Network Privacy Reflection using Internet of Things

K. Thamizhmaran
Department of Electronics and Communication Engineering, Government College of Engineering, Bodinayakkanur, Theni, Tamilnadu, India
Corresponding Author
E-Mail Id: tamil10_happy@rediff.com

ABSTRACT

The current IP and other networks such as Power Smart Grids are fast developing, thus ensuing in diverse connectivity methodologies. This has led to the emergence of "the Internet of Things" (IoT) methodology whose goal is to transform the current IP and related networks to Device-to-Device (D-2-D) basis. It will seamlessly interconnect the globe via intelligent devices and sensors of varying types, this resulting in voluminous generation and exchange of data in excess of 20 billion Internet-connected objects and sensors (things) by 2022. The resultant structure will benefit mankind by helping us make tough decisions as well as be provisioned of beneficial services. In this paper, we overview both IoT enabled network architecture as well as security for associated objects and devices. We commence with a description of a generalized IoT enabled network's security architecture as well as how the various elements constituting them interact. We then describe an approach that allows the protection of both constrained and unconstrained IoT devices through robust encryption as well as authentication so that both can equally leverage from the same security framework, but still maintaining low computational loads, by avoiding excessive computational operations.

***Key words**: Internet Protocol, Encryption, Federated Clouds, Information Security, IoT, Smart Grid, Smart Objects.*

INTRODUCTION

An IoT networking idea can be largely well-defined as facilitating networking along with communication among several kinds of physical objects across the IP network. Humanity areas that stand to benefit include healthcare, agriculture, environmental monitoring, disaster areas, supply chain management, transport systems, smart homes and cities. For example, as at 2018, in excess of 2 billion people were connected to the IP network and thus can access various kinds of resources, e.g., content browsing, online gaming, exchange emails, as well as social networking. On the implementation side, the IoT capability is enabled by extending and blending ICT technologies and capabilities into common daily things and facilitating connectivity in extended Internet technologies. This has created a global cyber-physical system interconnecting all objects and enabling them to be controlled remotely. The diverse heterogeneity in both the communication requirements as well as the hardware capabilities among the various types of devices will severely constrain transmission resource capabilities. At hardware level perspective, various objects have differing resource requirements, e.g. memory, power, computation, or communication capabilities. The various objects will also generally have varying Quality of Service (QoS) requirements in terms of resilience, reliability, data losses and latency or energy consumption constraints. As an example, it is not so critical that devices with power supply connection minimize the energy for computation/communication purposes, whereas that is a significant impacting constraint for battery-powered devices that do not have efficient energy replenishing or harvesting techniques. These two contrasting characteristics intricate a universal network designs that can satisfy both the general diversity of functionalities of things as well as capabilities. It is for this reason that adaptive cross-layer communication schemes are being followed in its place. Whereas there exist quite many cross-layer protocols for various wireless networks such as sensor(WSNs), mesh (WMNs), and Ad-Hoc (AHNs),[3] these however cannot be directly integrated or applied to the envisaged IoT enabled networks for various reasons such as, Typical IoT enabled networks comprise both centralized as well as hierarchical architectures which they inherit from IP networks, whereas on the other hand AHNs, WSNs and WMN networks have rather flat network architectures, in which devices link and communicate in a hopping manner without the involvement of core Internet. In WSNs, nodes normally will have a shared goal, thus similar hardware specifications and common communication protocols whereas IoT enabled networks' devices and things are highly heterogeneous in terms of QoS requirements, hardware capabilities, functionalities as well as individual goals. Addressing privacy as well as security challenges in IoT enabled networks is also of paramount importance. However, it is a challenge to do so as the vast numbers as well as diversity of “emerging things", heterogeneity, and dynamic changes in IoT environments complicate that task. Traditional security controls ordinarily must be kept to a domain *i.e.*, observing a predefined foundation unit and safeguarding a specific help, for example, access control. Notwithstanding, the IoT networks accommodate oblige bunches of asset compelled things for example body sensors and in this manner from a plan perspective, it may not be viable to straightforwardly actualize current security and access control measures.[7,8] These controls are also generally platform-specific and would not be cost effective or generally feasible to implement them in a multi-vendor/multi-domain heterogeneous space such as the IoT networks. Overall effective security and privacy in IoT enabled networks should generally satisfy basic criteria such as confidentiality, authorization, authentication, availability as well as integrity with regards to security concerns, the current focus is on developing D2D networking protocols rather than applying the existing M2M/IP communication security ones as this complexes characteristics and deployment environments. ITU’s ITU-T Y.2060.[6] Recommendation does provide an overview of the IoT’s concept and scope, identifies its key fundamental characteristics and high-level requirements, as well as describes the IoT reference model. It defines an IoT network as a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information furthermore, communication technologies, a completely fledged IoT is imagined to be a "dynamic just as general organization empowering interoperable systems administration protocol where both virtual and physical articles can impart Currently no normalized design for IoT empowered fills in just as the quantity of layer functionalities. However, most of the proposed models commonly define the following layers.[2,5]

Physical (Perception) Layer

This layer comprises sensor devices and objects for acquiring information about the vicinity environment.

Network Layer

This layer facilitates interconnecting other smart things, network devices, and servers within the IoT.

Transport Layer

This layer ensures process to delivery of data.

Application Layer
This layer defines the various services and as well delivers application specific services to end users or systems.

Processing Layer
It is responsible for processing data after the transport layer.

Enterprise /Business Layer
This layer generally regulates the entire IoT operations; this includes business and profit models as well as security.

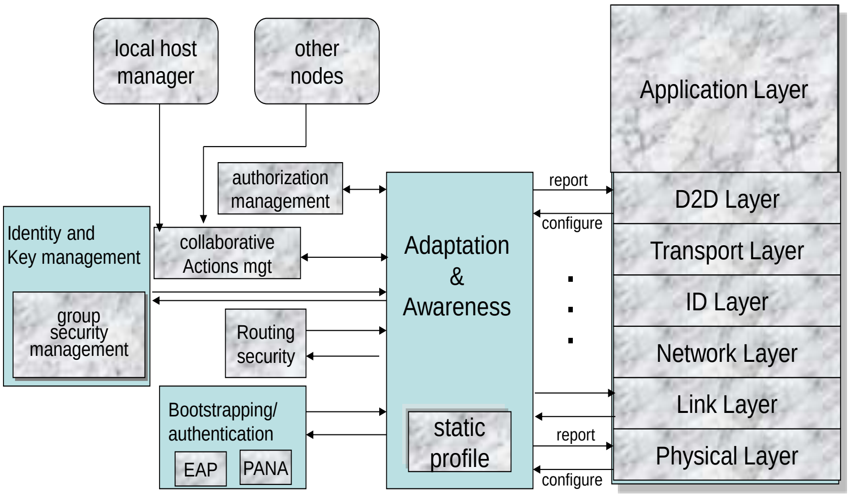

***Fig. 1:** IoT Generalized Secured Communications Architecture.*

Transport Layer's function are dependent on required QoS, but generally provides end-to-end delivery as well as performance guarantees between communicating endpoints. **Identification (ID)** layer's main function is to carry out resources identification. Decoupling this functionality from the network layer (traditional IP network) assists in enhancing security by making it possible to implement authentication service based on the node ID. A protocol such as the Host Identity Protocol (HIP) can be applied at this layer. **Network (NET)** layer has the IPng layer as its chief routing protocol that takes care of node to node addressing as well as packet routing. **MAC** layer governs usage of channel resources.[9] In so doing it minimizes contentions, that otherwise might ultimately degrade performance at this access layer. **Physical Layer (PHY)** addresses the physical specifications of the data associated signals, e.g. it deals with channel coding, modulation/ demodulation as well as transmission over a specified medium. Security is addressed by the security blocks such as: **Bootstrapping and Authentication** controls the addition of new nodes to the network. The Authentication service is utilized by each node, when joining a new network, typically after mobility. It relies on access protocols such the Extensible Authentication Protocol (EAP) and the Protocol for carrying Authentication for Network Access (PANA).[10,11] The latter is also utilized to ensure improved interoperability. **Static Profile** shares its own specifications with each endpoint, e.g, its power source size, storage capacity, processing power, desired security profile/preference. Typically, they mutually decide on a cryptographic suite during the negotiation phase. **Collaborative Actions Management** renders assistance to **a** resource constrained IoT node that suddenly cannot cope up with certain tasks, e.g. computations, hence seeking assistance from a *trusted entity* within the neighbourhood's *constrained* network topology to recommend possible assisting peers. **Identity and Key Management** block guarantees object or device privacy by picking a unique ID for data exchange sessions along with confirming and provisioning entire privacy during the communications session through the use of robust encryption. **Adaptation and Awareness** block gathers information about an IoT node, as well as configuring the necessary protocol(s). **Group Security Management** provisions and enforces multicast-related privacy at the Network layer. **Routing Security block** guards against possible classical routing attacks. It does that in conjunction with the Local Trust Manager and as well as with the Bootstrapping and Authentication modules. **Authorization Management** regulates access to resources and other related services. It will liaise with relevant Authorization infrastructure to retrieve trust certificates for accessing any resources as well as verifications on whether access can be granted without certificates.

CLOUDS OF THINGS

This is a platform for rapidly provisioning a set of pooled configurable computing resources by means of an enabling, on-demand network access in IoT enabled networks. Typical cloud computing characteristics are

On-Demand Self-Service

The ability to render user’s instantaneous access, to computing resources requirements (e.g. CPU time, storage space, network access etc.) without demanding any human interaction with the provider of those resources.

Network Access

Such requested resources are deliverable through the IoT enabled network and accessible to several clients as well as client applications with diverse platforms requiring standard protocols and mechanisms to access them.

Resource Pooling

The available resources are pooled together to serve many customers concurrently utilizing various dynamical assigned physical and virtual resources so as to satisfy customers' QoS expectations. This “multitenancy” model depends on the use of virtualization and in that way; IT resources can be dynamically allocated and reassigned, according to demands.

Rapid Elasticity

The service provisioned by cloud provider elastically deployed, assigned, released or scaled as per demand.

Measured Service

The ability of the cloud service to monitor and measure actual individual usage and charge fairly. In terms of infrastructural deployment within the IoT context, four models exist, and these are:

Private Clouds

This infrastructure is provisioned to an individual organization so that it restricts access and usage of the services it avails employees.

Community Cloud

This is an infrastructure to a community who share a mutual goal.

Public Cloud

Such an infrastructure's services are provisioned for open use on a pay-per-use model

Hybrid Cloud

In this case the infrastructure blends two or more distinct infrastructure deployment models.

Inter-Clouds (Cloud Federations)

This is a relatively newer cloud provisioning model that offers more flexibility, as well as improved reliability and a geographic distribution. Depending on cloud services that are rendering able by cloud providers, three service models are specified. These differ on control granted to request resources by a user as well as, the general functionalities and the architectural layer offered.

Software-as-a-Service (SaaS)

In this case, the users rent out their applications via service provider.

Platform-as-a-Service (PaaS)

This is mainly a development platform that is provisioned to customers to advance their accurate applications or services.

Infrastructure-as-a-Service (IaaS)

The users are allowed direct usage of the IoT infrastructure. This include processing, storage and network resources. In practice, this is implementable through virtualization techniques. The convergence between Cloud Computing and IoT has led to the "Cloud of Things" or Cloud IoT.

In the advent of IoT, storing data locally and temporarily will not be feasible anymore as more storage space would be required. In any case, most of the data would require processing externally (in the Clouds) where there are better, efficient and more capable computing resources. Primarily, IoT services are provided as isolated vertical solution in which a given application and related components are tightly coupled to the specific context of application. Coagulating and rendering IoT services via the Cloud will ease the delivery and the deployment of them by leveraging all the flexibility of Cloud models.

In this regard, the Cloud computing facilitates applications development and makes possible an abstract vision of the IoT systems. IoT can also provide a platform for the Smart Cities services that are envisaged in the next 5-10 years.

RELATED ALLIANCES, ORGANISATIONS AND STANDRADS

Key IoT Related Organisations

Key Organizations allied to IoT development and deployment activities comprise:

- The European Telecommunications Standards Institute (ETSI) concentrating on connecting "Things" as well as clustering them.
- The Internet Engineering Task Force (IETF): This is the current Internet's leading standards setting body that has since set up an additional IoT Directorate Group that is spearheading and coordinating related efforts in reviewing specifications for consistency, and monitoring IoT-related matters.
- The Institute of Electrical and Electronics Engineers (IEEE) focuses on IoT related innovations as well as specifications.
- Object Management Group (OMG) emphases on Data Distribution Service Portal;
- The Organization for the Advancement of Structured Information Standards (OASIS) whose MQTT Technical Committee spearhead IoT related issues;
- Open Geospatial Consortium (OGC) focusing on Sensor Web for IoT Standards Working Group;
- The European Lighthouse Integrated Project addressing the IoT Architecture (IoT-A) which emphases on the formulation of a standardized protocol/architectural reference model for the IoT.
- One_M2M, which suggests a single or one M2M and hence are also concentrating on developing technical specifications for a universally standardized M-2-M Service Layer whose compatibility with numerous hardware and software allows consistent interconnection of all devices with M2M application servers worldwide.

- Open Standards IoT (OSIoT,) whose focus is on developing and promoting free open source standards.
- Eclipse Paho Project: This is an organization that focuses on the overall integration of D-2-D/M2M applications.
- OpenWSN: This is a platform as well as repository for open-source applications of protocol stacks based on IoT standards.
- CASAGRAS: An initiative by Europe, the USA, China, Japan and Korea that addresses universal standards, concerning RFID and its overall role in realizing an IoT.

Alliances

The All Seen Alliance: which is focusing towards enabling and spearheading universal adoption of IoT related devices, systems and products through an open, universal development framework?

The AllSeen Alliance is currently converging with the Open Connectivity Foundation (OCF) and the consolidated consortium will hold the OCF name. In general the blended Alliance will zero in on a code base of assorted and different particular applications and administrations that encourage basic exercises, for example, pairing and disclosure of adjoining articles and gadgets, message routing, and security. The cross-platform nature of the open source codebase facilitates interoperability among diverse as well as basic objects and systems.

IP for Smart Objects Alliance (IPSO) – The IPSO Alliance is an open, forum comprising several organizations and individuals that promote the value of using the Internet Protocol for the networking of Smart Objects.

Its R&D hard work is geared towards attaining IoT interoperability by facilitating data metadata exchanges effortlessly, *i.e.* this is a method that eliminates the requirement for translators. The new approach universally defines all objects and devices, so that each no longer requires predefining or preregistering. Overall, it emphasizes as well as advocates for IP networked devices in healthcare, energy, consumer and industrial applications.

Wi-SUN Alliance: It promotes the use of IEEE’s 802.15.4g based interoperability protocol standard to advance seamless connectivity. Primarily, the Wi-SUN Alliance promotes open industry standards for: 1. Wireless Smart Ubiquitous Networks and related applications. 2. Advancement, standardization as well as interoperability of wireless Smart Ubiquitous Networks globally. 3. Other activities include user education, industry outreach and other support programs as well as lobbying regional regulatory bodies for spectrum allocation for smart grid services.

Protocols Broadly, IoT applicant conventions can be classified as: Infrastructural, Identification, Communications and Transport) Service Discovery, Data Protocols, Device Management and Semantic (security).

Infrastructure Protocols

IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN). It is an adaptation layer protocol for IPv6 over IEEE802.15.4 links.

Nano Internet Protocol (NanoIP): This is a concept that seeks to bring IP-like networking services to embed with sensor devices, by secluding the TCP/IP overheads.

Discovery Protocols

- Multicast Domain Name System (mDNS)- Can resolve and map device names to global IP addresses.
- Universal Plug and Play (UPnP) - This class of protocols allows self-

discovery and interaction abilities by networked sensors and devices.

Data Protocols

- MQTT for Sensor Networks (MQTT-SN): An open protocol designed specifically for mobile and M2M/D-2-Dapplications.
- Constrained Application Protocol (CoAP): An
- Application layer protocol for WSN nodes.

Communication / Transport layer

- IEEE 802.15.4: This is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs).
- ANT: A wireless sensor network technology- designed for collection and transfer of sensor data and the integration of remote control systems such as controlling indoor lighting or a television set.
- LoRaWAN: Network protocol intended for wireless battery-operated devices.

Semantic

- SensorML: It is an approved Open Geospatial Consortium standard. That mainly provides standard models and an XML encoding for relating sensors and measurement processes.
- Media Kinds for Sensor Markup Language (SENML): A simple sensor, such as a temperature sensor, could use this media type in protocols such as HTTP or CoAP to transport the measurements of the sensor or to be configured.

Security

- Open Trust Protocol (OTrP) - This protocol essentially is designed to enhance and manage security configurations in Trusted Execution Environments (TEEs). It goals at making an open universal protocol defining how things and devices belief each other in a networked environment. It usages the Public Key Infrastructure architecture (PKI) and certificate authorities, as its simple underlying system.
- X.509 - Standard for managing digital certificates and public-key encryption.

ACCESS CONTROL IN MULTI-DOMAIN FEDERATED CLOUDS

In this section, we describe a possible access control in Federated IoT Clouds. A federated cloud system is illustrated. Generally it suffices to have a specific user authenticated in a single domain. It is recalled that IoT enabled networks in general will be characterized by relatively dynamic nodes connectivity as well as network topologies. Because wireless channels are dynamic in nature, there is a need to accordingly incorporate a suitable flexible as well as dynamic access control system that is suitable for the federated Cloud IoT environment.[1,4]

Access Control Architecture

We propose access control architecture as illustrated in Figure 7 and was partly modified from a proposal in. Every domain has an Agent Unit (AU) to which all devices and components are connected. The domain is also connected to the IP backbone network. Features characterizing the architecture include authentication for each user's access request (s) as well as a QoS secure path selection.

The authentication network is decentralized and hence each domain handles authentication requests from all its devices and components. High bandwidth end-to-end verification channels are sensibly separated from encrypted and QoS ensured data channels. Within this block, the Access Control manager (ACM) together with a set of authentication/SSL protocols will negotiate for the desired access to a requested resource under the coordination of the contexts security unit (CSU). After the access is granted, an authentication notification in the form of a ticket is issued to the user. In a way, the CSU is a central point for security decisions. The control packet will also be utilized by the Path Level Security Control block in setting up an encrypted path between the ingress and egress nodes. In so doing it uses the routing topology/link state database. The path selection is based on random routing shortest path first. The explicit route information i.e. the set of nodes to be traversed along with requisite resources is now combined in the signal from the ingress node to the egress node over a safe and dedicated control/signalling channel and eventually in the process keeping the demanded secure path between the Agents. A summary message exchanges in authentication, channel reservation and data exchange processes is illustrated in figure 8.

RESULT

Figure 2 shows the average processing time at a single AU as a function of CPU utilization. Setting $C_a^2 = 2$ brings about increases in processing time thus indicating that variations in traffic arrival rates significantly affects the processing times.

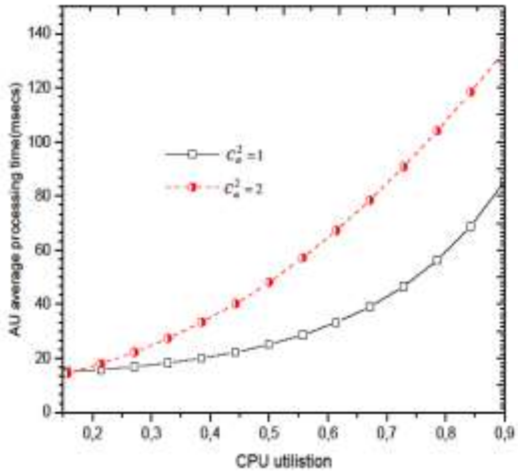

Fig. 2: *AU Processing time as a Function of CPU's Utilization.*

Shown in Figure 3 is the fractional processing time(s) as a function of the number of AUs in the distributed architecture. For both $C_a^2 = 1$and $C_a^2 = 2$ the processing times exponentially decays with increasing numbers of AUs.

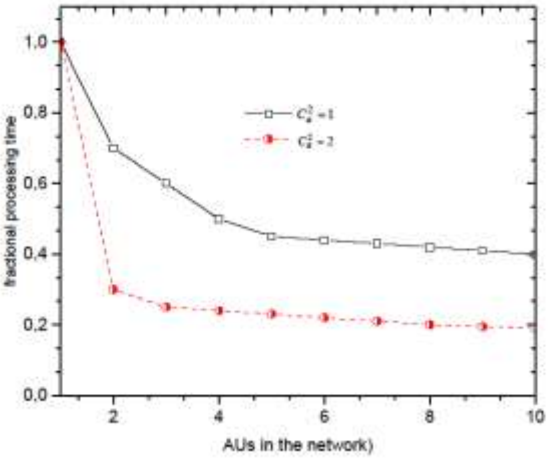

Fig. 3: *Number of AUs Versus Processing Times*

This infers a distributed architecture will significantly bring about a reduction in processing times. We further extend our performance analysis of the proposed authentication framework model by comparing three request negotiation algorithms (protocols) all of which relate to the manner in which end-to-end resources are negotiated by the ingress AU. These are: Algorithm I: The Sequential Resources Request negotiation Protocol(S-RRNP) in which the ingress AU negotiates the required end-to-end resources in a sequential manner. Algorithm II: Parallel Resources Request negotiation Protocol (P-RRNP), in which case the ingress AU identifies a candidate path before sending a resources request message to all associated transit AUs simultaneously. Algorithm III: Centralised Requests negotiation Protocol (C-RRNP): The resources negotiations within the entire federation are carried out in a centralised manner. As such the ingress AU at all times needs the essential resources and security via a designated central AU. In our simulation, we compare the performance of the various requests negotiation protocols. In order to carry out the simulation we make further assumptions as follows: that the AU receives a Resources Request from users and maintains a state in memory for each of such Requests (e.g. representing the processing state of this resources request).

- Two queues are required: one presents the AU's Resources request processing time, while the other presents the waiting time for the response.
- That the waiting time for the response from a remote AU equals it's processing time of the Resources |Request message as well as generation of the Response.

Each ingress AU searches for a suitable end-to-end channel by querying with all associated transit AUs on the desired path. When it fails to find a-channel, it may either discard, or loop it back. The looped back Requests are queued another time with novel arrivals therefore may cause bottlenecks. We describe three possibilities as follows:

- q - the probability that no channel was originate on the first attempt hereafter, the request is looped back (looping probability).
- p - is the probability of discarding the Request on as resources do not exist. In this case a *FAIL* message is relayed back to the user.
- m -is the probability of finding a suitable channel on the first attempt.

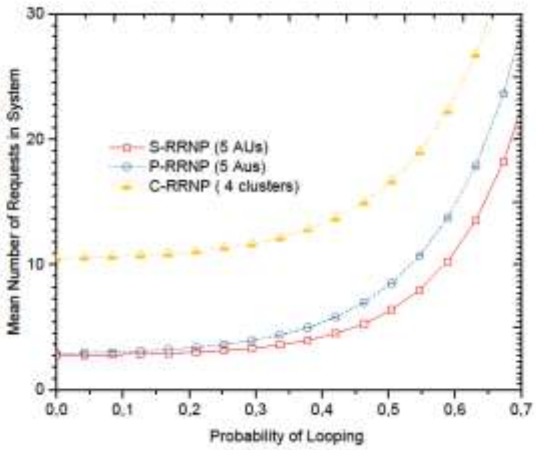

***Fig. 4:** Average Number of Requests at the Ingress AU's Scheduler.*

The average number of requests in the AU's scheduler (number in system) is explored for the three different protocols when the arrival rate is fixed to 30 requests per second. From Figure 4, we deduce that q greatly influences the number of requests in the system. Above a certain threshold value of q, the system can become unstable. It is thus essential to limit the looping probability so as to guarantee acceptable QoS specially with regards to processing delays.

CONCLUSIONS

In this paper we reviewed security and access and control in IoTs. We proposed distributed access control architecture as well as described its main blocks as well as functionalities. We also evaluated the performance of the proposed system framework in terms of processing times. Overall it is deduced that a distributed architecture will significantly bring about a reduction in processing times. Overall, whereas the architectural and related issues discussed earlier point to a realistic as well as feasible practical realization of the IoT, a significant research effort is still required in order to address various issues including technology, standardization, security and privacy. A full understanding and appreciation of industry and technology requirements and characteristics as a function of factors such as security, privacy, risk and cost is required before general acceptance of deployment of IoT in all aspects of humanity. Design of scalable, as well as cost effective Service Oriented Architecture (SoA) for IoT is quite challenging as IoT is a heterogeneous network platform. Its heterogeneity nature will aid to more complexity in terms of meeting a universal communication platform, thus standardization will not be achievable in the near future. Novel SDL may be developed to cope with product dissemination after validating the requisite SDL specific architecture. Sufficient bandwidth provisioning to cope up with the various interconnected IoT objects is necessary. Current database management systems may not be able to satisfy the real-time handling requirements. The current RAID technology needs revisiting in this regard. Mismatches in data type, size and formation generated by the diverse devices requires that researchers come up with big IoT data specific design tools to handle the data efficiently. Relevant architectural framework is required for handling data mining, analytics, and hence decision-making services. Big Data approach could be aggregated herewith. Defining both privacy and security from a legal, social as well as cultural point of view is of paramount importance. Core security and privacy approaches also require further enhancements. Whereas existing network security protocols and related technologies provide a basis for privacy and security in the IoT, further improvements are still necessary.

REFERENCES

1. Fremantle, P., Aziz, B., Kopecký, J., & Scott, P. (2014, September). Federated identity and access management for the internet of things. *In 2014 International Workshop on Secure Internet of Things* (pp. 10-17). IEEE.
2. Maria, P., Nicola, A., Xavier, V., Thomas, W., & Grieco, L. (2013). Standardized Protocol Stack for the Internet of (Important) Things. *IEEE Communication Surveys and Tutorials*, 15(3).
3. Souza, A. D., & Amazonas, J. D. (2015). A new internet of things architecture with cross-layer communication. In *Proceedings of the 7th International Conference on Emerging Networks and Systems Intelligence Emerging* (pp. 1-6).
4. Markmann, T., Schmidt, T. C., & Wählisch, M. (2015). Federated end-to-end authentication for the constrained internet of things using ibc and ecc. *ACM SIGCOMM Computer Communication Review*, 45(4), 603-604.
5. Bonetto, R., Bui, N., Lakkundi, V., Olivereau, A., Serbanati, A., & Rossi, M. (2012, June). Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)* (pp. 1-7). IEEE.
6. ITU. ITU-T Y.2060. Intro to Internet of Things. https://www.itu.int/rec/T-REC-Y.2060-201206-I/en, June, 2012.
7. IEEE 802 Working Group. (2011). IEEE standard for local and metropolitan area networks—Part 15.4: Low-rate wireless personal area networks (lr-wpans). *IEEE Std*, 802, 4-2011.
8. Piro, G., Boggia, G., & Grieco, L. A. (2013). A standard compliant security framework for Low-power and Lossy Networks draft-piro-6tischsecurity-issues-01 (work in progress). *IETF 6TiSCH WG*, 20, 13.
9. Sajjad, S. M., & Yousaf, M. (2014, June). Security analysis of IEEE 802.15. 4 MAC in the context of Internet of Things (IoT). In *2014 Conference on Information Assurance and Cyber Security (CIACS)* (pp. 9-14). IEEE.
10. Vollbrecht, J. R., Aboba, B., Blunk, L. J., Levkowetz, H., & Carlson, J. RFC 3748-Extensible Authentication Protocol (EAP).
11. Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., & Yegin, A. (2008). *Protocol for carrying authentication for network access (PANA)* (pp. 2070-1721). RFC 5191, May.