Evolving Authentication Design Considerations for the Internet of Biometric Things (IoBT)

Nima Karimian, Paul A. Wortman, Fatemeh Tehranipoor
University of Connecticut
Electrical & Computer Engineering
371 Fairfield Way, Storrs, CT
nima,paw10003, f.tehrani@engr.uconn.edu

ABSTRACT

The Internet of Things (IoT) is a design implementation of embedded system design that connects a variety of devices, sensors, and physical objects to a larger connected network (e.g. the Internet) which requires human-to-human or human-to-computer interaction. While the IoT is expected to expand the user's connectivity and everyday convenience, there are serious security considerations that come into account when using the IoT for distributed authentication. Furthermore the incorporation of biometrics to IoT design brings about concerns of cost and implementing a 'user-friendly' design. In this paper, we focus on the use of electrocardiogram (ECG) signals to implement distributed biometrics authentication within an IoT system model. Our observations show that ECG biometrics are highly reliable, more secure, and easier to implement than other biometrics.

CCS Concepts

•**Security and privacy** → **Biometrics;** *Embedded systems security;* Hardware-based security protocols; •**Hardware** → **Bio-embedded electronics;** *Emerging interfaces;*

Keywords

Internet of Things (IoT), Biometrics, Authentication, Embedded Design, Security, ECG, Reliability, NIST Statistical Test Suite.

1. INTRODUCTION

IoT networks can be generalized as a set of distributed embedded systems communicating over some pre-determined communication channel(s). These channels exist not only in the expected types of communication (i.e. Ethernet, wireless, Bluetooth), but also in the less widely used network protocols (e.g. Zigbee, WiMax). As with any distributed system there are performance, optimization, and security constraints that must be taken into account from the early design stages that will later be implemented. There is a rise in the use and adaptation of IoT devices for scenarios such as: a means of authenticating users and customers, ensuring the condition of one's home appliances, keeping track of the location of family members and identifying the health of patients. With the constant expansion of IoT devices into everyday use for the purpose of simplifying the lives of humans, there comes an expansion of possible attack vectors and sources for vulnerabilities. For this reason, as the market for IoT/embedded devices grows, it is the responsibility of developers to take into account the security needs and privacy concerns of their users and customers. Unfortunately, as with any optimization problem, the constraints of the scenario, operation parameters and needs of the consumer will differ by device, situation and implementation.

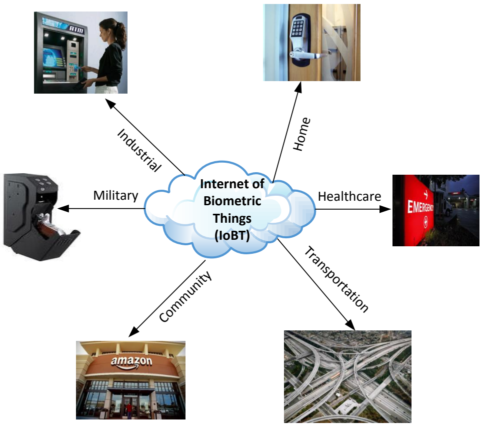


Figure 1: The Internet of Biometric Things (IoBT) Applications.

Different applications of IoT-centric usage or modeling can be found in the form of finger print authentication, vein recognition, smart gun implementations, smart door locks, and other forms of locality checking or two-factor authentication[1, 7, 24]. As Figure 1 illustrates the IoT, and by extension biometric implementations of the IoT model, are already in wide use. These common day implementations range from medical devices (such as heart monitors) to home security applications including smart door locks and window/door sensors. There are more obvious applications: for instance, traffic monitoring or remote sensor networks for determining weather patterns or spending habits of individuals. In some cases the IoT is being used to track a family's habits and personal information as a means of auditing the behavior of family members (e.g. children brushing teeth) [33]. Use of the Internet of Things has expanded into a variety of different markets, one of the more expansive fields being biomedical/biometric. Here we notice a combination of biometric authentication coupled with the augmentation of distributed, or cloud-computing, to form large networks of interconnected devices that can be used for real-time data

CODES/ISSS '16, October 01-07, 2016, Pittsburgh, PA, USA
© 2016 ACM. ISBN 978-1-4503-4483-8/16/10…$15.00
DOI: http://dx.doi.org/10.1145/2968456.2973748

exchange and integration [7]. This distributed computational power can further enhance two-factor authentication by merging larger access control mechanisms with locality information passed via an embedded, or IoT, device. As with any growing technology, especially when mixed into security authentication and policies, there are a variety of constraints and concerns that must be contemplated and tackled prior to its implementation and use.

One of the greater challenges of having widespread adoption of IoT devices is due to designers and developers either incorrectly implementing security, as discussed in Section 2.2, or a complete disregard to the importance of incorporating security before prototyping. The complexity of the security field is daunting, but even this should not deter research and implementation of new exciting expansions of IoT functionality and behavior [30, 25, 22, 35]. Neither does there seem to be a limit to the scenarios and utilization of embedded real-time systems. As the excitement and potential of IoT devices grows and more concrete implementations of new concepts and designs come forth, the need for convincing research into these applications, their security and reliability is a must.

Implementations of biometric-centric authentication can be seen in the military and public sectors with the development of devices such as "Identilock"[24], where fingerprint based authentication ensures that firearms can only be fired by an authorized user. This form of two-factor authentication generates the usual concern around reliability, the user's ability to depend on faithful implementation of the security design and implementation of any fail-safes desired (e.g. 'overrides' for a locked devices; a door key). With this surge of interest and early adaptation of biometric authentication and vigorous expansion of the 'Internet of Things', it is obvious that effort needs to be placed on the design considerations for implementing biometric authentication over a distributed network of embedded/IoT devices. In the case of "Identilock", one could couple ECG biometric data with fingerprint authentication to ensure that law enforcement do not use their weapons while under duress[4]. Foreseeable complications could include defining the difference between fear and anger. While the implementation is considered out of scope for this paper, with research this functionality could be expanded to allow for a biometric two-factor authentication in other scenarios as well. These forms of biometric authentication can be generalized as an other method for providing a password, or PIN, to a challenge-response pair. With this modeling in mind, one can see why biometrics/biometric authentication is more desirable, and also potentially more secure than traditional methods of access control. In this paper, we are using biometrics (mainly ECG and iris recognition) to make IoT devices more secure, robust, and user friendly.

Our main contributions can be summarized as follows:

1. Investigate two biometric modalities for the purpose of key generation. This required the evaluation and examination of generated keys based on uniqueness, reliability and key length.

2. Analysis of the keys generated using the two modalities, demonstrated that the ECG has better performance than the iris recognition in terms of the reliability, uniquess and key length. We were able to definitively show that ECG-based key generation is the more desirable methodology over the use of iris-based key generation.

3. Discussion of embedded real-time system implementation, security and adoptability. Background exploration of IoT devices, common complications and mistakes made in their implementation, and the further exacerbation due to the incorporation of security overhead to these already constrained systems.

4. Investigation of IoT architecture for adoptability of biometric authentication. Requiring study of the known limitations and capabilities of IoT peripherals to determine the most adventageous method for incorporating biometric authentication into exisiting systems while minimizing the need for alteration or redesign of current embedded devices.

5. Postualte use cases, implementation considerations, and ease of adoption for authentication via biometric readings. From alternate uses for biometric authentication to coupled implementation with other forms of biometric authentication to form a biometric two-factor authentication scheme. Future capabilities of ECG-based biometric readings are also speculation with alternative uses for the same collected data.

In the following, we first present the motivation and challenges that inspired our work in Section 2. In Section 3, we introduce the methodology used for generating keys from biometrics in terms of average key length, reliability, min-entropy, uniqueness and randomness. Section 4 shows the results of biometric key generation from ECG and iris databases along with evaluating the randomness of both modalities using the NIST statistical test. In Section 5 we illustrate how the ECG data can be incorporated into IoT devices along with consideration of security considerations brought about by implementation. We will discuss the merits of biometric authentication and its implementation in IoT devices in Section 6 and conclude the paper in Section 7.

2. MOTIVATION AND CHALLENGES

The exponential growth in the number of connected smart devices, and the resulting volumes of data, pose significant challenges for information security. Most cryptographic primitives rely on the ability to generate, store and retrieve unique 'keys'. These cryptographic keys (unencrypted) are used as an input to the known encryption engine to generate encrypted output that is used to authenticate the device or information. A shared cryptographic key enables strong authentication. Candidate sources for creating such a shared key include biometrics and physically unclonable functions (PUF) [36]. However, maintaining large databases of PUF challenge response pairs and dealing with PUF errors makes it difficult to use PUFs reliably [41]. The use of biometrics has been widely spread over the problems of identification, authentication, and key generation[12, 34, 27, 3, 5]. Most of the biometric authentication research is suffering from issues of universality, uniqueness, measurability, acceptability, and circumvention characteristics. In this paper, we introduce the use of a new biometric modality known as the electrocardiogram (ECG) signal. The ECG modality is permissible given that it addresses the problems encountered by other biometric authentication research. These heart signals can be found in virtually all living humans (Universality). The authentication capabilities of ECG signals for circumscribed groups of individuals has been shown (Uniqueness) [2]. ECG signals can be easily acquired using suitable devices (Measurability)[26]. Electrocardiogram modality has been shown to perform accurately for subsets of the population (Performance) [27],[28]. The "off the-person" approach has made use of ECG signals acceptable (Acceptability), and they are not easily spoofed as it depends on an internal body organ, the heart (Circumvention). It also has inherent real-time signs of liveliness, making it extremely difficult to steal and emulate a person's ECG signal.

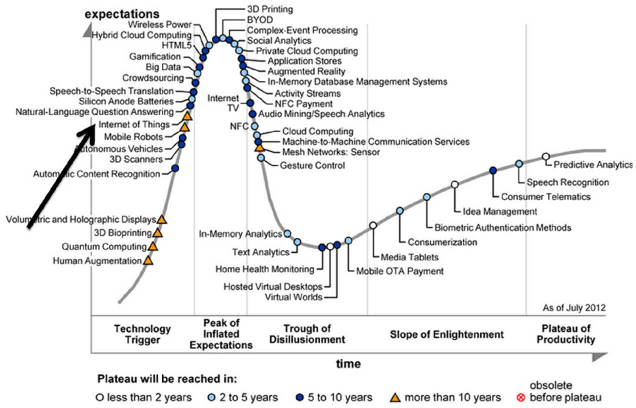


Figure 2: Gartner 2012 Hype Cycle of emerging technolgoies. Source: Gartner Inc. [23]

2.1 IoT Adoption and Expansion

The ‘Internet of Things’ and IoT devices have been on the rise as of late due to a shift towards more ‘cloud-centric’ models of interconnected devices performing actions or integrating with the everyday life of users. Over time the hype and expectations of IoT technology have changed, but the overall desire to have a more vibrant and interconnected ‘smart’ Internet still runs deep in the human conciousness[20]. As one can see in the Figure 2, the Internet of Things will continue to grow and develop, all while influencing its domain by providing new evolving data and the required computational resources for allowing users and developers to create revolutionary applications[20]. With this expansion of use cases and implementations comes a requirement to examine the security needs and specifications that can secure the new flux of information and data from prying eyes or malicious action.

2.2 IoT Design & Security Considerations

IoT is generally a large number of wireless devices that form a network. The resulting ‘Internet of Things’ is as powerful as it is susceptible to the same vulnerabilities and security flaws as any computer system or distributed system of computers. Securing any stored data, ensuring access control to sensitive or critical areas of function, encrypting communications channels and authenticating new/connected devices are all aspects of IoT security that must be taken into consideration when designing everything from a single IoT device to a distributed network of IoT devices. Security considerations for IoT devices are the same as those required for distributed systems or embedded devices. One must secure not only the information being interacted with on an internal level, but also ensure that any data/information exported by the device must maintain a level of security assurance desired by the developer and user. Work by West et. al. [40] has taken an in-depth analysis of the complications and errors that occur when security is implemented in fitness tracking IoT devices, along with a detailed postulation on how to suitably implement security policies and principles in an all-encompassing method.

Common erroneous implementations of security lead to issues ranging from denial of service vulnerabilities, falsification of data (both local and remote users), stealing or abuse of sensitive information, compromise of device integrity, or as simple as incorrect handling of shared data leading to sensitive information being leaked. A developer’s focus can be placed at a variety of abstractions, all with the intention of making a device, or larger system, more secure and trustworthy. Beyond the security concerns, embedded systems have greater constraints in system design then other computer systems. Being an embedded system, the non-security considerations boil down to power consumption, total PCB space, heat distribution, production costs, and component operation conditions. All of these different aspects play into the constraints and optimization of designing any secure embedded/IoT device.

3. INTERNET OF BIOMETRIC THINGS AUTHENTICATION

3.1 Biometrics in IoT

Biometric authentication, identification and key generation systems have assumed increasing importance in recent years. There are two types of biometric methods that can be categorized into internal and external physiological traits of humans. Each of the biometric modalities, including fingerprint based and iris based approaches, exhibits particular strengths and weaknesses. Fingerprints are very popular due to their low-cost implementation and well-developed feature extraction approaches. Iris identification is acclaimed for its high-level security, providing unique features even for identical twins. Even though these kind of biometrics are common, they are easy for attackers to access and are not robust against cloning. For instance, our fingers are involved in many daily tasks such as touching keyboards and doorknobs and can be easily replicated to bypass biometric systems. Iris systems are susceptible to being spoofed by printed photos. They are also expensive to implement. Electrocardiogram (ECG), Phonocardiogram (PCG), and Photoplethysmogram (PPG) are cardiovascular biometrics that are emerging as interesting choices for biometric systems that are internal physiological signals. Based on [31], bioelectrical signals recorded from the heart (electrocardiography, ECG) are distinctive enough for each individual person to be used for biometric applications, with the additional bonus of being inherently difficult, though not impossible, to forge. Also, they can be measured using low cost devices. Unlike other biometric systems, ECG signals can be monitored for prolonged periods of time: for example to continuously authenticate the user of a protected device after initial authentication. The Apple Watch applies the same principle of continuous monitoring, requiring the user to authenticate their identity with a password when the watch is strapped to their wrist, but then monitoring for constant heartbeat to avoid the need for further authentication. As additional security, once there is an interruption in the hearbeat detected by the watch, the watch locks itself down.

For the proposed key generation and authentication methodology there should be a requirement of two phases for implemented use: an enrollment phase where a user registers their ECG signal to generate keys, and an authentication phase where user provided data generates a new key that is compared to previous stored keys. Section 5 shows implementation of these phases for a postulated IoT device.

3.2 Biometric Key Generation

Frankly speaking, biometrics are suffering from different sources which are correlations to the original signal. For instance, the biological signal frequencies slightly overlap each other and can not be separated very well. Usually, the ECG signal suffers from different types of noises such as Electromyography (EMG), motion artifacts and power line interface. Therefore, for getting an almost clean signal, a pre-processing step is necessary that includes using a low and a high pass filter. However, this can generate errors with key generation. In order to overcome this limitation, we have considered a statistical approach to decline the intra-subject variation. It is desirable for biometric key generation systems to have maximal variability between subjects but minimal variability within a subject's variability. To deal with this, first of all the ECG signal is processed to remove artifacts. Then the feature extraction methods are applied for all of the population.

1) Pre-processing:

ECG: In this paper, we have employed 4^{th} Butterworth band pass filter with cutoff frequency 1Hz-40Hz to eliminate various kinds of noise in ECG signals based on empirical results. After filtering, R peak detection is generally required to segment individual heart beats and analyze the ECG signal. In this paper, we use the R peak detection algorithm proposed by Pan-Tompkins [29]. Then, we consider a fixed window by taking an identified R peak as a reference to segment the ECG signal in terms of the R–R interval (RR). ECG feature extraction has been applied to these segments. The discrete wavelet transform is a popular technique for time and frequency analysis. Since the ECG signal is quasi-stationary, we have employed the wavelet transform as a feature extraction technique.

Iris: An iris recognition system like ECG authentication typically consists of iris preprocessing and feature extraction. After localization, segmentation, and normalization of the iris data [11] , Gabor wavelet filter which is time-frequency transform, has been used as a feature extraction [10]. Since by changing the parameters of Gabor filter, the result has been changed, we have tried to consider an optimal one. In this work, we have only employed phase information for feature extraction.

2) Background PDF: The feature elements from the same location are extracted from the population and normalized into a standard normal distribution. Note that if a feature is determined as non-Gaussian, it is removed from investigation. The normalized probability density functions (PDF) of the population and subjects are illustrated in Figure 3.

3) Bit extraction: This module aims to transform the real valued features into a binary string of various lengths. The number of bits are dependent on the parameters and statistics that have been defined. A key will be selected if the standard deviation of the feature within the subject is close to zero and if across subjects it is large enough. Our approach for quantizing features to two bits is most clearly illustrated in Figure 3. The population probability density function of a feature is shown in blue. Statistical methods are applied onto each feature to determine boundaries to quantize the feature into one or more key bits. We have several input parameters which can be used to trade off reliability as well as output parameters which will be used to select "reliable" features. Note that all our parameters are illustrated on the left side of the PDF, in Figure 3, but the right side will have similar parameters due to symmetry of the zero-mean normal distribution.

In our approach, a feature space is partitioned into 2^n equal-width intervals with n denoting the intended number of bits to be allocated. This partitioning is applied on the user PDF. The thresholds are determined for optimal reliability for every given ECG feature in the space. The margin m determines the range of values in which we would consider the feature as reliable (based on noise statistics).

The boundaries ($Thr1$, $Thr2$) are calculated based on equal-width interval partitioning. After determination of the boundaries, the users can be enrolled. Because of variability within the subjects some features might be reliable for some subjects but unreliable for others. Therefore, our approach will only select reliable features from each individual. Then the information of the reliable features of each user will be stored in the helper data during the enrollment phase. In the authentication phase, the produced thresholds and helper data will be applicable. Based on proposed work, if the feature can meet the boundary that has been defined earlier, then it can be selected as a component key otherwise will be discarded. In [21], and [18], ECG for biometric key generation and key obfuscation have been investigated. But their approaches are based on the optimization of the boundary based on the standard deviation from entire subjects. Note that, based on [21], we can generate high reliable keys, but the key length will be reduced. But based on our approaches, the number of key that can be generated is more than their approaches. Since, we have some error in the reliability, we can apply Wei's technique [41], to increase the reliability.

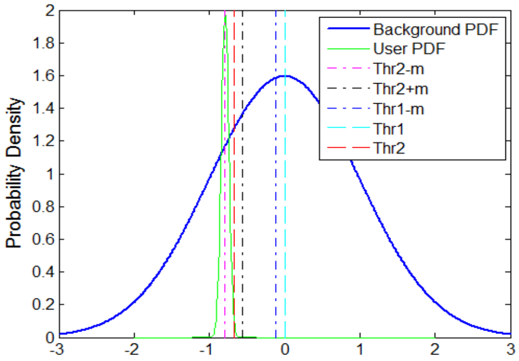


Figure 3: Illustration of the quantization scenario on a 2-bits.

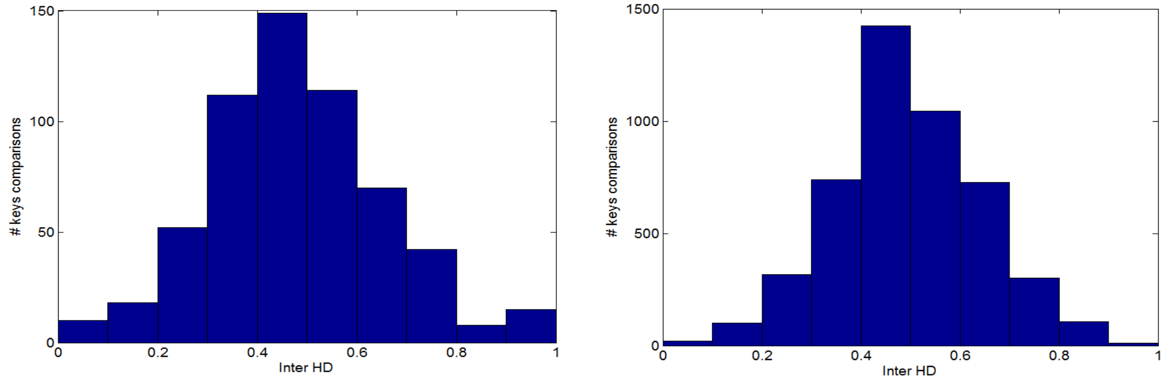
4. PERFORMANCE OF BIOMETRICS KEY GENERATION

In this section, we evaluate the security measurement of reliability and min-entropy of the keys generated from ECG signals. To investigate the reliability of the ECG recognition systems for personal authentication with smart door locks, we extract the keys at different times from the same person to represent how the keys are robust. Higher reliability corresponds to better agreement of the keys and small intra-class variation. To prove that the keys are random we considered min-entropy. Large entropy indicates excellent distinction among the keys generated by different people and how the keys are robust against an attacker. If the min-entropy value is close to 1 that means it has good quality as a key. We present the results in Table 1. Iris recognition is another biometric modality for its high identification accuracy. We apply the same algorithm with the same parameters on iris features as well to compare its performance with ECG. The iris results are shown in the last column of Table 1. Comparing the two biometrics modalities on average, ECG provides both the longest key, reliability, and highest 1-bit entropy while iris-based generation exhibits less effective results. As shown in Table 1, we achieved 727 as the average key length for normal ECG signals: roughly 200 bits more than produced by the iris modality. We have used freely available databases for two biometric modalities, the PTB diagnostic database [16] and iris database [8] to test the authentication process.

4.1 Biometric Data Randomness

4.1.1 Distributed Uniqueness Analysis

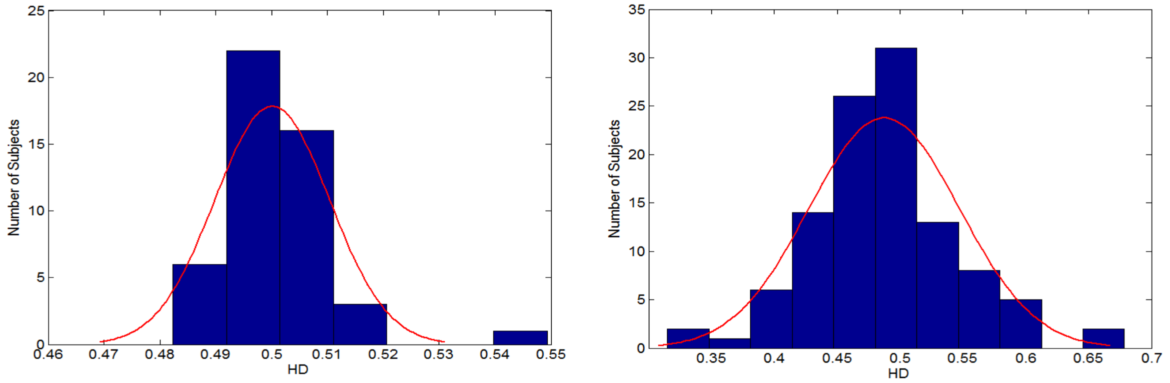
For authentication purposes, biometric keys should be as unique



(a)

(b)

Figure 4: Inter Hamming Distance distribution of key cross the subjects for (a) normal ECG signal and for (b) iris.



(a)

(b)

Figure 5: Histograms of intra Hamming Distance for (a) normal ECG signal and (b) iris.

Table 1: Reliability and Min-entropy Result based on Biometric Key Generation.

Biometric modality		Normal ECG	Iris
Reliability	Average	98.2	95.8
	Minimal	94.7	91.1
	Maximal	99.9	98.3
Entropy	Average	0.9810	0.855
	Minimal	0.864	0.546
	Maximal	1	0.997
Average Key bits		727	538

as possible. To quantify the uniqueness of keys, we compute the inter Hamming Distance (HD) by calculating the fractional Hamming Distance between the keys obtained from different subjects. For high uniqueness, it is desirable to have an inter Hamming Distance close to 50%, which means that half of the subjects keys are different. It also means that there is a low correlation between keys from different subjects, which makes predicting the keys' behavior more difficult. Figure 4 shows the distribution of inter Hamming Distance of key generation from ECG and iris modalities, respectively. The horizontal axis represents the percentage of bits differing across the subjects, and the vertical axis represents the number of keys compared corresponding to a Hamming Distance. Note that, althought the nth key has been generated from subject x it might be achieved from a different feature location of subject y. Therefore the way of calculating inter Hamming Distance can be different. In fact, we can arrange the keys from each subject to reach the ideal inter Hamming Distance. Calculation of the inter Hamming Distances can be further optimized, but for the purpose of this work we examine a scenario with complete lack of optimization.

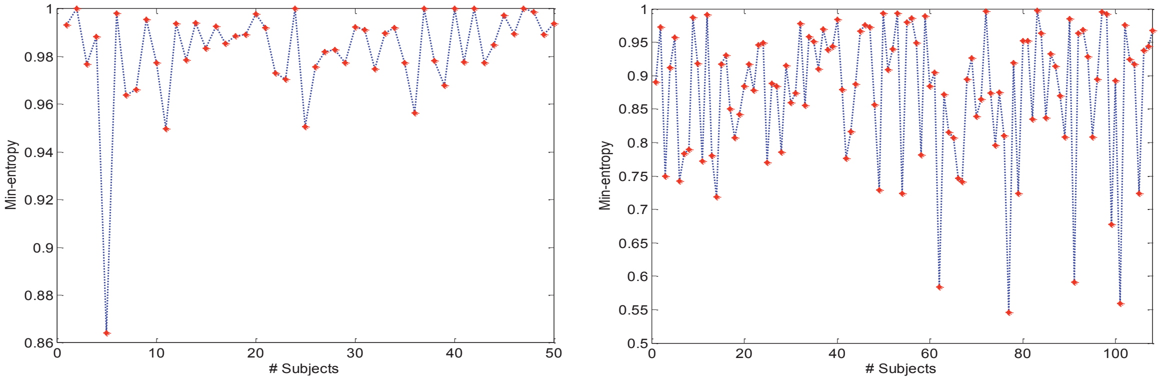
4.1.2 Individual Uniqueness Analysis

To measure the individual uniqueness of keys, we calculated the min-entropy of ECG keys for each subject. The min-entropy should be large enough to guarantee resistance against attacks. Consider n subjects, with each subject having k keys; k is variable. To estimate the min-entropy, we determine the fractional Hamming Weight of key k denoted HW(k) over all subject keys. HW(k) provides an estimate of the probability of key k to be 1. Let p_{max} denote the most likely outcome of key k as follows:

$$p_{max} = max\{HW(k), 1-HW(k)\} \tag{1}$$

$$H_{min} = \frac{1}{m}\sum_{k=1}^{m} -\log_2(p_{max}(k)) \tag{2}$$

Where the H_{min} is defined as min-entropy. The min-entropy is used as the measure of the strength of the key. In fact, if the entropy is close to the ideal value, which is 1,it shows that the adversary has a small chance of guessing the correct key on the first try. Figure 6 illustrates the trace of min-entropy for the ECG and iris keys. As can be seen, the min-entropy of the ECG signal for all subjects is



(a)

(b)

Figure 6: Plots of illustrating the min-entropy traces for each subject for (a) normal ECG signal and for (b) iris.

close to the ideal case (i.e. 1). The iris min-entropy is smaller than the ECG result, as shown in Figure 6. In addition, Figure 5 depicts the intra Hamming Distance for both ECG and iris data. In this context intra Hamming Distance is defined as the uniqueness of the bits generated for a single key for each subject; desiring a value near 0.5. When examining reliability, one would traditionally want an intra Hamming Distance of 0. As Figure 5 shows, the intra Hamming Distances of the ECG signal are very close to 0.5, while the standard deviation of the iris intra Hamming Distance is larger than that of the ECG data. The standard deviation of the ECG intra Hamming Distance is noticeably smaller than that of the iris.

4.1.3 NIST Test Results Analysis

As mentioned earlier, since electrocardiogram (ECG) signals are different from person to person, it can be used as a tool for biometric recognition. However, data extracted from ECG signals needs to have high quality randomness that results in a widely expanded key space, making it an ideal key generator for personalized data encryption [9]. For evaluating the randomness of ECG signals, we can apply NIST tests to the data. The NIST Test Suite (NTS) is a statistical package consisting of different types of tests to evaluate the randomness of binary sequences. Each statistical test is employed to calculate a p-value that shows the randomness of the given sequences based on that test. If a p-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A p-value >= 0.01 (normally 1%) means that sequence would be considered to be random with a confidence of 99% [32] [37]. Table 2 shows the results of 15 performed NIST tests of ECG and iris data, and since all test values are greater than 0.01, this indicates that the measurements pass the requirements for randomness. In table 2, the first column indicates the battery of tests that are incorporated in the NIST test, the second column displays the results of applying the ECG keys to the NIST test, the third column shows the results pertaining to iris keys being applied to the NIST test, and the fourth column indicates both ECG and iris passing the NIST tests. For most of the tests the values are very close to 1, which is the ideal case. At a first glance, the results of ECG and iris NIST tests show that either could pass the test, but the p-values indicate that the results of the ECG test are far more random than those of the iris. As an example the 'Approximate Entropy' p-value for ECG is 0.9152 while the iris p-value, for the same test, is only 0.7047. This distinction means that using an ECG signal for key generation is more adventageous because the produced key has a higher chance of being more random.

Table 2: NIST Statistical Tests Suite results for the Randomness Tests of ECG Signals and Iris Images.

NIST Tests	P-value-ECG	P-value-Iris	Status
Frequency	0.9981	0.8523	passed
Block Frequency	0.9977	0.8237	passed
Runs	0.8339	0.7532	passed
Longest Run	0.6671	0.4127	passed
Cumulative Sums	0.9820	0.7021	passed
Rank	0.7881	0.6914	passed
FFT	0.6942	0.4967	passed
Linear Complexity	0.9336	0.7469	passed
Overlapping Template	0.9754	0.8407	passed
Non Overlapping Template	0.9316	0.6571	passed
Approximate Entropy	0.9152	0.7047	passed
Universal Statistical Test	0.6537	0.4813	passed
Random Excursions Variant	0.6239	0.5687	passed
Random Excursions	0.7892	0.6023	passed
Serial	0.8659	0.5638	passed

5. HEART TO DEVICE AUTHENTICATION

Our solution for IoT is a system called heart-to-device (H2D) authentication. H2D is a simple access control for a smart door lock that a person can use any fitness tracking IoT device, such as 'nymi' [26], to access. To do so, first, all the subjects need to be enrolled. The enrollment phase contains biometric feature extraction, feature selection and finally the information of the helper data; as shown in Figure 7. The helper data contains the number of bits for each feature that can be quantized, the parameters of the boundaries, margin and the index of the features used for a given user. During authentication, an enrolled user supplies an ECG signal to the biometric system. The signal is preprocessed and features are extracted. The helper data is used to select the reliable features and quantize them to form the key. The key can be used to authenticate the individual by comparing it to a template. In a general case, the hardware requirements for a biometric authentication device would be the same, if not similar, to that of any standard 'smart' authentication device. The generated key could be stored in some temporary memory that could then be used for encryption or for the creation of a generated user identification certificate. This information would then be generated using the ECG data sent to the authenticating IoT device, which in turn would use this information to perform access control. H2D only allows a system to operate when the correct biometric is presented, thereby protecting it against unauthorized access, as shown in Figure 7.

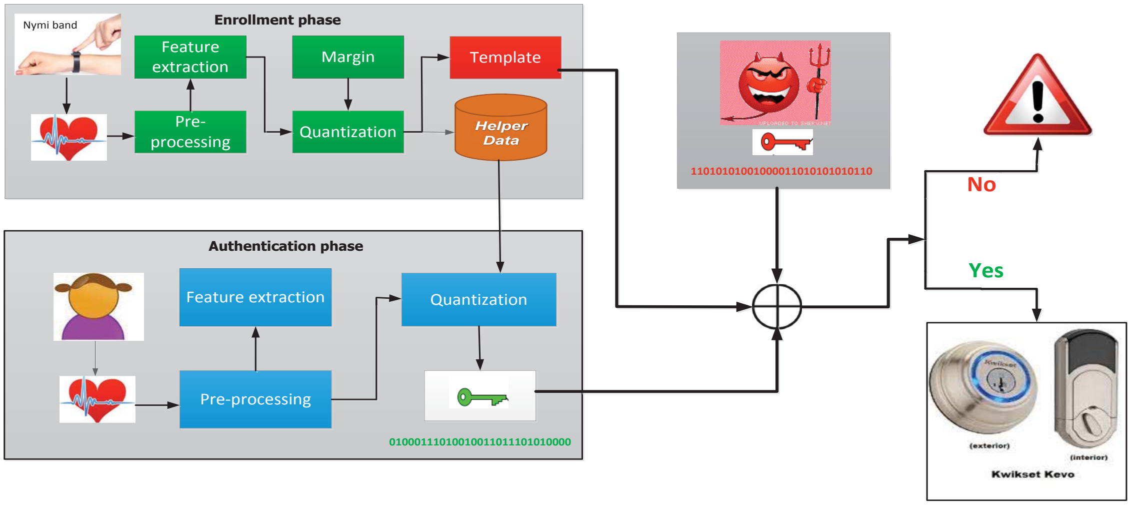


Figure 7: Schematic for key generation procedure.

Throughout the adoptation and implementation of the IoT model over the past few years there have been a string of recent attacks on IoT device authentication [39, 14, 38, 42, 17, 6]; for example, attacks on smart door locks. In addition to this work, it has been shown that other forms of biometric authentication (e.g. fingerprint authentication) can be easily reproduced/replicated. For these reasons, this work proposes a more effective and realiable method for implementing biometric authentication using current, standard IoT devices.

5.1 Architecture Hypothesis: IoT Device

As mentioned before, the concepts of an Internet of Biometric Things (IoBT) can be used in a wide variety of embedded applications that are connected to the Internet. Here, we specifically describe the architecture of an IoT device (Kwikset Kevo Smart Door Lock) in detail to show that it is a very suitable device (embedded system) to handle biometric authentication to become a more secure and reliable system. As shown in Figure 8, a generalized architecture of a 'smart' door lock consists of a microcontroller that contains a core processor, memory as embedded storage and input/output peripherals. The user input comes either from biometric readings (fingerprint, iris, ECG signals, etc) that are shown in Figure 8, digit codes for use with the keypad (passwords), or some other form of wireless communication of data (e.g. Bluetooth, Zigbee, WiMax). The lock mechanism is the common element of any door lock. The wireless communication of the Kwikset door lock can vary depending on user needs. In one variation of Kwikset's smart door locks, it was found that the wireless communication module, as seen in the right half of Figure 8, used the Zigbee protocol to interact with users. Another door lock variation replaced the Zigbee communication submodule with a Bluetooth variation. The advantage of this modular behavior is that regardless of the communication protocol used, a developer only has to create a new submodule rather than an entire PCB. This submodule connects to the larger door lock PCB through a communication channel (serial, I2C, etc.) that allows for exchange of data between the wireless antenna and the mixed signal microprocessor (16bit RISC). The processor itself contains embedded flash memory. This separation of functional components and those responsible for 'external communcation' shows the inherent design for resilience and adaptability as the needs and requirements of the smart door lock change over time. The left half of Figure 8 shows a simplified diagram example of Kwikset's door lock architecture and is meant as an easy to follow guide for continuing our discussion on the advantages of IoBT implementation.

Further investigation of the device's hardware revealed that the Zigbee protocol was used for communicating with the smart door lock device for an exchange of a traditional password/PIN. Surprisingly, there was no acknowledgement message sent back to the user interaction device confirming reception of the correct password/PIN. Upon realizing that no confirmation response was being transmitted by the smart door lock, we were able to determine that the authorized password/PIN combinations were stored locally on the door lock using the embedded storage. By no means is this the only implementation that can function for a door lock device; it is equally possible to have the door lock communicate with a remote database server for authentication or authorization needs. Through our examination of a smart door lock's architecture we have proposed that embedded devices have the opportunity of being more secure even in applications that are very crucial; home security devices, military applications, healthcare, etc. This does not mean that the other embedded devices are not eligible being used in IoBT concepts. As illustrated, although a subset of IoT devices may have been more advantageously designed for alteration, the design space for embedded real-time devices is vast and can easily be explored to produce a greater swath of modular IoT peripherals. We foresee a larger user adoptation of biometric authentication across a plethora of private and public sector implementations of IoT methodology.

5.2 Security Thoughts of ECG Biometric Results

As can be seen from Table 1, the normal ECG can generate a key with length approximately one and a third times greater than that of the iris reading. At these lengths, the normal ECG reading has potential for cryptographic communications or could be used as a 'password' for users to unlock some encrypted certificate or private key encrypted files. Either purpose used in conjunction with key stretching has a larger set of potential uses. By using simple ECG reading devices (e.g. 'fitbit' or 'nymi' devices [26][15]) it could be possible to perform a key exchange authentication with

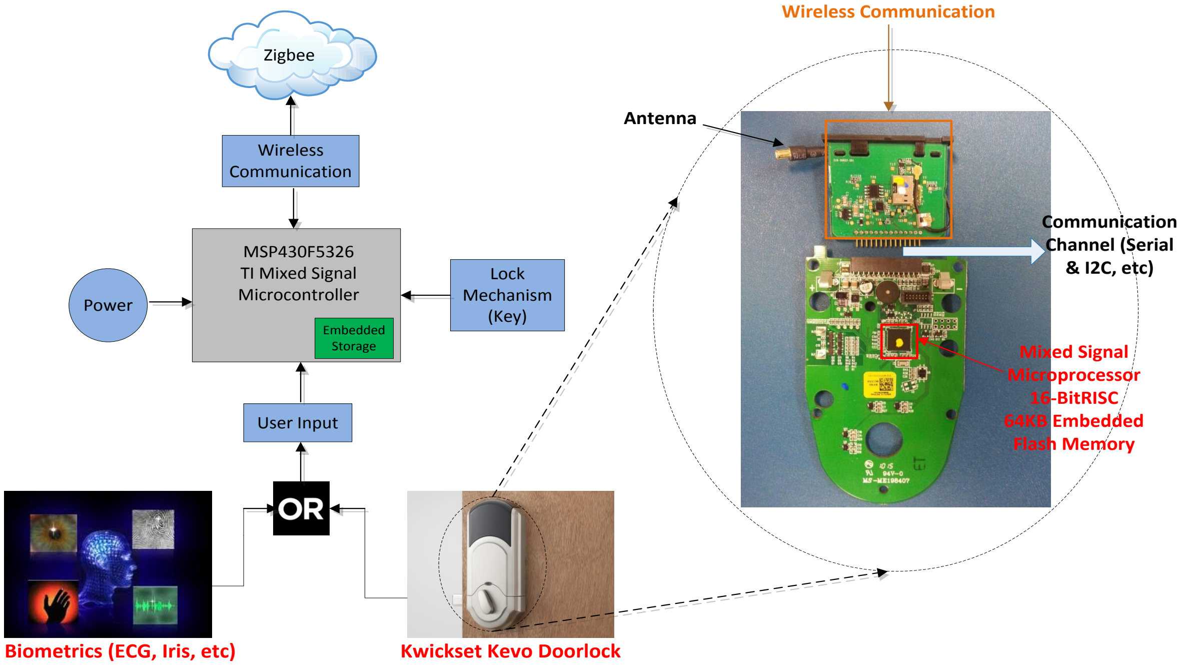

Zigbee
Wireless Communication
MSP430F5326 TI Mixed Signal Microcontroller
Embedded Storage
Power
Lock Mechanism (Key)
User Input
OR
Biometrics (ECG, Iris, etc)
Kwickset Kevo Doorlock
Wireless Communication
Antenna
Communication Channel (Serial & I2C, etc)
Mixed Signal Microprocessor
16-BitRISC
64KB Embedded Flash Memory

Figure 8: Illustration of additional authentication methods to existing smart lock model (Kwikset Kevo).

any IoT device that requires authentication to access or use. To help account for security concerns, one could have the 'fitbit'/'nymi' store the biometric readings in volatile memory that gets powered down/cleared whenever it detects being removed from the current user. This could allow for safe exchange of the 'biometric authentication device' between users without fear of having one user impersonate any other user.

One could also implement a similar concept to the authentication method proposed by Balfanz et. al. to implement 'location-limited' channels to exchange identifying information that can be used to authenticate over a larger wireless network, [13] assuming that these biometric IoT devices are seen through the lens of peer-to-peer adhoc interactions. However, further investigation of that implementation is seen as out of scope for this paper. Extensive research, work and effort has been placed in creating more secure variations of common 'secure communication protocols'. Biometrics can eventually reach that same level of interest but they must first be shown to be reliable and random enough before the same amount of time and effort can be spent. It is our belief that the results show that biometric authentication would make an ideal case for extended research and general implementation for this variety of IoT technology.

6. DISCUSSION

Whenever one begins to research the field of biometric authentication there are a plethora of concerns and conditions that needs to be examined, evaluated and validated. As always, there are concerns about the security of information gathered. Biometrics are a known to be a tricky method for authentication because should the personal 'key' be leaked (and/or reproducible by others) than it is very difficult, or even impossible, to change one's biological make-up (e.g. iris, heart, fingerprints). It would be possible to repurpose a 'fitbit' or 'nymi' device for reading and transmitting the ECG signal reading. Our proposed method for biometric authentication is assumed to be no less secure than the ID card model and does not introduce more complexity to the issues already seen with fitness tracking IoT devices [40]. In the case of having one's ID card stolen it would be possible to lift the personal identifiable information (PII) from the ID, where when using our Internet of Biometric Things (IoBT) authentication methodology if the fitness tracking device is stolen or lost, there is minimal possibility that information can be exfiltrated from the device. In this manner it would not require that the device store any of the biometric data, but that it simply act as a 'stupid transport layer' which would only transmit the ECG readings to whatever device requires the biometric authentication. The advantage of this methodology is that a user can pass the device to other people/users and each person has their own ECG readings. In this way it would not be possible to impersonate another human since the device would only transmit the current wearer's ECG signal. This would be an improvement on the current ID card model where each user has their own identification card and can not exchange that card with another user without effectively 'losing' their identity. While there is the concern that a malicious user may be able to cause the 'fitbit'/'nymi' device to erroneously transmit biometric information, this is no different than the current attack scenarios that an identification card may also posses and as such is seen outside the scope of this paper.

The cost of such a system implementation is always a concern. Should the cost of operating such a system outweigh the benefits of implementation, the adoptability will suffer. In addition, issues of leaked data and other possible complications can lead to zero community interest in the proposed biometric authentication scheme. Even the IoT device purposed for exchanging ECG data for key generation must be safe and secure for use. From a white paper released by Nymi Inc. [19], one can see that this IoT device places the utmost importance on protecting the passed ECG information from an active user. The cost for using an IoT device includes power used for operation, how often validation/authentication needs to occur, and even what should occur if a generated key is stolen. The benefit of using a device such as the 'nymi' is that the construction of the IoT already accounts for the majority of operational cost concerns. In the scenario that a key is stolen, a user would only have to wait until a new feature extraction method is implemented by the proposed biometric authentication scheme. Due to the manner by which keys are generated from user ECG data, if the method for feature extraction is altered, each user's generated key will change but will still be deterministic based on the original ECG signal provided by a given user. In that respect, there is the concern that an attacker who is able to successfully double the size of enrolled individuals may be able to alter the generated keys in a malicious manner, but the change in how features are extracted from raw ECG data would once again cause a shift in the generated keys, requiring an attacker to obtain a reproducible ECG signal from each user to impersonate them.

An added advantage to using this system is seen in the scenario: what to do if biometrics have changed? (e.g. heart murmur). From a security perspective, the first concern is whether or not the protected system (e.g. what requires authentication for access) still should be accessible if a failure occurs in the biometric authentication mechanism. One could implement a "regular" password as "backup" should a form of failure occur in the biometric authentication system. This could potentially leave a vector of attack for a malicious user, but no more than any other current authentication mechanism. On a more positive note, should there be an issue with biometric authentication (originating from the user and not the implementation of security) then this could be a sign that something is biologically wrong with the given user. Thus, the ECG reading device can double as heart monitoring for users. The line of thinking for the user could be "If the door does not open, then perhaps the user needs to see a doctor". In a more beneficial system it would be possible to "cloud link" problematic readings to the nearest doctor/hospital so that medical professionals can identify these problematic conditions before they become more harmful. Lastly, it would also be possible to automate a watchdog process to monitor the ECG readings for unexpected/harmful readings that then could send those specfic "windows of data" to medical professionals allowing for a cut down on time spent looking at the larger mass of ECG data.

7. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented the Internet of Biometric Things (IoBT) that can act as an interface between humans and devices for authentication purposes. Through thorough comparision of biometrics (e.g. ECG and iris), we have analyzed these reading based on their key generation properties (reliability, key length, min-entropy, uniqueness) in order to determine the most promising candidate for biometric authentication using IoT devices. Based on our observation, among all biometric sources, Electrocardiogram (ECG) has the most advantages in comparison to other sources in terms of security, convenience and even implementation. Furthermore, NIST test results comparison between the electrocardiogram and iris readings demonstrate the randomness of the ECG generated key data as being the more desirable of the two. We also examined the architecture of an IoT device (Kwikset Kevo door lock) and discussed on how to add the biometric features to the IoT device's architecture, with emphasis on the ease by which existing IoT devices could adopt new features, properties, or implementations. The purpose of this investigation was to prove that embedded real-time systems (IoT devices) are more than capable of integrating ECG-based biometric authentication.

In the future, we seek to implement the use of ECG signals as a strong biometric method to both secure IoT devices and to later unlock them. Future work includes: development and design of new submodules for different communication protocols and methods (e.g. wireless vs. wired), thorough examination of overhead costs from both a hardware and software standpoint, implementation of the biometric authentication within the architecture of an exsiting door lock, and distributed implementation of a biometric authentication service for the purpose of evaluating the effectiveness at scale of using ECG-based biometric authentication. Our hope is to see a more secure, reliable, and convenient implementation of biometric authentication become widely adopted as the 'Internet of Things' continues to grow and evolve.

8. REFERENCES

[1] The design of teaching management system in universities based on biometrics identification and the internet of things technology.

[2] ECG uniquness. http://www.physionet.org/pn3/ecgiddb/biometric.shtml, 2016.

[3] F. Agrafioti and D. Hatzinakos. Ecg biometric analysis in cardiac irregularity conditions. *Signal, Image and Video Processing*, 3(4):329–343, 2009.

[4] F. Agrafioti, D. Hatzinakos, and A. K. Anderson. Ecg pattern analysis for emotion detection. *Affective Computing, IEEE Transactions on*, 3(1):102–115, 2012.

[5] L. Biel, O. Pettersson, L. Philipson, and P. Wide. Ecg analysis: a new approach in human identification. *Instrumentation and Measurement, IEEE Transactions on*, 50(3):808–812, 2001.

[6] J. Brodkin. Comcast security flaw could help burglars break into homes undetected. http://arstechnica.com/security/2016/01/comcast-security/, 2016.

[7] S. S. Burak Kantarci, Melike Erol-Kantarci. Towards secure cloud-centric internet of biometric things. In *Cloud Networking (CloudNet), 2015 IEEE 4th International Conference on*, 2015.

[8] Casia. Irisv1. http://biometrics.idealtest.org, 2016.

[9] C.-K. Chen, C.-L. Lin, C.-T. Chiang, and S.-L. Lin. Personalized information encryption using {ECG} signals with chaotic functions. *Information Sciences*, 193:125 – 140, 2012.

[10] J. Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21–30, 2004.

[11] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11):1148–1161, 1993.

[12] K. Delac and M. Grgic. A survey of biometric recognition methods. In *Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium*, pages 184–193. IEEE, 2004.

[13] P. S. Dirk Balfanz, D. K. Smetters and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks, 2002, Book.

[14] P. Ducklin. IoT security in the spotlight at PrivacyCon. https://nakedsecurity.sophos.com/2016/01/22/iot-security-in-the-spotlight-at-privacycon/, 2016.

[15] Fitbit. Fitbit Website. https://www.fitbit.com/, 2016.

[16] A. L. e. a. Goldberger. Physiobank, physiotoolkit, and physionet components of a new research resource for complex physiologic signals. 101(23):e215–e220, 2000.

[17] D. Goodin. Why Algebraic Eraser may be the riskiest cryptosystem you've never heard of. http://arstechnica.com/security/2015/11/why-algebraiceraser-maybe-the-most-risky-cryptosystem/, 2015.

[18] Z. Guo, N. Karimian, M. Tehranipoor, and D. Forte. Hardware security meets biometrics for the age of iot. In *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016.

[19] N. Inc. nymi - white paper. 2015.

[20] S. M. M. P. Jayavardhana Gubbi, Rajkumar Buyya. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29:1645–1660, February 2013.

[21] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte. Highly reliable key generation from electrocardiogram (ecg). 2016.

[22] S. Li and T. Tryfonas. The internet of things: a security point of view. *Internet Research*, pages 1–34, 2015.

[23] I. LÃijtkebohle. Gartner's hype cycle special report for 2011. http://www.gartner.com/technology/research/hype-cycles, 2011.

[24] K. Monks. The guns that know who is firing them: Can smart tech make firearms safer?, 2014.

[25] H. Ning, H. Liu, et al. Cyber-physical-social based security architecture for future internet of things. *Advances in Internet of Things*, 2(01):1, 2012.

[26] Nymi. Nymi Website. https://www.nymi.com, 2016.

[27] I. Odinaka, P.-H. Lai, A. D. Kaplan, J. A. O'Sullivan, E. J. Sirevaag, and J. W. Rohrbaugh. Ecg biometric recognition: A comparative analysis. *Information Forensics and Security, IEEE Transactions on*, 7(6):1812–1824, 2012.

[28] D. W. Osten, H. M. Carim, M. R. Arneson, and B. L. Blan. Biometric, personal authentication system, Feb. 17 1998. US Patent 5,719,950.

[29] J. Pan and W. J. Tompkins. A real-time qrs detection algorithm. *Biomedical Engineering, IEEE Transactions on*, (3):230–236, 1985.

[30] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah. A systemic approach for iot security. In *Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on*, pages 351–355. IEEE, 2013.

[31] A. Rinaldi. Biometrics' new identity - measuring more physical and biological traits. *EMBO reports*, 17(1):22–26, 2016.

[32] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, DTIC Document, 2001.

[33] Sense. Mother Website. https://sen.se/mother/, 2016.

[34] F. Sufi, I. Khalil, and J. Hu. Ecg-based authentication. In *Handbook of Information and Communication Security*, pages 309–331. Springer, 2010.

[35] M. Sujithra and G. Padmavathi. Iot security challenges and issues–an overview. *Avinashilingam*, 2016.

[36] F. Tehranipoor, N. Karimian, K. Xiao, and J. Chandy. Dram based intrinsic physical unclonable functions for system level security. In *Proceedings of the 25th Edition on Great Lakes Symposium on VLSI*, GLSVLSI '15, pages 15–20, New York, NY, USA, 2015. ACM.

[37] F. Tehranipoor, W. Yan, and J. A. Chandy. Robust hardware true random number generators using dram remanence effects. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 79–84, May 2016.

[38] L. Vaas. IoT doorbell have up Wi-Fi passwords to anybody with a screwdriver. https://nakedsecurity.sophos.com/2016/01/27/iot-doorbell-gave-up-wi-fi-passwords-to-anybody-with\-a-screwdriver/, 2016.

[39] L. Vaas. We might use your IoT stuff to spy on you, says top spook James Clapper. https://nakedsecurity.sophos.com/2016/02/11/we-might-use-your-iot-stuff-to-spy-on-you-says-top-spook\-james-clapper, 2016.

[40] J. West, T. Kohno, D. Lindsay, and J. Sechman. Wearfit: Security design analysis of a wearable fitness tracker. Technical report, IEEE Center for Secure Design, February 2016.

[41] W. Yan, F. Tehranipoor, and J. A. Chandy. A novel way to authenticate untrusted integrated circuits. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, ICCAD '15, pages 132–138, Piscataway, NJ, USA, 2015. IEEE Press.

[42] Z. Zorz. WiFi jamming attacks more simple and cheaper than ever. https://www.helpnetsecurity.com/2015/10/13/wifi-jamming-attacks-more-simple-and-cheaper-than-ever/, 2015.