Securing MEMS Based Sensor Nodes in the Internet of Things

Hasan Tahir, Ruhma Tahir, Klaus McDonald-Maier

School of Computer Science and Electronic Engineering, University of Essex, United Kingdom
htahir@essex.ac.uk, rtahir@essex.ac.uk, kdm@essex.ac.uk

Abstract – **Security schemes are rendered impractical if their cryptographic keys are compromised. ICMetric technology is an innovation in the field of cryptography that generates a device identification based on the inherent features of a device. Devices in the internet of things (IoT) are cyber physical systems with varying purpose and platforms. Since these devices are deeply entwined with the physical world, the chances of a security failure are higher. In this paper we suggest coupling the ICMetric technology and IoT. We prove that device identification can be generated by using the accelerometer found in many pervasive devices. Our experiments are based on a set of health sensors equipped with a MEMS accelerometer. Periodic readings are obtained from the sensor and analysed mathematically and statistically to generate a stable ICMetric number.**

Keywords– Internet of things; ICMetric; IoT security; accelerometer; device identification

I. Introduction

Advancement in the field of embedded systems and pervasive computing has heralded the growth of a new technological phenomenon called the IoT. This technological advancement is the result of collaborations between internet capable devices. The collaboration allows interconnection between numerous devices thus facilitating data sharing, remote monitoring and knowledge distribution. IoT allows physical world objects (devices) to interact with each other and ultimately with the internet. Interactions between the digital and physical world [1] is often the cause of challenges associated with security and data privacy. As communications take place across a number of devices and networks the chances of a security failure escalates rapidly. Commercial pressures and a lack of understanding of security has resulted in a situation where devices are being marketed which lack essential security features like authentication, confidentiality and integrity [2] [3].

Security in most systems is seen as an add on feature which ensures that the system and its data is fully secure [4]. In the IoT security is a key enabling technology because communication traffic is handled by security systems, while the originating low level traffic from embedded systems is not protected and hence needs security enhancements. IoT faces new threats, challenges and constraints which can be addressed with a security technology that is resilient to conventional attacks on computation systems. A study of security flaws [5] [6] in the IoT shows that insecure software/ firmware, insufficient authentication, identity theft, weak user credentials are to blame for the lack of adoption of this emerging technology. We propose incorporating ICMetric security into IoT as a method for preventing security flaws which have limited the wide acceptance of this ubiquitous technology.

Traditionally, security algorithms rely heavily on the use of cryptographic keys. Capture/ theft of cryptographic keys results in exposure of the system security. ICMetric is a recent advancement in the field of cryptography which attempts to provide security services by using cryptographic keys that are generated using device characteristics. The cryptographic keys are generated by using device features which cannot be spoofed or predicted.

This paper proposes a novel security scheme, which links IoT and the ICMetric technology, to demonstrate how an ICMetric identification can be generated using values obtained from the MEMS accelerometer found in mobile embedded systems that track movements, accelerations and the physical environment.

IoT is an area undergoing research. For this domain to gain wide acceptance and adoption it must be secured. Since devices in the IoT are heterogeneous and possess varying resources and purpose. Therefore, securing these devices is not only challenging but also requires a new perspective. In this paper we first discuss how ICMetric security works. In section III we explain what the IoT is and the security challenges faced by this unique environment. In this section we also highlight how and why ICMetric based security can protect the unique IoT environment. Section IV explains how an accelerometer works followed by what imperfections are found in an accelerometer. In section VI we discuss in detail the composition of our experimental setup. Section VII explains how the ICMetric number is generated. The paper concludes by highlighting the accomplishments of our research.

II. Integrated Circuit Metric (ICMetric)

The security of cryptographic schemes lies in keeping the keys secret. If the keys are captured or exposed then the security of the system is rendered useless. ICMetric [7] [8] is a technology that attempts to resolve issues related to key theft by using the inherent features of a device when required and discarded thereafter. Having such a scheme eliminates the chances of having the key captured as the keying data is not stored on the system. Instead the key is regenerated every time it is required based on the features extracted from the system.

The use of ICMetric security has been successfully applied to applications in cloud computing [9], peer and group based security [10] [11] [12] [13].

The ICMetric technology uses many individual device characteristics while establishing an ICMetric (identification) for the device. The choice of features for establishing the ICMetric is a crucial element for ensuring the security of the ICMetric number. Features are chosen which are difficult to replicate and predict. For instance using the MAC address of a device may seem like a good idea since it is a unique characteristic. The problem with using the MAC address is that it can be extracted and spoofed using network monitoring tools. Therefore the ICMetric technology relies on using device features which are variable and cannot be predicted. To increase the complexity of the generated ICMetric, the extracted feature values are subjected to statistical and mathematical manipulation. The ICMetric generation is a two phase process:

A. Calibration Phase

In the calibration phase feature values are read from the device. Once the readings are taken they are processed statistically and mathematically. The calibration phase is applied only once when the ICMetric needs to be generated. In this phase those values are taken which exhibit stability and produce repeatable results. Features that exhibit erratic values cannot be used because this results in the generation of a different ICMetric every time.

B. Operation Phase

The operation phase is used to generate a final ICMetric. In this phase one of two number combination processes can be used for generating the final ICMetric. The operations which can be applied are feature addition and feature concatenation. In the feature addition technique the resulting values obtained from the calibration phase are combined by adding all the values. The resulting ICMetric is diverse but is small in length. The feature combination technique is used to combine values by using the concatenation operation. By using this operation, the resulting ICMetric is longer in length but lacks diversity.

When establishing the ICMetric, individual feature values are extracted and a statistical and probability analysis is performed on them. Readings are taken for a particular feature value and the mean, standard deviation and variance is computed.

III. Internet of Things

As individual devices connect to the internet it was inevitable to connect individual devices to each other so that a network of devices can be formed. IoT [14] is a recent development in the field of computing which studies the interconnection of devices to deliver services which are beyond conventional machine to machine communication. IoT possesses a unique environment where devices like cars, smart phones, health monitoring devices, home appliances, automation systems are sharing data between themselves and the users. By using IoT various users/ industries can benefit from real time tracking, process optimization and instantaneous control.

Since IoT is a technology which is strongly connected to the physical world [15] therefore the chances of a security failure are considerably high [16]. Commercial motivations have resulted in a market where initial devices are now being marketed but the devices do not address basic security requirements.

A. Security Issues in IoT

Security in IoT [17] [18] is a complex issue because this is a technology that has vague network boundaries. This combined with a lack of understanding regarding security in IoT has resulted in the following:

- Small and inexpensive devices that possess little or no ability to provide security at any level.
- Lack of authentication and authorization features.
- Lack of data encryption being offered.
- Scalability issues as increasing number of devices offer IoT connectivity.

IoT is faced with a range of security problems which are unique and thus require a revamped security approach.

B. ICMetric Security and IoT

ICMetric based security is different from conventional security because it uses device features and characteristics to deliver security. The ICMetric technology relies on using both hardware and software characteristics for generating the ICMetric number. By using the ICMetric technology we can achieve high levels of security by detecting cases of tampering, failure and malicious exploitation. The ICMetric technology in a multiparty environment will also ensure that devices are not cloned through ICMetric authentication

Using ICMetric technology in combination with IoT is an attempt to ensure security from the bottom up.

Conventional cryptographic scheme's deliver security at a higher layer and hence the system can be compromised by just a simple key theft. By using ICMetric security we address the fundamental problem of key theft by adding an early additional security layer to the existing IoT architecture. This ensures the deliverance of high levels of security with minimum intervention. Given below is the ICMetric based IoT architecture.

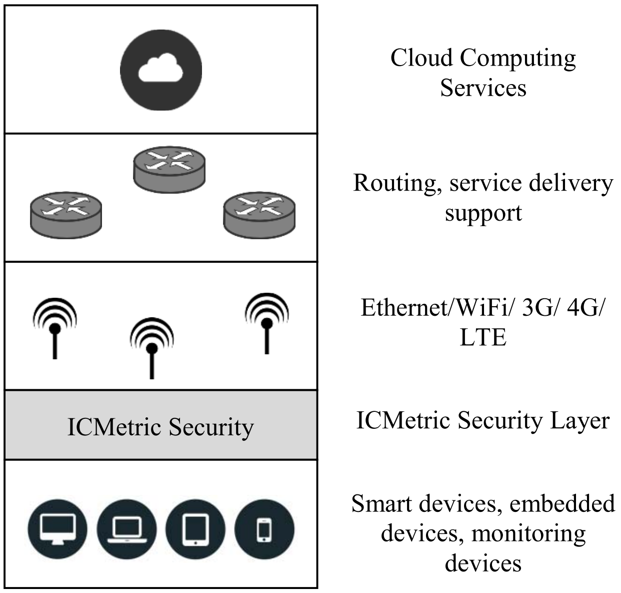

Cloud Computing Services
Routing, service delivery support
Ethernet/WiFi/ 3G/ 4G/ LTE
ICMetric Security
ICMetric Security Layer
Smart devices, embedded devices, monitoring devices

Fig 1: IoT architecture featuring ICMetric security

The ICMetric security layer has been strategically placed so that any communications to and from the device are protected with ICMetric security.

IV. MEMS Accelerometer

Devices in IoT have various capabilities and platforms. Accelerometer embedded devices are now IoT enabled for example smart phones, health monitoring devices, wearable devices, smart watches, laptops just to name a few. The accelerometer [19] is a specialized sensor which is a composed of micro scale mechanical and electrical components. The MEMS accelerometer is classified as a Micro Electro Mechanical System (MEMS) which is composed of fixed plates suspended within a movable mass. Having such an arrangement creates a capacitance across the plates. If the accelerometer sensor is at rest, then the capacitance across the fixed plates will remain the same. On the other hand if the accelerometer experiences an acceleration then the capacitance across the two suspended plates will change. Given in figure 2 is the structure of a MEMS accelerometer. When the accelerometer experiences an acceleration the capacitance C_1 and C_2 will not be same.

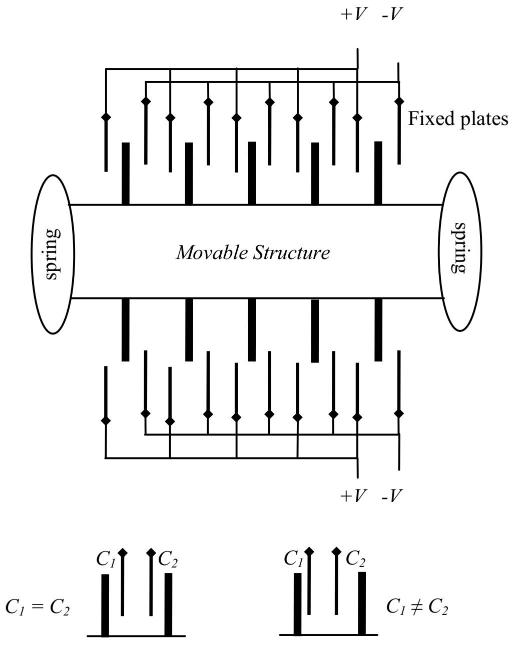


Fig 2: The MEMS accelerometer schematic

V. Exploiting imperfections in MEMS

Every MEMS accelerometer possesses a discrepancy owing to which it exhibits a bias which is particular to that device. This bias exists in every MEMS accelerometer due to slight imperfections in the manufacturing process. Since an accelerometer is a mechanical device, the stresses can be introduced in the many manufacturing processes concerning the accelerometer. For instance a bias is introduced when the MEMS component is assembled. Further bias can be introduced when the accelerometer is soldered, mounted and due to stresses introduced by the board. Since many individual factors influence the operations of the accelerometer, therefore it can be said that the introduced bias is a function of many individual variables which are beyond the control of the manufacturer and these variables cannot be predicted. Research [20] [21] has shown that it is feasible and recommended to generate a device identification [22] using an embedded accelerometer.

These individual variables cannot be predicted and are unique to each device, we employ the accelerometer offset to prove that an ICMetric identification can be generated for a device. This ICMetric identification can be used for delivering a wide range of cryptographic services. Owing to the unique qualities of ICMetric security we can prevent unauthorized access or device cloning to compromise identity and subsequent activities. Besides this the ICMetric can be used to detect cases of failure, tempering and malicious exploitation.

There are other MEMS sensors which can be used for generating the ICMetric identification for a device. For instance the sonar sensor found in modern driverless cars can also be used for generating ICMetric identification.

Although it is possible to exploit the imperfection in an accelerometer, the same is not possible for all embedded sensors. For instance many devices are embedded with a gyroscope, and to obtain the offset of a gyroscope the device has to be subjected to constant angular velocity. Constructing a device that can perform such a task is not only difficult but also an inconvenience since the ICMetric number needs to be generated without external intervention. Similarly the magnetometer can be used to generate an identification. The problem with using the magnetometer is that magnetometer readings are influenced by the presence of near metallic objects and devices that emit magnetic rays.

Some imperfections are easy to capture but they do not provide adequate identification data which can be used for generating an ICMetric identification. It is relatively easy to identify the misalignment of a touch screen sensor on top of the display. The problem with this sensor is that the imperfections are very minor due to which they do not reflect in the users behaviour during the use of the device. Hence the misalignment between the display and the touch screen sensor cannot be detected.

VI. Experimental Setup

Our experimental setup consists of a set of 5 Shimmer sensors [23] placed in an environment free from vibrations and magnetic interference. The shimmer sensor is a health sensor designed to read physiological signals at regular intervals. The programmable sensor can perform an electrocardiogram (ECG), galvanic skin response (GSR) and electromyography (EMG). The sensor is equipped with an accelerometer, gyroscope and a magnetometer. The shimmer is embedded with a Freescale MMA7260QT [24] triple axis accelerometer with adjustable sensitivity ranging from ±1.5g to ±6g We base our experiment on health sensors because these are specialized embedded devices commonly found in the IoT environment. Although the Shimmer is a fully functional body sensor, it has no cryptographic features. This creates the compelling case for establishing a security scheme for health sensors.

To generate the device ICMetric we obtain readings when the accelerometer is at rest (0g). A total of 1552 readings are recorded per axes. The Shimmer provides accelerometer readings in both calibrated (m/sec^2) and uncalibrated (raw) format. Since the uncalibrated readings do not have an associated unit we therefore base our study by using only the calibrated values. Each reading provided by the shimmer sensor is also composed of a timestamp (in milli seconds).

Once the values are obtained a mathematical and statistical analysis is done on the data obtained.

VII. Generating the ICMetric Identification

The accelerometer readings obtained from the shimmer sensor belong to a variable which is subject to change. The variable takes a set of possible values within a bounded range which is unique for individual sensor. This is why the accelerometer is chosen as a viable candidate for generating the ICMetric. The accelerometer readings are a discrete random variable hence we use a probability mass function to determine the probability that the variable is exactly equal to a precise value. The probability mass function $p(x)$ identified for generating the ICMetric is composed of other statistical functions. If $\bar{X}$ is the mean and x is an individual accelerometer sample reading then:

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

Where n is the total number of readings obtained.

If σ^2 is the standard deviation then

$$\sigma^2 = \sum_{i=1}^{n} p(x_i)\,(x_i - \bar{X})^2 \tag{2}$$

If σ is the standard deviation then the probability mass function is given by:

$$p(x) = \frac{1}{\sigma\sqrt{2n}}\, e^{\frac{-(x-\mu)^2}{2\,\sigma^2}} \tag{3}$$

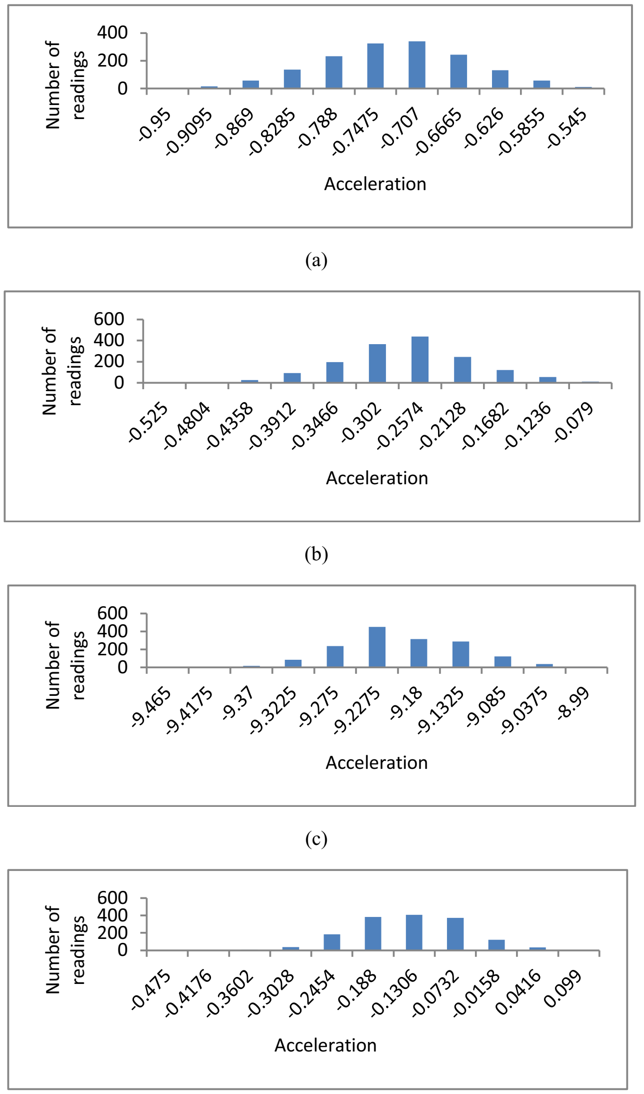
To further analyse the generated curve we use the confidence interval, inter quartile range and the skewness. To analyse the accelerometer readings we use a 95% confidence interval i.e.

$$\bar{X} - Z_{\frac{\alpha}{2}}\left(\frac{\sigma}{\sqrt{n}}\right) < \mu < \bar{X} - Z_{\frac{\alpha}{2}}\left(\frac{\sigma}{\sqrt{n}}\right) \tag{4}$$

Where $Z_{\frac{\alpha}{2}} = 1.96$ for a 95% confidence interval.

Our experiments show that even the smallest difference in readings obtained from one sensor to the other is sufficient for generating a stable ICMetric number.

Given in figure 3 are graphs that show normalization trends in four different sensors. Due to limitations of space we have provided the behaviour of only the x-axis and the y-axis of four different sensors. Our analysis shows that the readings are both repeatable and unique for each sensor. The x-axis readings in graph a and b both have different ranges. Similar results are also reflected in the y-axis graphs in figure 3. This implies that all sensors will have their own unique statistical and mathematical results. We regenerated the sensor readings by recreating the same environment and our experiments show that the results are not only unique for each sensor but also repeatable.



(a)

(b)

(c)

(d)

Fig 3: Reading obtained from four different sensors. (a) x-axis graph (b) x-axis graph (c) y-axis graph (d) y-axis graph

A statistical analysis of the measurements obtained from the accelerometer shows that each sensor exhibits a unique bias. While comparing individual devices we must highlight that the sensors do not follow any particular pattern or have no correlation, thus the individual sensor metrics cannot be predicted. Table 1 shows the metrics for the graphs shown in figure 3. Owing to lack of space the z-axis has not been provided, but our trials on the shimmer sensors showed similar results.

Table 1: Statistical analysis of x and y axis in two different devices.

		Device a	***Device b***
x axis	**Mean**	-0.7467	-0.292
	Standard Deviation	0.0757	0.0693
	Skewness	2.3250	0.0229
y axis	**Mean**	-9.266	-0.164
	Standard deviation	0.0678	0.074
	Skewness	0.0685	0.0728

CONCLUSION

IoT is the result of research aimed at pervasive computing. IoT studies how network capable computation devices can be used to communicate, share data, facilitate information sharing and remote access. IoT is a unique environment where network boundaries are often vague but security of high level traffic is ensured through firewalls, network intrusion detection hardware, protocols and software. These network systems cannot protect deeply embedded devices which have dedicated purpose and hardware. Even the strongest cryptographic scheme cannot prevent attacks targeting cryptographic keys. If the cryptographic key of a device is captured then the security of the device is impractical.

In this paper we propose the use of the ICMetric technology in the IoT. The ICMetric technology is recommended because it uses low level device features to generate a device identification which then provides cryptographic services. The device ICMetric can be used to detect cases of failure, tampering, malicious exploitation, device cloning and unauthorized access. The ICMetric technology is a key theft deterrence technology which adds an additional layer to the existing cryptographic services. This paper studies the generation of a device ICMetric by using the MEMS accelerometer found in many IoT enabled devices.

We use the embedded accelerometer in the Shimmer health sensor to establish an ICMetric for the device. In our experimental setup we obtain three axes readings from a set of 5 Shimmer sensors. A statistical study of the sensor readings proves that it is both feasible and recommended to use the MEMS accelerometer for the generation of a device identification. Experiments show that the regeneration of the ICMetric is possible and each device/ sensor generates the same identification provided there is not interference in the generation process. The entropy of the system can be increased by incorporating other device features. Features may include hardware identifications, addresses, sensory data etc.

REFERENCES

[1] M. Lawton, “The symbiosis of digital and physical security,” 19 February 2015. [Online]. Available: http://futurelab.assaabloy.com/en/the-symbiosis-of-digital-and-physical-security/. [Accessed 31 July 2015].

[2] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems,* vol. 29, no. 7, pp. 1645-1660, 2013.

[3] TRUSTED Computing Group, “ARCHITECT’S GUIDE: IOT SECURITY,” July 2015. [Online]. Available: http://www.trustedcomputinggroup.org/files/static_page_files/93061BAE-1A4B-B294-D0F3EBD27DB68FAB/IOT_Security_Architects_Guide_TCG.pdf. [Accessed 30 July 2015].

[4] R. Roman, P. Najera and J. Lopez, “Securing the Internet of Things,” *IEEE Computer,* vol. 44, no. 9, pp. 51-58, 2011.

[5] J.Greenough, “Security will be critical to the success or failure of Internet of Things products,” 13 April 2015. [Online]. Available: http://uk.businessinsider.com/ftc-top-recommendations-for-protecting-home-iot-2015-3. [Accessed 1 July 2015].

[6] Open Web Application Security Project, “Internet of Things Top Ten,” 30 July 2014. [Online]. Available: https://devcentral.f5.com/Portals/0/Cache/Pdfs/2807/internet-of-things-owasp-top-10.pdf. [Accessed 15 July 2015].

[7] E. Papoutsis, “Investigation of The Potential of Generating Encryption Keys For ICMetrics,” 2009.

[8] Y. Kovalchuk, G. Howells and K. McDonald-Maier, “Overview of ICMetrics Technology - Security Infrastructure for Autonomous and Intelligent Healthcare system,” *International Journal of u- and e- Service Science and Technology,* vol. 4, no. 3, pp. 49-60.

[9] H. Tahir, R. Tahir and K. McDonald-Maier, “A Novel Private Cloud Document Archival System Architecture Based on ICmetrics,” in *Fourth International Conference on Emerging Security Technologies (EST)*, 2013.

[10] R. Tahir, H. Hu, Dongbing Gu, K. McDonald-Maier and G. Howells, “A Scheme for the Generation of Strong ICMetric Based Session Key Pairs For Secure Embedded System Applications,” in *International Conference on Advanced Information Networking and Applications*, Barcelona, 2013.

[11] H. Tahir and K. McDonald-Maier, “A Group Secure Key Generation and Transfer Protocol Based on ICMetrics,” in *9th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, Manchester, 2014.

[12] H. Tahir, G. Howells, H. Hu, D. Gu and K. McDonald-Maier, “On Secure Group Admission Control Using ICMetrics,” in *Fifth International Conference on Emerging Security Technologies.*, Alcalá de Henares, 2014.

[13] H. Tahir, G. Howells, H. Hu, D. Gu and K. McDonald-Maier, “On the Incorporation of Secure Filter in ICMetrics Group Communications,” in *Fifth International Conference on Emerging Security Technologies*, Alcalá de Henares, 2014.

[14] L. Atzori, A. Lera and G. Morabito, “The Internet of Things: A survey,” *Elsevier Computer Networks,* vol. 54, no. 15, p. 2787–2805, 2010.

[15] S. L. Keoh, S. S. Kumar and H. Tschofenig, “Securing the Internet of Things: A Standardization Perspective,” *IEEE Internet of Things Journal,* vol. 1, no. 3, pp. 265-275, 2014.

[16] C. Morien, “Connectivity 101: The Internet of Things,” University of Texas at Austin: Center for Identity, Austin, 2014.

[17] A. Ukil, J. Sen and S. Koilakonda, “Embedded security for Internet of Things,” in *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, Shillong, 2011.

[18] Wind River Systems, “Security in the Internet of Things - Lessons from the Past for the Connected Future,” January 2015. [Online]. Available: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf. [Accessed 30 July 2015].

[19] M. Andrejasic, “MEMS Accelerometers,” Ljubljana, 2008.

[20] H. Bojinov, Y. Michalevsky, G. Nakibly and D. Boneh, “Mobile Device Identification via Sensor Fingerprinting,” Rafael, 2014.

[21] A. Aysu, N. F. Ghalaty, Z. Franklin, M. P. Yali and P. Schaumont, “Digital fingerprints for low-cost platforms using MEMS sensors,” in *Workshop on Embedded Systems Security*, Montreal, 2013.

[22] S. Dey, N. Roy, W. Xu, R. R. Choudhury and S. Nelakuditi, “AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable,” in *21st Annual Network and Distributed System Security Symposium NDSS*, San Diego, 2014.

[23] Shimmer, “Shimmer User Manual Revision 2RK,” Dublin, 2013.

[24] Freescale Semiconductor, “±1.5g - 6g Three Axis Low-g Micromachined Accelerometer,” 2008.