Overview of ICmetrics Technology – Security Infrastructure for Autonomous and Intelligent Healthcare System

Yevgeniya Kovalchuk,
Klaus McDonald-Maier
School of Computer Science and Electronic Engineering,
University of Essex
yvkova@essex.ac.uk, kdm@essex.ac.uk

Gareth Howells
School of Engineering and Digital Arts,
University of Kent
W.G.J.Howells@kent.ac.uk

Abstract

Recent developments in bio-, nano-, and digital technology have changed the way modern healthcare systems operate. The provision of healthcare servicing remotely and exploitation of monitoring and assistive technology within and outside medical institutions mean that medical staff and patients constantly interact with various electronic devices. It also means that sensitive patient data are stored on and being transmitted between these devices. To ensure safe and secure use of medical equipment, as well as authorised access to data, appropriate encryption and debugging infrastructure should be integrated into the modern healthcare system. This paper introduces a novel concept, ICmetrics, that can serve as a basis for developing such infrastructure. More specifically, the ICmetric technology is based on the idea of generating encryption keys directly from the characteristics of electronic systems' behaviour on both hard- and software levels. This may include features extracted from electronic circuits, sensors, machine-machine and machine-human interfaces, as well communication peripherals. While the proposed technology has a number of advantages over the existing security systems, it also poses interesting research challenges. These challenges along with the proposed solutions are discussed in the paper.

Keywords: *ICmetrics, healthcare systems, encryption*

1. Introduction

The continuous ageing of the world's population [1], as well as the recent advances in bio-, nano-, and digital technologies [2], change the way that healthcare services are provided. Active aging, support for independent living and support for rehabilitation, mobile health monitoring and health monitoring from homes, assistive technology and assisted-living homes, etc – are the topics that are currently under active investigation. Healthcare environments (within the hospital and the home) are becoming significantly complex and challenging to manage from the technological and information systems perspectives, as they are required to cope with an assortment of patient conditions under various circumstances with a number of resource constraints. Pervasive healthcare technologies seek to respond to a variety of these pressures by integrating them within existing healthcare services. It is essential that intelligent pervasive healthcare solutions are developed and correctly integrated to assist healthcare professionals in delivering high levels of patient care. It is equally important that these pervasive solutions are used to empower patients and relatives for self-care and management of their health to provide seamless access for health care services.

One of the major challenges in this process of transforming healthcare systems is associated with the issues of safety, privacy, and security [3]. For example, a medical electronic device may fail or been misused putting its user in danger; confidential patient's information may be disclosed; medical records may be manipulated. Therefore, it becomes vital to manage and control access to secret medical information stored on and transmitted between electronic devices, as well as to ensure integrity and authenticity of all medical equipment.

While a number of methods exist to protect data (passwords, biometrics, encryption etc), such systems are unable to fully address the relevant security requirements, nor can they detect improper operation of digital devices. Passwords can be forgotten or stolen if written down. Similarly, since biometric reference templates and private encryption keys have to be stored, unauthorised access to them may compromise the security of any data protected by them.

This paper advocates an alternative approach to generating encryption keys that does not suffer from the above disadvantages. In particular, the paper presents a novel concept, termed ICmetrics (Integrated Circuit metrics), where encryption keys are generated directly from measurements taken from electronic devices. This technology not only can ensure secure and safe data storage and transmission, but also helps to detect cases of failure of electronic devices, as well as their tampering and malicious exploitation. The significant advantages of ICmetrics are:

- The removal of the need to store any form of template for validating the device.
- The security of the system will be as strong as the ICmetrics and encryption algorithm employed (there is no back door). The only mechanisms to gain subsequent access are to provide another sample of the ICmetrics or to break the cipher employed by the encryption technology.
- The compromise of a system does not release sensitive ICmetric template data which would allow unauthorised access to other systems protected by the same ICmetrics or indeed any system protected by any other ICmetric templates present.
- Tampering with the constitution of a circuit will cause its behaviour to change, potentially causing the features underlying the ICmetrics to change, perhaps dramatically, thus causing the generated ICmetrics to change. Consequently, a faulty or maliciously tampered device will be autonomously prevented from decrypting its own stored data or participating in any initiated secure communications, as the regenerated keys will differ from those created before its integrity was compromised. In other words, the ICmetrics approach can be made to fail securely and provide a very high immunity from cloning and tampering.
- The removal of the need for the storage of the private key associated with the encryption system. This is a natural consequence of the system since the key will be uniquely associated with the given ICmetric sample and a further ICmetric sample may be used to regenerate the required private key. As there is no physical record of the key, it is not possible to compromise the security of sensitive data via unauthorised access to the key.

While our preliminary research [4-9] has shown the great potential of the ICmetric technology, the system has to date been tested on simulated data only. Based on the initial results, it is now possible to formally describe the system and precisely define tasks that are required to be solved in order to bring the system up to the level when it can be deployed in a real world scenario. In particular, we intend to integrate the ICmetric system into an intelligent and autonomous wheelchair [10] that is capable of operation in a real hospital environment. In order to function effectively, such wheelchairs should be able to communicate with both its users (the patient and associated members of the medical stuff) and external devices (e.g., the information system that keeps the patient's medical record) in a safe and secure manner.

The purpose of this paper is to introduce the ICmetric concept, formulate the tasks associated with its implementation, outline the results from the preliminary research related to these tasks, and finally define directions for the future research that would allow the integration of the system into a real healthcare system. Such system may include several remote locations providing and/or receiving healthcare servicing that extensively use various medical electronic equipment and computer nodes running information systems. Ensuring safe and secure operation on such system is of vital importance.

The paper is organized as follows. Related work is discussed first. The concept of ICmetrics is presented subsequently along with the primary benefits it provides for developing secure healthcare systems. Section 4 discusses the challenges associated with implementation of the ICmetric technology and proposes how to address them. Section 5 concludes the paper.

2. Related Work

An overview of the latest technology and devices supporting a personalized healthcare system is provided in [2]. In particular, various biosensors, nanosensors and biochips have become extremely popular as a tool for medical diagnostics and therapy due to their non-invasive or minimally invasive nature [11]. A lab-on-a-chip (LOC), a very small device that integrates one or several laboratory functions on a single chip, is another promising technology suitable for medical diagnostics [12]. While these technologies provide many benefits for healthcare provision, a number of barriers exist preventing their uptake by both medical staff and patients, such as ease and convenience, as well as safety and security of using such technology [2, 3].

With the development of various human-machine interfaces, biometric encryption has become a popular technology used to ensure secure access of the users to electronic systems and devices [13-24]. Biometric refers to any unique, measurable and biological characteristic used to recognize and verify the identity of a human [13]. As a biometric is an intrinsic feature of a human user, it typically cannot be transferred to a third party. One of the advantages of using a biometric-based key is that it removes the need for a user to remember their keys. This is particularly important in the context of healthcare environments, where medical staff are often overloaded with various items of potentially complex information, while patients may suffer from mental disorders affecting their memory functions. Physically disabled people may also have the problem with entering their passwords. While biometric-based systems may overcome this issue (for example, using such biometrics as voice or iris patterns) they are not flexible enough to address the diversity of disorders that can be observed in any hospital environment.

Another major weakness of the many existing biometric-based systems is that they rely on the explicit template storage [13-17]. Although some work has also been done on direct encryption of keys [18-24], these proposals apply to a restricted problem domain and do not successfully overcome the problems associated with intra-sample variation in the generic case.

The encryption system proposed in this paper addresses the above issues. First of all, it does not require the storage of any form of template or the private key associated with the encryption system. Second, it has the potential to work on previously unseen samples which significantly increases the potential utility of the system. Finally, it is designed to generate encryption key from diverse sets of features measured from electronic devices and/or interfaces of their interaction with their users. Regardless the conditions of using an electronic device (e.g., characteristics of its environment such as temperature or humidity, specification of the software running on it, or nature of the disability of its user), the system can be constructed to suite any specific needs. For instance, despite the means of operating an electrically powered wheelchair [10] (by voice, gesture, brain signal, or allow it to run fully automatically), the proposed encryption system can work equally efficient.

3. ICmentric Technology

The *Integrated Circuit metrics* or *ICmetric* technology is based on the idea of extracting features that, when combined, uniquely characterize the performance of the given electronic device. This is possible as typically devices operate under unique conditions; they sense different environments, run different software, perform different tasks and interact with different users. Examples of features an ICmetric engine could employ include states of the programmable System-on-Chip (SoC) at the heart of the embedded device (such as program sequence, content of selected memory locations, memory sub-system performance and the frequency and nature of system I/O) and the system environment as observed by the system through its sensors. Such features can be used for both, generating unique encryption keys or digital signatures (e.g. to encrypt message sent from or stored on the device), and detecting cases of untypical device behaviour (e.g., due to failure of its electronic elements or intrusion of a parasite program code).

The ICmetric concept has significant analogies with biometrics – the identification of individuals from the detection and evaluation of their physiological or behavioural characteristics such as handwriting, fingerprints, facial features, iris patterns, voice, etc. Although biometric systems have now reached a significant level of maturity, little alternative work has been undertaken in building analogous systems based on machine derived data and linking a machine's behaviour with the data. The later approach however is useful for environments where machine-machine or machine-human interaction takes place. This is particularly true in hospitals and other similar locations that provide and/or receive medical service. So far, the ICmetric concept has been investigated in relation to electronic circuits only. However, it has a potential to combine features derived from both electronics and human biometrics, as well as from signals used to interface electronic devices with their users (e.g., voice or brain signal used to navigate an electrically powered wheelchair).

In its current state, the ICmetric system is designed to be employed on previously unseen devices and to faithfully reproduce encryption keys for such devices on further application to them by examining a pre-defined set of measurable features of such devices. However, the system does require detailed knowledge of the likely distribution of such features within their domain of possible values for typical devices. Therefore, a significant calibration phase is required for each application domain for which the ICmetric system is to be employed prior to its employment in the generation of encryption keys. This calibration phase operates on samples taken from typical example devices which may or may not include devices for which encryption keys will subsequently be required. Although the system is, subsequent to the calibration phase, designed to operate on previously unseen devices, this is governed by the restriction that the measured features will behave approximately as predicted by analysis of the sample devices.

The ICmetrics is therefore a two phase system: the calibration phase is applied only once per application domain employing a number of known circuits as a calibration set, while the operation phase is applied each time an encryption key is desired for a given circuit. The steps involved in each phase are described below in more detail.

Calibration phase (applied once only per application domain)

1) For each sample circuit, record a set of desired measurements associated with the circuit known generically as features.

   The features employed so far have been extracted from circuits integrated within a SoC architecture; the circuits have been prototyped using an FPGA. Initial exploration has focused on generating a 128-bit number that reflects the activity of the system's processor, specifically the distributions of address and data values, and the instruction fetches and data accesses that have hit with the caches' contents.

2) Generate feature distributions for each feature tabulating the frequency of each occurrence of each discrete value within the given value scale for each sample circuit.

   Figure 1 demonstrates an example of the possible distribution of address data transactions for four different algorithms (M1-M4), each run on a separate circuit. It may be noted from Figure 1, that there are a number of tightly grouped address regions for each algorithm. For clarification, the most significant groups are marked with labels (e.g. M1a is a group relating to algorithm M1).

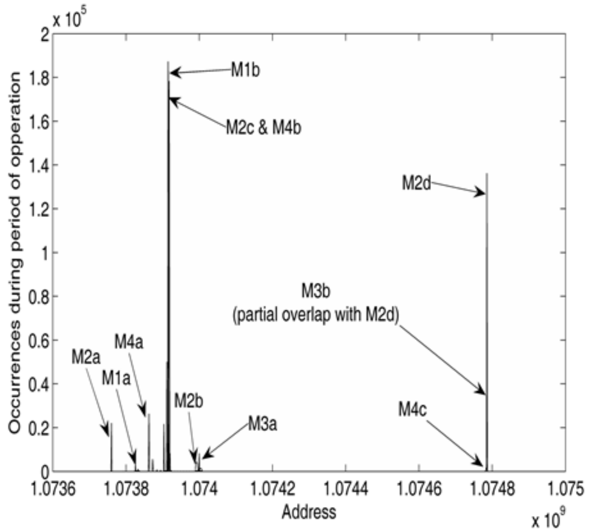

Figure 1. Address distribution of four benchmark algorithm's data transaction

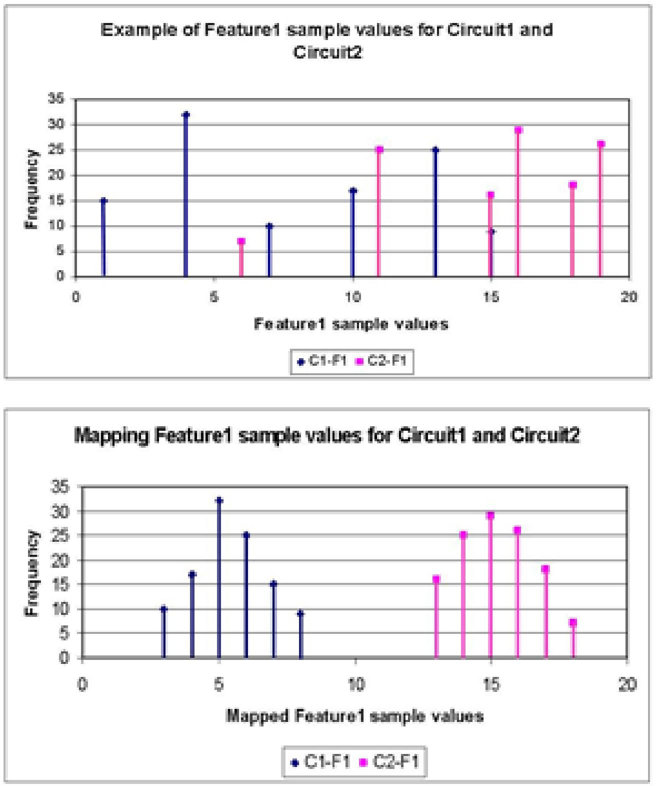

Figure 2. Mapping Feature1 Values of Circuit 1 and Circuit 2

3) Normalise the feature distributions generating normalisation maps for each feature.

As detailed in [8], the purpose of this step is to bring unusual distributions of measured features (as can be seen from Figure 1) to their normal (Gaussian) form so as values suitable for key generation could be defined. As an example, Figure 2 represents feature distributions for two circuits before and after applying the normalization procedure.

It should be noted that the features employed in the ICmetrics domain might be highly multi-modal in their nature (see Figure 3 for example). As discussed in [7], the initial classification of the modal clusters within the distributions may be required (depending on the nature of underlying features) prior building normalisation maps.

Operation phase (applied each time an encryption key is desired for a given circuit)

1) Measure features for the given circuit for which an encryption key is desired.

2) Apply the normalisation maps to generate values suitable for key generation.

3) Apply the key generation algorithm.

Subsequently to the normalization step, component feature values for a device must be combined in such a way to form a unique (basis) number so as to identify each device. This number will form the basis for the subsequent derivation of the key required for the actual encryption process.

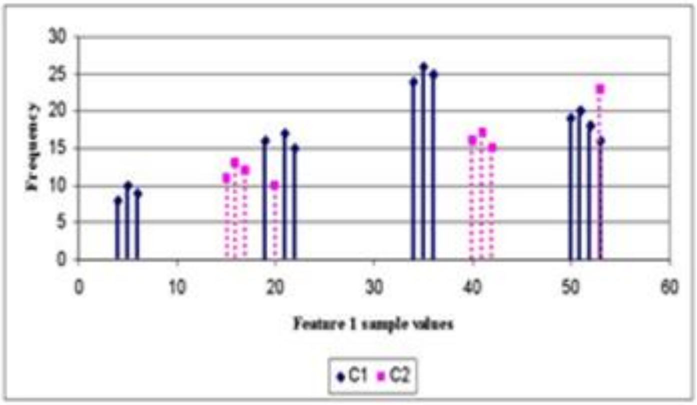

Figure 3. Example of multimodal features employed in ICmetrics

In summary, ICmetrics offers an entirely template-free encryption paradigm for protecting electronic systems and data exchange; it can be used in various scenarios where high-reliability authorization mechanisms are required. However, it is apparent that the issue of producing a stable encryption key for differing ICmetric samples represents a significant challenge and involves several research problems that are currently being addressed. The following section discusses these problems, as well as outlines the research currently pursued to address them so as to make the ICmetrics technology suitable for deploying in a working healthcare environment.

4. Tasks associated with ICmetrics implementation

This section investigates the practical barriers which need to be addressed in order to realise the ICmetric system that is capable of operating in a real complex environment (such as a healthcare environment). Several tasks are involved in implementing such a system and these tasks are outlined below.

4.1. Development of hardware and software instrumentation for feature collection

Securely collecting/measuring properties and features drawn from the performance of electronic devices is a major challenge. Appropriate interfaces are required in order to gain access to device’s features and properties during its performance. Such interfaces should allow for non-intrusive way of measuring and recording of feature values that does not change the system’s operation which is essential for all real-time applications.

Our preliminary work has focused mainly on offline analysis of detailed traces collected during the execution of simulations and simple online analysis made using an FPGA based test-bench [4]. However, it is not yet practical to employ the FPGA based diagnostic and debugging tools used so far outside of the lab.

To allow for measuring features associated with real electronic devices such as an electrically powered wheelchair, special hardware circuits along with a software-based monitoring infrastructure are required to be designed and integrated within the system. Various representations can be used as the basis for an array of metrics. Apart from electronic circuits within a complex hardware, features can be read from various integrated sensors as well as interface units connecting the device with its user (for example, brain-computer interfaces capturing and translating brain activity into computer commands or cameras recording patient's mimics). Such sensors and human-computer interfaces require different monitoring approaches to be taken, with more complex sensors requiring instrumentation software embedded within their associated sensing algorithms. An equally significant source of features is also the system's behaviour. This can be observed by creating an instrumentation fabric within the system's hardware and software that provides autonomous system profiling by taking online measurements of all high-level system tasks. These measurements may include a series of software routine execution times, metrics representing the effectiveness of any cache memories whilst the task is executed; and details of the instruction and data transactions made, such that an abstract representation of the execution can be constructed. Yet another possible source of features is communications statistics extracted from the various communication peripherals (e.g. instructions for navigation or patient's data sent from a central managing system to a wheelchair).

In summary, an adapted version of the hardware and software instrumentation is required to ensure non-intrusive monitoring of the system behaviour at all levels whilst it runs in its normal application environment.

4.2. Building an experimental platform for identification of candidate features

The specific characteristics that can be used in ICmetrics may take the form of internal signal distributions or metrics derived from the highly changing signals. Real examples investigated so far include: the address and value from the data transactions of a processor, its program address, and metrics for the effectiveness of the program and data caches derived from performance counters. The key observation made is that any modifications taking place to either the software executing on a given hardware configuration, in the form of the addition of Spyware or similar, or to the hardware, by tampering with its available memory, configuration or external sensors, manifest themselves in the form of variations in the measurable characteristics. This would have the significant effect of modifying any value derived from the data used for encryption or validation key production by the system, prohibiting its continued participation in any further secure communications. Thus, these are all good examples of features to be considered for generating encryption keys. In general however, various application domains may require different features depending on the context and environment of their operation. It is important to determine the most suitable ones that would allow for generating a stable and secure encryption key for each particular case.

The previously reported results [7, 8] are based on an analysis of simulated data. In particular, 128-bit numbers were generated to reflect the activity of a system's processor, specifically the distributions of address and data values, and the instruction fetches and accesses that have hit with the caches' contents. In order to integrate ICmetrics into a real healthcare system, an experimental framework is required that would allow for effective evaluation of selected features. We are currently developing such a platform based on a multiple processor core SoC design, emulated by loading it into an FPGA, where a very high level of observation is possible. In addition, various available open source packages for system modelling can be used for prototyping and experimenting with the features related to more complex sensors, human-machine interfaces, and communication peripherals as described above. Apart from effective experimentation with multimodal features, such approach allows the design to be modified on request which is important for the systems (often found in the healthcare environment) where frequent changes, updating, and upgrades are possible.

4.3. Analysis of measured feature data

In the context of ICmetrics, analysis of the feature distributions associated with the embedded circuit features presents some novel challenges as compared to many traditional pattern recognition tasks. This is because many of the observed features possess highly non-standard multi-modal distributions (see Figures 1 and 3 for example), often a product of the device under investigation operating in a number of distinct states. The problem of incorporating pattern features with unusual distributions is well known within pattern recognition problems, even if not easily addressed. The problem is, however, more acute when features are derived from characteristics of given integrated electronic circuits, and appropriate techniques should be developed. This includes finding right techniques for classification and normalisation of data in multi-dimensional space.

In our previous work [7, 8], the target space was linear in nature. We used enhanced Peak-Trough detection [25, 26] and kernel estimation algorithms [27] to determine the various modal clusters taking one feature at a time. Our current research, however, is focused on investigation of multi-dimensional spaces combining various features where each circuit mode is equi-distant from every other. This would allow the system to be applied to circuits which have not formed part of the calibration sample within any enrolment of known samples from the circuit. Such a generalization provides an improved mapping onto the key generation space and allows the multi-modal nature of the feature distributions to be effectively integrated within the overall system.

Considering multiple features that are different in nature has also another advantage of designing hybrid ICmetric systems that can include features derived not only from hardware characteristics, but also from signals employed in human-computer interfacing (voice, gestures, brain signals etc). Such an approach is particularly useful for autonomous and intelligent healthcare environments where patients and medical staff frequently use and interact with electronic devices. For example, data transmitting to and from a wheelchair can be encrypted using features extracted not only from its working electronic circuits, but also from the signals generated by the patient operating the wheelchair.

4.4. Encryption key generation from normalised feature data

The generation of encryption keys requires developing suitable methods for combining selected features so as to produce a unique basis number – an initial number unique to the electronic system from which actual encryption keys may be derived. The main requirement for such methods is that they should allow for generating basis numbers with low intra-sample variance (that is, the values produced for the same device) but high inter-sample variance (that is, the values produced for different devices) with the ideal case being no inter-sample overlap of potential basis numbers [9].

In our earlier work [9], we have investigated two alternative techniques for combining features, namely, feature addition and concatenation. Gray code method is proposed to be applied over the binary representation of the basis number in order to increase its stability. It has been found that although with the concatenation technique a bigger encryption key in length is produced, this key is less stable compared to the one produced with the addition technique, since the fluctuation between the bits in the pattern is much higher. Moreover, when feature combination is employed using addition, a lower number of samples is required in order to reproduce successively the same basis number for each ICmetric device compared to applying the concatenation combination technique.

Although both techniques provide a decent level of stability (the same basis number is generated with up to 94% of accuracy depending on the number of samples employed in training [9]), we aim to increase it further by applying the multimodal approach to analysing features as described above.

4.5. Developing evaluation and calibration platform

The stability of encryption keys generated by the ICmetric system depends on several factors as discussed above, including: (i) number of devices available for training and the environment of their operation (section 4.1) (ii) features employed (section 4.2); (iii) mathematical algorithms and their settings used for feature processing (in particular, clustering and normalization techniques as discussed in section 4.3, and de-correlation methods as mentioned in section 4.4); (iv) methods applied for combining selected features to generate a basis number (section 4.4). Therefore, it is important to ensure the evaluation platform is in place to allow for controlled experiments to test and compare performance of various algorithms for feature extraction and processing, both in isolation and their various combinations. It may well appear that certain algorithms work better for certain types of devices, and there should be a way to find right techniques for each case quickly and reliably.

In addition to experimenting with various algorithms during the calibration phase, it is equally important to evaluate the system’s performance during its operational phase (see section 3 for details). In other words, once the system is trained on test devices, its ability to generate stable encryption keys for unseen devices of similar type has to be estimated. Furthermore, taking into account that the conditions of operation of the same electronic device may change (e.g., a wheelchair serving a different patient, or desktop computer running a different software), the evaluation and calibration platform should also include interfaces for fast recalibration of the ICmetric system. The interfaces should be convenient to use by non-experts to allow for the system to be deployed outside the laboratory.

We build such evaluation and calibration platform by extending publically available tools for system modelling. Such approach allows prototyping various wheelchair configurations and generating data sets from a number of sources related to the wheelchair system, namely its hardware, software, and signals derived from interfaces connecting the wheelchair with its user and its external environment (e.g. other electronic systems and devices).

5. Conclusion

This paper has introduced an overview of the application of ICmetric technology to a healthcare environment – a novel approach to debugging and encryption that allows for safe and secure use of electronic devices, as well as protecting data stored on and transmitted between the devices. The technology is based on the idea of deriving encryption keys directly from characteristics of electronic systems’ performance. The main advantage of the proposed concept over the existing security systems is that it offers an entirely template-free encryption paradigm for protecting electronic systems and data exchange. More specifically, ICmetric technology offers the following operating advantages:

- Secure communication from mobile and pervasive computing devices via the direct generation of digital signatures and encryption keys from the internal behavioural characteristics of software and hardware associated with the device. This naturally implies the major advantage that no encryption keys or device characteristic templates are stored.
- Prevention of unauthorised access to embedded and distributed devices that are increasingly connected wirelessly.
- Prevention of the fraudulent cloning or imitation of a device in order to compromise its identity and subsequent communication.
- Implicit detection of tampering of the software or hardware associated with the device via the inclusion of spyware or similar virus software since this will implicitly cause the digital signature to vary.

In addition to the above benefits, the ICmetrics also allows for secure communication in case of both human-machine and machine-machine interaction, which makes it particularly suitable for supporting distributed healthcare systems and medical assistive devices.

Apart from presenting the current state of the ICmentric system's development, the paper has highlighted the major limitations of the current solution, as well as proposed alternative approaches. The paper has formally specified the tasks involved in the development process of the ICmetrics system and can serve as the guidance for future research. The tasks are formulated in such a way so they can be tackled independently from each other allowing for the relevant solutions found to be applied in other problem domains. For example, one of the interesting research problems encountered during the development of the ICmetric system, which cannot be efficiently addressed using traditional pattern recognition techniques, is of normalizing and classifying features that possess highly non-standard multi-modal distributions. Finding appropriate techniques able to deal with the problem would contribute to the subject of pattern recognition in general.

6. Acknowledgement

This research is supported at the School of Computer Science and Electrical Engineering at the University of Essex and at the School of Engineering and Digital Arts at University of Kent through the European Union ERDF Interreg IVA initiative under the SYSIASS grant.

References

[1] W. Lutz, W. Sanderson1, and S. Scherbov, "The coming acceleration of global population ageing", Nature 451, 2008, pp. 716-719.

[2] Y. Kovalchuk and V. Callaghan, "A Self-Organizing System for Online Maintenance of a Living Organism", Proceedings of the 6th International conference on Intelligent Environments, 2010, pp. 283-288.

[3] Y. Kovalchuk, "The Ministry of Interfaces (Doors)", Intelligent Environments, Creative Science 2011, IOS Press, 2011.

[4] A.B.T. Hopkins, K.D. McDonald-Maier, E. Papoutsis, W.G.J. Howells, "Ensuring data integrity via ICmetrics based security infrastructure", IEEE, NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2007), 2007, pp. 75-81.

[5] A.B.T. Hopkins, K.D. McDonald-Maier, E. Papoutsis and W.G.J. Howells, “Adaptive Online Profiling Hardware for ICmetrics Based Security”, IEEE, NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2008), 2008, pp. 498-504.

[6] A.B.T. Hopkins and K.D. McDonald-Maier, “Debug Support Strategy for Systems-on-Chips with Multiple Processor Cores”, IEEE Transactions on Computers, Vol. 55, No. 2, 2006, pp. 174-184.

[7] E. Papoutsis, G. Howells, A.B.T. Hopkins, K.D. McDonald-Maier, “Integrating Multi-Modal Circuit Features within an Efficient Encryption System”, Journal of Information Assurance and Security, Vol. 2 No. 2, 2007, pp. 117-126.

[8] G. Howells, E. Papoutsis, A.B.T. Hopkins, and K.D. McDonald-Maier, “Normalizing Discrete Circuit Features with Statistically Independent values for incorporation within a highly Secure Encryption System”, 2nd NASA/ESA Conference on Adaptive Hardware and Systems (AHS 2007), 2007, pp. 97-102.

[9] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, “Integrating Feature Values for Key Generation in an ICmetric System”, IEEE NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2009), 2009, p. 5.

[10] L. Wei and H. Hu, “A Hybrid Human-machine Interface for Hands-free Control of an Intelligent Wheelchair”, International Journal of Mechatronics & Automation, Vol. 1, No. 2, May 2011, pp. 97-111.

[11] T. Vo-Dinh, “Biosensors, nanosensors and biochips: frontiers in environmental and medical diagnostics”, Proc. of the 1st International Symposium on Micro and Nano Technology, Honolulu, Hawaii, USA, 14-17 March, 2004, pp. 1-6.

[12] E. Oosterbroek and A. van den Berg, “Lab-on-a-Chip: miniaturized systems for (bio)chemical analysis and synthesis”, 2nd ed., Elsevier Science, 2003.

[13] D. R. C. Soutar, A. Stoianov, R. Cilroy and B. V. K. Vijaya Kumar, “Biometric Encryption”, ICSA Guide to Cryptography, R. K. Nichols, Ed. New York: McGraw-Hill, 1999, pp. 649-675.

[14] A.K. Jain, S. Prabakar and A. Ross, “Biometrics Based Web Access”, Tech Report TR98-33, Michigan State University, 1998.

[15] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, “Biometric Encryption (TM) – Enrolment and verification procedures”, Optical Pattern Recognition, vol. 3386, 1998, pp. 24-35.

[16] S. Hoque, M. Fairhurst, G. Howells, and F. Deravi, “Feasibility of generating biometric encryption keys”, Electronics Letters, vol. 41, 2005, pp. 309-311.

[17] J. Lee, M. Tehranipoor, C. Patel, J. Plusquellic, “Securing Designs against Scan-Based Side-Channel Attacks”, IEEE, Trans. Dependable and Secure Computing, Vol. 4, No. 4, Oct. 2007, pp. 325-336.

[18] Bodo, “Method for Producing a Digital Signature with Aid of a Biometric Feature”, German patent DE 42 43 908 A1. 1994.

[19] P. K. Janbandhu and M.Y. Siyal, “Novel Biometric Digital Signatures for Internet-based Applications”, Information Management and Computer Security, Vol.9, No.5, 2001, pp. 205-212.

[20] J. Daugman, “Biometric Decision Landscapes”, Tech Report TR482, University of Cambridge Computer Laboratory, UK, 2000.

[21] Y. Yamazaki and N. Komatsu, “A Secure Communication System Using Biometric Identity Verification”, IEICE Transaction on Inf. and Syst. E84-D (7), July 2001, pp. 879-884.

[22] W. Sheng, G. Howells, M. C. Fairhurst, F. Deravi, K Harmer, “Consensus Fingerprint Matching with Genetically Optimised Approach” Pattern Recognition Vol. 42, No. 7, 2009, pp. 1399-1407.

[23] W. Sheng, G. Howells, M. C. Fairhurst, F. Deravi, “Template-free Biometric Key Generation by means of Fuzzy Genetic Clustering”, IEEE Transactions on Information Forensics and Security, Vol. 3 No. 2, 2008, pp. 183-191.

[24] W. Sheng, G. Howells, M. C. Fairhurst, F. Deravi, “A Memetic Fingerprint Matching Algorithm”, IEEE Transactions on Information Forensics and Security, Vol. 2, No 3, Part 1, 2007, pp. 402-412.

[25] B. S. Todd, “An algorithm for the detection of peaks and troughs in physiological signals”, Oxford University Computing Laboratory Programming research Group, Sept 1997.

[26] K. Harmer, G. Howells, W. Sheng, M. C. Fairhurst, and F. Deravi, “A Peak-Trough Detection Algorithm Based on Momentum”, International Congress on Image and Signal Processing (CISP2008). Sanya, Hainan, China, May 2008.

[27] G. H. Givens, “Consistency of the Local Kernel Density Estimator”, Department of Statistics, Colorado State University, Fort Collins, Colorado, 1994.