CHAPTER 1

INTRODUCTION

This chapter discusses the background, state of the art, problems, proposed research methods, and the importance of the study. This chapter consists of the subsequent subsections, specifically: (1) Rationale; (2) Theoretical Framework; (3) Conceptual Framework/Paradigm; (4) Statement of the problem; (5) Hypothesis; (6) Assumption; (7) Scope and Delimitation; and (8) Significance of the study

1.1 Rationale

The Internet of Things (IoT) is a technology that allows devices to connect with each other and/or to an edge network or even a cloud environment in order to process data using open-standard interoperable communication protocols [9, 14, 21, 47]. The use of remote devices to form IoT infrastructure has increased drastically. In 2025, it is estimated that the average usage of devices per person will reach 14.46, with the global IoT market expected to reach $1.567 billion [2, 33]. When implementing IoT technology, the aspect of data and information security stands out as a significant challenge. Numerous instances of IoT technology applications involve sensitive and personal data, or they may be unmanned remote devices that are vulnerable to physical attacks, such as gaining access to the device's internal memory, etc. It is imperative that only the original and authorized IoT devices can transmit data to maintain data privacy [40, 52]. Therefore, to establish secure communication as needed in the application of IoT technology, a secure, reliable, and scalable authentication mechanism is proposed.

The conventional approach of authentication mechanism has several drawback, since secrets are stored statically. Storing a static confidential key within non-volatile memory, like fuses or EEPROM, and employing cryptographic techniques such as digital signatures and encryption to verify a device's authenticity and safeguard sensitive data, can be both costly and challenging to securely handle the secret key. Non-volatile memory technologies are frequently susceptible to invasive attacks because secrets persist in digital form, and even battery-backed RAMs can be read after keys have been stored for an extended period [5, 6, 41]. To ensure a strong level of physical security, costly tamper-detection circuitry must safeguard the IC, requiring constant battery power for operation [41]. Utilizing secure hardware elements, such as Hardware Security Module (HSM) and Trusted Platform Module (TPM), is not a viable option since there are limited resources available in IoT devices (such as power and space available) [12].

PUF overcomes the conventional approach since it requires the key to be generated dynamically rather than being stored on the device, as the conventional approach did. A Physical Unclonable Function (PUF) is a mechanism that generates a unique response specific to a device by analyzing its inherent physical attributes, like particle diffusion and microscopic variations in silicon components [1, 4, 19, 25, 28, 37, 54, 56]. These device-specific physical traits are essentially impossible to replicate [23]. Even though the PUF response is generated dynamically and can act as a "biometric" of the device, there is still vulnerability to certain types of attacks. Deep learning techniques can be employed to breach the security of the PUFs [27], and signatures generated from two memory chips may exhibit highly correlated properties if they share the same set of specifications and originate from a similar manufacturing facility [51]. Moreover, invasive attacks, where the attacker acquires the device and gains access to the PUF functionality, further compound these vulnerabilities [12]. Therefore, optimization of the PUF's secret key (in this case, the PUF responses) is needed to improve system's security performance (such as decidability, randomness, and the confusion matrix covering the true/false rate), and an additional secret key is needed to minimize reliance solely on the PUF functionality as the secret key.

In [12], the use of an additional secret key as a second-factor authentication through the implementation of two-factor fuzzy commitment has been conducted, but still without the optimization process of the PUF's secret key thus the vulnerability level to PUF attacks remained the same. The PUF's secret key (PUF responses) are utilized as the internal secret key (also known as the internal noisy source), and the image from the external camera serves as the additional secret key (referred to as the external noisy source as the key originates from outside the IoT device). However, using a camera for surveillance is costly, power-consuming, and difficult to maintain especially if placed outside as a remote IoT device (for instance, with a blurry or dirty lens). Additionally, errors caused by obstacles, whether indoors or outdoors (e.g., people or animals obstructing the camera), are common. Therefore, high t-bits (ECC error capability) are necessary for key reproduction which will result in a high false acceptance rate (false positives). Furthermore, in previous research, there was also an overlap between the t-bits required to correct all genuine noisy sources and the t-bits needed to ensure that no corrected attacker noisy sources remained. Based on the conditions above that need to be improved, this research presents an IoT device based on PUF with an optimized PUF's secret key (PUF responses) to enhance system's security performance, along with dynamic environmental parameters (as a second factor authentication) using cheaper and easy-to-maintain sensors that has lower t-bits ECC error correction capabilities, thus reducing the likelihood of false positives regarding the secret key used.

1.2 Theoretical Framework

The previous work proposed by Dooho Choi et al. introducing a novel concept called two-factor fuzzy commitment [12]. The two-factor fuzzy commitment scheme employs dual sources of noise, originating both from within (PUF responses) and outside the IoT device (camera surveillance), in contrast to the traditional fuzzy extractor concept. In essence, when this mechanism is deployed on the IoT device, it effectively secures the device within its authorized operational environment. This is because the mechanism is incapable of extracting the correct key in an unauthorized location, even if an attacker gains access to the device's internal noisy data.

On the other hand, the previous work has not implemented optimization of PUF's secret key, thus the performance of PUFs covering decidability, randomness, and confusion matrix has not been improved. Additionally, the use of camera surveillance as a second factor authentication in two-factor fuzzy commitment has several shortcomings and difficulties as follows:

1. Using a camera for surveillance is costly. The camera used cannot be a low-resolution camera. A low-resolution camera doesn't have the capability to define the surrounding environment accurately & will lead to higher t-bits ECC error correction capability.

2. The possibility of errors due to obstacles is quite high, both indoors and outdoors (such as people or animals walking/standing in front of the camera, etc.). Thus, it requires high t-bits (ECC error capability) to reproduce the key during the reproduction phase. In previous work, they needed at least 20 bits to achieve a key recovery rate above 95

3. The attacker can be more easily to create a rogue image for second-factor authentication, since the IoT device implements high t-bits to correct the images during the reproduction phase. This can lead to false positives, as the system corrects the rogue image and assumes it is authentic as long as the "difference" between the rogue image and the authentic image remains below the error correction capability, i.e., the t-bits.

4. It is difficult to maintain the remote IoT device if it is using a camera for second-factor authentication due to factors such as the quality of the camera, including avoiding blurry or dirty lenses.

Hence, there is a requirement for an IoT device utilizing a PUF with optimized response datasets to improve the security performance. It should incorporate dynamic environmental parameters as a second factor authentication, employing cost-effective and easily

maintainable sensors with lower t-bits ECC error correction capabilities, thereby reducing the chances of false positives related to the secret key.

1.3 Conceptual Framework/Paradigm

The PUF's secret key (PUF responses) needs to be optimized to avoid attacks on PUF devices, as done in [12, 27, 51], at least by adding an additional layer of security so that the authenticity of PUF response data does not solely rely on the dynamic secret key generated by PUF. The optimization mentioned involves processing the bits of PUF responses that have a significant impact on the deterioration of security parameters quality.

Furthermore, due to the objective of utilizing second-factor authentication in the implementation of two-factor fuzzy commitment, in this case, being to demonstrate the authenticity of IoT devices in specific environmental conditions, it is necessary to use a dynamic second factor that does not result in a high t-bits during the reproduction phase. High t-bits imply the presence of many secret key bits that can be corrected, thus increasing the likelihood of false positives (rogue secret keys with bit error counts below the error correction capability may be considered authentic secret keys). The second factor used should also be inexpensive and easy to maintain, particularly when IoT devices are deployed remotely (unmanned IoT devices).

1.4 Statement of the Problem

Optimizing the PUF responses dataset as the secret key (in this case, the internal secret key or internal noisy source in two-factor fuzzy commitment) needs to be conducted to address various attacks on PUF while also reducing reliance on the authenticity of the secret key solely based on the dynamics of the secret key from the PUF device. Additionally, the use of the second factor in two-factor fuzzy commitment (in this case, the external secret key or external noisy source) that is dynamic should not result in high t-bits during the reproduction phase as it can increase the likelihood of false positives. The second factor used should also be inexpensive and easy to maintain, particularly if IoT devices are deployed remotely (unmanned).

1.5 Objective and Hypotheses

For a secure, reliable, and scalable IoT device authentication mechanism, it is imperative to incorporate two-factor fuzzy commitment with optimized internal PUF responses and dynamic external noisy sources with low-cost, easy-to-maintain, and low t-bits error correction capability during the reproduction phase. This approach enables the presence of an internal noisy source (i.e., PUF responses) that is robust (resilient against various

PUF attacks) due to optimization of the PUF response bits, while maintaining that the authenticity of IoT devices can only be achieved through specific environmental conditions (IoT devices can only be used in particular environments) through the implementation of dynamic external noisy sources.

The quantitative objective of this research is to enhance the quality of system performance parameters such as higher True Acceptance and Rejection rates, as well as lower false acceptance and rejection rates. Additionally, the decidability value, which determines whether two-factor noisy sources (comprising internal and external noisy sources) can be declared authentic or not, needs to be improved. This is achieved through various data processing schemes applied to bits of data, thus requiring the examination of randomness values in this study as well.

1.6 Assumption

The assumptions and constraints of this study include:

1. The length of PUF Responses is 128 bits. It should be noted that IoT devices tend to have limited compute resources; processing too many bits of data can overwhelm IoT devices. However, security quality must still be maintained.
2. The second factor used is related to environmental parameters.
3. To generate a genuine PUF dataset, this research uses Arty Z7: Zynq-7000 SoC Development Board
4. To generate an attacker/rogue PUF dataset, this research uses a Python algorithm with artificial noise level to create these datasets.

1.7 Scope and Delimitation

The primary focus of this research is on the data processing involving genuine/attacker PUF datasets as internal noisy sources, dynamic external noisy sources, and the implementation of two-factor fuzzy commitment. Security aspects will be evaluated through the confusion matrix, which includes False Acceptance Rate, False Rejection Rate, True Acceptance Rate, and True Rejection Rate. Additionally, the research will assess the Hamming distance between these processed datasets, their randomness, and the level of decidability.

1.8 Significance of the Study

This research enables the use of IoT devices in a secure and scalable manner, with generated cryptography that is unique, dynamic, and more robust through the optimization process of

the internal secret key and dynamic over time through the use of dynamic external secret keys that are low-cost, easy-to-maintain, and have low t-bits error correction capability during the reproduction phase, thus minimizing the occurrence of false positives.