Musab KAMAL, Imran RASHID, Waseem IQBAL, Muhammad Haroon SIDDIQUI, Sohaib KHAN, Ijaz AHMAD, 2023. Privacy and security federated reference architecture for Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 24(4):481-508. https://doi.org/10.1631/FITEE.2200368

Privacy and security federated reference architecture for Internet of Things

Keywords: Architecturally significant requirement (ASR); Architecture trade-off analysis method (ATAM); Internet architecture board; Internet of Things (IoT); Privacy enhancing technologies; Privacy validation chain

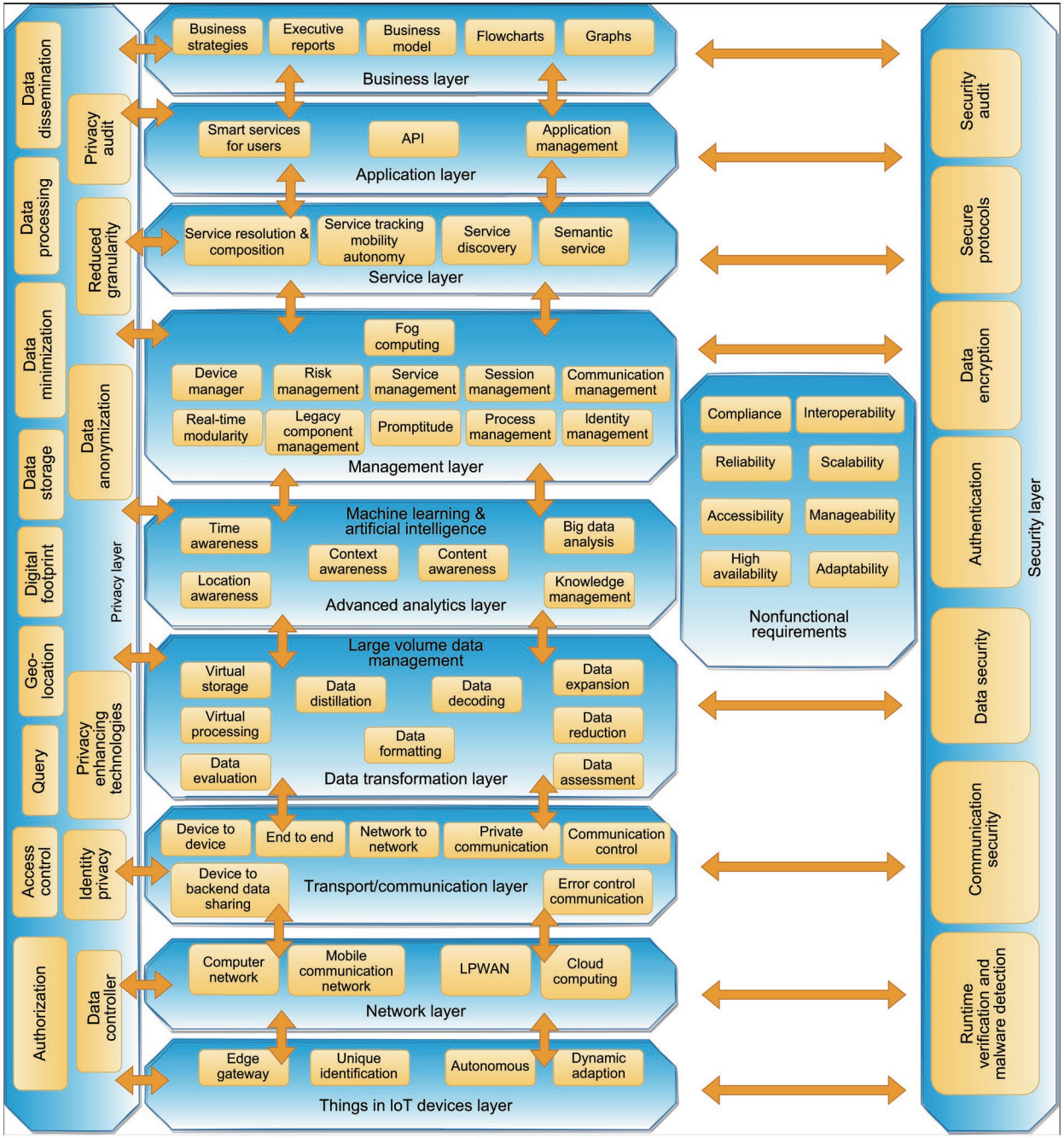
Corresponding author: Waseem IQBAL
E-mail: waseem.iqbal@mcs.edu.pk
ORCID: https://orcid.org/0000-0002-3616-2621

Motivation

- There are vulnerabilities in the Internet of Things (IoT) ecosystem considering security and privacy issues. There are systematic privacy flaws in the form of missing encryption certificate validations:
  - Where to store the data collected from sensors, actuators, and lightweight IoT devices, and for what purpose? Are they profiled or not?
  - User data and confidential information are not safe in the heterogenous IoT network.
  - Use of multitude languages, protocols, and standards.
- There is no standard architecture for the IoT.

Main idea

- Identifying the core requirements from the standards for the IoT
- Analysis of existing reference architectures and identifying the shortcomings
- Incorporating privacy and security metrics in the analysis and the proposed reference architecture
- Proposing a novel privacy-federated IoT security reference architecture (PF-IoT-SRA) and its countermeasures against IoT threats and attacks in the IoT ecosystem
- Validation of the proposed PF-IoT-SRA



Framework

Fig. 3 Proposed reference architecture (API, application programming interface; LPWAN, low-power wide area network)

Method

- Analyze 12 existing architectures of IoT comprehensively.
- As IoT-based systems are vulnerable to various types of threats and attacks, identify which metric of PF-IoT-SRA will counter threats and attacks in the IoT communication environment.
- Validate PF-IoT-SRA using the architecture trade-off analysis method (ATAM), an industry recognized scenario based approach.
- ATAM gives us the trade-offs, sensitivity points, and risks associated with the proposed IoT reference architecture. It gives us a clear sight of how the reference architecture should be performed under brainstormed real-time scenarios.

Method

Table 5 Brainstormed scenarios and their priorities

Scenario	Description	Priority
1	A smart home where all the appliances are connected to the Internet. A user requests to unlock the door through a mobile application rather than just normal keys (functionality: a smart door lock; accuracy should be >96%)	(H, M)
2	A connected self-driven car can optimize its operation and maintenance driving on the road without a driver (reliability: IoT system should have a fault tolerance of no less than 94%)	(H, M)
3	Industrial IoT, also known as Industry 4.0, the revolution of industry; production units highly rely on sensors, actuators, and controllers; temperature, voltage, frequency, seismic sensors not giving correct readings to PLCs; giving false negatives (usability: all the sensors and actuators should be checked during boot time within 50 ms)	(M, M)
4	In smart health care, patients use a connected battery-powered pacemaker to control abnormal heart rhythms (security: hardware disk failure or power outage; the services should resume <5 s)	(H, H)
5	In smart retail, a large number of users request for transaction checkout at the same time using mobile POS (performance: in heavy load conditions and with parallel users, a simple entity should be updated in <3 s)	(M, L)
6	IoT medical devices collect health care data, including blood pressure, sugar level, oxygen, and weight; the data of users are stored online (privacy: no profiling of user data based on identity and geolocation)	(M, H)
7	The developer should be able to create new applications in an IoT ecosystem (portability: the developer should be able to create applications in 2–3 months)	(M, L)
8	The patches should be installed on the software and operating systems of things (installing ability: the upgrades should be remotely installed to the things)	(H, M)

H, high; L, low; M, medium; PLC, programmable logic controller; POS, point of sale

Major results

Proposed architecture decision and response to the stimulus

Table 8 Scenario 3

Item	Description
Attribute	Usability
Environment	Starting up the system
Stimulus	Failure of boot time check of sensors and actuators within 50 ms
Response	Will not affect the overall system operations
Architecture decision	(Layer 1) Devices layer: things in IoT
Sensitivity	The devices such as sensors, actuators, and wearables should be able to check, protect, and configure themselves within the specified boot time
Trade-off	Portability, reliability, and functionality
Risk	Could result in false negatives; can halt the production units, resulting in financial loss

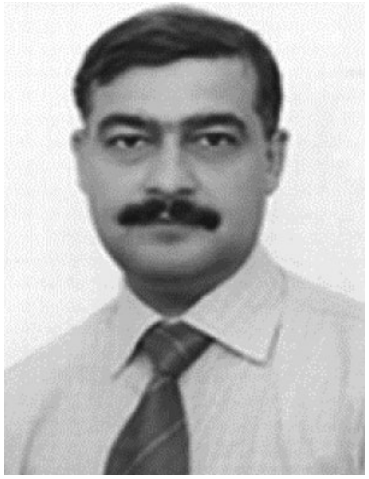
Table 9 Scenario 4

Item	Description
Attribute	Security, availability
Environment	Recovering from a failure
Stimulus	The hardware or battery of the pacemaker fails during the operation
Response	The recovery mechanism supported will not affect the security and availability of the system
Architecture decision	(Layer 6) Management layer: risk management
Sensitivity	There should be no common mode of failure; to ensure different types of hardware and operating systems
Trade-off	Installing ability, reliability
Risk	This could result in fatal hazards; the management layer might be helpful in risk minimization; might not address hardware redundancy

Summary

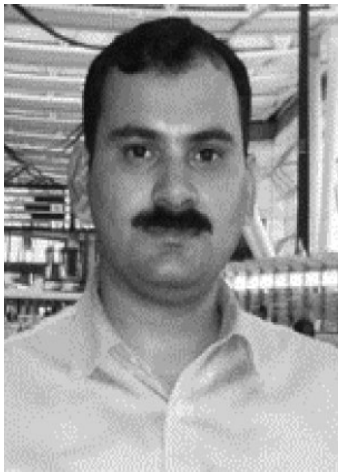
- We have identified the core requirements from the standards. Based on these requirements and metrics, we have analyzed 12 existing reference architectures. We have identified their shortcomings and proposed PF-IoT-SRA, which will help make a concrete and standard architecture.
- PF-IoT-SRA will counter major threats and attacks in IoT communication and address all the concerns for the domain system from a functional point of view.

Musab KAMAL received his BS degree in computer engineering from Comsats University, Islamabad, Pakistan in 2012, and his MS degree in systems engineering from the National University of Sciences and Technology, Islamabad, Pakistan in 2021. He has professionally served in various industries in information technology and information security since 2014. His main research interests include computer and network security, IoT security, information security management, cloud computing, and information security for system integration and validation.



Imran RASHID received his BE degree in electrical engineering from the National University of Sciences and Technology, Islamabad, Pakistan in 1999, his MS degree in telecommunication engineering (optical communication) from the Technical University of Denmark (Danish: Danmarks Tekniske Universitet) in 2004, and his PhD degree in mobile communication from the University of Manchester, UK in 2011. He is currently the Chief Instructor of the Engineering Wing with the National University of Sciences and Technology. His research interests include mobile and wireless communication, MIMO systems, MU-MIMO systems, compressed sensing for MIMO OFDM systems, massive MIMO systems, M2M for mobile systems, cooperative communication systems, cognitive radio systems, RFID security protocols, and information security for wireless and mobile systems.

Waseem IQBAL is currently employed as an associate professor at the National University of Sciences and Technology (NUST), Islamabad, Pakistan. Other than this, his professional services include, but not limited to, industry consultation, workshops organizer/resource person (international workshops/seminars), technical program committee member, member accreditation team, conference chief organizer, invited speaker, teaching (UG/PG/PhD) courses, research & development, and guest editor/reviewer for several international journals/conferences. He has been an academician and researcher since 2012 and has published more than 70 scientific research articles related to healthcare security, digital forensics, cryptography, and IoT security in prestigious journals like *IEEE Comm Surv Tutor*, *IEEE Int Things J*, *ACM Comput Surv*, *Fut Gener Comput Syst*, and *Multim Tools Appl*, along with reputed conferences like ICC.



Muhammad Haroon SIDDIQUI received his BE and MS degrees in electrical engineering from the National University of Sciences and Technology, Islamabad, Pakistan in 2002 and 2010, respectively, where he is currently pursuing his PhD degree. He is currently a faculty member of the Department of Electrical Engineering, National University of Sciences and Technology. His research interests include MIMO systems, massive MIMO systems, cooperative communication systems, cognitive spectrum sensing, and wireless channel modeling.

Sohaib KHAN received his BE degree in telecommunication engineering and his MS degree in information security from the National University of Sciences and Technology, Pakistan. He has been teaching various core subjects related to information security since 2017. His active areas of interest include computer security, network security, digital forensics, and cryptography.

Ijaz AHMAD is Director of Quality Assurance and Senior Lecturer in the Faculty of IT. He has been in Majan University College since 2013. He became a senior fellow of the UK Higher Education Academy in September 2018. He has completed his MS degree in information security from NUST (Islamabad, Pakistan) and was awarded the President Gold Medal for holding the first position. He has completed his BE degree in computer science with distinction. Before joining Majan University College, he served as a lecturer in various renowned universities in Pakistan including NUST and FAST-NUCES. He is a Certified Ethical Hacker by EC Council. His areas of interest include cyber security, ethical hacking, digital forensics, cryptography, cloud computing, and computer networks.