general information on some of these are presented in this section. For further clarification, an illustration of a general overview of a stack applicable to M-IoT is shown in Fig. 5, which can be further studied from EU Butler Project (https://iot-butler.eu/) [59], [60]; and an exemplary illustration of security, trust and privacy formations in M-IoT is presented in Fig. 6. At present, M-IoT is based on low power and wide range technologies, which include 6LoWPAN, LPWAN-based LoRaWAN, Random Phase Multiple Access (RPMA), NB-IoT, Ultra Narrow Band-IoT (UNB-IoT) Weightless-W, Weightless-P, and Weightless-N [12], [66]–[70]. Besides these, existing network architectures such as 3G, 4G/LTE, Worldwide Interoperability for Microwave Access (WiMAX), ZigBee, Global System for Mobile Communications (GSM), can be used for supporting

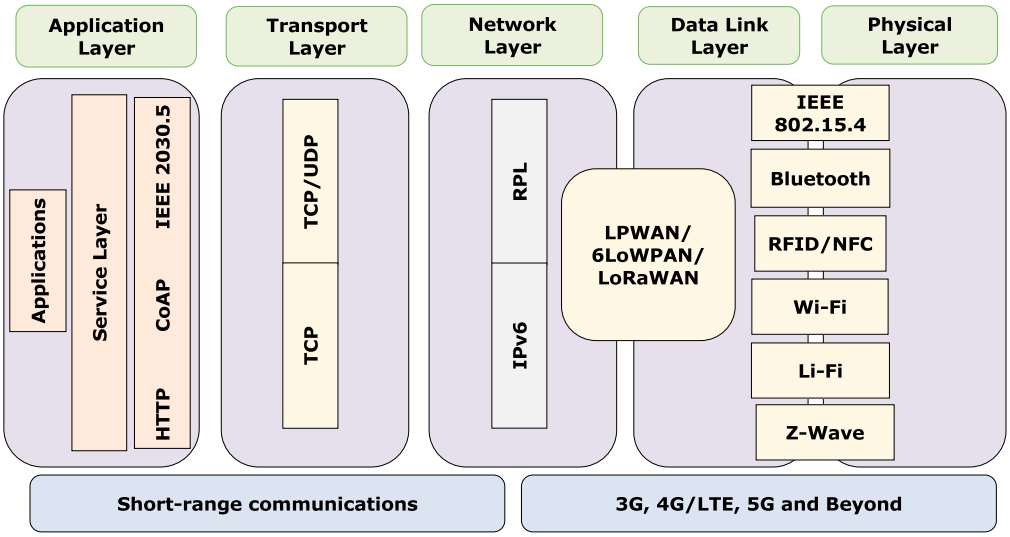


FIGURE 5. An exemplary overview of a general communication stack applicable to smart M-IoT (EU Butler-IoT Project (https://iot-butler.eu/)) [59], [60].

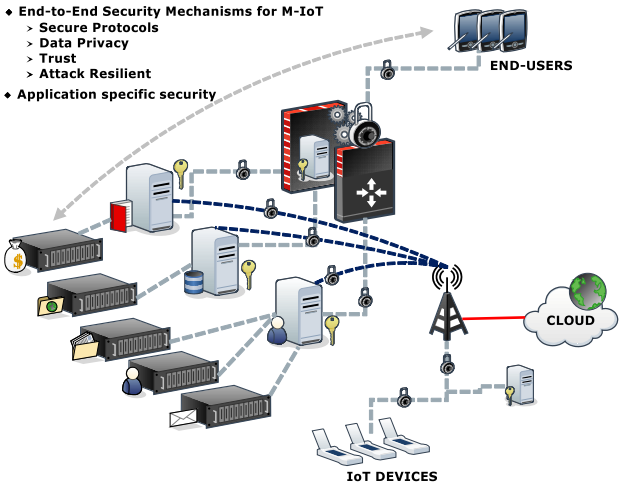


FIGURE 6. An exemplary illustration of security, trust and privacy aspects in M-IoT.

applications in M-IoT. The standards for IoT vary depending on the application scenario and the configurations of the devices used in M-IoT. In general, various open projects, organizations, alliances, and IEEE provide a series of standards that primarily focus on supporting smart applications in IoT networks. Some of these are TR-069, OMA-DM, DNS-SD, IEEE series 2413, 21451, 11073, 2200, 2030, 1905, 1900-03, 1701-03, etc. Further details on each of them can be obtained from [71] and [72]. Apart from these technologies and standards, there are different types of stacks used for supporting smart mobile communications in IoT. However, the general use of stack can be application or network-specific and varies as per the configurations of each device. Usually, the stack selections will be affected by the technologies adopted for communications in M-IoT. It is recommended to form compatible and ready-to-integrate models which can be easily deployed in any sort of scenarios irrespective of the device configurations, type and make. Stacks applicable for general IoT can be used for extending services in M-IoT but with modifications to their operating policies as the majority of the traffic flow is maintained on the devices that are non-static in nature [73]. Some of the key solutions for IoT stacks include IBM-Watson IoT [74], Microsoft Azure IoT suite [75], OpenIoT [76], OCF [77], etc.

D. VULNERABILITIES IN SMART M-IoT

Information security is the major factor driving security in smart M-IoT. These are lead by the studies on vulnerabilities and loopholes at the hardware level, protocol-level, and application-level of M-IoT. Vulnerabilities are studied based on the mode of attack and assessment into different types of classes, related to hardware, protocol, application, software or organizational [78], [79]. The exploitation of the known vulnerabilities can be prevented by taking several countermeasures against each of the exploits, however, for unknown vulnerabilities, it is tedious to distinguish and resolve until the severity of exploits are unknown [80].

For major of the smart M-IoT, date of release or disclosure plays a crucial role in prevention and it helps to decide the window of prevention. The release of security patches and security updates are further accounted for the disclosure dates. Usually, increasing the speed of deliverables causes an impact on the debugging phase, which may lead to several possible vulnerabilities unhandled. In smart M-IoT, most common vulnerabilities are identified as the OS level or the application level. The protocol level vulnerabilities are usually known and steps can be determined based on the deployment. However, in several cases, where protocol

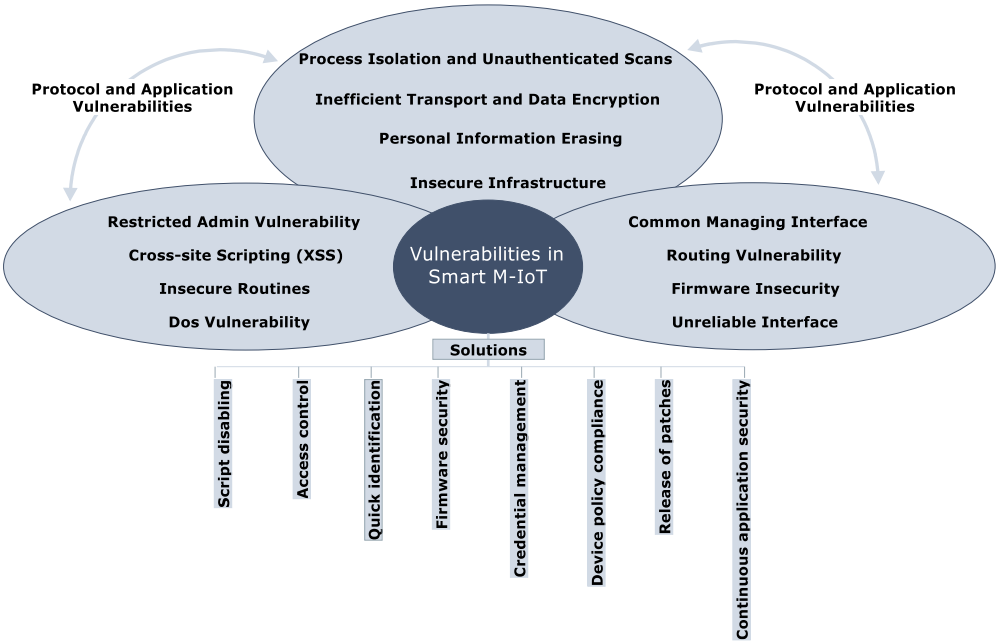


FIGURE 7. An illustration of vulnerabilities in smart M-IoT with possible remedies.

security is based on credentials, their theft can lead to severe consequences. Some of the key issues causing/leading to vulnerabilities, as discussed by Open Web Application Security Project (OWASP) [81]–[84] (Fig. 7), for smart M-IoT are listed below:

- Insecure infrastructure: One of the main causes of vulnerabilities in smart M-IoT is the insecure infrastructure that supports transmissions for the involved devices. Architectural layout plays a key role in accessing the network and prioritizing its security. The dominant mode of connections for M-IoT is a cloud, edge, fog architectures, which needs to be prevented from unauthorized access.
- Common managing interface: The services which are obtained through a common managing interface are more likely to fall prey to vulnerabilities than the services which are handled by the individual servers. This can be further seen from another dimension. The exploit of vulnerabilities over a common interface may expose the additional services provisioned through it.
- Insecure protocols: The protocols mounted for data sharing and authentication in smart M-IoT may be vulnerable to attacks leading to authorization and access control. Thus, the unlimited role of users and non-predetermining the security of the underlying protocol can be other issues causing vulnerabilities in smart M-IoT.
- Inefficient transport and data encryption: Usually the broadcasted traffic is not encrypted to avoid performance issues. Thus, vulnerabilities related to access control, such as eavesdropping, is always possible because majority messages are not encrypted.
- Cross-site scripting (XSS): Such vulnerabilities are related to insecure web access and are based on access controls such as the same-origin policy, which is applicable to all the devices in M-IoT. Self and mutated XSS are major concerns to be taken care of while dealing with these types of vulnerabilities.
- Firmware insecurity: Identification and decision on firmware insecurity is not an easy task. These involve expertise and a common user may easily be fooled to disclosing his/her devices to malicious agents. Such agents exploit the firmware insecurity and lead to several open ports which allow backdoors, worms, trojans, botnet and ransomware to exploit the known/unknown issue on the device.
- Process isolation and unauthenticated scans: Several users allow different processes to take control of the device and allow unauthenticated scans. Majority of them are caused by presenting the requirements of an installed application. Non-evaluation of the downloaded application and free access to control the devices leads to several application-level vulnerabilities.
- User policies and patching: In the majority of the cases, vulnerabilities are exploited due to limited action from the users. Delays in updating the security settings and unawareness of the released patches lead to the majority of the vulnerabilities. Nowadays, organizations are taking several key steps to force the security updates, still, there is a gap between the user-understandings and update procedures, which lead to several exploits and threats on smart M-IoT.

Key solutions and possible remedies for preventing the above-discussed vulnerabilities are given below:

- Access control: Limiting the control over device-data and allowing authorized applications to access can help limit the exploits on the known vulnerabilities. Evaluating the content to be accessed and components of shared-data can further elevate the security of devices in smart M-IoT.
- Quick identification and release of patches: It is determined that mode and action and time of action play a key role in preventing a device. Thus, quick identification of vulnerability, the release of security patches and installing them are major actions that can prevent severe attacks.
- Credential management: For the network-based vulnerability prevention, credential-management, its security, and protection can help to ensure security and privacy for devices. Credential management prevents access to sensitive data and keys which are necessary for encryption as well as securing the communication channels.
- Firmware security: It is desired at the developer level to maintain the bug-free release of firmware. Thus, a strong debugging and evaluation against known vulnerabilities must be carried before supplying it to the users or even assemblers.
- Device policy compliance: It is necessary that users must comply with the policies laid for a particular device and should not break the codes, which may allow unauthorized applications to take control over a device. Such a vulnerable device may expose the entire network and it is the responsibility of the user to maintain the functionality of the device within the laid guideless.
- Script disabling: Majority of developers have shifted their focus on developing applications which do not require client-side scripts. Thus, from futuristic developers, preventing scripts can allow security against vulnerabilities without affecting the services.
- Continuous application security: Identification of application security must be followed by the release of the security update or newer versions. Thus, continuous monitoring of applications is required to prevent possible vulnerabilities. Moreover, this is also an effective strategy to prevent the possibilities of zero-day threats and attacks.

There are several studies that have been dedicated to vulnerabilities in M-IoT and can be followed from [85]–[92]. Based on these, it becomes inevitably important to understand the concept, issues, scope and strength of the present state of security, privacy and trust for smart M-IoT.

E. SECURITY, PRIVACY, AND TRUST FOR SMART M-IoT

Because of a difference in the mode of deployment and applicability, security, privacy, and trust of M-IoT devices are of utmost importance. These differences in the characteristics of involved devices raise an alarming factor for securing and isolating each user's operations as the variation in behaviour and operations of each device may lead to different kind of threats based on their specifications [93]. Thus, it is important to study all the aspects related to the security, privacy, and trust of smart M-IoT networks. Majority of the threats occur due to inadequate configurations of security properties and some of them are the vulnerabilities that remain undetected over a course of time due to the negligence of their developers [94], [95]. Minimizing data acquisition, supporting M2M routing, resolving hidden terminals and encryption can help to secure and privatize each user's data and information.

F. METHODOLOGIES FOR ANALYSES OF SECURITY, PRIVACY, AND TRUST IN SMART M-IoT

An approach is secure for the time being it is not broken, which means security is difficult to analyze as there are no direct simulators and emulators to be used for evaluation of a system for these requirements. Visualization is another big issue for such requirements. Visualization of trust can be obtained as it is comparatively easier to define trust as a metric between the communicating entities; whereas security and privacy are governed by rules and policies which can only be evaluated in an attacker environment. Creation and demonstration of such an environment are difficult as it requires a lot of automation, which is not applicable to most of the available tools. Majority of the solutions are formally analyzed using Burrows–Abadi–Needham (BAN) logic, which is operated on belief theory [119], [120]. Some approaches follow reduction techniques, while others simply rely on evaluating the computational cost of operations. Apart from these, some other methods include formal semantic evaluations, equational theory, etc [121]. Cryptographic solutions can be evaluated using the random oracle model, inductive methods, provable security, etc [122]–[124]. Model-checking and theory of proving are used by some approaches for evaluating the flow of their solution. There are certain tools available which can be used for these evaluations like, Automated Validation of Internet Security Protocols and Applications (AVISPA), A Computational Logic for Applicative Common Lisp (ACL2), ProVerif, Scyther, etc [125]–[128]. Irrespective of these evaluations, it is recommended that solutions should conduct certain case studies while presenting outputs of their proposed schemes and should demonstrate the effects on the performance of the system and the network.

IV. SECURE FRAMEWORKS FOR SMART M-IoT

M-IoT networks are vulnerable to a different set of attacks which can be launched due to improper configurations and deployment strategies. It is required that these networks are deployed with ultra-reliable formations, which help to hinder the launching of any unknown as well as known attacks. Further, security implications, assessment, and threat modelling can help to identify any such possibilities at a prior, which may support prevention against intruders during the operations of IoT devices [129]–[131]. Siboni *et al.* [132] highlighted the importance of a framework for securing the content in wearable IoT devices, which are considered as an important part of M-IoT systems. The authors developed

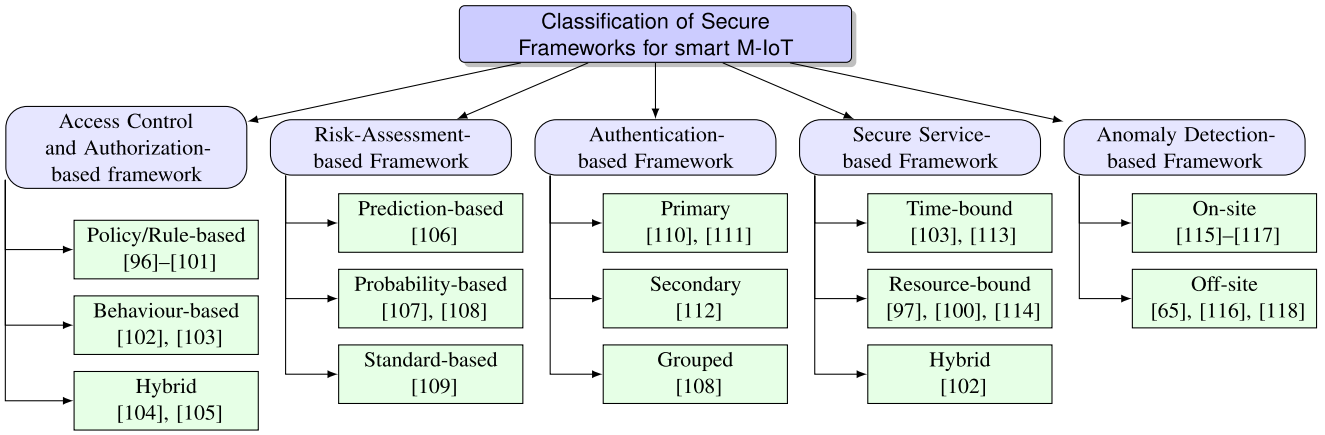


FIGURE 8. A broad classification of the security framework for smart M-IoT. The security approaches focusing on the frameworks for M-IoT can be broadly classified on the basis of Access control and Authorization, Risk-Assessment features, Authentication, Secure Services, and Anomaly Detection.

an innovative testbed setup for evaluating the security policies of dynamic IoT devices. The need of the hour is to provide such a framework that can be used for supporting the security requirements of Cyber-Physical Systems (CPS) that heavily rely on M-IoT devices for their regular operations [133]. Authorization, privacy as well as physical security and anonymity should be the core aspect of frameworks, which primarily focus on the security of smart M-IoT networks [134], [135]. Although the existing frameworks provide a base for network formations, these have to be operated with a different set of schemes, protocols, as well as policy-mechanisms for a fully-reliable and secure network establishment.

The smart frameworks should also support the cryptic techniques, that can be built into its system through separate modules [136]–[138]. Deployment of M-IoT through SDNs and the use of smart IDS are the future aims of the present systems, which tend to facilitate the security of applications operating over low-powered devices [139], [140]. Use of newer concepts, such as fog architecture, Internet of drones, catalytic computing and osmotic computing, can be considered as a base for developing frameworks that can sustain the burden of security as well as the performance at the same time [141]–[145]. Based on the security requirements, a taxonomy is presented which classifies the security frameworks for smart M-IoT, as shown in Fig. 8. The details of these classifications are presented below:

A. ACCESS CONTROL AND AUTHORIZATION-BASED FRAMEWORK

The security of devices in M-IoT is subject to the management of accessibility and authorization for using particular services as well as personal data. This type of frameworks helps to limit control over the usability of network components and provides strong mechanisms for securing the users. The strength of its security lies in the novelty of architecture used for supporting convergence services to M-IoT users. There are some works in this direction, which highlights the main features of access control and management along with user and service authorizations. However, the majority of them operates on general IoT scenario and lacks evidential commitment on their applicability to smart M-IoT scenarios. The access control and authorization-based frameworks can be further classified into three main types as shown below:

- Policy/Rule-based: The main aspects of such type include user authentication, device authentication, resource authorization, Constrained Application Protocol (CoAP) access control and etc. The solutions in this direction focus on acquisition and control over services and user modules to infrastructure security of its network. The main property of this type is the formation of governing conditions, on the basis of which, certain rules and policies are defined for securing the users and services. Solutions in [96]–[101] focus on providing frameworks which utilize user and device authentication through policy and rules over device operations in different network setups.
- Behaviour-based: This type of access control and authorization depends on the way of a user's interaction with other users and entities in the network. The operational activity of the users is taken into account for access control and defining conditions of authorization for demanded services. Such types of security frameworks are well suited for modern services such as smart building, smart cities, and smart factory [102], [103].
- Hybrid: There are certain solutions for access control and authorization, which form policies or rules by using behavioural aspects of the network entities to ensure its security and continuity in operations. Such types of frameworks are termed as hybrid access control and authorization-based frameworks. Credential-based services and intelligent solutions use such kind of mechanism for ensuring security in a network [104], [105].

B. RISK-ASSESSMENT-BASED FRAMEWORK

Identification of potential conflicting components and users through detection modelling is mainly studied under risk-assessment-based frameworks for security in

smart M-IoT. Such kind of frameworks helps to pre-identify any potential risks involved in leveraging services through a particular aspect of the network. These aspects may include situational awareness of every involved entity of the network. Based on the mode of identification, risk-assessment-based frameworks can be further classified into three main types as shown below:

- Prediction-based: The Framework which identifies and manages risk through predictive or estimated evaluations of the network components are termed as prediction-based risk assessment frameworks [106]. Such type of frameworks considers prior and current states to identify the mode of operations and uses decision modelling to arrive at a decision of potential risks in the network.
- Probability-based: In probabilistic-based, the network is evaluated for different kind of operations which are executed over a period of time. Then, each process is operated with a probabilistic model which then helps to finalize the probabilistic cost of the networks, while providing knowledge about the factors which dominates the most and can affect the performance as well as security policies. The most common aspect of such frameworks is to identify attack success possibilities in a network while using parameters like false positives, false negatives, accuracy, recall, and precision as considered in [107], [108].
- Standard-based: Most of the organizations have a pre-defined set of conditions which are to be fulfilled by every framework which aims to provide a special kind of services to its users. Majority of these conditions are the benchmark and supported by standards organizations such as the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunications Union (ITU). These organizations provide guidelines for every framework to justify its security considerations for the defined services. One of the examples can be the forensic study of a framework for its applicability to support on-demand services to mobile users [109].

C. AUTHENTICATION-BASED FRAMEWORK

Authentication of the users and devices in smart M-IoT is of utmost importance and highly crucial. It is required that all the services are provided only to the users which authenticates themselves with the security servers usually Authentication, Authorization, and Accounting (AAA) in any network. These secure servers ensure the safety of other legitimate and authenticated users by providing a secure mode of communications. One of the crucial aspects of authentication is the positioning of authentication-server along with the number of passes required to reach it. The mode of authentication is quite vast, but for smart M-IoT, it can be classified into the primary mode of authentication, the secondary mode of authentication and group-authentication. The choice among each of them depends on the types of device, network architecture and types of services to be supported by the involved entities. The details on each of them are provided below:

- Primary: The authentication which is performed with the core of any network while using the secure channels between the entity and the authentication server is known as primary mode [110], [111]. Such kind of authentication is much secure but often suffers from the consequences of long paths and requirements of route optimizations. Despite its advantage of providing robust security, it often causes additional overheads if each time an entity has to be authenticated through it even in the cases it is always present in the perimeter of the same network. However, the majority of existing solutions prefer a primary mode of authentication because of the ease of deployment and maintenance.
- Secondary: Usually, networks which have data to be constrained in a particular periphery or premises opt for the secondary mode of authentication. Such a model is responsible for securing a particular set of nodes which are entitled to communication within the zone of the secondary authentication server [112]. Secondary authentication also uses an initial primary authentication for registering its services and users to the core of the network and after initial phases, all the security concerns are managed by it. With the evolution of smart networks, it is preferred to use a hybrid mechanism as it helps to provide a flexible as well as robust security that too with lower overheads.
- Grouped: Another mode of authentication can be the group authentication, which entitles similar entities to be authenticated as a group through a common gateway. Group authentication depends on the type of devices involved in a group, and the procedure of authentication depends on their type. Some groups with highly crucial devices may involve strong authentication while the ones with limited resources may require light-weight authentications so as to prevent any excessive utilization of their resources [108].

D. SECURE SERVICES-BASED FRAMEWORK

Type of services affects the security of a network. Some services may require light-frameworks which are easy on resources while others may require fast processing frameworks which operate with lesser delays and fewer overheads. Such type of framework is usually related to the authentication facilities for managing the security of the network as the authentication phase is itself responsible for resource consumption and delays. Based on the requirements of services, these frameworks can be classified into time-bound, resource-bound, and hybrid framework as explained below:

- Time-bound: The frameworks which operate with time as a crucial entity in securing the services and the users of a network are studied as a time-bound services-based framework. As studied in [103], [113], such frameworks are lightweight and highly fast in processing and

evaluation of security policies. Usually, such frameworks perform periodic evaluations on the time consumed in authenticating users and allocating communication uplink for data transmissions. Evaluation time, discovery time, and authentication time are the crucial parameters in time-bound security frameworks.

- Resource-bound: Most of the devices in smart M-IoT are low on resources and suffer from the threat of average lifetime. Usually, their lifetime is driven by the energy and memory consumed by the services operational on each device and often the mandatory services consume the majority of their services [97], [100], [114]. Thus, it becomes important to develop frameworks which focus on the security while keeping control of the utilization of M-IoT resources with a limited burden on the operational control and activity of the device. Such type of frameworks uses checkpoint mechanism to manage the resource consumption for the security of M-IoT applications.
- Hybrid: Nowadays, smart applications tend to be time-bound as well as resource-bound. Thus, there is a requirement of frameworks which can apply both these features while forming a hybrid services-based framework that can use both the resource-checkpoints as well as periodic evaluation of security policies for securing activities in smart M-IoT. Accessibility and response time can be considered as mutual parameters for accessing the performance of such frameworks [102].

E. ANOMALY DETECTION-BASED FRAMEWORK

Identification of false users, false services and false entities in a network are studied under this category. It is a responsibility of the security framework to identify communities and users which pose potential risks to legitimate users of the network. Further, such a classification helps to manage the flow of information as well as limit the accessibility of users with harmful properties and high risks to network services. Anomaly detections are performed by checking the correctness of a device or user against the predefined policies of accurate operations. On a broader side, such frameworks can be classified into on-site and off-site evaluators with the description as given below:

- On-site: The real-time evaluation of the users for legitimate and accurate operations is classified as on-site or real-time anomaly detection. Such type of detections is performed by deploying real-time Intrusion Detection System IDS) which dedicated sniffs the traffic without breaking its flow and without any excessive overheads [115]–[117]. Majority of evaluations are conducted through sandboxes which do not reveal their identity to the users and prohibits anomaly users from accessing the services across the network.
- Off-site: In some cases, real-time evaluations may pose an excessive burden on the network and it is difficult to analyze the high flow of data. Such networks are evaluated off-site at their respective data centres which check for the presence of any abnormal activity for each of its users. Usually, such type is suitable for scenarios which allow delayed transactions without affecting the services such as payment gateways or smart-phone updates [65], [116], [118].

F. SUMMARY AND INSIGHTS

In this section, we have summarized different types of frameworks, which help to secure the operations as well as the network layout of smart M-IoT. The summarized study divides the existing solutions into five broad categories and considering their evaluation metrics and ideologies, a state-of-the-art comparison is presented in Table 5, which compares the key IoT frameworks with specification on smart mobile network formations. The table helps to understand the reachability of each approach and their primary application of interest. These comparisons can be used for understanding what has been attained so far and what are the directions yet to be focused while securing applications in smart M-IoT networks. Hybridizing network layouts with security policies and involving vulnerability assessments can be used for developing security middleware for smart M-IoT applications. As discussed in [96], [97], security resources, user authentication, device authentication, resource utilization and data investigations should be included while developing frameworks for securing smart M-IoT. There are many solutions, which only relies on CoAP, but it is desired to make strategic shifts for enhancing the security of devices and users against known as well as unknown cyber threats.

V. SECURITY-AWARE PROTOCOLS FOR SMART M-IoT

It is to be considered that with the introduction of new technologies for communications, the links between the M-IoT devices have grown up to many Gigabits, which means the window to perform security operations has further decreased, and it is extremely challenging for the researchers to accommodate existing security policies in such a short timing window. Thus, protocols for M-IoT security are yet to be revolutionized on the basis of their applicability and reachability for M-IoT applications. Security protocols prevent unauthorized attempts for using resources or data in a defined network [31], [175]. Communications in M-IoT are usually handled by the dissemination protocols like CoAP, Advanced Message Queuing Protocol (AMQP), Message Queuing Telemetry Transport (MQTT), Domain Name Server-Service Discovery (DNS-SD), etc [176], whereas security is supported either by enhancing the features of these protocols; or by using existing security protocols with the routing schemes; or by designing novel security and communication schemes which are usually specific to applications [177], [178]. Such solutions may operate well in one scenario and may fall prey to different types of attacks if their application area is changed. The success of the security protocols is affected by the compliance degree of a user with the

TABLE 5. State-of-the-art frameworks applicable to M-IoT security.

Approach/ Model	Author (Year)	Ideology	Parameters Focussed	Description
Policy driven security	[Dsouza et al. 2014] [96]	Secure collaboration for users in Fog networks	Security resources, User authentication, Device authentication	This approach focuses on a secure collaboration between the IoT devices by using policy-management of resources through Fog computing architecture. Policy enforcement point is used as a decisive metric, but conflict resolution and anomaly detection are not evaluated in this model.
IoT-OAS	[Cirani et al. 2015] [97]	Authorization architecture for secure services	Computational overheads, Memory utilization, Energy consumption, Authorization	This approach is based on Open Authorization (OAuth), which is a third party for simple and secure authorization of services. HTTP/CoAP services are targeted for security while maintaining the flexible, dynamic and easily configurable properties of the architecture.
DFIF-IoT	[Kebande and Ray 2016] [109]	Digitalized forensic investigation of IoT	Initialization, Acquistion, Investigation	This framework is capable of supporting digital forensics over IoT infrastructures. The authors focused their framework with standard compliance of ISO. The framework operates by classifying content into digital forensic module through reactive and proactive processing.
Authorization and access control	[Pereira et al. 2014] [100]	Secure SOA for IoT	CoAP overheads, CoAP access control	This framework supports security of IoT devices by using a service oriented architecture, which uses Constrained Application Protocol (CoAP) for IoT. This approach also provides strategy for tickets and access control for utilizing the features of existing security protocols.
Security assessment of IoT	[Ge and Kim 2015] [107]	Evaluating security of large scale networks	Reliability, Risk assessment, Attack cost, Attack success probability	This approach provides methodology and technique for assessing security of large-scale IoT networks. The authors use a set of parameters for analyzing the reliability of the network through risk assessment.
VeCure	[Wang and Sawhney 2014] [110]	Resolution of mutual authentication issue for Internet of vehicles	Trust formations, Delay evaluations	This approach provides a mechanism for mutual authentication of nodes in Internet of vehicles. The authors illustrated their approach through a verified proof of concept and illustrated lower-delay approach for message evaluations through trust properties.
SDN-based security framework	[Gonzalez et al. 2016] [101]	Security framework for IoT in grid using SDN	Number of messages, OpenFlow modifications	This framework builds a cluster model for IoT devices through SDN. The common controller is employed to form an intrusion detection and prevention system by using predefined rules on the controller.
Security framework for smart home IoT	[Tao et al. 2018] [113]	Multi-layer cloud architecture-based and ontology-based security	Response time, Token assertion	This framework helps in privacy-preservation and maintain security of devices in a multi-hierarchical cloud formation on the basis of ontology, which is formulated over token and encryption assertions.
Authorization framework	[Seitz et al. 2013] [102]	Access control and authorization through key management	Request processing time, Accessibility	This framework supports a fine grained and a flexible access control to devices with limited power and memory constraints. The framework is capable of supporting authorization requirements of IoT devices.
SecIoT	[Huang et al. 2016] [111]	Robust and transparent security for IoT	User authentication, Device authentication, Authorization, Access management	This framework is capable of resolving the basic security requirements such as authentication, authorization, access control and risk assessment. Trust evaluation and availability are yet to be resolved by this framework for IoT networks.
RFID security framework	[Ray et al. 2014] [108]	Group-based and collaborative approach for scalable security	Computational complexity, Payload analysis, Hash operations, Probability evaluations, Scalability tags	This framework emphasizes on the novel identification technique, which is based on a hybrid approach that helps to support security check handoff for RFID systems in an IoT environment.
SAFIR	[Hernández-Ramos et al. 2015] [103]	Access framework for smart-buildings IoT networks	Access control, Authentication, Evaluation time, Discovery time, Energy conservation	This framework focuses on the security and privacy of smart building IoT networks. The framework provides security functional components for the establishment of flexible sharing models, context-aware security on IoT scenarios s realized through physical-context awareness.
Sensor to cloud security	[Rahman et al. 2016] [114]	Cloud-IoT ecosystem security	Security threats Assessment, (Sensor level, Network Level, Cloud level, Data level)	This framework discusses IoT security framework for mitigating threats identified in the sensor to cloud ecosystem. The framework uses layered hierarchy for securing IoT devices.
SDN framework for IoT	[Sahoo et al. 2015] [98]	SDN-based security framework	Accessibility, Authentication	This framework helps to authenticate devices through policies which are governed by the controller. Also, the policy rules are used for IoT security by managing the node accessibility.
Trustworthy smart car services	[Pacheco et al. 2016] [99]	Anomaly behaviour analysis	Detection rate, Classification Rate	This framework provided IoT security for trustworthy smart car services. This framework uses a set of functions and services for securing these services through threat modeling.
Adaptive security	[Abie and Balasingham 2012] [106]	Risk prediction and assessment	Risk evaluation	This framework focuses on risk-based adaptive security for e-health applications in IoT. The framework uses game theory and context-awareness techniques for prediction of involved risks and upcoming damages.

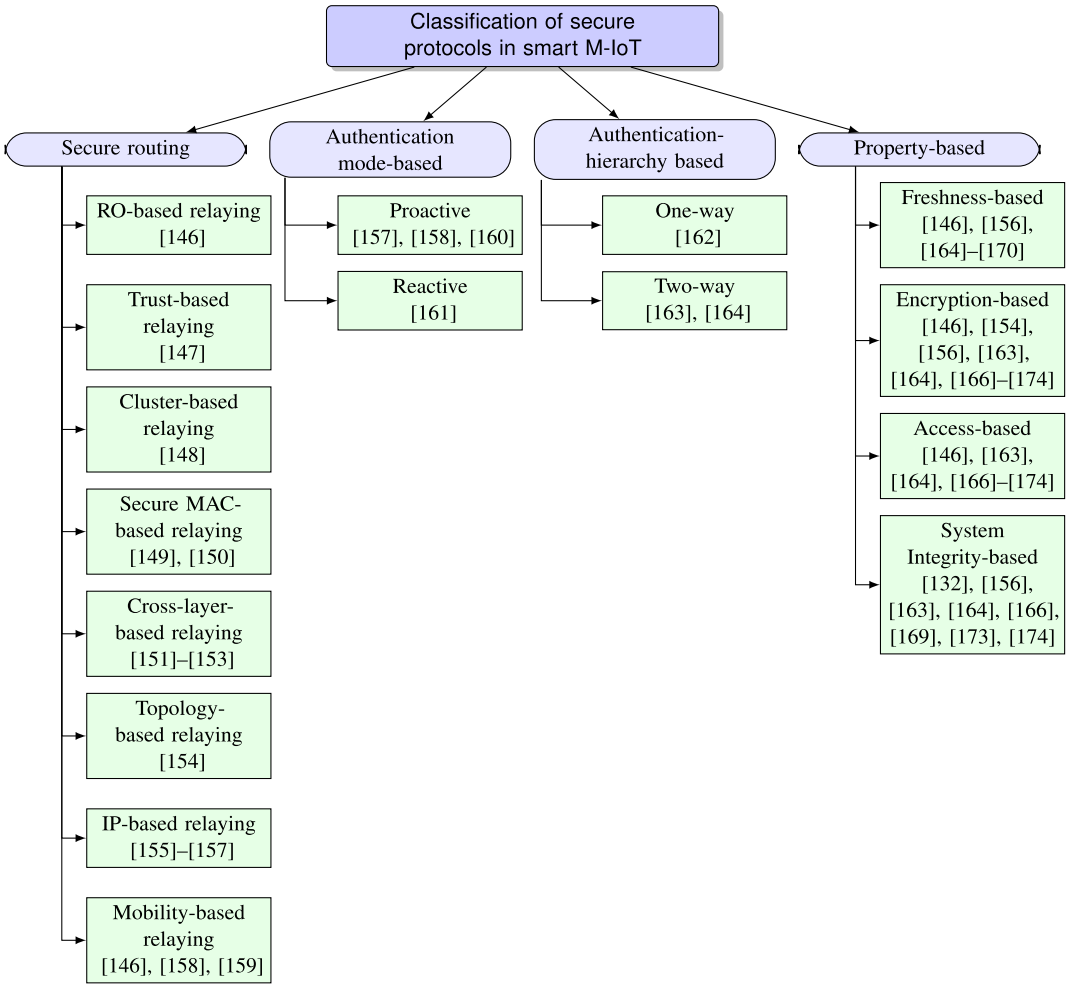


FIGURE 9. A broad classification of secure protocols in smart M-IoT. The existing solutions can be classified into secure routing, authentication mode and hierarchy, and property-based secure protocols.

recommended settings [179], [180]. It is required that security protocols should not affect the performance and their operations (like encryption and decryption) should be completed without many overheads.

Protection of Peer to Peer (P2P) and Peer to Multi-Peer (P2MP) links is one of the major challenges while designing protocols for the security of M-IoT. Protocols can be protected either by following asymmetric mode or symmetric mode in their key operations. The location of the AAA server and its optimized placement are other issues to be resolved in M-IoT. Moreover, Route optimizations are additional concerns which have to be taken care by the security protocols. Previously known protocols, like Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS), Session Initiation Protocol (SIP), can be adopted for network security while authentication can be governed by Authentication and Key Agreement (AKA) as it is one of the standard protocols used for security in 3G. Some other crucial protocols include Extensible Authentication Protocol (EAP), Remote Access Dial-In User Service (RADIUS), DIAMETER, Protocol for Carrying Authentication for Network Access (PANA), Lightweight Extensible Authentication Protocol (LEAP), Protected Extensible Authentication Protocol (PEAP), etc. EAP is further facilitated with suitable extensions as AKA, AKA-prime (AKA'), Transport Layer Security (TLS), Message Digest-5 (MD5), Tunneled Transport Layer Security (TTLS), Encrypted Key Exchange (EKE), Generic Token Card (GTC), Pre-Shared Key (PSK), Password (PWD), etc [181], [182]. Handover protection is also related to the protocols as these are identified as a crucial part of security in M-IoT. Majority of them use EAP-based authentication (EAP-TLS). Some of the key contributions on handover security include Security Protocol for Fast PMIPv6 (SPFP), Handover Optimized Ticket-based Authentication (HOTA), Ticket-based authentication (TA), Secure Password Authentication Mechanism (SPAM), etc [157]. These protocols can be classified into routing-based, authentication-mode based, authentication-hierarchy-based, and property-based mechanisms, as shown in Fig. 9.

A. SECURE ROUTING-BASED

The routing schemes which are available for general networks, be it reactive or proactive, holds true for smart M-IoT setups. Existing routing mechanisms can be used while leveraging the security guidelines to secure the communications between the M-IoT users. From a broader point of view, secure routing-based protocols can be classified into the following types:

- Route Optimization (RO)-based relaying: Finding shortest paths and reducing the path of authentication can be attained through optimized relaying in the networks. Such RO-based relaying often removes dependencies from the intermediate entities to provide low-overhead based solutions for security [146].
- Trust-based relaying: Finding nodes on the basis of trust calculations and using them for transmissions are another kind of security protocols. Such protocols use trust as a weighted metric for calculating paths between the users in M-IoT [147].
- Cluster-based relaying: In some scenarios, network entities operate in a group while depending on a core entity which acts as their head leading to the formation of multiple clusters in the network. There are certain routing protocols which aim to support the security of communication between the cluster heads allowing secure relaying between the nodes with lesser overheads and computational complexity [148]. Clustering is effective in case the protocols depend on group-based authentication, however, in primary and secondary modes of authentication, it may cause excessive overheads.
- Secure-Medium Access Control (MAC) based relaying: Control over timing policies and accessibility of user operations lead to the requirements of a secure MAC-based relaying for users in smart M-IoT. Such relaying protocols use command over congestion window and packet forwarding policies to control the flow of packets as well as uses cryptographic solutions for securing its relaying procedures [149], [150].
- Cross-layer-based relaying: Secure routing can be obtained over the network layer while obtaining properties from other layers such as the transport layer or the MAC layer. The protocols on the network layer use parameters like Received Signal Strength Indicator (RSSI) and use it as a weighted condition to select nodes in smart M-IoT [151]–[153]. Such a relaying can be effective in scenarios where the resources are limited and the lifetime of the network is of utmost importance.
- Topology-based relaying: Identification of nodes on the basis of their location and checking the path of authentication before transmissions lead to the formation of secure topology-based routing [154]. Such protocols are effective where the dynamic nature of nodes is crucial and often changes. However, it is difficult to control such a scenario and topology-aware relaying is often combined with mobility-management procedures for attaining a secure and fast relaying.
- IP-based relaying: This is the core relaying mechanism for the majority of the mobile applications as it uses Mobile IPv6 (MIPv6) and Fast Mobile IPv6 (FMIPv6) procedures to support the selection of nodes. Further, the security in such protocols is provided by proxy-mechanisms and can be seen in various proxy-based protocols such as Proxy Mobile IPv6 (PMIPv6) and F-PMIPv6 [155]–[157]. Such relaying solutions can be combined with media independent schemes to form Media Independent Handover (MIH)-PMIPv6 relaying with specific implementation over smart M-IoT applications.
- Mobility-based relaying: Mobility management is often studied as a part of handovers; however, existing routing schemes can be classified on the basis of mobility management. Such schemes are responsible for securing the path of the nodes when they are moving in an intra- or inter-mode of a given authentication server. Mobility management schemes can be studied as distributed, centralized, semi-distributed or even hierarchical [146], [158], [159].

B. AUTHENTICATION MODE-BASED

Similar to authentication-based frameworks, authentication protocols allow identification of legitimate users which can interact with each other for acquiring particular services over the network. Authentication protocols help to validate the users for transmissions in M-IoT. These protocols help to achieve reliable trust and security for exchange information. On the basis of mode of operations, the authentication protocols can be classified into the following two types:

- Proactive: Authentication protocols which focus on pre-verification of the users before beginning the transmissions are termed as proactive authentication [157], [158], [160]. Such schemes are highly reliable but sometimes slower in operations. Thus, these are often the primary preference of setups that focus on the services over smart M-IoT.
- Reactive: Authentication protocols which focus on the on-demand verification of the users and support a direct linking between the network users are termed as reactive authentication [161]. Reactive authentication is fast in operations, but is usually, vulnerable to a lot of network attacks which raises a question about their secure usability for smart M-IoT. However, with modern solutions like crowdsourcing [183] and blockchains [184]–[186], reactive protocols can be extended and secure for their usability in smart M-IoT setups.

C. AUTHENTICATION HIERARCHY-BASED

Authentication involves multiple entities which secure themselves by verifying each other either directly or through an Authentication Server (AS). On the basis of operations and hierarchy, authentication protocols can be classified into one-way or two-way authentication based protocols.

- One-way authentication: One-way authentication involves user-side verification with respect to the rules provided by the governing server (AAA or AS) [162]. The genuineness of the users is proved by the properties which are only shared by the user itself.
- Two-way authentication: Two-way authentication involves both user-sides as well as server-side verifications [163], [164]. The genuineness of the users, as well as the servers, is proved through their respective properties which are shared amongst them. Two-way authentication can further be extended into different modes of handshakes depending on the level of security to be verified before beginning the transmissions.

D. PROPERTY-BASED

Security protocols can also be classified on the basis of properties which are used for securing the transmissions between the nodes. Based on some key requirements, the security protocols can be categorized on the basis of the following properties:

- Freshness-based: Freshness means that messages exchanged in a session are generated specifically for a particular session. The attacker cannot use the previous session for messages. Freshness based protocols are used for communication between the two parties by establishing a secure channel on the basis of the freshness of sessions. The receiver believes that the obtained information is fresh and authenticated. Freshness is achieved by updating keys and sessions through consistent changes in parameters like seeds, nonce and sequence numbers of involved entities in smart M-IoT. Approaches based on freshness of keys and sessions are discussed in [146], [156], [164]–[170].
- Encryption-based: Encryption is an interesting piece of technology that works by scrambling data or information so it is unreadable by attackers. Encryption is a key-based approach to combine confidentiality and integrity, and provides a secure mechanism against external threats such as chosen-plaintext and chosen-ciphertext attacks. Encryption based protocol ensure the confidentiality of sharing information between the users in smart M-IoT [146], [154], [156], [163], [164], [166]–[174].
- Access-based: Limiting users from accessing a particular service is one of the key requirements of smart M-IoT applications. Protocols which can help to define a role to every user and control their activity are classified into access-based security protocols. There are a lot of existing solutions, which aim at enhancing the security of the mobile network by limiting the user operations while using the policies for information flow, management, and control [146], [163], [164], [166]–[174]. A highly stabilized access control protocol can prevent misleading or eavesdropper from gaining access to crucial information in smart M-IoT.
- System Integrity-based: System integrity protection is a necessary step to ensure a high level of security. As discussed in [132], [156], [163], [164], [166], [169], [173], [174], development of system integrity protection protocols can help to manage information disturbances and prevent attacks. The involved parties in smart M-IoT setups want to assure that all the remote data they receive is from systems that satisfy the users' integrity requirements. Therefore, it is important that system integrity based protocols can protect the information results from being polluted by attackers.

E. SUMMARY AND INSIGHTS

In this section, we presented a detailed study of security-aware protocols for smart M-IoT. Following the above-discussed classification, some major contributions to security protocols which are applicable to M-IoT are highlighted in Table 6. The existing protocols are evaluated on the basis of system integrity, freshness, confidentiality, mutual authentication, access control, overheads, encryption, and non-repudiation. Apart from these, several schemes can be followed by SPORE [204], which is a repository of security protocols. Over the last decade, protocols have been improvised by utilizing security as a crucial metric to decide a path; however, with the evolution of new CPS, dynamic nodes, and energy-constraint mobile devices, this direction of research remains open and require protocols, which can operate beyond authentication. Research can be extended towards the designing of a secure protocol stack, which can include channel as well as message protection without compromising the QoS to its users. Network patrolling, perimeter evaluation, and deployment of intrusion detection protocols can help to further secure the operations of smart M-IoT.

VI. PRIVACY PRESERVATION APPROACHES FOR SMART M-IoT

Data in M-IoT is highly crucial as well as sensitive and any eavesdropping may result in leakage of users' personal information [205], [206]. With data processing reaching a fine granularity level, it becomes tedious to privatize the content as new issues arise because of many dependencies on the platform used for transmissions. The collection and control of data are two of the main reasons that increase threat-level for data privacy in M-IoT [207]–[209].

With the difference in architectural deployment, smart M-IoT possesses large-scale implications for removing issues which may leak the entire information of the networks. Most of the approaches fail to support access control and authorization while deploying applications for smart M-IoT networks. Reducing the reachability of every user and keeping a watch on the amount and level of contents accessed by an individual can help in privacy-preservation [29], [210], [211].

Encryption of data for every link can further help this cause, however, with the networks attaining a high-speed property, it becomes necessary to support both encryption and decryption at a rapid pace [212]. Majority of the intermediate

TABLE 6. State-of-the-art protocols for M-IoT security.

Approach	Author (Year)	Ideology	System Integrity	Freshness	Confidentiality	Mutual Authentication	Access Control	Overheads	Encryption	Non-repudiation
Light weight authentication	[Amin et al. 2018] [165]	Distributed cloud computing environment	✗	✓	✓	✓	-	Medium	✗	✗
RFID authentication scheme	[Gope et al. 2017] [166]	Distributed IoT infrastructure	✓	✓	✓	✓	✓	High	✓	✗
Anonymous private authentication	[Rahman et al. 2017] [171]	Security of RFID systems	-	✗	✓	✗	✓	High	✓	✗
Key agreement mechanism	[Ermis et al. 2017] [172]	Partial backward confidentiality	-	✗	✓	✗	✓	Medium	✓	✗
two-way authentication	[Kothmayr et al. 2013] [163]	DTLS based security	✓	✗	✓	✗	✓	Medium	✓	✗
Secure authentication scheme	[Kalra and Sood 2015] [167]	Authentication of IoT and cloud servers	-	✓	✓	✓	✓	Medium	✓	✗
User authentication scheme	[Dhillon and Kalra 2017] [173]	Lightweight biometrics based	✓	✗	✓	✓	✓	Medium	✓	✗
Key management protocol	[Raza et al. 2012] [155]	Lightweight IKEv2	✗	✗	✗	✗	-	Medium	✗	✗
Constrained application protocol	[Raza et al. 2013] [174]	DTLS based security	✓	✗	✓	-	✓	Low	✓	✗
End-to-End IP security	[Hummen et al. 2013] [156]	Common protocol functionality-based IP security	✓	✓	-	✓	-	Medium	✓	✓
Secure multi-hop routing	[Chze and Leong 2014] [154]	Secure IoT Communication	✗	✗	-	✗	-	Medium	✓	✗
Two-phase authentication	[Porambage et al. 2014] [164]	Authentication of distributed IoT applications	✓	✓	-	✓	✓	Low	✓	✗
Authentication protocol for multimedia	[Mishra et al. 2017] [168]	Secure multimedia communications	✗	✓	✓	✓	✓	Low	✓	✗
Authentication and key Agreement	[Alkuhlani and Thorat 2017] [169]	Anonymity-preserving agreement	✓	✓	-	✓	✓	-	✓	✗
Secure route optimization	[Shin et al. 2017] [146]	Security of PMIPv6-smart home IoT	✓	✓	✓	✓	✓	Low	✓	✗
Remote user authentication scheme	[Sharma and Kalra 2017] [170]	Authentication for e-governance applications	-	✓	-	✓	✓	-	✓	✗

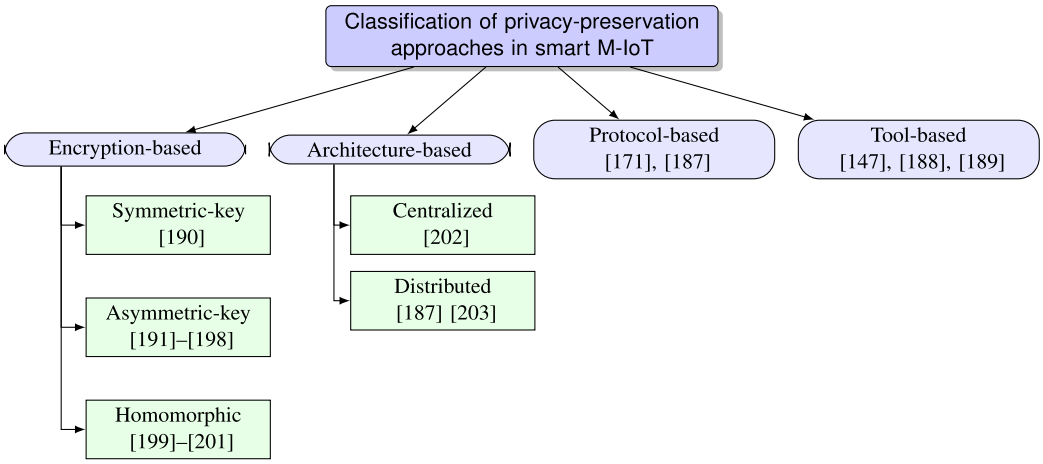


FIGURE 10. A broad classification of privacy-preservation schemes for smart M-IoT. The existing solutions can be studied by classifying them into encryption-based, architecture-based, protocol-based, and tool-based mechanisms for privacy preservation.

procedures should be done on the cipher itself, as this will help to prevent any unauthorized decryption of the text being shared between M-IoT devices. Further, approaches can use customized identifiers for creating policies for maintaining the anonymity of access between its users. Along with these, prevention of hidden terminals is another major requirement for privacy-preservation [213]–[216].

Practical problems like network partitioning and isolations increase the risks of leakage of data and it is necessary to formulate approaches that can help to identify such issues before-hand and with low-complexity [217]–[221]. Data privacy can be guaranteed by using solutions, which prevent sniffing and do not yield any information even if discovered by intermediates [222]–[224]. This can be further enhanced by using a non-store approach, which refers to the immediate forwarding of the data without consuming the excessive time stamp as well as keeping the freshness of the keys. Privacy can further be assured by preventing third party-based evaluations as these may disclose the encryption mechanisms of the entire route as well as of the traffic [225].

Distribution of incoming traffic not only prevents DoS or DDoS but also helps to make sure about the identification of any eavesdropper that may be listening to the incoming or outgoing traffic [226], [227]. Updating security policies, maintenance of logs and refining network architecture at regular intervals for the detected traffic and anomalies can further help in privacy-preservation of M-IoT networks [228].

Some of the major contributions on data privacy in IoT, which are applicable to M-IoT architecture, are discussed in Table 7. These schemes can be further classified into four major types, encryption-based, architecture-based, protocol-based and tool-based privacy preservation, as shown in Fig. 10. The details of each of these are provided below:

A. ENCRYPTION-BASED

Privacy is mainly the protection of personal information of users and devices in smart M-IoT. Disclosure of information can be protected through encryption of data which prohibits any eavesdropper from obtaining any knowledge even if he or she is able to capture the majority of its parts. Encryption-based schemes are not different from usual encryption algorithms. Thus, the existing solutions can be classified into traditional encryption schemes on the basis of an algorithm or mechanism used by them for protecting the data. These types are as follows:

- Symmetric encryption: The symmetric key encryption relies on the same key for encryption and decryption i.e. the key used for the encryption and the decryption should be same at both the parties. Symmetric-key encryption is essentially the same as a secret code that each of the two entities must know in order to encrypt and decrypt information. The symmetric key encryption has the major problem of exchange overheads of keys between the two parties, especially with maintaining trust when encryption is used for authentication and integrity checking [190].
- Asymmetric encryption: Asymmetrical encryption is also known as public-key cryptography, uses two keys to encrypt or decrypt of a plain text. The secret keys are exchanged over the Internet or a large network. The message encrypted by a public key can only be decrypted using a private key and similarly, data encrypted using a private key can only be decrypted using a public key [191]–[198]. Asymmetric encryption is far better in ensuring the security of information transmitted during communication.
- Homomorphic encryptions: Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. The encrypted data set is transformed into another data set by preserving relationships between elements in both sets. Studies conducted on the topic of Homomorphic encryption in [199]–[201] highlight their applicability over the smart M-IoT.

TABLE 7. State-of-the-art approaches for data privacy in M-IoT.

Approach	Author (Year)	Ideology	Application Area	Encryption	End to End Security	Perfect Forward Secrecy	Persistence against Replay attack	Password Protection	Trust-Assessment
End to end privacy	[Jayaraman et al. 2017] [191]	Privacy preserving IoT architecture	IoT	✓	✓	✗	✓	✗	✓
Decentralized anonymous authentication	[Alcaide et al. 2013] [187]	Privacy preserving protocol	IoT target-driven applications	✓	✗	✗	✓	✗	✓
Multi-authority attribute based encryption	[Belguith et al. 2018] [192]	PHOABE (Policy-Hidden Outsourced ABE scheme)	Cloud-assisted IoT	✓	-	✓	✓	✗	✓
Privacy and integrity preservation	[Bamasag 2015] [193]	ID-based signcryption scheme	Smart grid	✓	✗	-	✓	✗	✓
Identity-based personal location system	[Hu et al. 2011] [194]	Identity-based privacy preservation	IoT	✓	-	✗	✗	✗	✓
Data protection mechanism	[Doukas et al. 2012] [195]	PKI encryption	IoT m-Health devices	✓	✓	✗	✗	✗	✓
Privacy management mechanism	[Evans et al. 2012] [188]	Efficient data tagging	IoT	✗	-	✗	-	✗	✓
Attribute-based encryption	[Wang et al. 2014] [196]	public key encryption	IoT	✓	-	-	-	✗	✓
Privacy preservation protocol	[Li et al. 2014] [197]	Attribute-based encryption (ABE) key management	Smart grid	✓	-	✗	-	✗	✓
Reference software architecture	[Addo et al. 2014] [203]	Collaborative pervasive systems	Cloud enabled IoT applications	✓	-	✗	-	✗	✓
RERUM:Reliable, Resilient and secure IoT for smart city applications	[Pohls et al. 2014] [229]	Smart object (SO) hardware prototypes	Smart city IoT	✓	✓	-	✓	✗	✓
Private data aggregation with fault tolerance (DPAFT)	[Bao and Lu 2015] [199]	Boneh-Goh-Nissim cryptosystem	Smart grid	✓	-	-	✓	✗	✓
Network-level security and privacy	[Sivaraman et al. 2015] [230]	SDN-based approach	Smart-home IoT	✓	-	-	✓	✗	✓
Privacy protection mechanism	[Gong et al. 2015] [200]	Lightweight private homomorphism algorithm and encryption algorithm	Medical IoT	✓	-	-	✓	✗	✓
Data-centric security	[Wrona et al. 2015] [231]	End to End security solution	Military applications	✓	✓	-	-	✗	✓
Lightweight privacy-preserving data aggregation (LPDA)	[Lu et al. 2017] [201]	Homomorphic Paillier encryption, Chinese Remainder theorem	Hybrid IoTs	✓	-	-	✓	✗	✓
Lightweight data report scheme	[Bao and Chen 2016] [198]	Pseudonym identity-based privacy-preserving	Smart grid	✓	-	-	✓	✗	✓
Negotiation-based privacy preservation scheme	[Ukil et al. 2012] [189]	Data masking tool	IoT	✗	✗	✗	✓	✗	✓
CP-ABE Application	[Perez et al. 2017] [190]	Symmetric key encryption techniques	IoT	✓	-	✓	✓	✗	✓

[6pt]

B. ARCHITECTURE-BASED

Privacy preservation schemes can also be marked on the basis of architecture used for deployment and operations. Generally, the existing solutions depend on a centralized mechanism, but with solutions like blockchain which primarily uses public key operations, the architectural deployments become distributed.

- Centralized: Approaches which use a controller or centralized entity as a key enabler for privacy-preservation are studied in this type. Centralized solutions are effective from the monitoring perspective, but these pose a threat to a single point of failure which is difficult to sustain for any network [202]. Especially, in smart M-IoT, if all the traffic is regulated by the centralized authority, it becomes necessary to develop schemes which will define the policies of load management as well as prevent excessive utilization of resources for the traffic coming from a single source.
- Distributed: Such schemes depend on the distributed and flat nature of architectures and prevent a common point of failure as privacy preservation is initiated by the user or a node which are abstracted from other components of the network. In some scenarios, multiple nodes are used for defining policies for privacy preservation. However, the success of such approaches depends on their compliance degree and synergy in supporting common algorithms for a large set of nodes [187], [203].

C. PROTOCOL-BASED

As discussed in the protocol section, privacy can be supported by defining rules which are operated as a part of conditions and help to decide on the sharing of information between the users. Protocol-based privacy is easier to achieve and an efficient way for networks that operate in close proximity to each other [171], [187]. Such schemes are extremely useful for networks using crowdsourcing and can be used as broadcast mechanisms for blockchain-based distributed solutions for privacy preservations.

D. TOOL-BASED

Such an approach is easier to manage as it only involves process like masking, tagging or user-controlled policies [147], [188], [189]. Tool-based privacy is governed by the properties and services offered by the application platforms running for smart M-IoT. However, the correctness of such solutions is dependent on the legitimacy of the service providers and their honesty which cannot be measured through any tool and depends on the level of commitment to their users.

E. SUMMARY AND INSIGHTS

In this section, we summarized the privacy-preservation approaches for smart M-IoT on the basis of encryption, architecture, protocols, and tools. Data privacy is achievable through message protection and protocols can be used for authorizing applications and users before accessing personalized data of the smart M-IoT owner. Privacy can be attained through novel security protocols as well as the positioning of AAA that can ensure the end to end data privacy.

Policy-based, identity-based, ID-based, attribute-based encryptions and Public Key Infrastructure (PKI) can be the major enables for privacy preservation. Solutions, like blockchain and tangle (directed acyclic graph), can be used for preserving privacy through transactions between smart M-IoT users. The choice of encryption plays a key role as it affects the policies of session management between end to end devices based on the factors like freshness, integrity and perfect forward secrecy, which are attainable through secure key operations. More advances are expected in tool-based privacy preservation as well as personalized management as users are becoming much aware and demand personalized settings for each operation.

VII. TRUST MANAGEMENT APPROACHES FOR SMART M-IoT

M-IoT aims at maintaining a secure relationship between the entities involved in service provisioning as well as data dissemination [253], [254]. Most of the trust-enabled networks establish a reputation system based on a centralized entity that can help to check whether a particular node in the network can be relied upon or not. Such evaluations of reliability are an integral part of trust management systems [255]. With a billion of devices, the complexity of maintaining trust increases and it becomes relatively difficult to handle such an enormous number of devices, which leads the network into attacks by false reputation enhancement of an intruder [256].

Most of the trust management systems are governed by policies which are decided on the basis of the configurations of the network as well as the types of services supported by the M-IoT devices [257]. Trust management depends heavily on the distributed computations as slow computations may cause excessive overheads which are a hazard for secure systems. Crowdsourcing, computational offloading, dividing of service accessibility, distributed policy formations, distributed trust maintenance, and D2D computations, help in reducing the overheads and complexities associated with the building of trust-relaying systems for M-IoT [258]–[261]. Trust-based solutions for smart M-IoT can be classified into the following types, as shown in Fig. 11:

A. ARCHITECTURE-BASED

Trust in smart M-IoT is attainable through a unique implementation of architecture while placing each entity in such a way that it provides a pathway for believing each other before communications. On the basis of architectural setup, trust management approaches can be classified into the following three types:

- Centralized: It constitutes an entity which is present at the centre of a given network and is responsible for handling trust computations for the entire network [232]. The problem with such a deployment is the risk of a single point of failure.

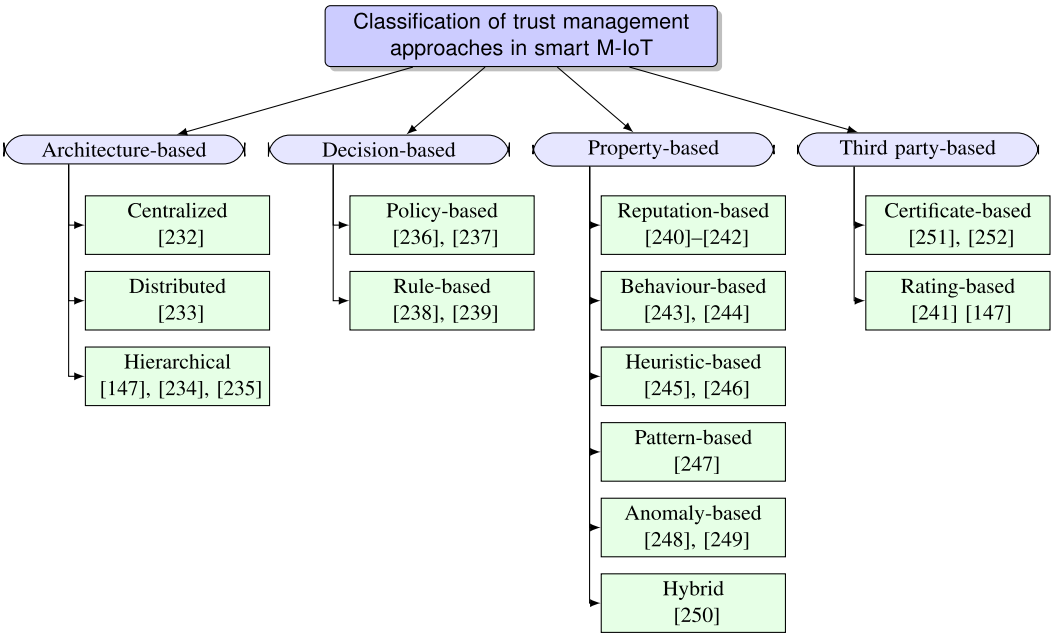


FIGURE 11. A broad classification of trust-management schemes for smart M-IoT. The existing solutions can be studied by classifying them into architecture-based, property-based, decision-based, and IDS-based trust management in smart M-IoT.

- Distributed: It constitutes trust evaluation through distributed entities which prevent a single point of failure. Distributed trusts are usually operated as P2P or P2MP, but not peer to all [233].
- Hierarchical: It constitutes calculations by using a layered architecture which focuses on evaluating trust for entities on each layer [147], [234], [235]. This allows the selection of accurate nodes in the next order of hierarchy.

B. DECISION-BASED

Trust is a decision-based entity, which in some cases is marked by following certain principles of communications. Node management and selection of the next-hop are two of the examples of decision-based trust management. On the basis of ideology, decision-based trust management can be categorized into the following two types:

- Policy-based: Using conditions to take a decision on the situation of entities is treated as a policy-based solution. The policy-based approach often results in a centralized or hierarchical solution as a governing body is required to form the policies for evaluating trust of the involved entities in smart M-IoT [236], [237].
- Rule-based: Using conditions to evaluate given information for generating relevant knowledge regarding the trust of an entity is treated as a rule-based solution. The rule-based approach utilizes any type of architecture; however, it always has dominance for deciding rules or a consensus model for arriving at a common decision while formulating principles of trust evaluations [238], [239].

C. PROPERTY-BASED

Trust is itself a property of a device in smart M-IoT. However, this core property can be classified into sub-categories through which trust can be ensured in any type of network as explained below:

- Reputation-based: Reputation is a fundamental concept in several situations which can be involved in the interaction between mutually distrusting parties [240], [241]. Reputation-based trust relies on a "soft computational" approach to formulate the problem of trust. The trust systems rely on the basic idea of analyses and a combination of paths and networks of trust relationships. Trust and reputation systems play a significant role in decision support for Internet-mediated service provisioning. Reputation-based trust management helps to mitigate the security complications of smart M-IoT [242].
- Behaviour-based: Behaviour-based trust models include a fixed evaluation scheme. The scheme uses the knowledge of behaviour in previous interactions and derives the trustworthiness of an entity [243], [244]. The behaviour-specific knowledge can be obtained from the feedbacks and recommendations.
- Heuristics based: Heuristics are used to aid the decision or estimation process by evaluating the indirect trust of an agent into the direct trust estimation. The decision formulation is handled with the estimation through metrics [245], [246].
- Pattern-based: A set of design patterns are used for designing systems with the explicit intention of increasing trust between entities. The behavioural patterns are followed to achieve sustainable trust. Patterns are used to

solve recurring problems in trust-based communications for smart M-IoT. Patterns have been developed in a range of disciplines for a variety of domains to make a trust model. The patterns can be obtained by behaviour, rules, policy, flow, etc [247].

- Anomaly detection based: The anomalies are abnormal behaviour which is intended to affect the systems. Anomalies can be detected based on their own signatures and settings. The rules and threat modelling can be done with the help of system behaviours and signatures. Anomalies are inspected over the high malicious network traffic to improve the detection accuracy of trust model [248], [249]. Signature-based IDS are the well-known anomaly detection systems in smart M-IoT networks.
- Hybrid: Such a trust management system which combines all the above-discussed solutions into a single mechanism is a part of hybrid trust management in smart M-IoT. Hybrid approaches use all the existing property-based approaches and choose the one which suits best to the given conditions and configurations [250].

D. THIRD PARTY-BASED

Depending on external mode for calculating trust is one of the prominent solutions of modern-day networks. Such a solution uses mechanisms like deep learning, data analytic, neural networks or AI for evaluating the trust of communicating entities. Based on the outputs from third-party evaluations, there can be two main types:

- Certificate-based: Providing a certificate of assurance on the successful evaluation of required trust is easier and a comprehensive solution, which is also capable of providing a detailed report on the operations of a device [251], [252]. Third parties use certain policies, cookies, and cached entries to ensure trust while generating certificates for the required device in a smart M-IoT.
- Rating-based: In certain scenarios, third parties are involved in giving ranking or ratings to each individual involved in the formation of the network. Such an approach is termed as rating-based trust management. A threshold is marked on the basis of some predetermined score and each entity is evaluated against this threshold value [147], [241].

E. SUMMARY AND INSIGHTS

In this section, we provided a detailed classification of trust management approaches for smart M-IoT. Trust relationships not only secure the M-IoT but also help in building reliable CPS. Evaluation of trust by using a limited set of metrics is a challenge for M-IoT, however, such a system offers huge scalability and can be operated with less management and better control [32]. Incorporation of software security, privacy control, and security constraints further strengthen the trust modelling in M-IoT. Along with these, trust-based solutions can be modelled into secure communication systems through security protocols, which use encryption policies for defining new security schemes by using a similar model of trust-relaying systems [35], [266], [267]. To summarize, a detailed state-of-the-art comparative study on various trust management schemes is presented in Table 8, which can be extended for their use in the smart M-IoT environment. The table helps to understand the key features and parameters focused by most of the existing solutions along with their core ideology for maintaining trust between the IoT entities.

VIII. PHYSICAL LAYER SECURITY FOR SMART M-IoT

Unlike traditional security solutions, which focus on the logical aspects of the networks, physical security is hardest and difficult to follow because of a difference in the type and make of an M-IoT device. With each device following a different set of parameters and configurations, it becomes difficult to provide a common solution which can withstand the Channel State Information (CSI) requirements of the entire network while securing the physical transmission of the network [282]–[284]. Network coding and multiplexing approaches usually rely on cryptographic solutions only to reduce the complexity of physical layer; however, this makes the system vulnerable to different types of attacks that can be launched over the used mechanisms. With devices being operated on battery, physical layer security becomes far more challenging and should be attained with lesser overheads as well as a lesser number of computations. A highly burdened operation may deplete the energy resources and an operational M-IoT network becomes of no use. The types of technology, 3G, 4G/LTE or upcoming 5G, play a crucial role in selecting an approach that can fit into the physical configurations as well as can support the load at a dedicated frame size [283], [285], [286].

Designing of security schemes on the physical layer may seem to be difficult, but it provides all set of new opportunities for improving the QoS as well as QoE for the end-users. The strength of the physical layer security depends on the adversary model which is used for evaluating the developed solution [282], [288]. Such solutions are usually driven by the assumptions of the CSI as well as device type and may or may not stand once new vulnerabilities are discovered over a course of time [289]–[291]. The existing solutions can be broadly classified into two main types, service-based physical layer security, and channel-based physical layer security, as shown in Fig. 12. The details on both of these are presented below:

A. SERVICE-BASED

Physical layer security in smart M-IoT can be obtained through service management, control over interference issues and performing accessibility management. Based on the services supported by the smart M-IoT, physical layer security can be studied in three parts:

- Cryptographic: The solutions, which use cryptographic mechanisms for preventing any eavesdropping, are

TABLE 8. State-of-the-art approaches applicable for trust management in M-IoT.

Approach	Author (Year)	Ideology	Application Area	Parameters focused	Computational Offloading	Visualization	Reliability	Security Constraints
ORDAIN	[Kravari and Bassiliades 2017] [244]	Identification of social and non-social metrics	IoT	Social and Non-social features	-	✗	✗	✗
Multi-domain trust management	[Wu and Li 2017] [234]	Hierarchical trust management framework	RFID	Convergence speed, Malicious event detection rate, Mobility	-	✗	-	✓
Multidimensional trust-based anomaly detection	[Gai et al. 2017] [248]	QoS and social relationship	IoT	Trust level evolvement, False alarm rate, Malicious nodes percentage	-	✗	✓	✓
CTM-IoT	[Alshehri and Hussain 2017] [232]	Centralized trust management	IoT	Trust management module, Communication module	-	✗	-	-
Resilient routing mechanism	[Khan et al. 2017] [243]	Routing protocol for low power and lossy networks	IoT	Delivery ratio, Path length, Bad paths, Network reliability	-	✗	✓	✓
Trust-based policy hidden communication	[Peshwe and Das 2017] [236]	SIGMA-I - policy hiding prefix based encryption	IoT	Private service discovery, SIGMA-I, RSSI	-	✗	-	✓
Timely trust establishment	[Yusof et al. 2017] [262]	Swift trust formation	IoT	Swift trust, Global virtual teams	-	✗	✓	✓
Hybrid trust-based IDS	[Ozcelik et al. 2017] [250]	Functional reputation and misuse	WSNs	Energy consumption, Network lifetime	✗	✓	✓	✓
ANASTACIA	[Ziegler et al. 2017] [237]	Trustworthy-by-design autonomic	CPS-IoT	Policy-based access control, Smart security planning	-	✓	✓	✓
Trust-based decision making	[Al-Hamadi and Chen 2017] [263]	Trust-based information sharing	Health-IoT	Correct decision ratio (CDR), Malicious nodes	✓	-	✓	✓
TMCoI-SIoT	[Abderrahim et al. 2017] [264]	Trust management in SIoT	SIoT	Trust evaluation, Trust prediction	-	-	✓	✓
Trust estimation scheme	[Son et al. 2017] [240]	Interaction history and stereotypical reputation	IoT	Trust value	-	✗	-	✓
Hierarchical trust management	[Guo and Chen 2017] [235]	Hierarchical trust management in mobile cloud	IoT	Trust value	✓	✗	✓	✓
Trust-based distributed intrusion detection	[Khan and Herrmann 2017] [265]	Distributed IDS	IoT	False positives, False negatives	✗	✗	✗	-
Computational offloading for efficient trust management	[Sharma et al. 2017] [241]	Osmotic computing	POSNs	Trust visualization, Monitoring cost, Average osmosis time	✓	✓	✓	✗
Trust management via SOA	[Chen et al. 2016] [233]	Distributed collaborative filtering	SOA-based IoT	Trust value, Decay parameter, Trust convergence	✗	-	-	-
Trust-based access control	[Mahalle et al. 2013] [239]	Fuzzy-based approach	IoT	Energy consumption, Residual energy	✗	✗	-	-
TRM-IoT	[Chen et al. 2011] [242]	Fuzzy-reputation	IoT	End-to-end packet forwarding ratio (EPFR), Energy consumption, Convergence speed, Detection probability	✗	✗	✗	✗
Cooperative spectrum sensing data fusion	[Wang et al. 2018] [249]	Mechanism design theory	Cognitive radio networks	Malicious nodes percentage, Decision rate, Trust threshold	✗	✗	✗	✗
Cooperative trust relaying and privacy preservation	[Sharma et al. 2017] [147]	Edge-crowdsourcing via fission computing	SIoT	Fission time, Combined entropy, Integration cost, Per node relaying time	✓	✓	✗	✗

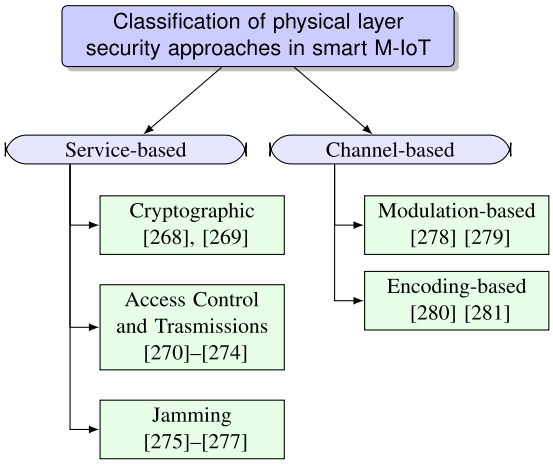


FIGURE 12. A broad classification of secure physical layer schemes for smart M-IoT. The existing solutions can be classified into service-based and channel based mechanisms.

studied in this type. As discussed in [268], [269], these systems combine physical layer properties with cryptographic mechanisms to ensure the safety of communication between the devices in M-IoT. Such security is complex to attain but has powerful applicability.

- Access Control and Transmissions: The solutions, which control the signal possessions by the users as analyzed in [270]–[274], are studied in this type. Access control and transmission-based solutions are generally low complex and focus on interference management along with control over secrecy probability.
- Jamming: There are certain solutions as provided in [275]–[277], which prohibit users from unintentional uplink or downlink in a specified zone. These approaches are responsible for energy-efficient security at the physical layer.

B. CHANNEL-BASED

Physical layer solutions which emphasize the security of channel used for communications are dependent on the signal alterations and induction of bit codes into the transmission medium. Such solutions should operate with a low-complexity and their operations must be completed in a few nanoseconds. The success of these solutions depends on the type of communication setup used for transmissions and the approaches used for securing the bits. Based on the mode of operations, these can be classified into modulation-based and encoding-based solutions:

- Modulation-based: Such schemes changes the signal properties (Amplitude, Phase, or Frequency) for preventing any eavesdropping on the transmitted data. In general, secure-spectrums can help to attain modulation-based channel security in smart M-IoT. These solutions are performed by using carrier waves [278], [279].
- Encoding-based: Using different codes for the security algorithms at the physical layer helps to secure the traffic and such an approach is classified into encoding based solution. These are performed through binary codes [280], [281].

C. SUMMARY AND INSIGHTS

In this section, we summarized the existing studies into two main categories of physical-layer approaches namely, service-based and channel-based solutions. These solutions were further studies by classifying them on the basis of cryptographic mechanism, access control and transmission policies, jamming facilities, modulation, and encoding. From the study, it is evident that channel estimation, M2M modelling, fading losses, noisy models, energy-constraints are some of the crucial aspects to be taken care of while deploying security solutions for physical layer in M-IoT [303]–[306].

Physical security of the M-IoT network is also impacted by the burden of devices and interference-management, which are driven by the density of the network. Most of the physical layer security solutions are driven by Signal-to-Interference Ratio (SIR), Signal-to-Interference-plus-Noise Ratio (SINR), secrecy, outage policies, and transmit energies. Despite a plethora of approaches for IoT's physical layer security, there are only a few solutions which can withstand the requirements of M-IoT; thus, a comparison study is presented in Table 9, which helps to understand the reach and level of security provided by the existing solutions.

IX. HANDOVER SECURITY FOR SMART M-IoT

Handovers can be hard, soft, horizontal, vertical, terminal and network controlled, and terminal and network-initiated, as shown in Fig. 13. The handovers allow the shifting of radios between the same or different media in a network. M-IoT devices undergo handoffs once they leave their service-space and enter an area governed by a different entity. Most of the handovers in M-IoT are vertical that require efficient security measures for the protection of links during their switching [158], [307], [308]. There is a huge requirement of trust as well as seamless shifting of services across the terminals while performing handoffs and mobility management in the network [309], [310]. Usually, the M-IoT networks focus on using an Access Point (AP), M-IoT device, AS, and core terminals for shifting services across the network [157]. Most of the networks require seamless services and faster authentication which can be obtained through proactive mechanisms [311]. These proactive approaches define a pre-determined system model over which the authentication is performed and verified against the attacker models. Most of the approaches are selected on the basis of handoff latency, and time consumed in laying off their services onto the next terminals along with their cost of operations [312]. SDNs, media-independent technologies, network slicing and the inclusion of PMIPv6-based solutions can enhance the performance of security solutions that aim at securing the handovers in M-IoT [146], [159], [313]–[316]. The proactive and reactive handover authentication approaches can be further classified into initiation-based, architecture-based, and

TABLE 9. State-of-the-art approaches for physical layer security in M-IoT.

Approach	Author (Year)	Ideology	Application Area	Parameters focused	Computational Complexity	Memory Consumption	Energy Efficiency	Scalability	Secrecy
Security enhancement against eavesdropping	[Xu et al. 2016] [270]	Secure relay communications in IoT	IoT	Secrecy outage probability, Secrecy rate, Achievable communication distance	-	-	-	High	✓
Securing uplink transmissions	[Chen et al. 2016] [271]	Light-weight mechanism for preventing eavesdropping	MIMO-IoT	Symbol error rate	Low	-	-	High	✓
Securing cyber-physical communications	[Xu et al. 2017] [287]	Security aware wave formations	CPS	Secrecy rate, Transmit energy	Low	-	High	High	✓
Channel aware security	[Choi 2017] [275]	Opportunistic jamming	IoT	Secrecy rate, Achievable rate, Outage Probability	-	-	High	High	✓
Physical layer security	[Hu et al. 2017] [276]	Cooperative jamming in IoT	IoT	Secrecy outage probability, Power allocation ratio,	-	-	High	High	✓
Secure communications in C-IoT	[Li et al. 2016] [277]	Worst case channel jamming for spectrum leasing	Cognitive-IoT	SINR, Energy-harvesting, Channel Uncertainty	High	-	High	-	✓
Secure distributed Detection in IoT	[Zhang and Sun 2016] [272]	Security in energy-constrained IoT networks	IoT	Error probability, SNR	Low	-	High	High	✓
Secure communications in CIoT	[Hu et al. 2017] [273]	Secure energy-efficient relay communications	Cognitive-IoT	Secure transmission rate, SNR	-	-	High	-	✓
Security enhancement during inteference	[Islam et al. 2017] [274]	Confidential transmission in IoT-relays	IoT	Mean square error, SNR	-	-	-	High	✓

property-based schemes for security in smart M-IoT. Note that all of the handover authentication solutions may either use primary, secondary or group mode for authentication irrespective of the classification. The details are as follows:

A. INITIATION-BASED

Handovers are operated through a governing entity which initiates the procedures of attachment and detachment of a node in the network. Based on the initiation, the handovers authentication procedures can be divided into the following two types:

- Host-initiated: When the service consuming entity starts the procedures of handovers, this type of handover is marked as host-initiated. Host-initiated handovers consume much signalling and might have weak security because of a failure in the identification of requests which may come from an anomaly node [292].
- Network-initiated: When the service providing entity starts the procedures of handovers, this type of handover is marked as network-initiated. This type of handover is low complex and more secure in because of control by a centralized authority [293]. However, security layouts and architectural complexity can affect the performance of such handovers.

B. ARCHITECTURE-BASED

As discussed earlier, the handovers authentication procedures can also be studied from the architectural point of view and can be distinguished into the following two types:

- Centralized: This includes the authentication procedures, which are driven by a centralized authority. SDN-based or topology-based authentications are usually centralized in nature and consequently pose a risk of a single point of failure [294]. Further, the centralized layout increases the security path, which requires RO approaches for increasing the performance.
- Distributed: This includes solutions like blockchain-DMM, P2P, P2MP and crowdsourcing like authentications which can help to remove the dependencies on a single entity in smart M-IoT [186], [293].

Moreover, location privacy is another factor to be considered for mobility of M-IoT. It helps to maintain the

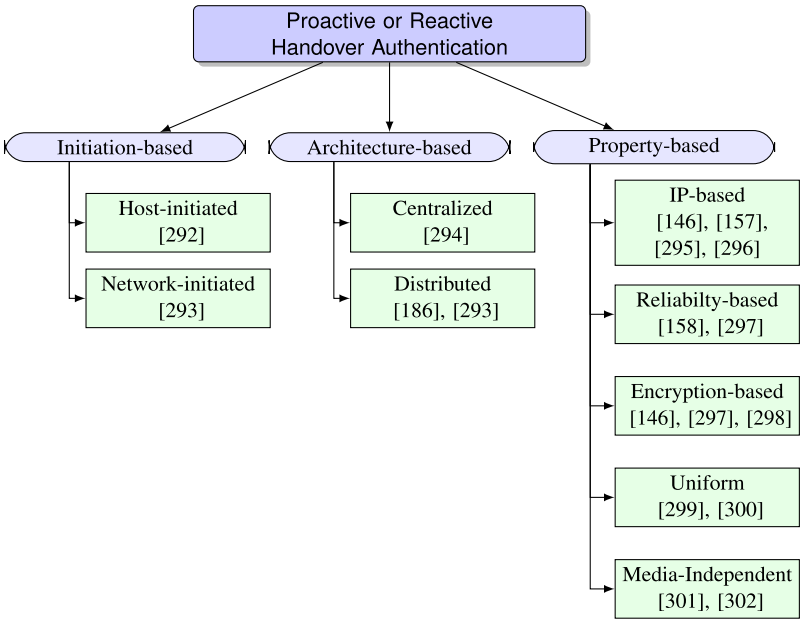


FIGURE 13. A broad classification of secure handover schemes for smart M-IoT.

anonymity of user location and its specifications. Considering the inclusion of location-based services in M-IoT, use of location-privacy solutions helps to protect the system at the network as well as the user's end [43], [317], [318]. M-IoT can also be facilitated by using location-privacy through obfuscation [319]. This will also allow the extension of M-IoT to opportunistic scenarios. Liao *et al.* [320] developed a trajectory-protecting solution, which supports location-based service privacy for IoT-cloud systems. The authors rely on K-Anonymity Trajectory (KAT) algorithm, which shows low complex simulated results. Location-privacy can also be considered as an additional metric for trust evaluation [321], [322]. Such solutions are facilitated by hybrid security architectures and uses different algorithms for different modules of the architecture. With the involvement of crowdsources in M-IoT, location-privacy is a dominant metric to be considered for protecting location-based threats and prevent issues related to backward broadcasting or tunneling [323]–[325]. Especially, for the inclusion of such solutions to M-IoT, it is desired to developed novel key distribution and credential management system that can elongate the efforts for location-based privacy preservation.

C. PROPERTY-BASED

Handover authentication mechanisms can be classified on the basis of property which governs their security aspects. These include

- IP-based: This includes authentication mechanisms followed by the majority of mobile applications as it uses proxy procedures to support the security of nodes in smart M-IoT. PMIPv6 and F-PMIPv6 are among the popular solutions for secure and seamless handovers [146], [157], [295], [296].
- Reliability-based: Approaches like [158], [297], which not only provides strong authentication but also supports the reliability of connections, are studied under this category. Such approaches help to sustain the connections for longer duration without affecting compromising the security considerations of the network.
- Encryption-based: Authentication solutions, which focus on using encryption-based solutions for security, are studied under this type. Encryption based handovers help to protect the user data as well as the control information which is passed between the entities laying off from a zone of one entity and moving into the zone of other entity [146], [297], [298].
- Uniform: Such types of handovers authentication are more prominent in LTE and LTE-A networks as these can be used for all types of networks [299], [300]. This is one of the most suitable handovers procedures for smart M-IoT networks. Such mechanisms are low-complex, computationally-inexpensive and highly secure solutions for mobile security.
- Media-Independent: Such types of handovers rely on the security governed by IEEE 802.21a-2012 for supporting security along with media independence while shifting services from one entity to another in an inter-handover mode [301], [302], [345], [346]. The amalgamation of MIH solutions with F-PMIPv6 techniques is gaining popularity because of their low complexity and high security [159].

D. SUMMARY AND INSIGHTS

In this section, we surveyed solutions for the secure handover of smart M-IoT devices. The devices can perform intra- or inter-handover depending on the layout of the network.

TABLE 10. Proactive authentication mechanisms for secure handovers.

Approach	Author (Year)	Ideology	Scalable	Latency	Bandwidth	Handoff Time	Mutual Authentication	Location Privacy
Delay optimization handoffs	[Lopez et al. 2007] [326]	Network layer authentication	-	-	-	Low	✗	✗
BASH	[He and Perkins 2008] [327]	Backhaul-aided seamless handovers	✓	Low	High	Low	✗	✗
Efficient handover authentication	[Fu et al. 2012] [328]	Privacy preservation for 802.16m	✓	-	-	High	✓	✓
Ticket-based handoffs	[Xu et al. 2014] [160]	Handoff authentication for mesh networks	-	-	-	-	✓	✓
Secure and efficient handovers	[Zhang et al. 2014] [329]	Authentication using EAP in wireless networks	✓	-	High	Medium	✓	✗
Fast pre-hand authentication	[Chien et al. 2008] [330]	Minimized overhead and high security	-	Low	-	Low	✓	✗
Handover authentication	[Choi and Jung 2010] [331]	Backhaul-aided seamless handovers	✓	Low	-	Medium	✓	✓
Re-authentication for 3GPP	[Shidhani and Leung 2011] [332]	Mutual re-authentication	-	Low	-	Low	✓	✗
Secure continuous handovers	[Kalong et al. 2010] [333]	Dynamic key management	✓	Low	High	-	✓	✗
Handover for seamless multimedia transmissions	[Saxena and Roy 2011] [334]	Proactive authentication over 802.11	✓	Low	High	-	✗	✗
Privacy preserving handover	[Jing et al. 2011] [335]	EAP-based wireless networks	✓	Low	-	Low	✓	✗
Secure inter-ASN handovers	[Nguyen and Ma 2012] [336]	EAP-based pre-authentication	✓	Low	-	Medium	✓	✗
Mechanism for E-UTRAN and Non-3GPP	[Cao et al. 2012] [299]	Uniform handover authentication	✓	Low	-	-	✓	✗
CPAL	[Lai et al. 2014] [337]	Privacy-preserving authentication with access linkability	-	Low	-	High	✓	✗
Secure fast WLAN handoff	[Chien and Hsu 2009] [338]	Time-bound delegated authentication	✓	Low	-	-	✓	✗
Re-authentication scheme for handovers	[Ma et al. 2013] [339]	Proxy signature approach	✓	Low	High	-	✓	✗
Handauth	[He et al. 2013] [340]	Authentication with conditional privacy	✓	Low	-	-	✓	✗
EAP-based pre-authentication	[Wang et al. 2017] [341]	Inter-WRAN Handover authentication	✓	Low	-	Low	✓	✗
Fast handovers in 5G Xhaul	[Sharma et al. 2018] [158]	Secure and fast handoffs in 5G-Xhaul and IoT	✓	Low	-	Low	✓	✓

Proactive authentication plays a key role in securing service layoffs between the devices and can ensure long-sessions without disrupting the services of a user under movement. Distributed security protocols play a considerable role in managing nodes under high mobility scenarios by preventing unnecessary passes to the core for re-authentication of devices.

Handoff latency, discovery time, bandwidth support, mutual authentication, and overheads are some of the key metrics to be considered for selecting an efficient handover scheme for M-IoT, as shown in Tables 10 and 11. There are plenty of solutions which have diversified the security aspects of handovers and provide a wide range of services for handling billions of IoT devices. Despite this, the majority of them fails on the aspect of performance and does not account for the tradeoff between the security and Quality of Experience (QoE). Thus, new approaches are required that can take into account these requirements of security as well as the performance before their final deployment and testing while causing minimum overheads during handoffs.

X. RESEARCH CHALLENGES, OPEN ISSUES AND FUTURE DIRECTIONS

Security, privacy, and trust are supported through specific requirements of a system, which are the open challenges to be resolved in M-IoT. Most of the challenges and issues can be acquired from the studies presented in [29]–[45], [347]–[352]. From these studies, it is noticeable that the major open issues to be resolved for M-IoT are:

- Satisfaction of the security requirements: It is of utmost importance that any approach which aims to facilitate security, privacy and trust in M-IoT must satisfy certain security requirements that are listed below:
  - *Mutual Authentication*: Security agreement between each entity in M-IoT is of utmost importance. Each device must be able to identify the correctness of every other device involved in transmission. The trust relationship between the devices can help to attain the requirements of mutual authentication.
  - *Secure Key Exchange*: Security keys are the pillar for preventing attacks in a network. It is a must that keys are exchanged secretly over a secure

TABLE 11. Approaches for secure handovers in M-IoT.

Approach	Author (Year)	Ideology	Application Area	Parameters focused	Mutual Authentication	Handoff Time	Latency	Reliability	Security Constraints
Inter-LMA domain handover	[Chai et al. 2017] [295]	Proxy-based FPMIPv6	Mobile IPv6 networks	Handover latency	✓	Low	Low	-	✓
Mobility management scheme	[Chai et al. 2015] [296]	Proxy-based FPMIPv6	IoT	Handover latency, Inter-domain movement	-	Low	Low	-	✓
Uniform handover	[Cao et al. 2012] [342]	E-UTRAN	LTE-A Networks	Signaling messages,Computational cost	-	-	-	-	✓
Uniform handover	[Haddad et al. 2016] [300]	Authentication and registration with HSS	LTE-A networks	Computational delay, Communication overhead, Storage cost	✓	Low	Low	-	✓
Session key management	[Kong et al. 2017] [343]	Mobile relaying-based session management	LTE-A networks	Computational delay, Communication overhead, Storage cost	✓	Low	Low	-	✓
Secure and efficient protocol	[Sharma et al. 2018] [158]	Key exchange and authentication	5G-Xhaul	Handover latency, Failure factor, Signaling overheads	✓	Low	Low	✓	✓
Route optimization	[Shin et al. 2017] [146]	PMIPv6-based RO	Smart home IoT networks	Transmission rate, Packet loss, Network throughput	✓	Low	Low	-	✓
Seamless handover	[Feirer et al. 2017] [344]	IEEE 802.11k-based handover	Industrial WLAN	Message overhead	✗	Low	-	-	✓
Authentication protocol	[Saxena et al. 2016] [298]	Symmetric key cryptosystem	LTE Networks	Storage overhead, Computation overhead, Bandwidth consumption	✓	-	Low	-	✓
Mutual authentication handoff	[Ndibanje et al. 2017] [297]	RSS and PKC-based protocol	IoT-Sensor networks	RSS	✓	Low	-	✓	✓

channel and must not reveal at any instance of operations.
- *Session Key Management*: This is a requirement which helps to secure the communication between the M-IoT devices. It is necessary for an approach to use a secure key which is different from other keys while communicating with a particular device in a network. Session keys must be renewed consistently for preventing any attacks because of the lack of key freshness.
- *Perfect Forward Secrecy*: In a communication setup, capturing of long-term keys should not be able to generate past session keys. This helps to secure previous contents and also protect future compromises and password sharing.
- *Defense against a Replay Attack*: Repetition of valid data can reveal the security policies as well as lead to overconsumption of resources in the protection of the system. Such kinds of attacks are caused by interceptions and must be avoided as the traffic in M-IoT is very sensitive and crucial.
- *Access Control and Authorization*: It is required that the new solutions are able to provide control on the accessibility limits of each device and also provide policies for authorization and management of content along with session formations.
- *Defense against a Resource Exhaustion Attack*: This type of attack should be prevented as resource exhaustion attacks can exploit the network and the M-IoT devices through excessive key operations. Such an attack may lead to the shutdown of the entire network.

- Performance tradeoff: Apart from the security requirement, it is required that a solution should not compromise the performance of the system and must be capable of handling the performance tradeoffs due to computational burden of security mechanisms. The approaches must be able to handle the implementation-overheads during continuous operations.
- Platform compatibility: Due to a difference in the types of devices and their configurations, it is difficult to support platform compatibility in M-IoT. However, there is still a strong requirement of such solutions which

can be operated irrespective of the types of technologies being operated over M-IoT devices. Platform compatibility can be obtained by defining security mechanisms which rely on operations that have lesser variations when shifted across devices.

- Resource utilization: Efficient utilization of resources like memory and power and prevention of their over-consumption can save the operations up to a longer duration. Resource utilization can be attained by using novel network architectures as well as independent layers for each operation in M-IoT. Such a facility can be obtained through SDN-NFV technologies. As discussed earlier, facilities like osmotic computing, fog computing, catalytic computing and edge-crowd modelling can be used for handling resource utilization while providing security and privacy solutions for M-IoT.
- Insider threat management: Prevention of theft, fraud, and damage through non-compromising models is required as this can help to manage the false-occurrences caused by the criminal aspects of M-IoT users. Models like blockchain, distributed mobility management, and crowdsourcing can be used for management of insider threats in a system.

Future aspects of M-IoT are quite vast as it has to deal with a lot of dependencies of the underlaid architecture. Network designing and placement of components play a key role in providing security in M-IoT; whereas privacy has a lot to do with an individual as well as the service providers. Trust is built on the backbone of security and privacy and its management is as crucial as other services. Till date, two of the major aspects to achieve in trust management is its visualization and formal way of expressing for a large set of users. Even in the lights of different solutions, there are no standard mechanisms which can help to visualize trust as a property of a device. Thus, future approaches must consider formally defining trust and building some standard rules which should operate together with the security and privacy considerations for enhancing the practicality of M-IoT services to users. In lieu of various properties of existing solutions as discussed throughout this article, the following key points can be used for directing further research on different aspects of smart M-IoT.

A. SECURITY RELATED FUTURE RESEARCH DIRECTIONS

- Network Monitoring in M-IoT: M-IoT security relies on the true operations of the entities involved in providing services to the users. Any faulty equipment can result in sets of failures which may compromise the operations in M-IoT leading to the devastation of infrastructure as well as data. Futuristic approaches must ensure efficient deployment of solutions like IDS, network monitors, and ethical packet sniffers for enhancing the security requirements. Network monitoring should emphasize the resource-based evaluation of the involved devices so as to prevent service halts and offer ultra-reliable QoE to its users. New tools can be developed which can analyze the traffic passes between the devices. In addition, the security of network monitors is to be considered for preventing any eavesdropping on the ethically gathered data. Monitoring tools and procedures should possess encapsulation as a key property and prevent and disclosure of type and make of equipment even if the attacker possesses maximum data [353], [354].
- Vulnerability Assessment: For secure operations, it is of utmost importance that the entire network is consistently monitored for potential vulnerabilities that may lead to different types of threats. Such a task can be attained by defining security policies for each entity in the network and building profilers which can help to assess devices in case of weird behaviour or functioning [355]. Vulnerability assessment can help to determine the influence of attack on a particular set of entities [86]. The vulnerability assessments should be conducted at both the user-side and network-side. User-side evaluations should be abstracted and must not consume excessive operations and must be low on overheads; network-side evaluations should be conducted with zero-maintenance time and any service halts. Anomaly detection, community classification and attacker marking are the main targets of vulnerability assessment [116]. All of these are open issues and their applicability are subject to application and operational scenarios.
- Policies for Zero-day Attack: Zero-day attacks in software modules of M-IoT are the key threats to its security. It is difficult to identify such possibilities unless made public by the attacker. Most of these are identified during the development stage, but some of these are marked during the regular testing operations. It becomes the liability of service providers and software-distributors to provide security patches as soon as vulnerabilities are identified. Further, providing customer knowledge and making mandatory to download and install security updates should be considered for effective countermeasures against such attacks [356]–[358].
- Hacking and Accessibility: Despite always being a hot topic, hacking and accessibility are yet open future challenges in smart M-IoT. It is required that new solutions are developed for code obfuscation and new policies are made for controlling the accessibility to M-IoT components and its services [359], [360]. Pre-authentication mechanisms and multi-registration phases can help to attain these requirements. However, performance and overheads are the major issues attached to such provisioning, and any approach controlling the accessibility must not cause performance overheads and should not disturb the regular operations of the network.

B. PRIVACY RELATED FUTURE RESEARCH DIRECTIONS

- Prevention of Device Profiling: Data gathering is one of the key requirements of modern-day organizations to provide a personalized experience to their users. However, the process of data gathering and information

analysis may cause different types of threats by deliberately breaching the privacy of users. Collection of data and using it for evaluating user behaviour and controlling the preferences may allow a threat to confidentiality and integrity of an individual; further, hold on information by an eavesdropper leads to vulnerable conditions, which violates the network policies [361], [362]. Thus, to overcome such issues, it is required that futuristic solutions should not allow unauthorized device profiling and information gathering procedures must be controlled by the service providers. In addition, no selling of data should be done as this violates the personal space of an individual. Use of device profiling for advertisements for generating revenues is fine, but it should not affect the preferences of an individual.

- Control over Data Gathering: M-IoT devices are sensitive to information and data across their network is delicate to threats. Classification of data and generating knowledge by data-processing disclose different types of vulnerabilities, which are the tools of hackers for exploiting the network and its users. Approaches are required that prohibits uncontrolled data gathering and limits the service providing apps from collecting excessive information other than the required ones. Data gathering procedures should be controlled by app hosting platforms and as per the individual is concerned, they must be provided with knowledge of using authenticated sources to prevent any enforced data gatherings [191], [195].
- Personalized Settings: Every application, be it open source or proprietary, must provide preferential settings to its users, where they can manage and control the amount of information to be shared across the M-IoT platforms. It is necessary that every user should be able to monitor the amount of information and extend up to which his/her information is used and for what purposes. Personalized settings should be supported by access management, accountability and authorization controls.
- Managing Information Flow: For sufficiently high privacy settings, every entity in M-IoT must be provided with facilities for managing information flow. These information flows should be manageable remotely, thus, different techniques and solutions can be developed for such requirements which pave a way for controlling the information flow even being present on-site. Development of toolkits and apps for information flow are other future research challenges in smart M-IoT. Further, these can be used with AI techniques to perform a priori probabilistic checks on the occurrence of attacks for a particular set of settings.

C. TRUST RELATED FUTURE RESEARCH DIRECTIONS

- Dedicated Node Management: Trust is a compliance degree between the entities to ensure accurate operational behaviour in the network. M-IoT is dedicated to operating networks which will heavily depend on the crowdsources for the majority of their operations. Such a dependency raises a crucial requirement of node management and control over the service-relationships between the devices. Research must be conducted in this direction while ensuring how the devices will interact on the basis of what policies they can accurately judge each others' correctness [263], [264]. It is required that certain solutions must be developed that can provide dedicated node management at a fine granular level while leveraging the properties of existing solutions for trust management. Different type of protocols can be designed that takes situational awareness as one of the key properties for ensuring trust-aware communications in M-IoT. In addition, contextual behaviour monitoring and aspect-based classification can help to ensure trust-compliance between the entities of M-IoT.
- Trust Visualization and Markings: There are a huge set of applications and approaches which emphasize on computing trust in different types of the network as per the requirements of the applications. But the majority of these fail to provide any conceptualization on the visualization process which helps to easy identification of service-law violators. It is required that research must be conducted in this direction while finding a benchmark which can be used as a backbone for trust-visualization and markings [241]. In addition, facilities must be provided to check trust roles and authorization activities across the network.
- Anomaly Detection and Recovery: Anomaly detection is the other key aspect of trust maintenance solutions. Futuristic research must focus on providing enhanced, on-demand and real-time facilities for detecting anomalies. This must accompany the solutions which can help to recover the users which are marked as anomalies by allowing them to re-justify their associations with the networks' terms and conditions and their flow control [116]. It is required that trust evaluations must lift themselves from the traditional reputation-based systems as such facilities can easily fall prey to Sybil attacks and may mislead the trust-maintenance process.
- Distributed Evaluations and Trust offloading: Apart from trust-management, the approaches are required which can operate in a distributed manner and yet provide competitive results as that of centralized solutions. This will help to prevent any single point of failure [143], [241], [243], [265]. Such solutions can be fixated on different offloading techniques which can be operated in parallel to data evaluations and do not interfere with the regular network operations. Development of distributed IDS and crowd-sourced IDS can be crucial solutions for attaining distributed evaluations as well as trust offloading.

D. NECESSITY OF AMALGAMATION

Security, privacy, and trust in M-IoT go hand in hand. A breach of policies of one may lead to attack through others.

Security policies must be strong enough to prevent any unauthorized access to the personal information of an individual in M-IoT and privacy policies must ensure that the data is always shared with the trusted party. Such activity is also operational in reverse and holds true for any sort of network formations in smart M-IoT. The necessities for amalgamating these solutions can be accounted for the following points:

- Prevention against Cyber Spies: Combining all the aspects of security, privacy and trust for smart M-IoT ensure protection against cyberbullies, spies, and service breachers [90], [363], [364]. These three requirements ensure that the network is operating in closed perimeter even its operations are distributed across the huge cyber network. Here, close perimeter refers to the path lengths and routes which can be tracked down easily and conterminously without many overheads.
- Risk Assessment and Mitigation: A network should be assessed for potential risks in its operations. It is necessary that the risk evaluations are conducted on the basis of combined rules for security, privacy, and trust. Risk evaluations are usually probabilistic, however, with complete details of all possible rules, these can be used for generating a particular output that yields visible results for risk assessments [365]–[367].
- Reliable Communications: Modern network services, especially the ones operating for smart M-IoT, require reliable connections for their continuous operations. Such a requirement can be ensured only if the network components and their services satisfy the requirements associated with security, privacy, and trust. In fact, the upcoming applications in smart M-IoT not only demand reliable communications, instead their focus is on ultra-reliable communications [368], [369] with lower dependencies and controlled cohesion and coupling amongst their software solutions.

Thus, it becomes inevitably important to develop solutions, which hold true justifications for security, privacy, and trust at the same instance and at the same level.

XI. CONCLUSION

Security solutions must be able to fortify authentication, confidentiality, integrity, freshness, access control and authorizations for M-IoT devices and its platforms, whereas privacy must support information protection for every device and its users. Both of these requisites can be obtained by building trust relationships across the networks. However, there exists a mixture of approaches that consider one of these requisites but ignore the other requirements. Previous studies have lighted such issues and withal compared the majority of them on the substructure of different parameters. However, prior studies have shown a constrained role in evaluating security, privacy and trust especially for keenly intellective and connected M-IoT networks. This paper considered the shortcomings of existing literature and provided an in-depth evaluation of different approaches which fixates on the crucial aspects of security, privacy, and trust.

This article covered the concept and ideology of smart M-IoT networks and its devices followed by their applications, advances, challenges, characteristics, technologies, and standards. Then the literature evaluations were presented for approaches which emphasized secure frameworks, data-privacy, secure protocols, physical layer security, and handover protections for smart M-IoT. Next, different ways for analyzing the security, privacy, and trust in M-IoT were discussed followed by a roadmap and open issues along with highlights of some pertinent materials which can be followed for improving understandings in this direction of research. This study has highlighted the requirements of new solutions, which can collectively resolve the issues related to security, privacy, and trust in smart M-IoT without compromising the performance and complexity of operations.

REFERENCES

[1] I. Farris, A. Orsino, L. Militano, A. Iera, and G. Araniti, "Federated IoT services leveraging 5G technologies at the edge," *Ad Hoc Netw.*, vol. 68, pp. 58–69, Jan. 2018.

[2] W. Liu, K. Nakauchi, and Y. Shoji, "A neighbor-based probabilistic broadcast protocol for data dissemination in mobile IoT networks," *IEEE Access*, vol. 6, pp. 12260–12268, 2018.

[3] A. Ghasempour and T. K. Moon, "Optimizing the number of collectors in machine-to-machine advanced metering infrastructure architecture for Internet of Things-based smart grid," in *Proc. Green Technol. Conf. (GreenTech)*, 2016, pp. 51–55.

[4] S. Misra and N. Saha, "Detour: Dynamic task offloading in software-defined fog for IoT applications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1159–1166, 2019.

[5] B. Afzal, M. Umair, G. A. Shah, and E. Ahmed, "Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 718–731, Mar. 2019.

[6] Z. B. Celik, E. Fernandes, E. Pauley, G. Tan, and P. McDaniel, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Comput. Surv.*, vol. 52, no. 4, p. 74, 2019.

[7] S.-M. Cheng, P.-Y. Chen, C.-C. Lin, and H.-C. Hsiao, "Traffic-aware patching for cyber security in mobile IoT," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 29–35, Jul. 2017.

[8] S. K. Goudos, P. I. Dallas, S. Chatziefthymiou, and S. Kyriazakos, "A survey of IoT key enabling and future technologies: 5G, mobile IoT, sematic Web and applications," *Wireless Pers. Commun.*, vol. 97, no. 2, pp. 1645–1675, 2017.

[9] A. Ghasempour, "Optimum number of aggregators based on power consumption, cost, and network lifetime in advanced metering infrastructure architecture for smart grid Internet of Things," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2016, pp. 295–296.

[10] *Low Power, Wide Area Networks (lpwan)*. Accessed: Sep. 2018. [Online]. Available: https://www.link-labs.com/blog/past-present-future-lpwan

[11] V. Sharma, I. You, G. Pau, M. Collotta, J. D. Lim, and J. N. Kim, "Lorawan-based energy-efficient surveillance by drones for intelligent transportation systems," *Energies*, vol. 11, no. 3, p. 573, 2018.

[12] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 34–40, Sep. 2017.

[13] P. Neumann, J. Montavont, and T. Noël, "Indoor deployment of low-power wide area networks (LPWAN): A LoRaWAN case study," in *Proc. 12th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, 2016, pp. 1–8.

[14] J. Jermyn, R. P. Jover, I. Murynets, M. Istomin, and S. Stolfo, "Scalability of machine to machine systems and the Internet of Things on LTE mobile networks," in *Proc. 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, 2015, pp. 1–9.

[15] R. P. Jover and I. Murynets, "Connection-less communication of IoT devices over LTE mobile networks," in *Proc. 12th Annu. Int. Conf. Sens., Commun., Netw. (SECON)*, pp. 247–255, 2015.

[16] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Proc. 12th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, 2015, pp. 190–198.

[17] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in *Proc. Globecom Workshops (GC Wkshps)*, 2016, pp. 1–6.

[18] V. Sharma, F. Song, I. You, and H.-C. Chao, "Efficient management and fast handovers in software defined wireless networks using UAVs," *IEEE Netw.*, vol. 31, no. 6, pp. 78–85, Nov. 2017.

[19] Y. Bi, G. Han, S. Xu, X. Wang, C. Lin, Z. Yu, and P. Sun, "Software defined space-terrestrial integrated networks: Architecture, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 22–28, Jan. 2019.

[20] A. Muthanna, A. A. Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy, "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *J. Sensor Actuator Netw.*, vol. 8, no. 1, p. 15, Feb. 2019.

[21] H. Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, "Advertising in the IoT era: Vision and challenges," 2018, *arXiv:1802.04102*. [Online]. Available: http://arxiv.org/abs/1802.04102

[22] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[23] Y.-W. Sawng, H.-W. Kim, S.-J. Lee, and J.-W. Choi, "Technology forecasting of IoT healthcare with big data analysis," in *Proc. ICCC Soc. Korea*, 2017, pp. 89–90.

[24] A. Ghasempour, "Optimized scalable decentralized hybrid advanced metering infrastructure for smart grid," in *Proc. Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2015, pp. 223–228.

[25] A. Ghasempour, "Optimum packet service and arrival rates in advanced metering infrastructure architecture of smart grid," in *Proc. Green Technol. Conf. (GreenTech)*, Apr. 2016, pp. 1–5.

[26] A. Ghasempour, "Optimized advanced metering infrastructure architecture of smart grid based on total cost, energy, and delay," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Sep. 2016, pp. 1–6.

[27] A. Chasempour, "Optimizing the advanced metering infrastructure architecture in smart grid," Ph.D. dissertation, Dept. Elect. Eng., Utah State Univ., Logan, UT, USA, 2016, vol. 5023.

[28] V. Sharma, F. Song, I. You, and M. Atiquzzaman, "Energy efficient device discovery for reliable communication in 5G-based IoT and BSNs using unmanned aerial vehicles," *J. Netw. Comput. Appl.*, vol. 97, pp. 79–95, Nov. 2017.

[29] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of Things," in *The Internet of Things*. New York, NY, USA: Springer, 2010, pp. 389–395.

[30] G. M. Køien, "Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 495–510, Dec. 2011.

[31] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–7.

[32] K.-D. Chang and J.-L. Chen, "A survey of trust management in WSNs, Internet of Things and future Internet," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 1, pp. 5–23, 2012.

[33] T. Bhattasali, R. Chaki, and N. Chaki, "Study of security issues in pervasive environment of next generation Internet of Things," in *Proc. Comput. Inf. Syst. Ind. Manage.* Berlin, Germany: Springer, 2013, pp. 206–217.

[34] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[35] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[36] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[37] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[38] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and security in Internet of Things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99–109, Apr. 2015.

[39] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the Internet of Things," *Comput. Netw.*, vol. 102, pp. 83–95, Jun. 2016.

[40] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: A security point of view," *Internet Res.*, vol. 26, no. 2, pp. 337–359, Apr. 2016.

[41] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[42] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[43] L. Chen, S. Thombre, K. Järvinen, E. S. Lohan, A. Alén-Savikko, H. Leppäkoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[44] W. Feng, Z. Yan, H. Zhang, K. Zeng, Y. Xiao, and Y. T. Hou, "A survey on security, privacy, and trust in mobile crowdsourcing," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2971–2992, Aug. 2018.

[45] K. Yang, D. Blaauw, and D. Sylvester, "Hardware designs for security in ultra-low-power IoT systems: An overview and survey," *IEEE Micro*, vol. 37, no. 6, pp. 72–89, Nov. 2017.

[46] S. Sen, J. Koo, and S. Bagchi, "TRIFECTA: Security, energy efficiency, and communication capacity comparison for wireless IoT devices," *IEEE Internet Comput.*, vol. 22, no. 1, pp. 74–81, Jan. 2018.

[47] X. Tang, P. Ren, and Z. Han, "Jamming mitigation via hierarchical security game for IoT communications," *IEEE Access*, vol. 6, pp. 5766–5779, 2018.

[48] B. L. Parne, S. Gupta, and N. S. Chaudhari, "SEGB: Security enhanced group based AKA protocol for M2M communication in an IoT enabled LTE/LTE-A network," *IEEE Access*, vol. 6, pp. 3668–3684, 2018.

[49] N.-N. Dao, Y. Kim, S. Jeong, M. Park, and S. Cho, "Achievable multi-security levels for lightweight IoT-enabled devices in infrastructureless peer-aware communications," *IEEE Access*, vol. 5, pp. 26743–26753, 2017.

[50] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-cost security of IoT sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 327–340, Feb. 2018.

[51] J. Wang, Z. Hong, Y. Zhang, and Y. Jin, "Enabling security-enhanced attestation with Intel SGX for remote terminal and IoT," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 1, pp. 88–96, Jan. 2018.

[52] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource IoT devices," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9381–9393, Oct. 2017.

[53] R. Giuliano, F. Mazzenga, A. Neri, and A. M. Vegni, "Security access protocols in IoT capillary networks," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 645–657, Jun. 2017.

[54] W. Yu and S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 11, pp. 2934–2944, Nov. 2017.

[55] T. Ulz, T. Pieber, A. Höller, S. Haas, and C. Steger, "Secured and easy-to-use NFC-based device configuration for the Internet of Things," *IEEE J. Radio Freq. Identificat.*, vol. 1, no. 1, pp. 75–84, Mar. 2017.

[56] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, 2017.

[57] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

[58] A. Ghasempour and J. H. Gunther, "Finding the optimal number of aggregators in machine-to-machine advanced metering infrastructure architecture of smart grid based on cost, delay, and energy consumption," in *Proc. 13th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2016, pp. 960–963.

[59] *IoT Standards and Protocols*. Accessed: Sep. 2018. [Online]. Available: https://www.postscapes.com/Internet-of-Things-protocols/

[60] *GSMA IoT Security Guidelines*. Accessed: Sep. 2018. [Online]. Available: https://www.gsma.com/IoT/IoT-security/IoT-security-guidelines/

[61] V. Sharma, K. Lee, S. Kwon, J. Kim, H. Park, K. Yim, and S.-Y. Lee, "A consensus framework for reliability and mitigation of zero-day attacks in IoT," *Secur. Commun. Netw.*, vol. 2017, pp. 1–24, Nov. 2017.

[62] F. Kammüller, M. Kerber, and C. W. Probst, "Insider threats and auctions: Formalization, mechanized proof, and code generation," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 8, no. 1, pp. 44–78, 2017.
[63] V. Sharma, I. You, and G. Kul, "Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain," in *Proc. Int. Workshop Manag. Insider Secur. Threats*, 2017, pp. 81–84.
[64] G. Li, H. Zhou, G. Li, and B. Feng, "Application-aware and dynamic security function chaining for mobile networks," *J. Internet Services Inf. Secur.*, vol. 7, no. 4, pp. 21–34, 2017.
[65] V. Sharma, I. You, and R. Kumar, "ISMA: Intelligent sensing model for anomalies detection in cross platform OSNs with a case study on IoT," *IEEE Access*, vol. 5, pp. 3284–3301, 2017.
[66] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Exp.*, vol. 5, no. 1, pp. 1–7, Mar. 2019.
[67] J. Petäjäjärvi, K. Mikhaylov, M. Hämäläinen, and J. Iinatti, "Evaluation of LoRa LPWAN technology for remote health and wellbeing monitoring," in *Proc. 10th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Mar. 2016, pp. 1–5.
[68] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, vol. 43. Hoboken, NJ, USA: Wiley, 2011.
[69] C. A. Trasviña-Moreno, R. Blasco, R. Casas, and A. Asensio, "A network performance analysis of LoRa modulation for LPWAN sensor devices," in *Ubiquitous Computing and Ambient Intelligence*. Cham, Switzerland: Springer, 2016, pp. 174–181.
[70] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2016, pp. 1–5.
[71] *Standards*. Accessed: Mar. 10, 2018. [Online]. Available: http://standards.ieee.org/innovate/IoT/stds.html
[72] *IoT Standards and Protocols*. Accessed: Mar. 10, 2018. [Online]. Available: https://www.postscapes.com/Internet-of-Things-protocols/
[73] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) things," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389–1406, 3rd Quart., 2013.
[74] *IBM-Watson IoT*. Accessed: Sep. 2018. [Online]. Available: https://developer.ibm.com/IoTplatform/
[75] *Microsoft Azure IoT Suite*. Accessed: Sep. 2018. [Online]. Available: https://www.microsoft.com/en-us/Internet-of-Things
[76] *OpenIoT*. Accessed: Sep. 2018. [Online]. Available: http://www.openIoT.eu/
[77] *OCF*. Accessed: Sep. 2018. [Online]. Available: https://openconnectivity.org/
[78] Y. Amit, R. Hay, R. Saltzman, and A. Sharabani, "Pinpointing security vulnerabilities in computer software applications," U.S. Patent 8 510 842, Aug. 13, 2013.
[79] O. H. Alhazmi, Y. K. Malaiya, and I. Ray, "Measuring, analyzing and predicting security vulnerabilities in software systems," *Comput. Secur.*, vol. 26, no. 3, pp. 219–228, May 2007.
[80] K. Benton, L. J. Camp, and C. Small, "OpenFlow vulnerability assessment," in *Proc. 2nd ACM SIGCOMM workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 151–152.
[81] *Open Web Application Security Project (OWASP)*. Accessed: Oct. 2018. [Online]. Available: https://www.owasp.org/index.php/Main_Page
[82] K. Peguero, N. Zhang, and X. Cheng, "An empirical study of the framework impact on the security of JavaScript Web applications," in *Proc. Companion The Web Conf. Web Conf.*, 2018, pp. 753–758.
[83] Y. Fang, Y. Li, L. Liu, and C. Huang, "DeepXSS: Cross site scripting detection based on deep learning," in *Proc. Int. Conf. Comput. Artif. Intell.*, 2018, pp. 47–51.
[84] D. Sagar, S. Kukreja, J. Brahma, S. Tyagi, and P. Jain, "Studying open source vulnerability scanners for vulnerabilities in Web applications," *IIOAB J.*, vol. 9, no. 2, pp. 43–49, 2018.
[85] G. Lancioni, S. Hunt, and M. D. Wood, "Method and system to accelerate IoT patch propagation and reduce security vulnerabilities exposure time," U.S. Patent 15 476 219, Oct. 4, 2018.
[86] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly, and H. Chen, "Identifying supervisory control and data acquisition (SCADA) devices and their vulnerabilities on the Internet of Things (IoT): A text mining approach," *IEEE Intell. Syst.*, vol. 33, no. 2, pp. 63–73, Sep. 2020.
[87] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial Internet of Things (IIoT)," *IEEE Access*, vol. 6, pp. 43368–43383, 2018.
[88] K. Kim, J. Lee, and W. Jung, "Method of building a security vulnerability information collection and management system for analyzing the security vulnerabilities of IoT devices," in *Advanced Multimedia and Ubiquitous Engineering*. Singapore: Springer, 2017, pp. 205–210.
[89] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[90] K. Kim, I. Kim, and J. Lim, "National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1140–1151, Mar. 2017.
[91] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.
[92] W. Xie, Y. Jiang, Y. Tang, N. Ding, and Y. Gao, "Vulnerability detection in IoT firmware: A survey," in *Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2017, pp. 769–772.
[93] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Inf. Sci.*, vols. 412–413, pp. 223–241, Oct. 2017.
[94] J. Li, J. Li, D. Xie, and Z. Cai, "Secure auditing and deduplicating data in cloud," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2386–2396, Aug. 2016.
[95] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Comput.*, vol. 21, no. 1, pp. 277–286, 2017.
[96] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proc. IEEE 15th Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2014, pp. 16–23.
[97] S. Cirani, M. Picone, P. Gonizzi, L. Veltri, and G. Ferrari, "IoT-OAS: An OAuth-based authorization service architecture for secure services in IoT scenarios," *IEEE Sensors J.*, vol. 15, no. 2, pp. 1224–1234, Feb. 2015.
[98] K. S. Sahoo, B. Sahoo, and A. Panda, "A secured SDN framework for IoT," in *Proc. Int. Conf. Man Mach. Interfacing (MAMI)*, Dec. 2015, pp. 1–4.
[99] J. Pacheco, S. Satam, S. Hariri, C. Grijalva, and H. Berkenbrock, "IoT security development framework for building trustworthy smart car services," in *Proc. IEEE Conf. Intell. Secur. Informat. (ISI)*, Sep. 2016, pp. 237–242.
[100] P. P. Pereira, J. Eliasson, and J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," in *Proc. IECON 40th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2014, pp. 5293–5299.
[101] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "SDN-based security framework for the IoT in distributed grid," in *Proc. Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2016, pp. 1–5.
[102] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the Internet-of-Things," in *Proc. IEEE 14th Int. Symp. 'World Wireless, Mobile Multimedia Netw.' (WoWMoM)*, Jun. 2013, pp. 1–6.
[103] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," *J. Comput. Syst. Sci.*, vol. 81, no. 8, pp. 1452–1463, Dec. 2015.
[104] A. Guchhait, M. B, and K. D, "A hybrid V2V system for collision-free high-speed Internet access in intelligent transportation system," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 3, p. e3282, Mar. 2018.
[105] N. Dagdee and R. Vijaywargiya, "Credential based hybrid access control methodology for shared electronic health records," in *Proc. Int. Conf. Inf. Manage. Eng.*, 2009, pp. 624–628.
[106] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in *Proc. 7th Int. Conf. Body Area Netw. (ICST)*, 2012, pp. 269–275.
[107] M. Ge and D. S. Kim, "A framework for modeling and assessing security of the Internet of Things," in *Proc. 21st Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2015, pp. 776–781.
[108] B. R. Ray, J. Abawajy, and M. Chowdhury, "Scalable RFID security framework and protocol supporting Internet of Things," *Comput. Netw.*, vol. 67, pp. 89–103, Jul. 2014.
[109] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proc. 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 356–362.

[110] Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," in *Proc. Int. Conf. Internet Things (IoT)*, Oct. 2014, pp. 13–18.
[111] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: A security framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3083–3094, Nov. 2016.
[112] J. G. Mclachlan, A. J. Farrugia, and N. T. Sullivan, "Adaptive secondary authentication criteria based on account data," U.S. Patent 9 043 887, May 26, 2015.
[113] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018.
[114] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing sensor to cloud ecosystem using Internet of Things (IoT) security framework," in *Proc. Int. Conf. Internet Things Cloud Comput.*, 2016, p. 79.
[115] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real-time anomaly detection for streaming data," *Neurocomputing*, vol. 262, pp. 134–147, Nov. 2017.
[116] V. Sharma, R. Kumar, W.-H. Cheng, M. Atiquzzaman, K. Srinivasan, and A. Y. Zomaya, "NHAD: Neuro-fuzzy based horizontal anomaly detection in online social networks," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 11, pp. 2171–2184, Nov. 2018.
[117] M. Toledano, I. Cohen, Y. Ben-Simhon, and I. Tadeski, "Real-time anomaly detection system for time series at scale," in *Proc. KDD-Workshop Anomaly Detection Finance*, 2018, pp. 56–65.
[118] M. Ahmed and A. N. Mahmood, "Network traffic pattern analysis using improved information theoretic co-clustering based collective anomaly detection," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Cham, Switzerland: Springer, 2014, pp. 204–219.
[119] D. Monniaux, "Decision procedures for the analysis of cryptographic protocols by logics of belief," in *Proc. 12th IEEE Comput. Secur. Found. Workshop*, 1999, pp. 44–54.
[120] M. Cohen and M. Dam, "Logical omniscience in the semantics of ban logic," in *Proc. Found. Comput. Secur.*, 2005, pp. 121–132.
[121] S. Matsuo, K. Miyazaki, A. Otsuka, and D. Basin, "How to evaluate the security of real-life cryptographic protocols?" in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2010, pp. 182–194.
[122] G. Bleumer, "Random oracle model," in *Encyclopedia of Cryptography and Security*. New York, NY, USA: Springer, 2011, pp. 1027–1028.
[123] W. Mao, *Modern Cryptography: Theory and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.
[124] L. C. Paulson, "Inductive analysis of the Internet protocol TLS," *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 3, pp. 332–351, Aug. 1999.
[125] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heám, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2005, pp. 281–285.
[126] M. Kaufmann, P. Manolios, and J. S. Moore, *Computer-Aided Reasoning: ACL2 Case Studies*, vol. 4. Berlin, Germany: Springer, 2013.
[127] R. Küsters and T. Truderung, "Using ProVerif to analyze protocols with Diffie-Hellman exponentiation," in *Proc. 22nd Comput. Secur. Found. Symp. (CSF)*, Jul. 2009, pp. 157–171.
[128] C. J. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Proc. Int. Conf. Comput. Aided Verification*. Berlin, Germany: Springer, 2008, pp. 414–418.
[129] P. Urien, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things," in *Proc. IEEE 10th Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2013, pp. 845–846.
[130] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommun. Syst.*, vol. 64, no. 1, pp. 193–209, Jan. 2017.
[131] C. Ma, S. Kulshrestha, W. Shi, Y. Okada, and R. Bose, "E-learning material development framework supporting VR/AR based on linked data for IoT security education," in *Proc. Int. Conf. Emerg. Internetwork., Data Web Technol.* Cham, Switzerland: Springer, 2018, pp. 479–491.
[132] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," *ACM Trans. Internet Technol.*, vol. 16, no. 4, p. 26, 2016.
[133] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future Internet of Things," *Adv. Internet Things*, vol. 2, no. 1, pp. 1–7, 2012.
[134] J. B. Bernabe, J. L. Hernández, M. V. Moreno, and A. F. S. Gomez, "Privacy-preserving security framework for a social-aware Internet of Things," in *Proc. Int. Conf. Ubiquitous Comput. Ambient Intell.* Cham, Switzerland: Springer, 2014, pp. 408–415.
[135] D. Lake, R. Milito, M. Morrow, and R. Vargheese, "Internet of Things: Architectural framework for eHealth security," *J. ICT Standardization*, vol. 1, no. 3, pp. 301–328, 2014.
[136] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li, "A system framework of security management in enterprise systems," *Syst. Res. Behav. Sci.*, vol. 30, no. 3, pp. 287–299, May 2013.
[137] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Procedia Comput. Sci.*, vol. 52, pp. 1028–1033, 2015.
[138] H. Shafagh and A. Hithnawi, "Security comes first, a public-key cryptography framework for the Internet of Things," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2014, pp. 135–136.
[139] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "An IDS framework for Internet of Things empowered by 6LoWPAN," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1337–1340.
[140] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," in *Proc. 29th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, 2015, pp. 688–693.
[141] V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, "Smart human security framework using Internet of Things, cloud and fog computing," in *Intelligent Distributed Computing*. Cham, Switzerland: Springer, 2015, pp. 251–263.
[142] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.
[143] V. Sharma, K. Srinivasan, D. N. K. Jayakody, O. Rana, and R. Kumar, "Managing service-heterogeneity using osmotic computing," 2017, *arXiv:1704.04213*. [Online]. Available: http://arxiv.org/abs/1704.04213
[144] V. Sharma, I. You, and R. Kumar, "Resource-based mobility management for video users in 5G using catalytic computing," *Comput. Commun.*, vol. 118, pp. 120–139, Mar. 2018.
[145] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.*, vol. 72, pp. 1–12, Jan. 2018.
[146] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks," *IEEE Access*, vol. 5, pp. 11100–11117, 2017.
[147] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things," *Future Gener. Comput. Syst.*, vol. 92, pp. 758–776, Mar. 2019.
[148] C. Deepa and B. Latha, "HHSRP: A cluster based hybrid hierarchical secure routing protocol for wireless sensor networks," *Cluster Comput.*, pp. 1–17, Jul. 2017.
[149] S. Ullah, M. Imran, and M. Alnuem, "A hybrid and secure priority-guaranteed MAC protocol for wireless body area network," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 2, Feb. 2014, Art. no. 481761.
[150] Y. Yang and S. Roy, "Secure MAC protocol for periodic smart metering data communication with compressive sensing," in *Proc. Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.
[151] N. Li, J.-F. Martinez-Ortega, and V. Hernandez Diaz, "Cross-layer balanced and reliable opportunistic routing algorithm for mobile ad hoc networks," 2017, *arXiv:1710.00105*. [Online]. Available: http://arxiv.org/abs/1710.00105
[152] J. K. Vinayagam, C. H. Balaswamy, and K. Soundararajan, "Adopting cross layer approach for detecting and segregating malicious nodes in MANET," in *Proc. Int. Conf. Signal Process. Commun. (ICSPC)*, Jul. 2017, pp. 457–461.
[153] S. Adibi, "A novel energy-efficient cross-application-layer platform with QoS-security support," *Int. J. Commun. Syst.*, vol. 30, no. 2, p. e2940, Jan. 2017.
[154] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *Proc. World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 428–432.
[155] S. Raza, T. Voigt, and V. Jutvik, "Lightweight IKEv2: A key management solution for both the compressed IPsec and the IEEE 802.15. 4 security," in *Proc. IETF Workshop Object Secur.*, vol. 23, pp. 1–2, 2012.
[156] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring end-to-end IP security protocols to the Internet of Things," in *Proc. 21st IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2013, pp. 1–10.

[157] I. You and J.-H. Lee, "SPFP: Ticket-based secure handover for fast proxy mobile IPv6 in 5G networks," *Comput. Netw.*, vol. 129, pp. 363–372, Dec. 2017.
[158] V. Sharma, I. You, F.-Y. Leu, and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5G mobile xhaul networks," *J. Netw. Comput. Appl.*, vol. 102, pp. 38–57, Jan. 2018.
[159] J. Guan, V. Sharma, I. You, and M. Atiquzzaman, "Extension of MIH to support FPMIPv6 for optimized heterogeneous handover," 2017, *arXiv:1705.09835*. [Online]. Available: http://arxiv.org/abs/1705.09835
[160] L. Xu, Y. He, X. Chen, and X. Huang, "Ticket-based handoff authentication for wireless mesh networks," *Comput. Netw.*, vol. 73, pp. 185–194, Nov. 2014.
[161] P. Yadav and M. Hussain, "A secure AODV routing protocol with node authentication," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, vol. 1, Apr. 2017, pp. 489–493.
[162] K. D. Kang, "A practical and lightweight source authentication protocol using one-way hash chain in CAN," Ph.D. dissertation, Inf. Commun. Eng., DGIST, Daegu, Republic of Korea, 2017.
[163] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2710–2723, Nov. 2013.
[164] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 2728–2733.
[165] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment," *Future Gener. Comput. Syst.*, vol. 78, pp. 1005–1019, Jan. 2018.
[166] P. Gope, R. Amin, S. K. Hafizul Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018.
[167] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervas. Mobile Comput.*, vol. 24, pp. 210–223, Dec. 2015.
[168] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," *Multimedia Tools Appl.*, pp. 1–31, 2017.
[169] A. M. I. Alkuhlani and S. Thorat, "Lightweight anonymity-preserving authentication and key agreement protocol for the Internet of Things environment," in *Proc. Int. Conf. Intell. Inf. Technol.* Singapore: Springer, 2017, pp. 108–125.
[170] G. Sharma and S. Kalra, "A secure remote user authentication scheme for smart cities e-governance applications," *J. Reliable Intell. Environ.*, vol. 3, no. 3, pp. 177–188, Sep. 2017.
[171] F. Rahman, M. E. Hoque, and S. I. Ahamed, "AnonPri: A secure anonymous private authentication protocol for RFID systems," *Inf. Sci.*, vol. 379, pp. 195–210, Feb. 2017.
[172] O. Ermiş, C. S. Bahtiyar, E. Anarım, and M. U. Çağlayan, "A key agreement protocol with partial backward confidentiality," *Comput. Netw.*, vol. 129, pp. 159–177, Dec. 2017.
[173] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 34, pp. 255–270, Jun. 2017.
[174] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.
[175] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet of Things," in *Proc. Int. Symp. Next-Gener. Electron. (ISNE)*, May 2014, pp. 1–2.
[176] D. Garcia-Carrillo and R. Marin-Lopez, "Lightweight CoAP-based bootstrapping service for the Internet of Things," *Sensors*, vol. 16, no. 3, p. 358, Mar. 2016.
[177] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based Internet of Things," *Wireless Pers. Commun.*, vol. 61, no. 3, pp. 527–542, Dec. 2011.
[178] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[179] Q. Guo, Y. Cui, X. Zou, and Q. Huang, "Generic construction of privacy-preserving optimistic fair exchange protocols," *J. Internet Services Inf. Secur.*, vol. 7, no. 2, pp. 44–56, 2017.
[180] N. Accettura and G. Piro, "Optimal and secure protocols in the IETF 6TiSCH communication stack," in *Proc. 23rd Int. Symp. Ind. Electron. (ISIE)*, Jun. 2014, pp. 1469–1474.
[181] H. Syafruddin and A. S. J. Putra, "Performance analysis of using a reliable transport layer protocol for transmitting EAP message over RADIUS in inter-domain WLAN roaming," in *Proc. 3rd Int. Conf. Inf. Commun. Technol. Moslem World (ICT4M)*, Dec. 2010, pp. G1–G5.
[182] M. Nakhjiri and M. Nakhjiri, *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*. Hoboken, NJ, USA: Wiley, 2005.
[183] J. Irazabal, R. O. Laprida, D. A. Masini, and D. B. Ponceleon, "Blockchain enabled crowdsourcing," U.S. Patent 15 789 635, Apr. 25, 2019.
[184] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K.-R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5723–5736, Oct. 2019.
[185] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," *IEEE Trans. Eng. Manag.*, early access, Jun. 21, 2019, doi: 10.1109/TEM.2019.2920154.
[186] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based DMM," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 22–31, May 2018, doi: 10.1109/MCOM.2018.1700863.
[187] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Secur.*, vol. 37, pp. 111–123, Sep. 2013.
[188] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the Internet of Things," in *Proc. IEEE Int. Conf. Green Comput. Commun. (GreenCom)*, Nov. 2012, pp. 244–248.
[189] A. Ukil, S. Bandyopadhyay, J. Joseph, V. Banahatti, and S. Lodha, "Negotiation-based privacy preservation scheme in Internet of Things platform," in *Proc. 1st Int. Conf. Secur. Internet Things*, 2012, pp. 75–84.
[190] S. Pérez, D. Rotondi, D. Pedone, L. Straniero, M. J. Núñez, and F. Gigante, "Towards the CP-ABE application for privacy-preserving secure data sharing in IoT contexts," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.* Cham, Switzerland: Springer, 2017, pp. 917–926.
[191] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017.
[192] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Comput. Netw.*, vol. 133, pp. 141–156, Mar. 2018.
[193] O. Bamasag, "A lightweight privacy and integrity preserving data communication in smart grid," *Eur. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 4, pp. 21–30, 2015.
[194] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IoT," in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimedia Technol. (IC-BNMT)*, Oct. 2011, pp. 192–195.
[195] C. Doukas, I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, "Enabling data protection through PKI encryption in IoT m-health devices," in *Proc. IEEE 12th Int. Conf. Bioinf. Bioeng. (BIBE)*, Nov. 2012, pp. 25–29.
[196] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 725–730.
[197] D. Li, Z. Aung, J. Williams, and A. Sanchez, "p3: Privacy preservation protocol for automatic appliance control application in smart grid," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 414–429, Oct. 2014.
[198] H. Bao and L. Chen, "A lightweight privacy-preserving scheme with data integrity for smart grid communications," *Concurrency Comput. Pract. Exper.*, vol. 28, no. 4, pp. 1094–1110, Mar. 2016.
[199] H. Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," *IEEE Internet Things J.*, vol. 2, no. 3, pp. 248–258, Jun. 2015.
[200] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. 7th Int. Symp. Parallel Archit., Algorithms Program. (PAAP)*, Dec. 2015, pp. 217–222.
[201] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[202] S. Mascetti, C. Bettini, and D. Freni, "Longitude: Centralized privacy-preserving computation of users' proximity," in *Proc. Workshop Secure Data Manage.* Berlin, Germany: Springer, 2009, pp. 142–157.

[203] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, "A reference architecture for improving security and privacy in Internet of Things applications," in *Proc. IEEE Int. Conf. Mobile Services (MS)*, Jun. 2014, pp. 108–115.

[204] *Spore*. Accessed: Sep. 2018. [Online]. Available: http://www.lsv.fr/Software/spore/table.html

[205] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the security and privacy of Internet of Things architectures and systems," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Sep. 2015, pp. 49–57.

[206] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT)," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2014, pp. 1244–1248.

[207] H. Kupwade Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2014, pp. 762–765.

[208] E. Bertino, "Data security and privacy in the IoT." in *Proc. EDBT*, 2016, pp. 1–3.

[209] C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zomaya, "Big data privacy in the Internet of Things era," *IT Prof.*, vol. 17, no. 3, pp. 32–39, 2015.

[210] Y. H. Hwang, "IoT security & privacy: Threats and challenges," in *Proc. 1st ACM Workshop IoT Privacy, Trust, Secur.*, 2015, p. 1.

[211] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. 7th Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Nov. 2014, pp. 230–234.

[212] X. Jiang, X. Ge, J. Yu, F. Kong, X. Cheng, and R. Hao, "An efficient symmetric searchable encryption scheme for cloud storage," *J. Internet Services Inf. Secur.*, vol. 7, no. 2, pp. 1–18, 2017.

[213] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf.*, 2015, p. 54.

[214] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proc. World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 67–72.

[215] X.-J. Lin, L. Sun, and H. Qu, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," *Comput. Secur.*, vol. 48, pp. 142–149, Feb. 2015.

[216] M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, "Experiments with security and privacy in IoT networks," in *Proc. 16th Int. Symp. A World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–6.

[217] A. Campan and T. M. Truta, "Data and structural k-anonymity in social networks," in *Privacy, Security, and Trust in KDD*. Berlin, Germany: Springer, 2009, pp. 33–54.

[218] J. Cheng, A. W.-C. Fu, and J. Liu, "K-isomorphism: Privacy preserving network publication against structural attacks," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2010, pp. 459–470.

[219] L. Zou, L. Chen, and M. T. Özsu, "K-automorphism: A general framework for privacy preserving network publication," *Proc. VLDB Endowment*, vol. 2, no. 1, pp. 946–957, 2009.

[220] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Proc. Int. Conf. Privacy Secur. Mobile Syst.*, May 2014, pp. 1–8.

[221] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[222] D. Kozlov, J. Veijalainen, and Y. Ali, "Security and privacy threats in IoT architectures," in *Proc. 7th Int. Conf. Body Area Netw.*, 2012, pp. 256–262.

[223] A. Ukil, S. Bandyopadhyay, and A. Pal, "Privacy for IoT: Involuntary privacy enablement for smart energy systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 536–541.

[224] A. Ukil, S. Bandyopadhyay, and A. Pal, "IoT-privacy: To be private or not to be private," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2014, pp. 123–124.

[225] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[226] A. Abhishta, R. Joosten, and L. J. Nieuwenhuis, "Comparing alternatives to measure the impact of DDoS attack announcements on target stock prices," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 8, no. 4, pp. 1–18, 2017.

[227] I. Kotenko, I. Saenko, and A. Kushnerevich, "Parallel big data processing system for security monitoring in Internet of Things networks," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 8, no. 4, pp. 60–74, 2017.

[228] W. Zhou and S. Piramuthu, "Security/privacy of wearable fitness tracking IoT devices," in *Proc. 9th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2014, pp. 1–5.

[229] H. C. Pöhls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. D. Rodriguez, and T. Mouroutis, "RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects," in *Proc. Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2014, pp. 122–127.

[230] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2015, pp. 163–167.

[231] K. Wrona, A. de Castro, and B. Vasilache, "Data-centric security in military applications of commercial IoT technology," in *Proc. 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 239–244.

[232] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IoT)," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Cham, Switzerland: Springer, 2017, pp. 533–543.

[233] I.-R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Services Comput.*, vol. 9, no. 3, pp. 482–495, May 2016.

[234] X. Wu and F. Li, "A multi-domain trust management model for supporting RFID applications of IoT," *PLoS ONE*, vol. 12, no. 7, Jul. 2017, Art. no. e0181124.

[235] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A mobile cloud hierarchical trust management protocol for IoT systems," in *Proc. 5th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Apr. 2017, pp. 125–130.

[236] N. Peshwe and D. Das, "Algorithm for trust based policy hidden communication in the Internet of Things," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 148–153.

[237] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, and S. Bianchi, "ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.

[238] R. K. Chahal and S. Singh, "Fuzzy rule-based expert system for determining trustworthiness of cloud service providers," *Int. J. Fuzzy Syst.*, vol. 19, no. 2, pp. 338–354, Apr. 2017.

[239] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in Internet of Things," in *Proc. 3rd Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. (VITAE)*, Jun. 2013, pp. 1–5.

[240] H. Son, N. Kang, B. Gwak, and D. Lee, "An adaptive IoT trust estimation scheme combining interaction history and stereotypical reputation," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 349–352.

[241] V. Sharma, I. You, R. Kumar, and P. Kim, "Computational offloading for efficient trust management in pervasive online social networks using osmotic computing," *IEEE Access*, vol. 5, pp. 5084–5103, 2017.

[242] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for Internet of Things," *Comput. Sci. Inf. Syst.*, vol. 8, no. 4, pp. 1207–1228, 2011.

[243] Z. A. Khan, J. Ullrich, A. G. Voyiatzis, and P. Herrmann, "A trust-based resilient routing mechanism for the Internet of Things," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, p. 27.

[244] K. Kravari and N. Bassiliades, "ORDAIN: An ontology for trust management in the Internet of Things," in *Proc. OTM Confederated Int. Conf. Move Meaningful Internet Syst.* Cham, Switzerland: Springer, 2017, pp. 216–223.

[245] I. Santos, F. Brezo, X. Ugarte-Pedrero, and P. G. Bringas, "Opcode sequences as representation of executables for data-mining-based unknown malware detection," *Inf. Sci.*, vol. 231, pp. 64–82, May 2013.

[246] R. Zhou, J. Pan, X. Tan, and H. Xi, "Application of CLIPS expert system to malware detection system," in *Proc. Int. Conf. Comput. Intell. Secur.*, vol. 1, Dec. 2008, pp. 309–314.

[247] A. Niki, "Drive-by download attacks: Effects and detection methods," in *Proc. 3rd IT Secur. Conf. Next Gener.*, 2009.
[248] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Multidimensional trust-based anomaly detection system in Internet of Things," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2017, pp. 302–313.
[249] J. Wang, I.-R. Chen, J. J. P. Tsai, and D.-C. Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," *Comput. Commun.*, vol. 116, pp. 90–100, Jan. 2018.
[250] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2017, pp. 1–6.
[251] M. F. Hinarejos, F. Almenárez, P. A. Cabarcos, J. L. Ferrer-Gomila, and A. M. López, "RiskLaine: A probabilistic approach for assessing risk in certificate-based security," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1975–1988, Aug. 2018.
[252] A. A. Obaidi and E. W. Yocam, "Persona and device based certificate management," U.S. Patent 14 985 273, Jul. 6, 2017.
[253] S. Namal, H. Gamaarachchi, G. MyoungLee, and T.-W. Um, "Autonomic trust management in cloud-based and highly dynamic IoT applications," in *Proc. ITU Kaleidoscope Trust Inf. Soc. (K-2015)*, 2015, pp. 1–8.
[254] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *Proc. 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.
[255] N. A. Mhetre, A. V. Deshpande, and P. N. Mahalle, "Trust management model based on fuzzy approach for ubiquitous computing," *Int. J. Ambient Comput. Intell.*, vol. 7, no. 2, pp. 33–46, Jul. 2016.
[256] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.
[257] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internet of Things," *China Commun.*, vol. 11, no. 2, pp. 148–156, Feb. 2014.
[258] J. Duan, D. Gao, D. Yang, C. H. Foh, and H.-H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 58–69, Feb. 2014.
[259] I.-R. Chen, J. Guo, and F. Bao, "Trust management for service composition in SOA-based IoT systems," in *Proc. Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 3444–3449.
[260] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, "Distributed trust management mechanism for the Internet of Things," *Appl. Mech. Mater.*, vol. 347, pp. 2463–2467, Aug. 2013.
[261] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, Nov. 2013.
[262] S. A. M. Yusof, N. Zakaria, and N. Ab Rahman Muton, "Timely trust: The use of IoT and cultural effects on swift trust formation within global virtual teams," in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, May 2017, pp. 297–303.
[263] H. Al-Hamadi and I. R. Chen, "Trust-based decision making for health IoT systems," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1408–1419, Oct. 2017.
[264] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoI-SIoT: A trust management system based on communities of interest for the social Internet of Things," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 747–752.
[265] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for Internet of Things," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Mar. 2017, pp. 1169–1176.
[266] F. Bao and I.-R. Chen, "Trust management for the Internet of Things and its application to service composition," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2012, pp. 1–6.
[267] F. Bao and I.-R. Chen, "Dynamic trust management for Internet of Things applications," in *Proc. Int. Workshop Self-Aware Internet Things*, 2012, pp. 1–6.
[268] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, vol. 7. New York, NY, USA: Springer, 2010.
[269] I. U. Zaman, A. B. Lopez, M. A. Al Faruque, and O. Boyraz, "Polarization mode dispersion-based physical layer key generation for optical fiber link security," *Opt. Sensors*, Paper JTu4A-20, Jul. 2017.
[270] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[271] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V. C. M. Leung, and J. J. P. C. Rodrigues, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.
[272] G. Zhang and H. Sun, "Secure distributed detection under energy constraint in IoT-oriented sensor networks," *Sensors*, vol. 16, no. 12, p. 2152, Dec. 2016.
[273] H. Hu, Z. Gao, X. Liao, and V. Leung, "Secure communications in CIoT networks with a wireless energy harvesting untrusted relay," *Sensors*, vol. 17, no. 9, p. 2023, Sep. 2017.
[274] S. N. Islam, M. A. Mahmud, and A. M. T. Oo, "Secured communication among IoT devices in the presence of cellular interference," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–6.
[275] J. Choi, "Physical layer security for channel-aware random access with opportunistic jamming," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2699–2711, Nov. 2017.
[276] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.
[277] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIoT networks," *Sensors*, vol. 16, no. 3, p. 339, Mar. 2016.
[278] D. Wei, L. Liang, M. Zhang, R. Qiao, and W. Huang, "A polarization state modulation based physical layer security scheme for wireless communications," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Nov. 2016, pp. 1195–1201.
[279] Z. Gao, H. Hu, D. Cheng, J. Xu, and X. Sun, "Physical layer security based on artificial noise and spatial modulation," in *Proc. 8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2016, pp. 1–5.
[280] Y. Li, T. Jiang, and J. Huang, "Compressed sensing method for secret key generation based on MIMO channel estimation," in *Proc. 3rd Int. Conf. Commun., Signal Process., Syst.* Cham, Switzerland: Springer, 2015, pp. 419–428.
[281] A. Limmanee and W. Henkel, "Secure physical-layer key generation protocol and key encoding in wireless communications," in *Proc. GLOBECOM Workshops (GC Wkshps)*, Dec. 2010, pp. 94–98.
[282] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[283] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
[284] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *Information*, vol. 7, no. 3, p. 49, Aug. 2016.
[285] J. Zhang, T. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the Internet of Things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, p. 420, Aug. 2017.
[286] A. Kitana, I. Traore, and I. Woungang, "Impact study of a mobile botnet over LTE networks.," *J. Internet Serv. Inf. Secur.*, vol. 6, no. 2, pp. 1–22, 2016.
[287] Q. Xu, P. Ren, H. Song, and Q. Du, "Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1924–1933, Dec. 2017.
[288] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[289] D. Altolini, V. Lakkundi, N. Bui, C. Tapparello, and M. Rossi, "Low power link layer security for IoT: Implementation and performance analysis," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2013, pp. 919–925.
[290] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 67–72.
[291] L. Brilli, T. Pecorella, and L. Mucchi, "Physical layer security for IoT devices configuration and key management-a proof of concept," in *Proc. AEIT Int. Annu. Conf. (AEIT)*, 2016, pp. 1–6.
[292] J.-H. Lee, J.-M. Bonnin, and X. Lagrange, "Host-based distributed mobility management support protocol for IPv6 mobile networks," in *Proc. IEEE 8th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2012, pp. 61–68.
[293] J.-H. Lee, J.-M. Bonnin, P. Seite, and H. Chan, "Distributed IP mobility management from the perspective of the IETF: Motivations, requirements, approaches, comparison, and challenges," *IEEE Wireless Commun.*, vol. 20, no. 5, pp. 159–168, Oct. 2013.

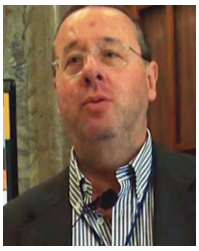
[294] B. S. Ghahfarokhi and N. Movahhedinia, "Context gathering and management for centralized context-aware handover in heterogeneous mobile networks," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 20, no. 6, pp. 914–933, 2012.
[295] H.-S. Chai, J. Jeong, and C.-H. Cho, "Security analysis of fast inter-LMA domain handover scheme in proxy mobile IPv6 networks," *Pervas. Mobile Comput.*, vol. 39, pp. 100–116, Aug. 2017.
[296] H.-S. Chai, J.-Y. Choi, and J. Jeong, "An enhanced secure mobility management scheme for building IoT applications," *Procedia Comput. Sci.*, vol. 56, pp. 586–591, 2015.
[297] B. Ndibanje, K. Kim, Y. Kang, H. Kim, T. Kim, and H. Lee, "A secure and efficient mutual authentication hand-off protocol for sensor device support in Internet of Things," *Sensors Mater.*, vol. 29, no. 7, pp. 953–960, 2017.
[298] N. Saxena, S. Grijalva, and N. S. Chaudhari, "Authentication protocol for an IoT-enabled LTE network," *ACM Trans. Internet Technol.*, vol. 16, no. 4, p. 25, 2016.
[299] J. Cao, M. Ma, and H. Li, "An uniform handover authentication between E-UTRAN and non-3GPP access networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3644–3650, Oct. 2012.
[300] Z. Haddad, M. Mahmoud, I. A. Saroit, and S. Taha, "Secure and efficient uniform handover scheme for LTE–A networks," in *Proc. Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1–6.
[301] M.-S. Chiang, C.-M. Huang, P. B. Chau, S. Xu, H. Zhou, and D. Ren, "A forward fast media independent handover control scheme for proxy mobile IPv6 (FFMIH-PMIPv6) over heterogeneous wireless mobile network," *Telecommun. Syst.*, vol. 65, no. 4, pp. 699–715, Aug. 2017.
[302] H. Ameur, M. Esseghir, L. Khoukhi, and L. Merghem-Boulahia, "Enhanced MIH (media independent handover) for collaborative green wireless communications," *Int. J. Commun. Syst.*, vol. 30, no. 7, p. e3029, May 2017.
[303] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—A comparison of link-layer security and IPsec for 6LoWPAN," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2654–2668, 2014.
[304] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song, "Toward a standardized common M2M service layer platform: Introduction to oneM2M," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 20–26, Jun. 2014.
[305] A. Rajaram, D. N. K. Jayakody, K. Srinivasan, B. Chen, and V. Sharma, "Opportunistic-harvesting: RF wireless power transfer scheme for multiple access relays system," *IEEE Access*, vol. 5, pp. 16084–16099, 2017.
[306] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.
[307] M. Khan, S. Din, M. Gohar, A. Ahmad, S. Cuomo, F. Piccialli, and G. Jeon, "Enabling multimedia aware vertical handover management in Internet of Things based heterogeneous wireless networks," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 25919–25941, Dec. 2017.
[308] H. Ju and Y. Yoo, "Efficient packet transmission utilizing vertical handover in IoT environment," *J. KIISE*, vol. 42, no. 6, pp. 807–816, Jun. 2015.
[309] J. E. Luzuriaga, J. C. Cano, C. Calafate, P. Manzoni, M. Perez, and P. Boronat, "Handling mobility in IoT applications using the MQTT protocol," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2015, pp. 245–250.
[310] A. J. J. Valera, M. A. Zamora, and A. F. G. Skarmeta, "An architecture based on Internet of Things to support mobility and security in medical environments," in *Proc. 7th IEEE Consum. Commun. Netw. Conf.*, Jan. 2010, pp. 1–5.
[311] A. S. Gaur, J. Budakoti, C.-H. Lung, and A. Redmond, "IoT-equipped UAV communications with seamless vertical handover," in *Proc. IEEE Conf. Dependable Secure Comput.*, Aug. 2017, pp. 459–465.
[312] K.-D. Baek and I.-Y. Ko, "Spatially cohesive service discovery and dynamic service handover for distributed IoT environments," in *Proc. Int. Conf. Web Eng.* Cham, Switzerland: Springer, 2017, pp. 60–78.
[313] T. Li, H. Zhou, H. Luo, I. You, and Q. Xu, "SAT-FLOW: Multi-strategy flow table management for software defined satellite networks," *IEEE Access*, vol. 5, pp. 14952–14965, 2017.
[314] J.-H. Lee, J.-M. Bonnin, I. You, and T.-M. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1077–1088, Mar. 2013.
[315] V. Sharma, J. D. Lim, J. N. Kim, and I. You, "SACA: Self-aware communication architecture for IoT using mobile fog servers," *Mobile Inf. Syst.*, vol. 2017, pp. 1–17, Apr. 2017.
[316] R. A. Khan and A. H. Mir, "Sensor fast proxy mobile IPv6 (SFPMIPv6)-A framework for mobility supported IP-WSN for improving QoS and building IoT," in *Proc. Int. Conf. Commun. Signal Process. (CCNC)*, Apr. 2014, pp. 1593–1598.
[317] L. Ni, Y. Yuan, X. Wang, M. Zhang, and J. Zhang, "A location privacy preserving scheme based on repartitioning anonymous region in mobile social network," *Procedia Comput. Sci.*, vol. 129, pp. 368–371, Jan. 2018.
[318] G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, "CASLP: A confused arc-based source location privacy protection scheme in WSNs for IoT," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 42–47, Sep. 2018.
[319] S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," *J. Netw. Comput. Appl.*, vol. 103, pp. 157–170, Feb. 2018.
[320] D. Liao, G. Sun, H. Li, H. Yu, and V. Chang, "The framework and algorithm for preserving user trajectory while using location-based services in IoT-cloud systems," *Cluster Comput.*, vol. 20, no. 3, pp. 2283–2297, Sep. 2017.
[321] S. Mirzamohammadi, J. A. Chen, A. A. Sani, S. Mehrotra, and G. Tsudik, "Ditio: Trustworthy auditing of sensor activities in mobile & IoT devices," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, 2017, p. 28.
[322] T. Mao, C. Cao, X. Peng, and W. Han, "A privacy preserving data aggregation scheme to investigate Apps installment in massive mobile devices," *Procedia Comput. Sci.*, vol. 129, pp. 331–340, Jan. 2018.
[323] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems," *Comput. Netw.*, vol. 135, pp. 32–43, Apr. 2018.
[324] I. Ullah, M. A. Shah, A. Wahid, A. Mehmood, and H. Song, "ESOT: A new privacy model for preserving location privacy in Internet of Things," *Telecommun. Syst.*, vol. 67, no. 4, pp. 553–575, Apr. 2018.
[325] G. Sun, V. Chang, M. Ramachandran, Z. Sun, G. Li, H. Yu, and D. Liao, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *J. Netw. Comput. Appl.*, vol. 89, pp. 3–13, Jul. 2017.
[326] R. M. Lopez, A. Dutta, Y. Ohba, H. Schulzrinne, and A. F. G. Skarmeta, "Network-layer assisted mechanism to optimize authentication delay during handoff in 802.11 networks," in *Proc. 4th Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Services*, 2007, pp. 1–8.
[327] Y. He and D. Perkins, "BASH: A backhaul-aided seamless handoff scheme for wireless mesh networks," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2008, pp. 1–8.
[328] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16 M network," *Comput. Secur.*, vol. 31, no. 6, pp. 741–749, 2012.
[329] Y. Zhang, X. Chen, J. Li, and H. Li, "Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks," *Comput. Netw.*, vol. 75, pp. 192–211, Dec. 2014.
[330] H.-Y. Chien, T.-H. Hsu, and Y.-L. Tang, "Fast pre-authentication with minimized overhead and high security for WLAN handoff," *WSEAS Trans. Comput.*, vol. 7, no. 2, pp. 46–51, 2008.
[331] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE Commun. Lett.*, vol. 14, no. 1, pp. 54–56, Jan. 2010.
[332] A. A. Al Shidhani and V. C. M. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 699–713, Sep. 2011.
[333] M. Kalong, S. Ngamsuriyaroj, and V. Visoottiviseth, "Dynamic key management for secure continuous handoff in wireless LAN," in *Proc. 6th Workshop Secure Netw. Protocols (NPSec)*, Oct. 2010, pp. 7–12.
[334] N. Saxena and A. Roy, "Novel framework for proactive handover with seamless multimedia over WLANs," *IET Commun.*, vol. 5, no. 9, pp. 1204–1212, Jun. 2011.
[335] Q. Jing, Y. Zhang, A. Fu, and X. Liu, "A privacy preserving handover authentication scheme for EAP-based wireless networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–6.
[336] T. N. Nguyen and M. Ma, "Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2173–2181, Jun. 2012.
[337] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 46–57, Feb. 2014.
[338] H.-Y. Chien and T.-H. Hsu, "Secure fast WLAN handoff using time-bound delegated authentication," *Int. J. Commun. Syst.*, vol. 22, no. 5, pp. 565–584, May 2009.

[339] C. Ma, K. Xue, and P. Hong, "A proxy signature based re-authentication scheme for secure fast handoff in wireless mesh networks.," *IJ Netw. Secur.*, vol. 15, no. 2, pp. 122–132, 2013.
[340] D. He, J. Bu, S. Chan, and C. Chen, "Handauth: Efficient handover authentication with conditional privacy for wireless networks," *IEEE Trans. Comput.*, vol. 62, no. 3, pp. 616–622, Mar. 2013.
[341] C. Wang, M. Ma, and L. Zhang, "An efficient EAP-based pre-authentication for inter-WRAN handover in TV white space," *IEEE Access*, vol. 5, pp. 9785–9796, 2017.
[342] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7246–7251.
[343] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 29–39, Feb. 2017.
[344] S. Feirer and T. Sauter, "Seamless handover in industrial WLAN using IEEE 802.11k," in *Proc. 26th Int. Symp. Ind. Electron. (ISIE)*, 2017, pp. 1234–1239.
[345] V. Sharma, J. Kim, S. Kwon, I. You, and F.-Y. Leu, "An overview of 802.21a-2012 and its incorporation into IoT-fog networks using osmotic framework," in *Proc. 3rd EAI Int. Conf. IoT Service*, 2017, pp. 1–6.
[346] V. Sharma, J. Kim, S. Kwon, I. You, and H.-C. Chen, "Fuzzy-based protocol for secure remote diagnosis of IoT devices in 5G networks," in *Proc. 3rd EAI Int. Conf. IoT Service*, 2017, pp. 1–6.
[347] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.
[348] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.
[349] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
[350] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, Jul. 2016.
[351] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[352] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.
[353] H.-C. Lee and K.-H. Ke, "Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 9, pp. 2177–2187, Sep. 2018.
[354] G. T. Garcia, V. M. Sanchez, C. N. L. Marin, J. I. Cortez, C. A. R. Acevedo, G. S. Gonzalez, J. L. H. Ameca, and M. D. C. M. Garcia, "Wireless sensor network for monitoring physical variables applied to green technology (IoT green technology)," *Eur. J. Electr. Eng. Comput. Sci.*, vol. 2, no. 2, pp. 1–7, Feb. 2018.
[355] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599–8609, 2018.
[356] V. Sharma, J. Kim, S. Kwon, I. You, K. Lee, and K. Yim, "A framework for mitigating zero-day attacks in IoT," 2018, *arXiv:1804.05549*. [Online]. Available: http://arxiv.org/abs/1804.05549
[357] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in Fog-to-Things computing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 169–175, Feb. 2018.
[358] A. G. P. Lobato, M. A. Lopez, I. J. Sanz, A. A. Cardenas, O. C. M. B. Duarte, and G. Pujolle, "An adaptive real-time architecture for zero-day threat detection," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[359] B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M. Hajjat, "Internet of Things: Convenience vs. privacy and secrecy," *Bus. Horizons*, vol. 58, no. 6, pp. 615–624, Nov. 2015.
[360] I. You and K. Yim, "Malware obfuscation techniques: A brief survey," in *Proc. Int. Conf. Broadband, Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2010, pp. 297–300.
[361] S.-Y. Lee, S.-R. Wi, E. Seo, J.-K. Jung, and T.-M. Chung, "ProFIoT: Abnormal behavior profiling (ABP) of IoT devices based on a machine learning approach," in *Proc. 27th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2017, pp. 1–6.
[362] T. M. Shaashua and O. Shaashua, "Physical environment profiling through Internet of Things integration platform," U.S. Patent 9 871 865, Jan. 16, 2018.
[363] J. A. Oravec, "Emerging 'cyber hygiene' practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security," in *Proc. IEEE Int. Prof. Commun. Conf. (ProComm)*, Jul. 2017, pp. 1–5.
[364] A. Chowdhury, "Cyber attacks in mechatronics systems based on Internet of Things," in *Proc. IEEE Int. Conf. Mechatronics (ICM)*, Feb. 2017, pp. 476–481.
[365] I. Chochliouros, S. Ziegler, L. Bolognini, N. Alonistioti, M. Stamatelatos, P. Kontopoulos, G. Mourikas, V. Vlachos, N. Gligoric, and M. Holst, "Enabling crowd-sourcing-based privacy risk assessment in EU: The privacy flag project," in *Proc. 21st Pan-Hellenic Conf. Informat.*, 2017, p. 31.
[366] R. Jiang, J. Luo, and X. Wang, "An attack tree based risk assessment for location privacy in wireless sensor networks," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM)*, 2012, pp. 1–4.
[367] R. Zheng, M. Zhang, Q. Wu, C. Yang, W. Wei, D. Zhang, and Z. Ma, "An IoT security risk autonomic assessment algorithm," *Telkomnika Indonesian J. Electr. Eng.*, vol. 11, no. 2, pp. 819–826, Feb. 2013.
[368] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–2.
[369] D. Soldani, Y. J. Guo, B. Barani, P. Mogensen, C.-L. I, and S. K. Das, "5G for ultra-reliable low-latency communications," *IEEE Netw.*, vol. 32, no. 2, pp. 6–7, Mar./Apr. 2018.

VISHAL SHARMA (Member, IEEE) received the B.Tech. degree in computer science and engineering from Punjab Technical University, in 2012, and the Ph.D. degree in computer science and engineering from Thapar University, India, in 2016. From November 2016 to March 2019, he worked with the Department of Information Security Engineering, Soonchunhyang University, South Korea, in multiple positions (from November 2016 to December 2017: as a Postdoctoral Researcher; January 2018 to March 2019: as a Research Assistant Professor). He also held a joint postdoctoral position with Soongsil University, South Korea. He was affiliated with the Industry-Academia Cooperation Foundation and the Mobile Internet Security Laboratory, Soonchunhyang University. Before this, he worked as a Lecturer with the Department of Computer Science and Engineering, Thapar University. He is currently working as a Lecturer (∼ Assistant Professor) with the School of Electronics, Electrical Engineering and Computer Science (EEECS), Queen's University Belfast (QUB), U.K. Before coming to QUB, he was a Research Fellow with the Information Systems Technology and Design (ISTD) Pillar, Singapore University of Technology and Design (SUTD), Singapore, where he worked on the future-proof blockchain systems funded by SUTD-MoE. He has authored/coauthored more than 100 journal/conference papers and book chapters and co-edited two books with Springer. His areas of research and interests are 5G networks, blockchain, aerial (UAV) communications, CPS-IoT, and mobile Internet systems. He was a recipient of three best paper awards from the International Conference on Communication, Management and Information Technology (ICCMIT), Warsaw, Poland, in April 2017; from CISC-S'17, South Korea, in June 2017; and from IoTaas, Taiwan, in September 2017. He is a Professional Member of ACM and the past Chair of ACM Student Chapter-TIET Patiala. He was the Track Chair of MobiSec'16 and AIMS-FSS'16, and a PC Member and a Reviewer of MIST'16 and MIST'17, respectively. He has served as the TPC Member for ETIC-2019, WiMO-2019, ITNAC-IEEE TCBD'17, ICCMIT'18, CoCoNet'18, and ITNAC-IEEE TCBD'18. Also, he serves as a reviewer for various ACM/IEEE Transactions and other journals. He also serves as the ATE for *IEEE Communications Magazine* and an Associate Editor for the IET-CAAI TRIT. He has served/serving as a Guest Editor for MIS, IJDSN, WCMC, and MDPI (*Sensors*, *Drones*, and *Future Internet*), and *Autosoft* journals.

ILSUN YOU (Senior Member, IEEE) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was with THINmultimedia Inc., Internet Security Company Ltd., and Hanjo Engineering Company Ltd., as a Research Engineer. He is currently a Full Professor with the Department of Information Security Engineering, Soonchunhyang University. He is a Fellow of the IET. He has served or is currently serving as a General Chair or a Program Chair for international conferences and workshops, such as WISA'19-20, MobiSec'16-19, AsiaARES'13-15, MIST'09-17, MobiWorld'08-17, and so forth. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. He is in the Editorial Board for *Information Sciences (INS)*, the *Journal of Network and Computer Applications (JNCA)*, IEEE Access, *Intelligent Automation & Soft Computing (AutoSoft)*, the *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, *Computing and Informatics (CAI)*, and the *Journal of High Speed Networks (JHSN)*. Especially, he has focused on 4/5G security, security for wireless networks & mobile internet, IoT security, and so forth while publishing more than 180 articles in these areas.

KARL ANDERSSON (Senior Member, IEEE) received the M.Sc. degree in computer science and technology from the Royal Institute of Technology, Stockholm, Sweden, and the Ph.D. degree in mobile systems from the Luleå University of Technology, Sweden. After pursuing postdoctoral research at the Internet Real-time Laboratory, Columbia University, New York, USA, and the National Institute of Information and Communications Technology, Tokyo, Japan. He is currently an Associate Professor of pervasive and mobile computing with the Luleå University of Technology. His research interests include green and mobile computing, the Internet of Things, cloud technologies, and information security. He is a member of ACM.



FRANCESCO PALMIERI received two Italian Laurea M.S. degrees and the Ph.D. degree in computer science from the University of Salerno, Italy. He is currently a Full Professor with the University of Salerno. Previously, he has been an Associate Professor with the University of Salerno, an Assistant Professor with the Second University of Naples, and the Director of the Telecommunication and Networking Division, Federico II University, Naples, Italy. At the start of his career, he also worked for several international companies on networking-related projects. He has been closely involved with the development of the Internet in Italy as a Senior Member of the Technical-Scientific Advisory Committee and of the CSIRT of the Italian NREN GARR. He has published a large number (more than 200) of papers in leading technical journals, books, and conferences. His major research interests include high performance networking protocols and architectures, routing algorithms, and network security. The actual focus of his scientific exploration and dissemination activity concern the use of soft computing, optimization, and artificial intelligence technologies for solving challenging problems in the above areas. He also serves as the Editor-in-Chief of an international journal (*Journal of High Speed Networks*) and is part of the Editorial Board or an Associate Editor of several other well reputed ones (i.e., the IEEE Transactions on Dependable and Secure Computing, the *Journal of Networks and Computer Applications*, *Information Sciences*, *Future generation Computer Systems*, *Applied Soft Computing*, *Soft Computing*, and the *International Journal of Intelligent Systems*). He also guest edited many special issues in leading technical journals (i.e., the IEEE Transactions on Industrial Informatics, the *Journal of Networks and Computer Applications*, *Information Sciences*, and many others). In his career, he has been involved, by also assuming strategic roles, in several national and international research and network development projects. Finally, he participated to several technology transfer initiatives also involving leading companies operating in the networking and security sectors.

MUBASHIR HUSAIN REHMANI (Senior Member, IEEE) received the B.Eng. degree in computer systems engineering from the Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently working as an Assistant Lecturer with the Department of Computer Science, Cork Institute of Technology, Ireland. Prior to this, he worked as a Postdoctoral Researcher with the Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology (WIT), Waterford, Ireland. He also served for five years as an Assistant Professor at the COMSATS Institute of Information Technology, Wah Cantt., Pakistan. He has authored/edited two books published by IGI Global, USA, one book published by CRC Press, USA, and one book with Wiley, U.K. He received Best Researcher of the Year 2015 of COMSATS Wah Award in 2015. He also received the certificate of appreciation, Exemplary Editor of the IEEE Communications Surveys and Tutorials for the year 2015 from the IEEE Communications Society. He received Best Paper Award from IEEE ComSoc Technical Committee on Communications Systems Integration and Modeling (CSIM), in IEEE ICC 2017. He consecutively received research productivity award in 2016–2017 and also ranked # 1 in all Engineering disciplines from the Pakistan Council for Science and Technology (PCST), Government of Pakistan. He received Best Paper Award in 2017 from Higher Education Commission (HEC), Government of Pakistan. He was a recipient of Best Paper Award in 2018 from the *Journal of Network and Computer Applications* (Elsevier). He is also an Area Editor of the IEEE Communications Surveys and Tutorials. He has served for three years (from 2015 to 2017) as an Associate Editor for the IEEE Communications Surveys and Tutorials. He is also serving as Column Editor for Book Reviews in *IEEE Communications Magazine*. He also serves as an Associate Editor for *IEEE Communications Magazine*, the *Journal of Network and Computer Applications (JNCA)* Elsevier, and the *Journal of Communications and Networks (JCN)*. He is also serving as a Guest Editor for *Ad Hoc Networks* (Elsevier), *Future Generation Computer Systems* (Elsevier), the IEEE Transactions on Industrial Informatics, and *Pervasive and Mobile Computing* (Elsevier).

JAEDEOK LIM received the M.S. degree in electronic engineering from Kyungbook National University, South Korea, in 2001, and the Ph.D. degree in computer engineering from Chungnam National University, South Korea, in 2013. He is currently a Principal Researcher with the Information Security Research Division, Electronics and Telecommunications Research Institute (ETRI). His research interests include the IoT security, mobile security, access control, secure operating systems, and system security.