Security Implementation and Verification in Smart Buildings

1st Walid Miloud Dahmane
saad dahlab university
Blida, Algeria
walid.miloud.dahmane@gmail.com

2nd Ouchani Samir
LINEACT, École d'Ingénieur CESI
France
souchani@cesi.fr

3rd Hafida Bouarfa
saad dahlab university
Blida, Algeria
hafidabouarfa@hotmail.com

***Abstract*—The homes are dangerous environments like outside since it contains risks affect on the life of the inhabitant (humidity, temperature, noise, light, etc.), especially with the increase of the attention on smart homes and buildings in the previous few years where studies focused on the IoT domain exclude partially these risks. Smart homes/buildings are equipped with IoT objects that capture the conflicting changes in a controlled manner and introduce actions that stop or declare the existing threats. A mechanism that guarantees to the inhabitant a stable and comfortable life is more than mandatory. In this context, we propose a global approach that defines the architecture of a smart home/building by formalizing the main nodes (sensors, actuator, server, etc.) and the technologies that bind them. Further, we define the characteristics and the functioning of nodes by a formal representation in the form of state machines, the applicable norms to build a secure environment, and further the security measures that must respect them in order to guarantee a protected environment. We finished our study by experimentation with Uppaal, a verification and validation tool, to ensure the accuracy of the system operations that showed a satisfactory results.**

***Index Terms*—Smart Home, Smart Building, Home risks, IoT, MQTT Protocol, Formal verification, Simulation, Uppaal.**

I. Introduction

For a better living quality, the smart spaces paradigm aims at constructing advanced service infrastructures that follow the ubiquitous computing approaches where smart objects are executed on a variety of digital devices and services are constructed as interaction of agents in a communication environment [19]. Recent advances in intelligent computer systems and communications have created the necessary conditions for the networking of a wide variety of heterogeneous devices. This led to the integration of short-range mobile transceivers into everyday life objects and has enabled new forms of communication between objects and even between people and objects. The concept of smart devices, i.e. the inclusion of software, identifiers and networking to devices typically not computerized, led to the "Internet of Things" (IoT) [7]. The main feature of this technology is the integration of heterogeneous and action elements (actuators) in a distributed system which performs different actions based on the information gathered by the sensors combined with the requirements of the particular application [25].

The inside environment has several factors that can affect it or the life of inhabitants or both at the same time (temperature, humidity, noise, light, *etc*). Nowadays different numerical models are available to describe the vapor balance of transient water in a room and predict indoor humidity. A typical room moisture balance includes water vapour production by moisture sources (humans, plants,...), convective water vapour transfer with ventilation air, and water vapour exchange with the building fabric and furniture.The water vapour exchange between room air and surrounding materials (walls and furniture) is governed by three physical processes: the transfer of water vapour between the air and the material surface, the moisture transfer within the material and the moisture storage within the material. The existing models mainly differ in the way this last part of the moisture balance is described [17]. In general, sensors communicate directly with the home gateway and feed the system information with regards to the obtained environment measures, for example light intensity inside a particular room, temperature inside and outside the home and motion sensing to name a few [29].

In this paper, we propose a smart living framework by modeling the different components needed for an indoor environment and developing a trustworthy architecture that ensure the well functioning correctness of such system, and also its configuration and control. First, we rely on the existing limitations and the requirements for a home that can affect the inhabitant like humidity which causes corrosion coating of the wall and household furniture, the appearance of molds and bacteria, the temperature also has to be regulated in the home according to the outside climate, loud noise especially at night, the handicapped can not open the doors of the room, natural and artificial phenomena such as the earthquake and fire that threatens the life of the human. The proposed solutions consider all indoor issues, implement sensors for each measure, collect data in real time and make reactions to prevent risks.

The proposed framework is a web service based solution where sensitive nodes are indoor planted and their measures change in real time. The architecture proposed for the framework considers different classes of nodes. A database node containing the collected data by sensors, a server node that ensures the communication and the reliability between nodes, and reacts when necessary by sending the appropriate control commands; the actuator node executes the received commands from the server and/or external actors who can extract or

edit home data. The architecture uses MQTT protocol [28] to ensure a reliable communication between the predefined internal nodes. Further, the architecture implements a precise constraints and requirements for the communication and during executing actions. Otherwise, the nodes do not respecting certain conditions are considered as unacceptable nodes. Finally we ensure the functional correctness of the nodes and their secure communication by simulation and verification in Uppaal tool [3]. The results show that the proposed framework is a deadlock free, secure, and respecting the indoor living requirements.

The remainder of this paper is organized as follows. Section II presents the related work and compares it with the proposed framework detailed in Section III. Then, the implementation with the experimental results are shown in Section IV. Finally, Section V concludes the paper and provides hints on the future works.

II. Related Work

In literature, we review the existing work related to IoT modeling, functional analysis, network architectures, and application in real life with concrete cases.

Ouchani [22] proposes a security analysis framework for IoT that covers the probability and costs of actions, formalizes IoT, analyzes the correctness and measures their security level by relying on the probabilistic model checking PRISM. To ensure the functional correctness of an IoT-based system, Ouchani develops five steps: defines the IoT components, formalizes the architecture in a process algebra expression. Then, it expresses the IoT requirements in PCTL and transforms the IoT model into the PRISM input language. Finally, PRISM checks how much a requirement is ensured on the IoT model. However, the proposed framework involves a large amount of data and messages which make the probabilistic model checking expensive in terms of time and memory.

Moreno-Salinas [13] proposes a method that detects the optimal position of sensors to receive information from several targets. To find the perfect place, they rely on FIM[1] to measure the amount of information that a random variable (sensor) carries about a parameter that is sometimes unknown (target). After several progressive tests, they use two separated tests, the first tries to find the optimal position for a sensor that receives data from a target transmitter with a known placement. This first test considers one sensor and one target, eight sensors and one target, four sensors and two targets, and five sensors and three targets. The second one finds the optimal positions of sensors with unknowns positions experimenting five sensors and two targets, then five sensors and three targets. However, FIM showed significant results for a small amount of objects but the cost of time computing is expensive when the target is unknown in a known area.

Centenaro [11] studies a start topology of LPWANs[2] in smart cities where the used network $LoRa^{TM}$ belongs to the same family of LPWANs. The goal is to know the number of gateways needed to cover the city (inexpensive or not), and to know the benefits in return after deployment. They experimented two tests, the first installs $LoRa^{TM}$ network in a 19-history building to measure temperature and humidity, using one single gateway and 32 nodes. The second estimates the number of gateways required to cover the city of Padova.They placed a gateway with no antenna gain at the top of two history buildings to assess the 'worst case' coverage of the topology since $LoRa^{TM}$ technology allows to cover a cell of about 2 km of radius. With simple calculations they concluded that to cover Padova city that has about 100 square kilometers, it needs 30 gateways. At the present, $LoRa^{TM}$ has an acceptable coverage in worst cases, but the number of gateway ports is limited and does not satisfy progressive evolution of IoT technology.

A. Zanella [32] apply the principles of smart cities for Padova city to collect environmental data. The architecture is composed of constrained IoT sensors, a database server which use technologies CoAP[3], 6LoWPAN[4], unconstrained devices that use traditional technologies like HTML. The interconnection between users and sensors is made by an intermediary gateway and HTTP-CoAP proxy-grown that plays the role of translator between the two sides. During a week of tests, the results show how do people react with different situations and phenomena, for example benzene consumption at the end of weeks. This architecture allows the compatibility between constrained and unconstrained devices through a cross proxy. In general, the constrained physical and link layer technologies are characterized by a low energy consumption, the transfer rate and data processing in constrained devices is relatively low, but the dependence on unconstrained ones increase in cost.

Based on the reviewed literature, we found few works that detail well the components of an indoor environment and their formal semantics, and less of them discussing a trustworthy communication between components. The proposed contribution considers these issues and we believe it is easy to extend and deploy a more secure smart building/home system.

III. Framework

Figure 1 illustrates the steps to how construct a secure smart building/home system and analyze it. The system's architecture is composed from a set of nodes, security constraints and management mechanism, and the communication protocols. The nodes are active/passive objects to collect the needed environment measures. The communication protocols ensure how well the connection between nodes is established and the measured data are packed and encrypted. The security management mechanism reinforces the architecture in order to create a protected system. It develops a set of security rules including the authentication and identification of nodes, the control access, and how to keep the availability of services.

[1]Fisher Information Matrix.
[2]LowPower Wide Area Networks.
[3]Constrained Application Protocol
[4]IPv6 Low power Wireless Personal Area Networks

The analysis step enables the verification of the accuracy of the implemented architecture with respect to the security rules. Finally, the results show the different scenarios, traces, or errors that might affect the security and the well functioning of the architecture in order to decide or not its deployment.

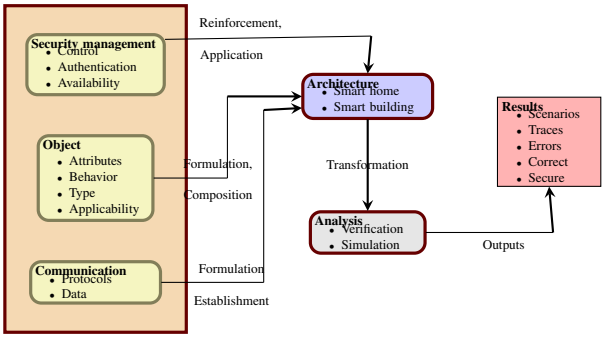

Fig. 1: A Security and Analysis Framework for Smart Homes and Buildings.

A. Smart object

A smart object ($\texttt{SoT} \in$ **SoT**) is identified by a set of dynamic and static attributes (T). The dynamic attributes are classified into two categories: data ($\texttt{d}_i$ of type real) and flags ($\texttt{f}_i$ of type Boolean). In the following, we cite the most used static attributes that describe the physicality and the technicality of an SoT.

- The identifier ($\texttt{id} \in \texttt{ID}$): is the unique reference to SoT, in our case id is IPv6 [10].
- The connectivity ($\texttt{COn} \in \mathsf{T}$) describes when devices have extensions to connect to each other [6].
- The battery life ($\texttt{BLi} \in \mathsf{T}$): represents the longevity of a battery [15].
- Powered by electricity ($\texttt{PEl} \in \mathsf{T}$): when SoT can be plugged with an electricity line.
- Data security ($\texttt{DSe} \in \mathsf{T}$) informs about the ability to encrypt informations stored or sent [8].
- Small size ($\texttt{SSi} \in \mathsf{T}$): describes the volume of SoT.
- High product quality ($\texttt{HPr} \in \mathsf{T}$) indicates the possibility to increase the service life and to reduce the cost of maintenance.
- Constrained device ($\texttt{CDe} \in \mathsf{T}$) describes if a cheaper device can cover a specific space [24].
- Price ($\texttt{PRi} \in \mathsf{T}$) helps in the budget management [4].
- Service availability ($\texttt{SAv} \in \mathsf{T}$) to check if the device works continuously or not [14].
- Minimum error ($\texttt{MEr} \in \mathsf{T}$) increases the quality of service [18].
- Easy to maintain ($\texttt{EMa} \in \mathsf{T}$) is to reduce time, effort and the cost of maintenance.
- Required a low connection rate ($\texttt{RLo} \in \mathsf{T}$): to stay connected in the worst case [12].
- Interoperability of nodes ($\texttt{INo} \in \mathsf{T}$) defines the technologies supported by the node [31].

The behavior of an object is the effect of the executed actions (Σ) that allows it to transfer from its current state S_i (the evaluation of dynamic attributes) to another one S_j. The following lists the set of possible actions.

- turnOn/turnOff to turn on/off the smart object [1].
- send/receive to send/receive data to/from another IoT node [33].
- collectData to collect the received information [33].
- applyAction apply an action after getting command [33].
- encrypt/decrypt to encrypt/decrypt a message.
- authenticate grants the possibility to send data.

We define in Definition 1 a smart node that can be a sensor, actuator, broker, database, server, or smartphone.

Definition 1 (Smart node)**.** *A smart object* $\texttt{SoT} \in$ ***SoT*** *is a tuple* $\langle \texttt{ID}, \texttt{Att}, \Sigma, \mathsf{B} \rangle$ *where:*

1) $\texttt{ID}$ *is a finite set identifiers* $\texttt{id}_\texttt{i} \in \texttt{ID}\{O_i, i \in N$ *where* $\texttt{id}_\varnothing \in \texttt{id}$ *is an empty object.*
2) $\texttt{Att} : \texttt{ID} \rightarrow 2^{\mathsf{T}}$ *is a function that assigns for each object a sequence of attributes.*
3) Σ *is the set of possible actions for an objects,*
4) $\texttt{Beh} : \texttt{ID} \rightarrow \mathsf{B}$ *returns the expression that precises the behavior of an object in the dominant case where :* $\mathsf{B} ::= \texttt{Start.actions}+_\texttt{g}\texttt{actions.End}$ *where* $actions = \alpha | \alpha.actions$ *such as* $\alpha \in \Sigma$ *and* $+_g$ *is a deterministic choice with respect to a guard* g*.*

Example 1 (Smart object)**.** *Based on Definition 1, the semantics of a general sensor is the state machine depicted in Figure 2 where states* s_0, s_1, s_2, s_3 *stand respectively for* Is_On, *detection, declaration,* Is_Off*. The attributes values specifying a state change regarding the executed action. The actions* α_1, α_2, α_3, α_4, *and* α_5 *represent respectively turn_on, detect , send,turn_off, and initialize.The dynamic attributes (*$\texttt{d}$ *and* $\texttt{f}$*) of a sensor are:* $\texttt{d}_1$ *evaluates the energy,* $\texttt{d}_2$ *measures other properties (smoke, noise, temperature,...),* $\texttt{f}_1$*: detection,* $\texttt{f}_2$*: availability,* $\texttt{f}_3$*: alerte_msg. Each state is presented by the following predicates where* Max_Val *is the maximum for the measure related to the smart object.*

1) $[\![s_0]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 < Max\_Val) \wedge (\texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\neg \texttt{f}_3)$
2) $[\![s_1]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 >= Max\_Val) \wedge (\texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\neg \texttt{f}_3)$
3) $[\![s_2]\!] = (\texttt{d}_1 > 0) \wedge (\texttt{d}_2 >= Max\_Val) \wedge (\texttt{f}_1) \wedge (\texttt{f}_2) \wedge (\texttt{f}_3)$
4) $[\![s_3]\!] = (\texttt{d}_1 = 0) \wedge (\texttt{d}_2 = 0) \wedge (\neg \texttt{f}_1) \wedge (\neg \texttt{f}_2) \wedge (\neg \texttt{f}_3)$

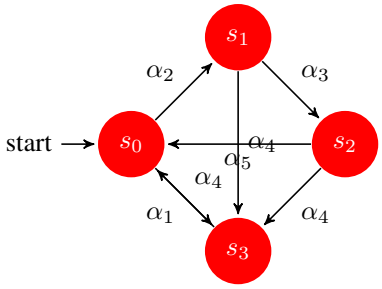

Fig. 2: The state machine of a sensor.

B. Smart environment

We define a smart environment sEnv as a structured physical infrastructure, building or home, that carries smart nodes. sEnv is composed of at least two smart rooms/locations disjointed by separators *like* walls, doors, and windows. To collect information and sensitive data, smart nodes are connected with a precise architecture mechanism that helps them to communicate easily through a dedicated protocols.

Definition 2 (Smart Environment)**.** *A smart environment* sEnv *is a tuple of* $\langle E, L, \boldsymbol{SoT}, \mathtt{pl}, \mathtt{dl} \rangle$*, where:*

1) E *is the environment name/id,*
2) $L = \{R_1, ..., R_i, ..., R_n | i, n \in \mathbb{N}\}$ *is the set of locations/rooms* (R_i) *composing* E*,*
3) $\boldsymbol{SoT} = \{ \mathtt{SoT}_1, ..., \mathtt{SoT}_\mathtt{m} | \mathtt{m} \in \mathbb{N} \}$ *is the set of smart nodes in* E*,*
4) $\mathtt{PL} = \{ pl_1, ..., pl_n | n \in \mathbb{N} \}$ *is the set of physical structure that defines* E*,*
5) $\mathtt{DL} = \{ dl_1, ..., dl_n | n \in \mathbb{N} \}$ *is the set of logical architecture that connects* ***SoT****.*

Figures 3 and Figure 4 show respectively an abstraction of the physical structure of E and the logical architecture between nodes in E.

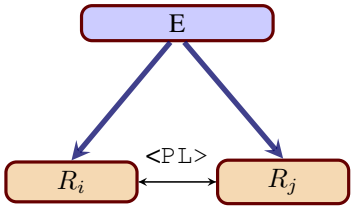

Fig. 3: The physical structure of E.

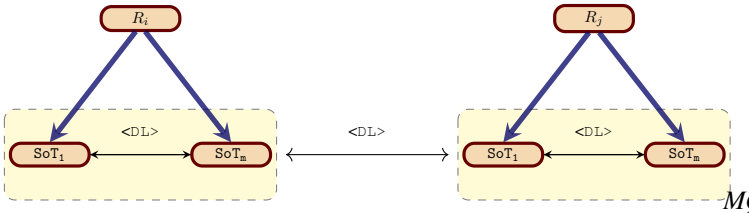

Fig. 4: A Logical/Digital structure in E.

C. Architecture

The architecture is grouped into five main levels depicted in Figure 5:
The first is the most important because it contains sensors that capture the state of smart home periodically then they report if there is a contradictory case (fire, humidity, high temperature, ...), the analysis devices as the database, web server and broker save or process the signals of the sensors then give the actuators the commands to do the necessary actions.
The second level is the set of objects referenced by an IP address linked with the router by a network wire; they can

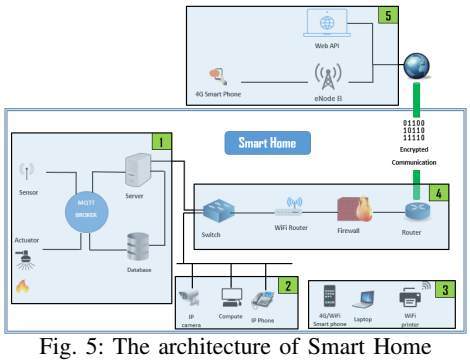

Fig. 5: The architecture of Smart Home

access the internet connection. The third level is IP objects use wireless technology like Wi-Fi, Bluetooth, 4G...
The fourth level has processing devices like router, firewall and switch, they are used to make an interconnection between smart home objects and they are like a point between the outdoor and indoor smart home.
The fifth level is the set of APIs and devices outside smart home that can access the smart home interior objects.

D. Communication

In this part we will present some protocols that can be used in the proposed framework that deals with architecture as the one showed in Figure 6. Herein we present the adopted protocols by the framework.

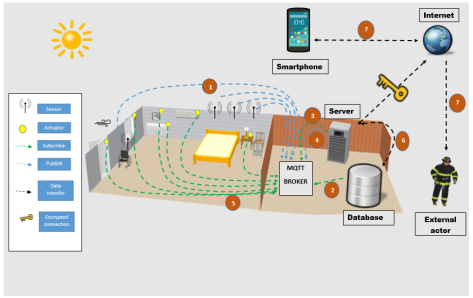

Fig. 6: Operation protocol MQTT in architecture.

MQTT: It is a machine-to-machine connectivity protocol designed as an extremely lightweight publish/subscribe messaging transport [2]. The operations of this protocol passes through steps shown in Figure 6, where it is applied on Smart room, and it is the first level represented in the architecture.

1) A sensor collects information (temperature, fire, humidity, etc.) then it *publishes* the data to the broker.
2) The database *subscribes* into the Broker that is periodically keep track of the retrieved data.
3) The web server *subscribes* into the Broker and *receives* the published sensors data.
4) The web server, including smart applications, *presents* the appropriate command, and *pulls* it into the MQTT Broker.
5) The actuators *subscribe* in the Broker then it *receive* and *execute* the commands.
6) The application *retrieves* or *updates* the database values.

7) External actors, through web and smart applications, communicate securely with web server.

ONVIF: It is used to establish a communication between the network camera and a point outside the building in order to monitor its status in real time.

Http: People authenticated in the web server can access through an API that uses this protocol to view or edit information about the building.

VoIP: Phones equipped with a network card can make calls using this protocol.

Ethernet: It is a data link layer protocol in the Open Systems Interconnection (OSI) model that allows objects affiliated with the same LAN to interchange data.

E. Security

The digital environment always at risk, for this we rely on the security side in our approach to avoid information theft, data interception or disservice. We consider the following five concepts in order to stop or decrease threats.

- **Confidentiality**: ensure that each data access only by objects (people, devices) that we define them through encrypting data with a strong encryption method. Ignoring this principle can cause a destruction of information.
- **Authentication**: Some smart home objects (such as the server) request objects that want to access it to define its identification in order to prevent unauthorized access.
- **Data Integrity**: Man in the middle [20] can intercept the flow of data between IoT objects, change it then send it back to the receiver. So we use some mechanisms like hashing [26] (MD5 and SHA-2) and electronic signatures [9] to control if the message is changed or no.
- **Access control**: Smart home objects with their security levels allow functions according to a predefined authorization and prevention rules. The architecture supports firewalls [30] at the gateway level that manage the input and output packets. Further, for security policies we are interested in access control mechanisms [16] (RBAC) and adapting the router by an access control list ACL [27].
- **Non-repudiation**: Since IoT objects always in contact it is important to check the legitimacy of the sender and the receiver. The most able method to realize that is the electronic certificate [21].

IV. Experimental Results

To test the accuracy of the proposed, we built it within the validation and verification tool Uppaal, by integrating the machine states of smart objects and create the smart home architecture where the smart home objects (composition of states machines) react. The logic behind this composition ensures that the proposed framework does not oppose the requirements. First we ensure through simulation then verification. The simulation is partitioned in four phases, the first tests the operations of MQTT protocol, the second tests the connectivity with a external point, the third tests for exceptional cases where IoT devices can not connect to each other and finally we verify the satisfaction of the security rules that we must respect in the proposed system.

A. MQTT protocol test

We test the MQTT protocol via a scenario simulates the case of fire in smart home, the first scenario steps are presented in the figure 7, our system function without deadlock.

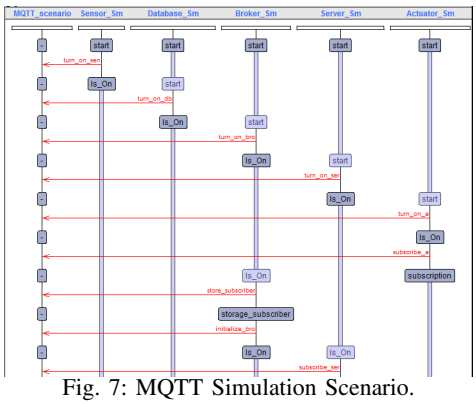

Fig. 7: MQTT Simulation Scenario.

B. Connection with distant points

The distant smart home users use IoT nodes to access smart home objects via the internet connection. In this point we will study two examples, the first is a user that accesses by his smartphone to the smart home server in order to extract data from the database, and the second is a web API accesses to a Webcam Home, system operation does not give errors.

C. Exceptional cases:

The nature of these tests simulates contradictory cases that affect the exchange of messages, in this test we check the operation of system with three cases contradictory with the natural operation(Webcam not linked, Firewall prevents webcam contact and The API does not authenticate the webcam), the resulat was that the test procedure is not finished.

D. Security rules verification

Uppaal has a language called 'query language' which allows to edit rules after the construction of states machines of the objects to test the accuracy of these objects. The language is written according to specific norms and symbols.To verify the security rules, we express the query language to check these goals Confidentiality, Authentication, Data Integrity, Access control and Non-repudiation. The verification results show that all the security rules are checked and satisfied.

V. Conclusion

The approach suggests to deploy a complete theoretical and practical framework that builds secure smart homes and buildings in order to protect the inhabitants, the environment, and to optimize the standard of living for an inhabitant. The proposed formalization considers the characteristics and the behavior of smart nodes and facilitates the expression of their operations. The flexibility of the architecture makes it applicable on different structures so it is not affected by the number of rooms, doors, style of construction, nature of wall, etc. The framework covers a number of technologies,

and fit the compatibility between them. Further we propose a set of security rules in order to reinforce the architecture and to check how much it is secure. For the security and the correctness analysis that helps to reduces the error rate after deployment, we rely on the simulation and the formal verification that showed the strong and the weak points of the a defined architecture. The results show that the implemented architecture is free from deadlocks, simulate the reality, and respect the security rules.

As a future work, we intend to extend the framework to support smart cites as first step. Then we look to how to optimize the architecture features such as minimizing energy consumption, large-scale coverage by limited number of gateways. Further, from a security perspective we will increase the security level by relying on a distributed architecture "Blockchain".

REFERENCES

[1] Iot sensors. https://fiware-tutorials.readthedocs.io/en/latest/iot-sensors/, 2019.

[2] Mqtt. http://mqtt.org/, May 2019.

[3] Uppaal home. http://www.uppaal.org/, 2019.

[4] M. Aazam and E. Huh. Fog computing micro datacenter based dynamic resource estimation and pricing model for iot. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, pages 687–694, March 2015.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.

[6] S. Andreev, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy. Understanding the iot connectivity landscape: a contemporary m2m radio technology roadmap. *IEEE Communications Magazine*, 53(9):32–40, Sep. 2015.

[7] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Comput. Netw.*, 54(15):2787–2805, October 2010.

[8] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the internet of things (iot). In Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki, and Dhinaharan Nagamalai, editors, *Recent Trends in Network Security and Applications*, pages 420–429, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[9] Jean-François Blanchette. The digital signature dilemma le dilemme de la signature numérique. 2006.

[10] Dr. Lakshmi Devasena C. Ipv6 low power wireless personal area network (6lowpan) for networking internet of things (iot) - analyzing its suitability for iot. 9, 01 2016.

[11] 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 Communications*, 23, October 2016.

[12] Y. Chen and T. Kunz. Performance evaluation of iot protocols under a constrained wireless access network. In *2016 International Conference on Selected Topics in Mobile Wireless Networking (MoWNeT)*, pages 1–7, April 2016.

[13] Antonio M. Pascoal David Moreno-Salinas and Joaquin Aranda. Optimal sensor placement for multiple target positioning with range-only measurements in two-dimensional scenarios. *Sensors*, 13(8), August 2013.

[14] P. Desai, A. Sheth, and P. Anantharam. Semantic gateway as a service architecture for iot interoperability. In *2015 IEEE International Conference on Mobile Services*, pages 313–319, June 2015.

[15] Xenofon Fafoutis, Atis Elsts, Antonis Vafeas, George Oikonomou, and Robert Piechocki. On predicting the battery lifetime of iot devices: Experiences from the sphere deployments. In *Proceedings of the 7th International Workshop on Real-World Embedded Wireless Systems and Networks*, RealWSN'18, pages 7–12, New York, NY, USA, 2018. ACM.

[16] David Ferraiolo and D Kuhn. Role-based access controls. 03 2009.

[17] Arnold Janssens and Michel De Paepe. Effect of moisture inertia models on the predicted indoor humidity in a room. *Proceedings of the 26th AIVC Conference*, 01 2005.

[18] Amos Kingatua. Iot system tests :: Checking for failure.

[19] Dmitry G. Korzun, Sergey I. Balandin, and Andrei V. Gurtov. Deployment of smart spaces in internet of things: Overview of the design challenges. In Sergey Balandin, Sergey Andreev, and Yevgeni Koucheryavy, editors, *Internet of Things, Smart Spaces, and Next Generation Networking*, pages 48–59, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[20] Avijit Mallik, Abid Ahsan, Mhia Md. Zaglul Shahadat, and Jia-Chi Tsou. Man-in-the-middle-attack: Understanding in simple words. 3:77–92, 01 2019.

[21] Mick O Brien and George Weir. Understanding digital certificates. 06 2019.

[22] Samir Ouchani. Ensuring the functional correctness of iot through formal modeling and verification. In *Model and Data Engineering - 8th International Conference, MEDI 2018, Lecture Notes in Computer Science*, pages 401–417. Springer International Publishing, 2018.

[23] Luis Sanchez, Luis Muñoz, Jose Antonio Galache, Pablo Sotres, Juan R. Santana, Veronica Gutierrez, Rajiv Ramdhany, Alex Gluhak, Srdjan Krco, Evangelos Theodoridis, and Dennis Pfisterer. Smartsantander: Iot experimentation over a smart city testbed. *Computer Networks*, 61:217 – 238, 2014. Special issue on Future Internet Testbeds – Part I.

[24] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder. Management of resource constrained devices in the internet of things. *IEEE Communications Magazine*, 50(12):144–149, December 2012.

[25] Giorgos Sfikas, Charilaos Akasiadis, and Evaggelos Spyrou. Creating a smart room using an iot approach. 05 2016.

[26] Rajeev Sobti and Geetha Ganesan. Cryptographic hash functions: A review. *International Journal of Computer Science Issues, ISSN (Online): 1694-0814*, Vol 9:461 – 479, 03 2012.

[27] Shipra Suman and Aditi Agrawal. Ip traffic management with access control list using cisco packet tracer. *International Journal of Science, Engineering and Technology Research*, 5:1556–1561, 05 2016.

[28] Konglong Tang, Yong Wang, Hao Liu, Yanxiu Sheng, Xi Wang, and Zhiqiang Wei. Design and implementation of push notification system based on the mqtt protocol. In *2013 International Conference on Information Science and Computer Applications (ISCA 2013)*. Atlantis Press, 2013/10.

[29] Dhiren Tejani, Ali Al-Kuwari, and Vidyasagar Potdar. Energy conservation in a smart home. 05 2011.

[30] A. Wool. A quantitative study of firewall configuration errors. *Computer*, 37(6):62–67, June 2004.

[31] G. Xiao, J. Guo, L. D. Xu, and Z. Gong. User interoperability with heterogeneous iot devices through transformation. *IEEE Transactions on Industrial Informatics*, 10(2):1486–1496, May 2014.

[32] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, Feb 2014.

[33] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin. Iot gateway: Bridging-wireless sensor networks into internet of things. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pages 347–352, Dec 2010.