Towards a Comparative Study of Authentication Mechanisms for Low-Resource Internet of Things Devices

Joel Sousa[1], **Emerson B. Tomaz**[1], **Allysson Allex Araújo**[2]

[1]Universidade Federal do Ceará (UFC)
Campus de Crateús
Crateús, Ceará – Brasil

[2]Universidade Federal do Cariri (UFCA)
Centro de Ciências e Tecnologia (CCT)
Juazeiro do Norte, Ceará – Brasil

joe_sousa@alu.ufc.br, emerson@crateus.ufc.br,
allysson.araujo@ufca.edu.br

Abstract. *Authenticity represents an essential facet of information security explored across various Information Systems (IS), including Internet of Things (IoT) devices in Industry 4.0. However, deploying authentication mechanisms in specific IoT devices poses significant challenges, particularly for those with energy, memory, and computational power constraints. Given this context, this ongoing research project aims to compare conventional authentication mechanisms for low-resource IoT devices and identify the most efficient one among them. As an initial result, this paper aims to present our methodological scope and discuss preliminary empirical results derived from a computational experiment using the Non-Interactive Zero Knowledge Proofs (NIZKP), algorithm in Arduino Nano. This research seeks to enhance the comprehension of authentication mechanisms in low-resource IoT devices, thus facilitating better decision-making processes in IS settings and contributing to academia and practice.*

1. Introduction

Industry 4.0 combines industrial technology, information and communication technologies to create a flexible production model for personalized digital products and services [Zhou et al. 2015]. Due to its current level of maturity and awareness, we opted to contextualize this work in the scenario of Industry 4.0, although we recognize that Industry 5.0 has been gaining attention. According to Liu *et al.*(2020), the benefits of Industry 4.0 stem from the incorporation of various emerging technologies, such as the Internet of Things (IoT). In summary, IoT is characterized as an open and comprehensive network of intelligent objects that can self-organize, share information, data, and resources, and react and act in response to situations and changes in the environment [Madakam et al. 2015].

IoT devices are embedded in various application domains, such as smart agriculture [Perwej et al. 2019] and smart cities [Lohiya and Thakkar 2020]. Baiyere *et al.* (2020) highlighted the position of Information Systems (IS) scholars in advancing research on IoT because IS operates at the intersection of information technologies, social, business, and technical aspects. Due to information security concerns, such as the potential for misuse and abuse by different actors, the impact of IoT on individuals, businesses, and society is significant [Qin et al. 2016]. Abomhara and Køien (2015) highlight

that IoT devices deal with different challenges, particularly in information security. Due to resource constraints, IoT devices often lack the capacity to support complex security schemes [Roy et al. 2018]. In order to ensure security, it is important to have mechanisms for authentication in place to verify the entities legitimacy [Alnahari and Quasim 2021].

Among the most popular authentication mechanisms, Galla *et al*. (2016) highlight RSA (Rivest, Shamir, Adleman). In this scheme, an entity employs its private key to digitally sign a message, while the recipient verifies the authenticity of the message using the entity's corresponding public key. Najjar (2015) discusses the HMAC (*Hashed Message Authentication Code*), which is a type of MAC function that uses hash functions and a secret key shared between two parties to ensure the authenticity and integrity of messages. Hung and Hsu (2018) emphasize the use of AES (*Advanced Encryption Standard*), this symmetric block cipher algorithm is used to cipher and decipher information using the same key. Additionally, Puthiyidam *et al* (2023) noted that NIZKP (*Non-Interactive Zero Knowledge Proofs*) enables secure IoT authentication by allowing devices to prove their identity without disclosing sensitive information and without requiring multiple rounds of interaction between the prover and verifier. Ensuring the authenticity of IoT devices is critical for maintaining data security and integrity in the context of Industry 4.0.

More recently, Eldefrawy *et al*. (2018) conducted an experiment to establish secure channels between components of an IoT infrastructure in industrial applications considering two different authentication mechanisms. They found that HMAC-SHA256 demonstrated advantages in energy efficiency and processing compared to ECC. In addition, Tomaz *et al*. (2020) explored the NIZKP in low-resource mobile health system. They ensured the patient's privacy-preserving throughout the system by addressing issues of storing, managing, and sharing data using blockchain. The aforementioned papers focused on the implementation of HMAC and NIZKP as authentication mechanisms for low-resource systems, but they did not provide any robust comparative analysis considering a pool of different authentication mechanisms. However, in an IoT scenario of Industry 4.0, for example, there are often several devices with considerable resource constraints. As a result, it is important to analyze which authentication mechanisms are most appropriate for these constrained scenarios.

In light of this motivation, this ongoing research project aims to conduct a robust comparison among different authentication mechanisms in the context of low-resource IoT devices to identify the most efficient one. We seek to investigate whether NIZKP over elliptic curves demands fewer computational resources compared to conventional authentication mechanisms, that is, HMAC, AES, and RSA. This paper aims to present our methodological scope to achieve this objective and discuss preliminary evidence of the feasibility of using the NIZKP algorithm on the Arduino Nano, which is a highly used open-source electronic prototyping platform created for projects with limited resources.

This expected comparative analysis contributes to the field of IS by aiding decision-making processes for authentication mechanisms in IoT settings, especially for Industry 4.0 scenarios with constrained-resource IoT devices where information security is critical. In addition, this perspective is closely related to the challenge of "Full Interoperability: Challenges and Opportunities for Future Information Systems" [Boscarioli et al. 2017], since dealing with the complexity of IS require to explore new models of interoperability, in which IoT plays a key role.

2. Research Method

This research positions itself as experimental with an descriptive approach. We delineate the methodological scope through a computational experiment, based on the comparative analysis of authentication mechanisms in low-resource IoT devices. The methodological design of the experiment is depicted in Figure 1.

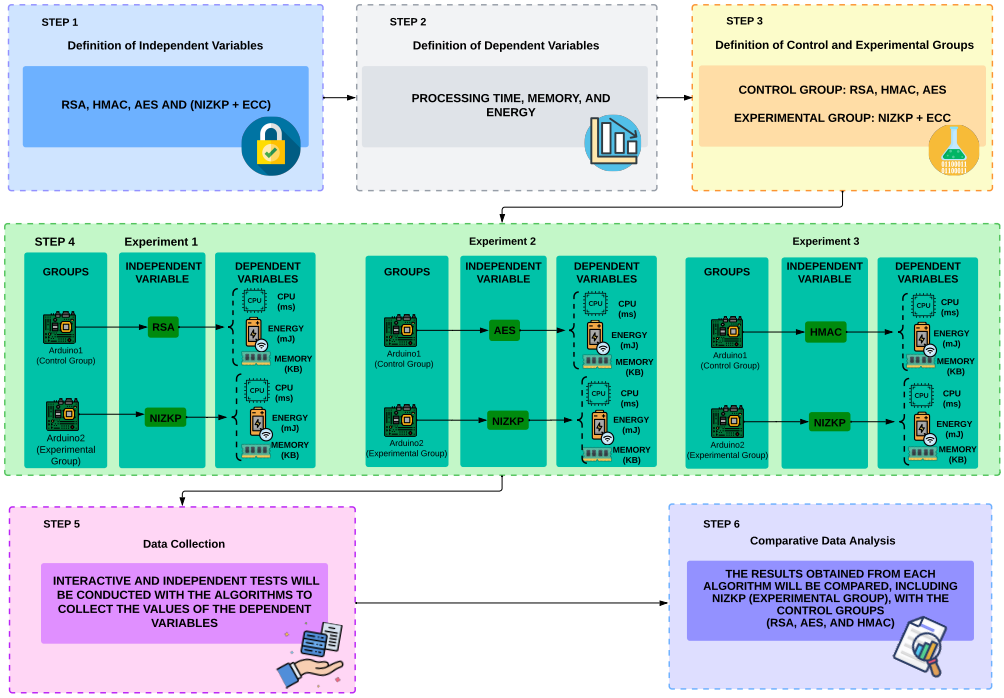

Figure 1. Methodological Procedures.

In **Step 1** (dashed lines in blue), the definition of independent variables will be carried out, represented by the authentication mechanisms that will be part of the experiment: NIZKP, HMAC, AES, and RSA. The selection of these mechanisms was based on their widespread application. In **Step 2** (dashed lines in gray), dependent variables will be delineated, such as computational processing time, memory allocation, and energy consumption. The careful selection of these variables was based on the challenges associated with limited computational capacity, energy constraints, and memory restrictions in IoT devices. In **Step 3** (dashed lines in yellow), the definition of the Control Group and Experimental Group will be carried out. The Control Group will include RSA, HMAC, and AES, while the Experimental Group will comprise NIZKP.

In **Step 4** (marked by dashed lines in green), we will conduct three distinct experiments to compare the performance. In Experiment 1, we will compare NIZKP with RSA; in Experiment 2, NIZKP with AES; and in Experiment 3, NIZKP with the HMAC. In **Step 5** (indicated by dashed lines in pink), we will conduct additional iterations of the tests from the previous step to improve the consistency of the results and reduce random errors. We will record the experimental conditions, tasks, and Arduino Nano configurations in each iteration to ensure the reproducibility of the results. We will collect the values of the dependent variables, that is: computational processing time in milliseconds (ms), memory allocation in kilobytes (Kb), and energy consumption in millijoules

(mJ). These records will be important for analyzing the performance of each mechanism. In **Step 6** (marked by dashed lines in purple), we will proceed with the analysis of the previously collected data, comparing the results of each mechanism, including NIZKP (experimental group), with the RSA, AES, and HMAC (control groups).

3. Preliminary Results

We conducted a brief experiment on Arduino Nano to assess NIZKP viability. We measured memory allocation, energy consumption, and computational processing time after 30 executions, focusing on key pair generation. In the experimental setup we employed the Arduino Nano equipped with a 32 KB Flash ROM, 2 KB SRAM memory, and an ATmega328 processor clocked at 16 MHz. Additionally, we used the HM-10 *Bluetooth Low Energy* (BLE) module, which is widely employed in IoT devices, as reported by [Dian et al. 2018]. This module enabled Arduino communication with an Android 10 smartphone featuring a Snapdragon 632 octa-core processor and 2GB RAM, which used the BetterTools[1] app for Arduino board interaction. All source code is open available at our supporting repository[2].

The mechanism deploy action produces a job output that provides information about the memory allocation. In turn, to measure the approximated energy consumption, we adopted the following equation (also widely adopted by [Chatzigiannakis et al. 2011, Ma et al. 2014, Moosavi et al. 2016, Li et al. 2017]):

$$E = V \cdot I \cdot t,$$

where:

- E is the consumption of energy in millijoules (mJ);
- V is the operating voltage in volts (V);
- I is the current in milliamperes (mA);
- t is the time in seconds of each operation.

According to the Arduino technical document[3], Arduino Nano consumes 19 mA at a voltage of 5V. Additionally, as mentioned before, a Bluetooth[4] BLE V4.0 HM-10 module was used for communication between the Arduino and the Smartphone. Therefore, when applied to the previous equation, we have:

$$\mathrm{E} = 5 \cdot (19 + 4.8) \cdot \mathrm{t},$$

where 19 mA is the current electric current of the Arduino Nano, and 4.8 mA refers to the electric current of the Bluetooth HM-10 module in active mode.

Figure 2 illustrates the behavior of the NIZKP during the key generation process, highlighting the energy consumption (in mJ) and computational processing time (in ms). This preliminary analysis of computational processing time revealed that the NIZKP required an average of 3739.07 ms, with a standard deviation of 3.86 ms. Regarding the

[1]Bluetooth Terminal eDebugger: `https://play.google.com/store/apps/details?id=com.e.debugger`

[2]Source code repository: `https://github.com/joe-sousa/nizkp_algorithm`

[3]Arduino documentation: `https://store.arduino.cc/usa/arduino-nano`

[4]Bluetooth module documentation: `https://seeeddoc.github.io/BLE_Bee/res/Bluetooth40_en.pdf`

energy consumption, we noticed an average of 514.12 mJ, with a standard deviation of 0.53 mJ. Lastly, we observed that NIZKP allocated 25832 bytes of Flash ROM, representing 84% of the available Flash memory space (30720 bytes). The NIZKP utilized 766 bytes of dynamic SRAM memory, accounting for 37% of the total available space (2048 bytes). We can conclude that NIZKP was successfully implemented and reached promising results, even considering the resource-constrained scenario of Arduino Nano.

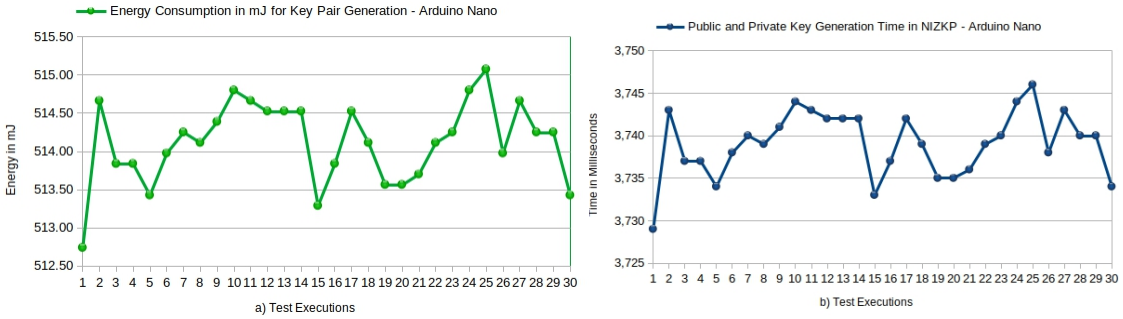

Figure 2. Time and Energy Estimation for NIZKP Key Pair Generation.

4. Final Remarks, Contributions for IS, and Next Steps

This ongoing research project aims to compare the NIZKP, HMAC, AES and RSA to determine the most efficient in the context of low-resource Internet of Things (IoT) in Industry 4.0. This research endeavor seeks to enhance the comprehension of authentication mechanisms in low-resource IoT devices, thus facilitating better decision-making processes in Information Systems (IS) settings. This perspective is also closely related to the challenge of "Full Interoperability: Challenges and Opportunities for Future Information Systems" which was discussed in I GranDSI-BR [Boscarioli et al. 2017].

More specifically, this paper aims to present the methodological scope to achieve this previous objective and discuss a preliminary experiment concerning the viability of deploying NIZKP on the Arduino Nano. Our next steps involve implementing the other authentication mechanisms to be compared with NIZKP, that is, HMAC, AES, and RSA. Subsequently, the results between the control and experimental groups will be assessed.

Acknowledgements

We thank the support of the Institutional Scientific Initiation Scholarship Program (PIBIC) from Federal University of Ceará (UFC) for funding this work.

References

Abomhara, M. and Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, pages 65–88.

Alnahari, W. and Quasim, M. T. (2021). Authentication of iot device and iot server using security key. In *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, pages 1–9. IEEE.

Baiyere, A., Topi, H., Venkatesh, V., and Donnellan, B. (2020). The internet of things (iot): A research agenda for information systems. *Communications of the Association for Information Systems*, 47.

Boscarioli, C., de Araujo, R. M., Maciel, R. S., Neto, V. V. G., Oquendo, F., Nakagawa, E. Y., Berrnardini, F. C., Viterbo, J., Vianna, D., Martins, C. B., et al. (2017). I grandsi-br: Grand research challenges in information systems in brazil 2016-2026.

Chatzigiannakis, I., Pyrgelis, A., Spirakis, P. G., and Stamatiou, Y. C. (2011). Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. In *2011 IEEE eighth international conference on mobile ad-hoc and sensor systems*, pages 715–720. IEEE.

Dian, F. J., Yousefi, A., and Lim, S. (2018). A practical study on bluetooth low energy (ble) throughput. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 768–771. IEEE.

Eldefrawy, M. H., Pereira, N., and Gidlund, M. (2018). Key distribution protocol for industrial internet of things without implicit certificates. *IEEE Internet of Things Journal*, 6(1):906–917.

Galla, L. K., Koganti, V. S., and Nuthalapati, N. (2016). Implementation of rsa. In *2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pages 81–87. IEEE.

Hung, C.-W. and Hsu, W.-T. (2018). Power consumption and calculation requirement analysis of aes for wsn iot. *Sensors*, 18(6):1675.

Li, F., Hong, J., and Omala, A. A. (2017). Efficient certificateless access control for industrial internet of things. *Future Generation Computer Systems*, 76:285–292.

Liu, Y., Ma, X., Shu, L., Hancke, G. P., and Abu-Mahfouz, A. M. (2020). From industry 4.0 to agriculture 4.0: Current status, enabling technologies, and research challenges. *IEEE Transactions on Industrial Informatics*, 17(6):4322–4334.

Lohiya, R. and Thakkar, A. (2020). Application domains, evaluation data sets, and research challenges of iot: A systematic review. *IEEE Internet of Things Journal*, 8(11):8774–8798.

Ma, C., Xue, K., and Hong, P. (2014). Distributed access control with adaptive privacy preserving property for wireless sensor networks. *Security and Communication Networks*, 7(4):759–773.

Madakam, S., Lake, V., Lake, V., Lake, V., et al. (2015). Internet of things (iot): A literature review. *Journal of Computer and Communications*, 3(05):164.

Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., and Isoaho, J. (2016). End-to-end security scheme for mobility enabled healthcare internet of things. *Future Generation Computer Systems*, 64:108–124.

Najjar, M. (2015). d-hmac—an improved hmac algorithm. *Int J Comput Sci Inf Secur*, 13(4):89.

Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., and Hassan, M. (2019). The internet of things (iot) and its application domains. *International Journal of Computer Applications*, 975(8887):182.

Puthiyidam, J. J., Joseph, S., and Bhushan, B. (2023). Enhanced authentication security for iot client nodes through t-ecdsa integrated into mqtt broker. *The Journal of Supercomputing*, pages 1–35.

Qin, Y., Sheng, Q. Z., Falkner, N. J., Dustdar, S., Wang, H., and Vasilakos, A. V. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, 64:137–153.

Roy, S. S., Puthal, D., Sharma, S., Mohanty, S. P., and Zomaya, A. Y. (2018). Building a sustainable internet of things: Energy-efficient routing using low-power sensors will meet the need. *IEEE Consumer Electronics Magazine*, 7(2):42–49.

Tomaz, A. E. B., Do Nascimento, J. C., Hafid, A. S., and De Souza, J. N. (2020). Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. *IEEE access*, 8:204441–204458.

Zhou, K., Liu, T., and Zhou, L. (2015). Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)*, pages 2147–2152. IEEE.