Authentication and the Internet of Things:

A Survey Based on a Systematic Mapping.

Emidio de Oliveira e Silva
CESAR - Recife Center for Advanced Studies and Systems
Recife, Brazil
eos@cesar.org.br

Wallace Thierre Souza de Lima
CESAR - Recife Center for Advanced Studies and Systems
Recife, Brazil
wtsl@cesar.org.br

Felipe Silva Ferraz
CESAR - Recife Center for Advanced Studies and Systems
Recife, Brazil
fsf@cesar.org.br

Francisco Icaro do Nascimento Ribeiro
CESAR - Recife Center for Advanced Studies and Systems
Recife, Brazil
finr@cesar.org.br

Abstract—The term Internet of Things (IoT) is used to describe many objects connected and communicating with each other. In this scenario, where different things share information in distinct environments, some security problems become evident. Among those issues, authentication is an important technique for ensuring a reliable and secure communication between objects in an IoT environment. This paper has mapped the current state of the authentication use in an IoT environment, highlighting the challenges and the main techniques used in authentication solutions.

Keywords- internet of things; authentication; authorization; systematic mapping;

I. INTRODUCTION

Nowadays it is natural to face a scenario in which smart objects are connected to the Internet, exchanging data and information, interacting with users and other devices. It is possible to notice these objects in several different areas, such as, healthcare monitoring, telecommunication, vehicular automation, traffic, elderly and children care, etc. [1]. This group of connected objects is denominated IoT.

According to Gartner institute, it is expected that 8.4 billion smart devices will be connected and in use by the end of 2017. It is also estimated that a number close to 20.4 billion devices will be connected by the end of 2020. This demonstrates a growing investment in the new business niche involving IoT solutions. Still, in the same article, it is presented that companies are expected to invest around US$ 1.7 trillion in IoT applications by the end of 2017 and reach US$ 3 trillion by 2020 [2].

IoT is not just a machine-to-machine network or a network, with smart and physical objects, that contains embedded technology to sense/interact with their internal state or external environment. IoT defines an ecosystem that includes things, communication, applications, data analysis, business opportunity and innovation [3]. In this context, IoT will enable a broad variety of new ways to interact in citizens cotidianum, connecting smart objects, interacting in different environments, using different protocols and combining a natural heterogeneous environment through a set of different approaches [4]. This way, many companies develop platforms to explore and facilitate internet solutions of things like the KNoT, a meta platform that focuses on implementing the integration between existing hardware and software IoT platform [5].

In this complex heterogeneous structure of IoT environments, in which connected solutions are already part of people and companies practices, manipulating and storing information, many security issues can be highlighted. Data privacy, device identification, authentication, authorization and software vulnerability are some of these concerns, that must be addressed while IoT are still in its early stages of development [4][6][7].

In order to provide trust of the information, that the confidentiality, integrity and availability of the information are not violated, security mechanisms must be considered. In terms of information security, authentication is a property of a system that is related to an actor being able to provide a set of information to prove that he is indeed who it claims to be.

In the context of IoT, authentication is related to any claim of an object, from a system, another object or user, and it validates if the claimer is who it affirms it is.

Authentication is important not only to authenticate a user, but also to manage credentials as a whole, ensuring that those who do not have permissions are blocked from accessing. Since IoT is a new and challenging area, this work will focus in a research about what has been studied and built in terms of authentication in IoT.

In order to provide a broad overview about authentication in an IoT environment and also identify opportunities, challenges and other matters on this topic, this paper conducts a systematic mapping. A systematic mapping aims to identify the quantity, type of research and results available within a specific area. It also aims to verify the evolution and state of the art in that area [8]. This work

 ISBN: 978-1-61208-590-6

is divided, as follows: in Section 2, the methodology used to perform this research will be described, along with the protocol, methods, and the processes used in this mapping review. Section 3 presents the results and summarizes the main points about the subject addressed. Finally, in the last section, conclusions and future works will be presented.

II. APPLIED PROTOCOL

Based upon the guidelines for the development of systematic reviews in software engineering described by Kitchenham et al. [8] and the analysis of the review model by Dybå and Dingsøyr [9], a new methodology for revision was created. Our review methodology is composed of six steps: (1) development of the protocol, (2) identification of inclusion and exclusion criteria, (3) search for relevant studies, (4) critical assessment, (5) extraction of data, and (6) synthesis. The steps applied to the study contained herein are presented below:

The objective of this review is to identify primary studies that focus on the use of authentication techniques that aims to solve IoT security problems. The following question helps identifying primary studies.

- How important are authentication techniques on IoT environments and what are the challenges, concerns, and expectations about these techniques?

From this central question and after an internal debate between the authors, other secondary questions were developed to help comprehending the problem:

1. What are the main challenges about authentication in an IoT environment?
2. What are the main authentication methods or techniques used in an internet environment of things?
3. What are the advantages, benefits and challenges in the use of techniques that use RFID as an authentication artifact?

A. Inclusion and Exclusion Criteria

For this review, studies that aim to analyze the use of authentication techniques to improve security in IoT environments were considered. Since this field of research is recent, this review limited the examined studies to the ones published starting from the year of 2015, due to the great emergence of relevant studies as of this year.

The following works were also excluded:

- Studies not published in the English language;
- Studies that were unavailable online;
- Studies not based on research or that are incomplete;
- Call for works, prefaces, conference annals, handouts, summaries, panels, interviews and news reports.

B. Search Strategies

The databases considered in the study were:

- ACM Digital Library;
- IEEE Xplore;
- SpringerLink;

Some terms were defined and combined based on the proposed questions. As a result, a set of five strings were defined and used to conduct the search in the databases.

((IOT or internet of things) and security) and authentication);

(((IOT or internet of things) and authentication) and challenges);

(((IOT or internet of things) and authentication) and techniques);

(((IOT or internet of things) and authentication) and methods);

(((IOT or internet of things) and authentication) and RFID);

In the process of extracting information from the databases, the search strings were used separately on each database. The searches were performed between March 2017 and April 2017. The results of each search were grouped together according to the database and were, later, examined closer in order to identify duplicity. Table 1 shows the amount of studies found on each database.

TABLE I. AMOUNT OF STUDIES FOUND ON EACH DATABASE

Database	Amount of studies
ACM Digital Library	*112*
IEEE Xplore	*417*
SpringerLink	*1366*

C. Studies Selection Process

This section describes the selection process from the beginning: from the initial search using the Search Strategies previously described to the identification of primary studies.

At the first step, an analysis was realized to remove all duplicated articles from the set of studies obtained. After removal, 1208 non-duplicated works remained, they were added to Mendeley's citation management tool.

In a second phase, the titles of all works selected in the previous step were analyzed to determine its relevance in this systematic mapping. At this stage, many works that did not mention using authentication into IoT, authentication techniques or methods were eliminated.

Due to the use of terms related to authentication in IoT environment, many works depicting about cloud authentication, biometric authentication and biological identification were found. In those cases, all works whose titles did not conform to the scope of the review were eliminated. In other cases, when the works titles were vague or unclear, they were put aside to be analyzed in the next step. At the end of this stage, 553 citations were excluded, thus remaining 205 items for further analysis.

 ISBN: 978-1-61208-590-6

In the third step, all abstracts of the filtered works were closely examined, showing an enormous quality variation. Once again, many studies were eliminated due to their non conformity to the scope of authentication being used to solve privacy and security issues in IoT environments. Others had no abstracts or had abstracts that did not clearly presented what the article was about. In the end, a total of 99 papers were selected.

Table 2 presents the amount of studies filtered in each step of selection process.

TABLE II. AMOUNT OF STUDIES FILTERED IN EACH STEP OF SELECTION PROCESS

Engine	Returned Studies	Title	Abstract
ACM	69	34	7
IEEE	298	112	40
Springer Link	391	59	10
Total	758	205	57

D. Quality Assessment

In this assessment stage, the works were submitted to a critical analysis. In this stage, the complete studies were analyzed, instead of only the titles or abstracts. After this, the last studies that were considered uninteresting for the review were eliminated resulting in the final set of works. After the quality assessment, relevance grades were attributed to the remaining works. The relevance grades are going to be useful in the next stage. Six questions, based on Kitchenham et al. [8], were used to guide quality assessment. Those questions determine the credibility, rigor and relevance of the article to be analyzed. Out of the six, the first is the most important due to its capability to determine if the work is addressed to the review subject. The five remaining questions are useful in determining the quality of the work, so they were used to classify the works according to the quality. The questions were:

1. Does the study analyze the benefits of using authentication in an IoT environment?
2. Is the study based on research - not merely on specialists' opinions?
3. Are the objectives of the study clearly stated?
4. Is the context of the study adequately described?
5. Was the research project adequate to reach the research objectives?
6. Were the research results adequately validated?

After a deep analysis at the quality assessment stage, 49 of the remaining 57 studies were selected to the stage of data extraction and synthesis and were, thus, considered as the primary studies. The quality assessment process will be presented in detail in the result section along with the assessment of the 49 remaining studies.

III. RESULTS

In total, 49 primary studies were identified, each one dealing with a wide array of research topics and using a wide set of exploration models for different scenarios.

After evaluating the primary studies, the works revealed patterns related with authentication and identification in IoT environment. Several studies had a theoretical essence centered on the proposal of an authentication mechanism, using it in two or more steps. Many of the solutions analyzed use the authentication scheme applying elliptic curve cryptosystem (ECC), which is a public key cryptography method, that uses points on an elliptic curve to derive a 163-bit public key, equivalent in strength to a 1024-bit RSA key and XOR operations. In further studies, authentication occurs through devices that use Radio-Frequency Identification (RFID). RFID is one of the most important technologies used in IoT area, as it can store sensitive data, communicate with other objects wirelessly and identify/track objects automatically in user identification.

A. Quantitative Analysis

The developed research process resulted in 49 primary studies. They were written by 193 authors linked to institutions based on different countries, distributed on four continents, and were published between 2015 and 2017. In total, the authors identified 225 different keywords in their work. In many works, the authors approach different ways to make authentication, with two or three steps or using RFID. To emphasize this affirmation, Figure 1 presents a word cloud generated with all works titles.

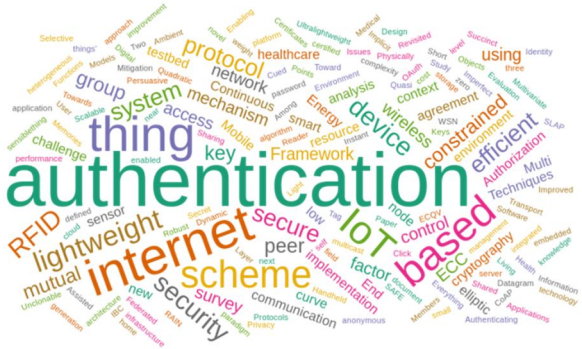

Figure 1. Word cloud from the primary studies.

The most common keywords used in the remaining works with their respective frequency were: authentication (10), Internet of things (8), security (3), privacy (3), wireless sensor networks (3), techniques (1), methods (1), RFID (1). The first three keywords - authentication, internet of things and security - reflect precisely the theme of the research

contained herein.

B. Qualitative Analysis

As described in the quality assessment, each one of the primary studies was assessed according to six quality criteria related to rigor and credibility, as well as to relevance. If considered as a whole, these six criteria provide a good measure to the conclusions that a particular study can bring to the mapping. The classification for each criteria used a scale of positives and negatives.

In Table 3, columns ‘q1’ to ‘q6’ represent the 6 criteria defined by the questions used on the quality assessment: Focus in Authentication, Research, Clearly, Context, Project, and Validation.

For each criteria, '1' represents the positive answer and '0' the negative one.

TABLE III. QUALITATIVE TABLE

Study	q1	q2	q3	q4	q5	q6	Total
[1]	1	1	1	1	1	1	6
[2]	1	1	1	1	1	0	5
[3]	1	1	1	1	1	0	5
[6]	1	1	1	1	1	0	5
[10]	1	1	1	1	0	0	4
[11]	1	1	1	1	1	0	5
[13]	1	1	1	1	1	1	6
[14]	1	1	1	1	0	0	4
[15]	1	1	1	1	1	0	5
[16]	1	1	1	1	1	0	5
[17]	1	1	1	1	1	0	5
[18]	1	1	1	1	1	1	6
[19]	1	1	1	1	0	0	4
[20]	1	1	1	1	1	0	5
[21]	1	1	1	1	1	1	6
[22]	1	1	1	1	1	1	6
[23]	1	1	1	1	1	0	5
[24]	1	1	1	0	1	1	5
[25]	1	1	1	1	1	1	6
[25]	1	1	1	1	1	0	5
[28]	0	1	1	1	0	0	3
[30]	1	1	1	1	1	0	5
[31]	0	1	1	1	1	1	5
[32]	1	1	1	1	1	1	6
[33]	1	1	1	1	0	0	4
[34]	1	1	1	1	1	1	6
[35]	1	1	1	1	1	0	5
[36]	1	1	1	1	1	0	5
[37]	1	1	1	1	1	0	5
[38]	1	1	1	1	0	0	4
[39]	0	1	1	1	1	0	4
[40]	1	1	1	1	1	0	5
[41]	0	1	1	1	0	0	3
[42]	1	0	1	1	1	0	4
[43]	1	0	1	0	1	1	4
[44]	1	1	1	1	1	0	5
[45]	1	1	1	1	1	1	6
[46]	1	1	1	1	1	1	6
[47]	1	1	1	1	1	0	5
[48]	1	1	1	1	1	0	5
[49]	1	1	1	1	1	0	5
[50]	1	1	1	1	1	0	5
[51]	1	1	1	1	1	0	5
[52]	0	0	1	1	1	1	4
[53]	1	1	1	1	1	1	6
[54]	0	1	1	0	0	0	2
[55]	1	1	1	1	0	0	4
[56]	1	1	1	1	1	1	6
[57]	1	1	1	1	1	0	5

Table 3 presented the quantitative analyses; based on that, it is possible to check that the following works were marked with higher scores: [1], [2], [3], [6], [11], [13], [15], [16], [17], [18], [20], [21], [22], [23], [24], [25], [27], [30], [31], [32], [34], [35], [36], [37], [40], [44], [45], [46], [47], [48], [49], [50], [51], [53], [55], [56] and [57]. These will serve as a base to the following section, in which discussion about the main topics will be conducted.

Some studies were analyzed [28], [31], [39], [41], [52] and [54] did not have positive result in the first question ("Q1"). However, the articles provided information on the context of the work and contributed, in some way, to the research.

 ISBN: 978-1-61208-590-6

IV. DISCUSSION

After analysis and data extraction, steps performed on the primary studies, it was possible to identify some aspects related with authentication in IoT application environments.

First, it is possible to conclude that security in IoT environment is a very recent field of research since the majority studies used in this article have been published after 2015. Secondly, it was possible to conclude that in many applications, different ways are used to make authentication. In some cases, when using two or more authentication steps, it is possible to work with digital and iris recognition or RFID for identification.

In these works, it was possible to identify the importance of creating an efficient mechanism against the most common internet attacks such as MitM, replay, forward secrecy and DoS. Therefore, in order to get this efficiency, many works used elliptic curve cryptosystem (ECC) scheme.

A. *What are the main challenges regarding authentication in an IoT environments?*

There are challenges that need to be addressed in IoT authentication. The first challenge is to reduce the energy cost on the authentication process; for example, elliptic curve cryptography (ECC) is an authentication protocol, which uses implicit certificate aiming to reduce energy consumption and computation overhead [11] in wireless sensor networks for distributed IoT Applications.

The second challenge [12] introduced is to deploy authentication protocols adapted to the IoT environment. Different network architectures are based on different IoT notions and need to deploy authentication schemes to secure communications [13].

Another challenge is to design an authentication scheme identifying the users in their respective devices without maintaining permanent contact between those parts [14].

The last challenge is to achieve cross network security in machine to machine communications issues like diverse channels, interfaces, and context environments of heterogeneous networks [15] need to be addressed.

B. *What are the main authentication methods or techniques used in the internet of things?*

Similar to the current internet applications, there are many mechanisms to provide authentication in an IoT platform. In this way, one possible solution is to use three factors for authentication which includes, ID, password and fingerprint [2]. In other words, Mbarek et al. [16] explains three methods used in authentication. The first method consists in a signature-based mechanism, this signature could be an ID or an elliptic curve signature, for example. The advantage of this authentication method is that it provides fast messaging authentication, with sender repudiation [16]. The second method ensures immediate messaging authentication and inherits security of different signatures, such as Winternitz, which is a one-time signature that are proven to be existentially unforgeable under adaptive chosen message attacks. The third method implements a lightweight symmetric primitives, like the ones used in µTESLA context, where the authentication key is secret for a time interval and will be disclosed after a certain period of time [16].

Other technique that can be used in IoT architecture is identification of neighbor nodes and a data aggregation to authenticate group members that uses an authentication scheme in wireless sensor network (WSN) using elliptic curve cryptosystem (ECC) and XOR operation [17].

Another paper cites RFID authentication due to its strong requirements and the ability to ensure secure communication between RFID tags and the server [18]. In the next question this subject will be more discussed.

Other uncommon mechanism used to improve security is presented in the second step of the authentication process. First, the user enters with his/hers username and password. If the verification is completed successfully, the second step of authentication is started by allowing the user to enter a registered and predefined sequence of events, such as menu or mouse activity, on a fake server screen [1].

One of the most secure mechanism of authentication is cited in [19]. It is the One Time Password (OTP) technique developed with elliptic curves cryptography (ECC). It is the most efficient and secure compared to the existing methods like the Key Distribution Center (KDC). This method does not store the device's private and public keys, it only stores their IDs.

Finally, the most popular method used to secure authentication is the two step verification. It sends a verification code to a mobile phone or uses a smart card for generating keys on the devices directly [19].

C. *What are the advantage, benefits and challenges in the use of techniques that use RFID as an authentication artifact?*

Radio-Frequency IDentification (RFID) is one of the most important technologies used in the IoT, as it can store sensitive data, communicate and identify objects [18]. The RFID system is composed of three components: RFID tag, reader and a trusted back-end server [19].

Zeadally et al. [18] show that the RFID has advantages if compared to the traditional barcode reader. It can be applied to objects with rough surfaces, provide both read/write capabilities, it requires no line-of-sight contact with RFID readers, it is able to read multiple RFID tags simultaneously, and provides strong authentication to the user data [21].

To reduce communication and computation overheads, the RFID reader uses a scheme that enables to resist various common attacks such as the MitM, replay, forward secrecy, and DoS [22]. ECC-based RFID authentication schemes

 ISBN: 978-1-61208-590-6

have attracted a lot of attention, Zeadally et al. [18] argue that the PKC-based RFID authentication schemes are necessary for secure communication in RFID systems because many security attributes cannot be implemented. However, elliptic curve cryptosystem (ECC) is more suitable because it can provide similar security level but with a shorter key size and has low computational requirements [18].

V. CONCLUSION

The purpose of this review was to identify primary studies that focus on the use of authentication, with its challenges and opportunities. In the searching phase, 1208 studies were found, out of which 49 were classified as primary studies after the selection and the quality criteria were applied. Many of the studies found in the first steps did not focus on IoT authentication solutions. Such works focused only in cloud computing and techniques that deal just with data privacy were not selected to compose the search.

In the analysis performed on the group of selected articles, theoretical and practical solutions that described techniques and methods of authentication were found. The vast majority of the studies were validated in a more superficial and theoretical way, highlighting their strengths and their advantages.

This systematic review has found different ways to perform authentication in IoT environments and, among them, the use of ECC was present in majority of articles aiming to ensure security with low power consumption.

This work also showed the main challenges of applying authentication in an IoT environment. The low energy storage capacity of connected devices can be highlighted as one of the main concerns. In the process of solving this major challenge, a large number of authentication solutions use elliptic curve cryptography (ECC) that provides security with low processing power, adding more efficiency in authentication algorithms.

Regarding the future work, a comparison between light authentication solutions based on elliptic curve cryptography is proposed. A more detailed analysis about elliptic curve cryptography can be performed in order to validate if the use of the technique satisfies the challenges of security and low power consumption in an IoT environment.

ACKNOWLEDGMENT

This work was developed under the Professional Master of Software Engineer's program of the Educational branch of CESAR, a Brazilian innovation center.

REFERENCES

[1] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, C. Conference, "Authentication Techniques for the Internet of Things: A Survey," 2016.

[2] "Gartner,"http://www.gartner.com/newsroom/id/3598917, accessed: 2017-05-02.

[3] K. Gupta, "Internet of Things: Security Challenges for Next Generation Networks," no. Icicc, pp. 315–318, 2016.

[4] M. Weber, "Security challenges of the Internet of Things," pp. 638–643, 2016.

[5] "Knot: the open source meta platform for iot," https://www.knot.cesar. org.br/, retrieved: August, 2017.

[6] O. O. Bamasag and K. Youcef-toumi, "Towards Continuous Authentication in Internet of Things Based on Secret Sharing Scheme."

[7] O. Bamasag, "Efficient Multicast Authentication in Internet of Things," pp. 429–435, 2016.

[8] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[9] T. Dybå and T. Dingsøyr, "Empirical studies of agile software development: A systematic review," Inf. Softw. Technol., vol. 50, no. 9–10, Aug. 2008, pp. 833–859.

[10] S. Lin and C. Wen, "Energy-Efficient Device-Based Node Authentication Protocol for the Internet of Things," no. 1, pp. 1–2, 2016.

[11] H. Khemissa, D. Tandjaoui, T. Information, T. Houari, and B. Algiers, "A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things," 2015.

[12] H. Khemissa and D. Tandjaoui, "A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things ∗†," 2016.

[13] N. W. Interfaces, "Continuous Authentication and Authorization for the Internet of Things," 2017.

[14] "ECC Based Self-Certified Key Management Scheme for Mutual Authentication in Internet of Things," pp. 3–8, 2016.

[15] S. Arasteh, S. F. Aghili, and H. Mala, "A New Lightweight Authentication and Key agreement Protocol For Internet of Things," pp. 52–59, 2016.

[16] B. Mbarek, A. Meddeb, W. Ben Jaballah, and M. Mosbah, "A Secure Authentication Mechanism for Resource Constrained Devices," pp. 1–7, 2015.

[17] Y. Park and Y. Park, "A Selective Group Authentication Scheme for IoT-Based Medical Information System," pp. 1–8, 2017.

[18] S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," vol. 4662, no. c, 2014.

[19] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," *Proc. - IEEE Symp. Comput. Commun.*, vol. 2016–Augus, pp. 1109–1111, 2016.

[20] P. Ghosh, "A Privacy Preserving Mutual Authentication Protocol for RFID based Automated Toll Collection System," 2016.

[21] S. M. Sujatha, "Design and Implementation of IoT Testbed with Three Factor Authentication."

[22] Y. Huang and J. Jiang, "Ultralightweight RFID Reader-Tag Mutual Authentication Revisited," 2015.

[23] J. Huang, W. Juang, C. Fan, Y. Tseng, and H. Kikuchi, "Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments," pp. 88–93, 2016.

[24] S. Janbabaei, H. Gharaee, and N. Mohammadzadeh, "Lightweight, Anonymous and Mutual Authentication in IoT Infrastructure," pp. 162–166, 2016.

[25] M. B. Tamboli, "Secure and Efficient CoAP Based Authentication and Access Control for Internet of Things (IoT)," pp. 1245–1250, 2016.

[26] T. Marktscheffel et al., "QR Code Based Mutual Authentication Protocol for Internet of Things," 2016.

[27] L. Feng, X. Yao, and C. Engineering, "RFID System Mutual Authentication Protocols Based on ECC," pp. 1645–1650, 2015.

[28] E. Song, "Enabling RFID technology for healthcare: application,

 ISBN: 978-1-61208-590-6

architecture, and challenges," 2014.

[29] J. Shen, H. Tan, Y. Zhang, X. Sun, and Y. Xiang, "A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment," 2017.

[30] S. Peter, "Multi-level Authentication System for Smart Home-Security Analysis and Implementation."

[31] B. Tank, H. Upadhyay, and H. Patel, "A Survey on IoT Privacy Issues and Mitigation Techniques," pp. 9–12, 2016.

[32] C. Author, "Study of Authentication with IoT Testbed," 2015.

[33] A. H. Moon, I. Technology, U. Iqbal, I. Technology, and G. M. Bhat, "Light Weight Authentication framework for WSN," pp. 3099–3105, 2016.

[34] M. Komar, S. Edelev, and Y. Koucheryavy, "Handheld Wireless Authentication Key and Secure Documents Storage for the Internet of Everything."

[35] Wei-Tsung Su, Wei-Ming Wong and Wei-Cheng Chen, "A survey of performance improvement by group-based authentication in IoT" Applied System Innovation (ICASI), 2016 IEEE International Conference on Applied System Innovation, 2016.

[36] A. Cherkaoui, L. Bossuet, L. Seitz, G. Selander, and R. Borgaonkar, "New Paradigms for Access Control in Constrained Environments."

[37] J. K. Zao, D. A. Ha, and K. T. Nguyen, "Efficient Authentication of Resource-Constrained IoT Devices based on ECQV Implicit Certificates and Datagram Transport Layer Security Protocol," pp. 173–179.

[38] C. Camichel, U. M. R. Cnrs, and A. Thomas, "Evaluation of RAIN RFID authentication schemes," 2016.

[39] H. Zhang and T. Zhang, "Short Paper: 'A Peer to Peer Security Protocol for the Internet of Things,'" pp. 154–156, 2015.

[40] I. Computing, M. Barbareschi, P. Bagnasco, and A. Mazzeo, "Authenticating IoT Devices With Physically Unclonable Functions Models," 2015.

[41] H. Luo, G. Wen, J. Su, and Z. Huang, "SLAP: Succinct and Lightweight Authentication Protocol for low-cost RFID system," *Wirel. Networks*, 2016.

[42] N. Singh, "Improved Authentication Scheme Using Password Enabled Persuasive Cued Click Points," pp. 1394–1398, 2015.

[43] A. V Kamath, K. Kataoka, N. Vijayvergiya, G. B. Reddy, and S. Phatale, "SAFE: Software-defined Authentication FramEwork."

[44] S. Emerson, Y. Choi, D. Hwang, K. Kim, and K. Kim, "An OAuth based Authentication Mechanism for IoT Networks," pp. 1072–1074, 2015.

[45] S. Patel and D. R. Patel, "Energy Efficient Integrated Authentication and Access Control Mechanisms for Internet of Things," pp. 304–309, 2016.

[46] M. A. Crossman and H. Liu, "Two-Factor Authentication through Near Field Communication," 2016.

[47] Y. Sharaf-dabbagh and W. Saad, "On the Authentication of Devices in the Internet of Things," pp. 1–3, 2016.

[48] P. H. Griffin, "Security for Ambient Assisted Living: Multi-factor Authentication in the Internet of Things," 2015.

[49] Y. Essadraoui, "Wireless sensor node's authentication scheme based on Multivariate Quadratic Quasigroups," 2015.

[50] M. P. Pawlowski *et al.*, "Towards a Lightweight Authentication and Authorization Framework for Smart Objects ∗," vol. 8716, no. c, pp. 1–14, 2015.

[51] W. Xi *et al.*, "Instant and Robust Authentication and Key Agreement among Mobile Devices," pp. 616–627.

[52] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, 2017.

[53] C. Shen, H. Li, G. Sahin, and H. Choi, "Low-Complexity Scalable Authentication Algorithm with Imperfect Shared Keys for Internet of Things," pp. 3–8, 2016.

[54] M. Schukat, "Peer to Peer Authentication for Small Embedded Systems," pp. 68–72, 2014.

[55] I. Technology *et al.*, "Digital Memories Based Mobile User Authentication for IoT," 2015.

[56] O. Bamasag, "Efficient Multicast Authentication in Internet of Things," pp. 429–435, 2016.

[57] T. Markmann, T. C. Schmidt, and M. Wählisch, "Federated End-to-End Authentication for the Constrained Internet of Things Using IBC and ECC," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 603–604, 2015.

 ISBN: 978-1-61208-590-6