Biometric Incorporation in Pervasive and Autonomous Systems Emphasising the use within e-Health Specific Smart Homes

Peter William Matthew
Edgehill University
Business School
St Helens Road, Ormskrik

Abstract

With an aging population and the increase in serious diseases smart homes and telehealth is becoming more and more prevalent. As these computer systems become increasingly widespread and complex, they become progressively harder to update, troubleshoot and configure without a large expert team of maintainers. One solution is to use autonomous systems to do the work much more quickly and efficiently. As autonomous systems become more sophisticated and understood, security concerns and authentication are coming to the fore as important areas in which more research is needed. With the constant search for the illusive ideal security identifier biometric systems have become more widespread and have entered the public eye. This paper will look at the connection between smart homes, biometrics devices and autonomous systems. into biometrics.

1. Introduction

Smart homes and assistive technology are becoming more and more important as the general population ages and as people live longer there will be more need for these kinds of technologies. However, with these new complex systems the maintenance and security aspects become more prevalent., aspects which can be incorporated into autonomous and biometric systems.

Autonomous systems are becoming more widespread as the complexity and sophistication of computer systems have been improving, and thus it has been possible to have a greater impact within the business and social worlds. Autonomous systems need varying degrees of human intervention, depending on their complexity, to operate and are therefore ideally suited to certain jobs that would be too costly, or impractical for humans to complete the tasks such as robotic production lines and automated teller machines.

The security and data retrieval aspects of these systems would be created using biometrics. It would fall to these biometric devices to gather the data necessary for smart home users to be monitored regarding any health issues they may have such as high blood pressure or diabetes.

2. Pervasive Systems

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."[18]. This exemplifies pervasive systems as systems that are saturated in technology but are not invasive but meld with the user's interaction creating a seamless union of computing and life [19] [20]. There are two very closely related areas to pervasive systems which are distributed systems and mobile computing. These areas influence pervasive systems in certain ways and some of their underlying principles aid the construct of pervasive systems [19].

Pervasive systems have a number of issues in common with mobile and distributed computing as well as some that are specific too pervasive systems. Four examples are:

- Effective use of smart spaces
- Invisibility
- Localized Scalability
- Masking Uneven Conditioning

The effective use of smart spaces, specific geographical areas such as a room or corridor, allows the combination of a building and computer infrastructure. This allows things such as lighting, heating, and resource changes depending on the user [19]. This is done by one system sensing something about the user and supplying the information to the other system thus creating the effect. This would be exactly how smart homes could, and are, implemented into autonomous systems [20]. As well as this concept there is the ability for certain objects and software's to react differently depending on their location, for example a piece of software may not run because the computer is not in a secure area of a building and the software will not access sensitive data [19]. This would be vital when dealing with personal data within a smart home system, such as bank details in a normal home setting or medical

information in a e-health setting. Reference [18] advocated an attempt at invisibility for the technology saturated systems, thus removing the computational devices from the user's perception but leaving all of the services and resources for use. This is a very difficult task to complete and thus there needs to be a level of acceptable user distraction [18][19].

As with all computational devices, as they get more complex they require more and more resources, this is especially true of pervasive computing as the interactions between smart spaces and devices needs more bandwidth, and energy. The main solution to this is to promote scalability in all things, this includes aspects such as; the further from a pervasive system a device gets the less interactions there are thus reducing the amount of data and resources needed allowing the devices and pervasive systems to use their resources more usefully [19]. The last area is masking uneven condition, and this is possibly one of the most important aspects currently, however as more pervasive systems appear and are used then this aspects importance will decrease. It is unlikely that there will be a uniform spread of pervasive systems across a moderate geographical location for many years therefore the solution is to make the user's personal computing space compensate for a lack of services and systems within an area.

2.1. Smart Homes

According to UN Department of Economic and Social Affairs Population Division, in the 21st century the average life expectancy will increase from 46-89 to 66–93 years of age [1]. Reference [2] indicates that this will mean between 2100 and 2300 the number of people within the 65 and over age group will increase from 24% to 32%, with a similar increase for the over 80s age group. This, coupled with the increase in disabilities and diseases that cause prolonged care such as Alzheimer's and strokes, means that there is a greater demand for health care and many hospitals and practices are searching for methods that will allow them to reduce costs but keep patient satisfaction [3]. This call for lower costs has seen healthcare authorities looking towards ICT for help. Now with the advancements in size, power and complexity of computing systems they are able to use some computer systems as part of e-medicine, e-health, telehealth etc [2].

Smart Homes are homes that hold a variety of sensors that can help monitor the house's occupants for a number of medical reasons [2]. These sensors can include: glucose sensor for diabetics, blood pressure monitors and respiration monitors, these then allow the smart home to compare a list of acceptable parameters and if not within a specified range then to contact a registered person most likely a carer, doctor or other health professional [2]. This detector would look for a specific illness and then would react to the data regarding the illness; however there are also forms of smart homes that are designed for disabled people, and elderly people. This is done so that these people are able to maintain their independence but may still need some level of constant care. As the levels of care required can differ wildly, from someone who has trouble lifting and opening things to someone who needs help dressing, the forms of assistive technology are also as ranging [2].

A Smart Home can be considered both pervasive and autonomous in nature as the sensors are integrated into the home environment and computing systems behind the sensors can make decisions on courses of action dependent upon readings gathered. Examples of these technologies can include, at the lowest level of invasive care, automated can and bottle openers to robots that are designed to aid in simple care tasks such as helping bath and dress a patient[3]. One or two of these technologies does not constitute a Smart Home, or a pervasive system. However when combined with a lot of different devices that communicate with each other and specific external sites such as hospitals and surgeries then it becomes a smart home which in essence is a variant of a pervasive system.

The obvious advantages of a Smart Home is that it can help and support people with disabilities or illness's that require regular monitoring and they can help the elderly live independently but with a level of care they would not have been able to access. These advantages can also be aspects of general healthcare such as regular blood pressure tests or walking ability by using pressure plates and blood pressure sensors which would then allow automated collection of the data which can be processed [4][5]. There are a number of disadvantages with the use of Smart Home with people who are ill or disabled and these are mainly due to a distrust of the systems. Many health care organisations mention the cost of implementation as the major problem as well as the problems about confidentiality and privacy of the patient [6]. Alongside social issues there are some ethical issues and a primary one is making sure the patient knows and understands what the proposed telehealth system will consist of and what to expect. Certain countries actually will not allow the use of Smart Home based health services to be used without the informed consent of the user and in other countries the use of telehealth systems will often not be covered for any insurance that the user might have [7]. This makes the use of Smart Home health systems very unlikely to be used until a change in legislation [8] However they will become an important area in which modern medicine and pervasive computing can, more completely, head.

3. Autonomous Systems

Smart homes have a number of issues that need to be balanced depending on the user's needs especially when dealing with disabled or ill people who need to have conditions maintained. This could be, at a basic level, maintaining a set level of rehabilitation and allowing the user to keep their illness under check, e.g. regulating the heat in a room for people that have fevers, or temperature related illness such as blood that clots easily. This is remedied using warfarin which is an anti-coagulant; however a known side effect of this drug is cold intolerance [9]. This can be achieved by using autonomous systems, or at least striving to follow an autonomous ideal.

Autonomous systems surround us, in both the natural and technical world, and we often do not realise what they are or how the work. From automated manufacturing devices to robotic creations and the human body. Reference [10] discusses the concept of the human nervous system being the ideal paradigm of an autonomous system and any autonomous systems should be developed with the human nervous system as the framework, this is also agreed on by [11]. The concept was consolidated by [11] who believed that the nervous system is one of the greatest autonomous systems in existence and thus deserving of mimicry. From these concepts, a small list of characteristics grew that defined the human nervous system and became the quantifiable way to create autonomous systems. It is these characteristics that the implementation of biometric device must turn to for complete immersion within the autonomous system. Another major reason that the human nervous system is an autonomic ideal is that it, whilst in conjunction with the endocrine system, is able to maintain a state of homeostasis [11]. This state is found whilst dealing with exceedingly complex autonomous systems, be it from a company, a cell or any other large, complex system. Homeostasis involves maintaining a complex system by developing and maintaining a series of equilibriums which are controlled by a specific rule set or mechanism [11] [10]. Examples of this include keeping bodily resources at a certain level by making sure they do not drop below a danger point such as glucose [12], or making sure that a stock level is automatically maintained so that there is always enough stock in to complete a certain order [11].

In doing this the system is kept stable and only small reactions are needed to maintain the delicate equilibrium. It is to maintain these equilibriums that biometric device would be able to affect. Biometric devices could gather biometric data about a user which could then be used to develop a profile. Then any deviation on that profile from further biometric input would allow the autonomous system to automatically balance the system thus maintaining the equilibrium. This would enable medical conditions to be monitored, as well as giving more data to the autonomous system which in turn can be used to maintain these equilibriums. When dealing with any machine, or system there are many variables that deal with everything within the system, however the essential variables within a system must be kept within a finite range, and within viable limits, and if these essential variables change too rapidly or do not stay within the safe parameters then the system can go into shock which can result in dissolution or death [11]. Reference [12] states adaptive behaviour is defined as following "the essential variables within the system limits". As adaptive behaviour is designed to prolong existence and the disregard of essential system variables can cause complex and fatal problems. Secondly [12] also states that if an essential system variable is pushed outside the system equilibrium then the adaptive system endeavours to return the equilibrium back to its original level. This is exactly what an assistive smart home aims to do thus lending more credence to a good encapsulation of different systems. Further postulation indicated that there were two ways that the system could be disturbed which are: often minor impulses to the main variables, and a method to change the parameters of the equilibrium [11].

4. The Human Nervous System Paradigm

The nervous system paradigm is the area in which biometric can be implemented with the greatest level of fore planning and ease. As each section is sub split up it gives the design a much greater area of implementation and thus this section is most important is it acts as the glue in which these two disciplines could be combined.

The ultra-stable system concept [12]says, an autonomous system must be able to adapt the behaviour depending on relevant input, in this case biometric device input, enabling the efficient changing of variables to keep the system equilibrium at the relevant level [11]. This adaptive behaviour is the most important aspect, and the most defining aspect, of an autonomous system as by maintaining this state of equilibrium the system is able to survive, recover from faults or attacks and reconfigure if needed [13][11]. This is the main reason that smart homes with autonomous systems implementation would be so useful, as the ability to adapt to a user's needs might, in certain circumstances, mean the difference between life and death.

To sense any potential changes, an autonomous system needs both internal and external sensors providing detailed information about its current state such as temperature, C.P.U usage, queue information, and when combined with biometric

systems things such as humidity for fingerprints, or ambient noise levels for vocal recognition [11][13][10]. These self knowing and adaptive behaviour concepts were quantified into four headings: self awareness, self configuration, self optimisation and self protecting [10] and then expended on to include context-aware, open, and anticipatory [11]. These headings, when taken together, create the gestalt entity that is an autonomous system. Implementing biometric devices within this subsection would make the most sense as the biometrics are gathering data that can then be used by other aspects of the system.

According to reference [10] and [11] self awareness is one of the primary and most important aspects of the autonomous system. This is because the autonomous system must keep a constant watch on its own process thus keeping its states and behaviours known and able to act accordingly. When dealing with biometric devices, the amount of data the system would be able to gather would increase dramatically, making awareness of the internal and external surroundings, when gathering this data, highly important [13]. For example, if the autonomous system had a vocal recognition biometric then the system would have to be aware of ambient noise at the biometric device, and be able to optimise the system because of this. Self awareness is knowing a systems state at a global, and local level and thus providing the information to the rest of the adaptive behaviour systems within the autonomous whole [11][13]. As this aspect of autonomous systems is wholly dependent on knowing what devices are attached to the system and understanding there data flows and resources within said system there is little a biometric device intervention would do here.

When a system is self-aware then it is able to use this knowledge to change the system in a number of ways, mainly keeping the equilibrium constant. Self configuration is therefore a vital attribute as it allows systems to react to changes within it and reconfigure accordingly. This allows a greater degree of autonomy and reduces the dependences, if any, on human influences [10]. As the system becomes increasingly complex more changes can occur, and if Ashby's ultra-stable system is the goal then the greater the need for this self configuration, as it would take human experts many times longer to complete the work, resulting in lower efficiency both in system and fiscal resources [10] [11]. As with self-awareness, the main goal of self configuration is to detect and install any new system devices seamlessly and to do this as efficiently as possible. Thus a new device will be installed and then configured to use a certain route, or use a certain set of external media such as printers or cameras. This area would be vital when concerning biometric device incorporation, as a number of different biometric complex devices would be used within the system such as multi model devices like an integrated hand, vein and eye scanner. These things would have to be configured and if done by hand would take a long time, when compared to an automated system. Self configuration is vital to any autonomous system and the biometric devices should be as heterogeneous as possible to allow the autonomous system to configure them. Additionally if a user logs into a system using a biometric device, and there is a two layer security such as a fingerprint first, then second biometric device, the data gathered from the first could configure the second security device. This means that if a user has entered primary data for two out of three devices then the autonomous system must be able to find the data and allow the user to enter more data into the correct device and not allow any information to be sent from the third erroneous device [11]. This occasion could occur if there were people unable to use one form of biometric e.g. blind people for iris/retina scans, hand geometry for amputees etc. This becomes increasingly more important as the system is used in a smart home context as there would be a variety of people using the smart home over the course of time, and each person might have different issues regarding the ability to use different biometric devices.

When a system is stable, and any configuration has been completed, the next stage in its lifecycle is to extract the maximum from the system without harming it, and thus optimisation is developed. Optimisation is the process of making something work better for a specific process [10] [11] [13]. Optimisation could include, making sure that when a biometric device is used it checks ambient superfluous data, such as sound or light, and then optimising the system to prevent these effects tampering with the overall integrity of the data. As with, and if not more so, self configuration self optimisation is a vital aspect of the autonomous systems as it improves the efficiency and compatibility of devices that are connected to it. With the complexity and quantity of optimisation potential within any system the man power in both time and expertise to conduct the changes would be staggering [11] [13]. This is why self-optimising autonomous system are useful as they not only can optimise the system in a general way but they can change and include different optimisation options much more quickly than a human team could [10]. Other aspects of self optimisation would include biological optimisation; including light, heat, and sound. When a user enters the system and uses a biometric input device the system is able to detect basic preferences and optimise the system accordingly such as changing lighting levels and volume levels. In addition to this, other improvements may occur such as the changing of

temperatures to match a preset depending on the body temperature of the user. As well as external biological optimisation the system could optimise itself to a user's resource preference such as providing more in-depth image software to web designers and providing powerful coding software to developers, thus optimising their use of the system the possibilities with this form of optimisation are endless.

After the configuration and optimisation of system devices, the next issue that will normally occur is a failure safeguard, and it is the second most important aspect of autonomous systems [10]. The normal fault procedure is that it is detected by the human administrators, and then it is fixed. However due to the self- awareness aspect of autonomous system, the system itself is able to detect an error and then act accordingly [11]. According to reference [14] self healing systems reconfigure themselves to heal after a fault has been detected, and as a result the next stage of this process the system should be able to change its behaviour and possibly the basic equilibrium of the system in response to a fault. If a biometric node is damaged for some reason, then the system should be able to stop people using the node and direct them to another, this would be the behaviour change [11]. This concept could be coupled with user preferences for biometric device. The same route would be taken if the user was unable to use a certain biometric device due to disability, similar to when a device had failed and the user was being rerouted to another device whilst the broken device was being assessed. Alternatively, if the fault is software based then the system should be able to fix it by using a number of diagnostic programs. However, if the problem is a hardware issue then the complexity of the system and its surrounds plays a significant part in the fault correction process. For example: if the system is held within a larger automated structure then there may be some robotic ability to change hardware and fix problems. However if there is no such external structure then the fault would have to be fixed by a human administrator [14]. When dealing with large systems of any kind, tracking down and solving problems and failures is a paramount issue, and within an autonomous system it must have the ability to do so. The system must be able to detect the issues and then solve them as reference [10] and [13] state; in addition the system should be able to checking on users' needs, resources issues and other aspect related to self optimisation as demonstrated by [15] [14].

The next, and last of the original areas, to be observed is self protecting. The current trend for system protection includes hardware, software and policies set out by the human administrators [10]. Whilst most errors will be found by the system, it will not be capable of fixing the errors and will need the human administrator to implement the solution [11]. Defence and protection are vital parts to any system and an autonomic system needs to be able to defend itself from both internal and external threats, thus keeping the system secure and not compromising its integrity. The autonomous system will not only be able to find the faults but will be able to isolate them and fix the fault, and this is where the autonomous system excels as it links to the self healing aspect and the self configuration and optimisation [11]. This is all done a lot more quickly than a human would be able to do and more efficiently [10]. In spite of these problems the self protection aspect would work very well with biometric systems as the biometric failure protocols could be linked to the autonomous self protection system thus integrating both the technologies in a harmonious group, this combined with the self awareness, optimisation and configuration would strength the cross discipline system [11].

After the initial four characteristics had been considered they were expanded upon by [11] to include context aware which is very similar to the self aware stage. As with self awareness the autonomous system must be aware of its surroundings, and react accordingly should they change. Thus this provides more data for the autonomous system to deal with. This could be very important depending on the system as it would provide data from outside the system giving the system more chance to optimise its processes.

An example of this would be a system including a biometric scanner, such as a fingerprint scanner. This device would have a number of issues relating to it and research into "gummy" shows that 'liveness' detection is a very important aspect of certain biometric devices. Therefore to be able to detect extremes such as temperature would be vital. If the temperature was to low then the scanner may not be able to pick up the 'liveness' data that it was looking for such as perspiration and heat. However with a context aware autonomous system it would allow the system to see these local issues and optimise the system in light of them such as changing the security style or heating up the scanner [11]. The biometric device would have to be optimised to the locale that they were being used. The local temperature, weather and humidity would play important roles by supplying the system with data hence allowing it to self optimise itself for user within that locale.

The next stage explored was the openness of the system, and in many ways this could be deemed as the most important aspect. This option had little to do directly with the autonomous system, and more with the system development and continuous redesign [11]. For the system to work it needs to be heterogeneous so that everything will be able to work on it and with it. This includes, hardware, software and with policies, as failure to provide this

heterogonous system would stop aspects working and thus reducing its effectiveness . However the size of the system would be a paramount factor in this as the larger the system the more devices, and more complex devices, the more software's and other parts of the system would be introduced. This calls for heterogeneous systems and especially if there would be biometrics involved, as the amount of biometric devices needed would be very large and the incorporation of them would take a lot of software across a wide range of both systems and devices [11].

Lastly when provided with all of these features an autonomous system can work well and efficiently, however to reach the heights of efficiency the system would need to understand what the consequences of certain actions would be and thus anticipate certain actions[11]. This anticipatory knowledge would be there to enable the system to react to any new configuration or optimisation needed. For example if the system knows that at eight thirty every morning there will be a large influx of people using the security systems then it can optimise those systems with more resources, or opening extra nodes etc [11]. Additionally if the system knows that a fault has been detected and that it must be fixed then it can anticipate a potential hardware or software fix, and therefore optimise the system so that the fixes would cause the least amount of disruption. This could be a very useful and vital aspect of autonomous systems and if it could be linked to machine learning then it would improve the system exponentially [11].

5. Biometric Issues

Biometrics "*refers to the automatic identification or identity verification of living persons using their enduring physical or behavioural characteristics. Many body parts, personal characteristics and imaging methods have been suggested and used for biometric systems: fingers, hands, feet, faces, eyes, ears, teeth, veins, voices, signatures, typing styles, gaits and odour" [15]*. As biometric and medical technologies have evolved more and more biological features are being considered as the elusive perfect identifier. There are some major worries within the biometric fields and these concerns would have to be addressed if the vision of a biometric secure future is to be realised [15].

Biometric data gathering techniques, by their nature, individualises users resulting in the need for a more robust database system to store the details in. Passwords, usernames and other similar data types are easy to store for both size and security in an authentication system [16]. When the data is a two-dimensional or three-dimensional image of a user's eye or fingerprint, for example, then the amount of storage space required alone will increase dramatically [16]. This therefore creates a requirement for either better database design or advanced compression formats to be developed to support the use of biometric data [15]. Additionally, there exist the potential problems of having audio files for speech recognition or brain scan results. Also, by having this data within a database the cost of losing any of it through negligence or attack would be excessive, especially if there is a wider spread of biometric devices providing very personal data to people with malicious intent [15]. Due to the very nature of smart homes, they collect and store data about its occupants. This could take the form of blood pressure statistics, periodic weight checks and balance calibration checks. As this data is already being stored then the reuse of it to be used as authentication data would decrease the amount of storage required as certain areas could be combined, such as iris/retina scans and cataract monitoring.

Any complex system will face threats and often there will be sensitive data held within systems, but with a smart home the information is even more sensitive both legally and personally. Thus threat models are needed to highlight any potential threats that the system might face and specifically what the threats would entail, and thus who would be the main threat group and how would they threaten the system. Therefore for a biometric system to succeed there would need to be a threat model that has been verified and well designed [16]. This would enable biometric authentication and smart homes to be completely encapsulated and until this has been fully successful there can be no full implementation within a wider systems. Due to the fluidity and interchangeable issues that each smart home might face, a biometric and smart home encapsulation would face specific extra threats, but there would need to be a backbone of standard threat responses that are generic across all systems. This model would provide the security system guidelines on how to deal with security failures, such unauthorised users getting access to the system or security successes, such as prosecution for users who tried to access the system without correct authorisation.

Normally a biometric system will benefit from other systems gathering other pieces of information. For biometrics to operate at peak efficiency a number of other data gathering techniques need to be incorporated into the system. For example, confirming an individual's identity from a voice map only says who that person is, but nothing about them. With other data held within the database the authentication aspect can confirm or deny a user's access into the system, and then by interfacing with the other information the user's preference can be found, such as office temperature. This would normally be a list of preferences within an office or personal environment. However when considering biometric implementation in a smart home system the information held could be a host of medical data

which in turn could allow the smart home to operate at a greater level of competence. This encapsulation of technologies is what is needed for the secure and comprehensive incorporation of biometric techniques in today's technological world [15].

One of the first, and most important process within biometric authentication, is the capture of the original specimen [15], whatever this may be. The gathering and registering of the original specimen is of the utmost priority, as no matter how robust the authentication system is, if the original specimen gathering technique is ineffective or flawed the rest of the system will follow. This means that adequate capture and compression formats would need to be used, as well as regular checks to make sure they have not degraded in any way.

A significant problem to widespread implementation of biometric systems is the public reluctance to accept biometrics as a mechanism for security. This is due to a wide-held view that biometric systems are intrusive and can be used to get identity information easily by people with nefarious motives. Moreover many people have fears about using identifiers that use body parts as the identification means [17]. These fears can be consolidated into a number of specific worries which include security of the data repository that holds the templates, the confidentiality of the data and whether the programs gathering these data fragments are only being used for their purpose. This might be a more important area to consider when combining with a smart home system. This is because the people using the smart home will be using it as an assistive technology and will be ill or disabled. It is possible that these demographics will have more reluctance in providing biometric data that involves using parts of the body that are affected by either the illness or a disability. A potential solution to some of these issues would be to develop a third party regulator that standardises security and codes of conduct within biometric feedback [17]. Using this body some of the fears about biometrics, which comes from the lack of understand and widespread public ignorance would be alleviated in some way. These questions about, public fears, issues and potential solutions will be expanded on within the questionnaire.

Apart from reluctance on the part of the public, to use biometric systems, sometimes biometric security systems are overly elaborate for the system requirements. If all that is needed is simple age verification then there is no need to know who the customer is, simply if they are of age. There are a number of solutions to this, and one of the simplest ones is to use normal ID cards for age verification. A second solution is to use cut down versions of biometrics which would only provide certain information that would be required, such as age, or membership number etc.

As with all security related systems, there has to be complete coverage of everyone who needs access to the system. This causes a substantial problem as some people may not be able to provide certain biometric data such as fingerprints, for example amputees, or retina scans for people with vision problems. The only way to solve this issue is to have the system take multiple items of biometric data. Either the users can then be permitted to determine a certain kind of data to use, or the system can decide which to use. Some people may not see the urgency of this problem. However if a company has 5,000 users on site, and one percent of those users cannot be biometrically authenticated, this results in fifty users who cannot access the information or services they need. If this kind of system was to become national, or even global, then the numbers become even more problematic [15]. This becomes an even greater problem if used within a smart home scenario as the users might well have problems providing certain biometric data such as retina/iris scans.

A final issue is the security within the system itself. Even though it is providing a security system, the security within itself needs to be paramount. With other identification systems, such as passwords or cards if one is lost or stolen then it is a easy job of cancelling the identity and creating a new one. With biometrics it is not possible to get rid and change a fingerprint or voice pattern without extensive surgery, thus providing a problem if they were to be lost [15].

6. Conclusion

Smart homes are a thing of the future, something that will enable the aging population to live out their lives in relative comfort. This when coupled with biometric devices for both security and authentication allows a harmonious encapsulation of systems. There are many biometric systems in place today that work, which are efficient, and have been in place for a number of years which indicates that they are an accepted security system

One of the major drawbacks of the biometric systems is the need for massive amounts of storage, this is due to the different authentication styles, such as video files, images, audio files etc. Another issue with biometric devices is that they have a set of security issues that are not present in other devices, and this is predominantly due to the data they use. When dealing with human data there is the issue that things such as blackmail and physical coercion may become more prevalent and a greater risk to be contended with. Thus other security methods would have to be taken, such as security guards and cameras near the biometric devices. Overall it seems the best option when dealing with biometrics is not to depend on one biometric aspect instead to use a multi-model style security. This could mean that the

main biometric is a fingerprint scanner which in turn is combined with a password or number, and finally combined with a key card. This multi-model system is much harder to break and much more secure, and provides some defence against biometric only threats such as blackmail and physical coercion.

Overall it has become obvious that the autonomous systems could benefit a smart home as it would enable quicker reactions to different scenarios and would be able to make decisions based on what it knew and not what it would be told when an administrator was able to check it

7. References

[1] United Nations Department of Economic and Social Affairs Population Division (2004) 'World Population Prospects the 2004 Revision' http://www.un.org/ (1 May 2011)

[2] Chan M, Campoa E, Estèvea D & Fourniolsa J (2009) 'Smart homes — Current features and future perspectives' *Maturitas* 64(1) p.90-97.

[3] Forlizzi J (2005) 'Robotic products to assist the aging population' *Interactions* p16–8.

[4] Celler B, Lovell N & Basilakis J (2003) 'Using Information technology to improve the management of chronic disease' *Medical Journal of Australias* 179(5) p.242–6

[5] Paré G, Jaana M & Sicotte C (2007) 'Systematic review of home telemonitoring for chronic diseases: the evidence base' *Journal of the American Medical Informatics Association.* 14 p.269–77.

[6] Rahimpour M, Lovell N, Celler B & McCormick J (2008) 'Patients' perceptions of a home telecare system' *International Journal of Medical Informatics.* 77 p.486–98.

[7] Wooton R, Bloomer S & Corbett R (2000) 'Multicentre randomized control trial comparing real time teledermatology with conventional outpatient dermatology care: societal cost-benefit analysis' British Medical Journal 320 p.1252–6.

[8] Callens S (2003) 'Telemedicine and European law' *Medicine law* 22(4) p.733–41.

[9] Drugs.com (2011) Warfin *Side effects http://www.drugs.com/* (29 March 2011)

[10] Kephart, J and Chess, D (2003) 'The vision of autonomic computing' IEEE Computer 6(1) 41–503

[11] Hariri, S & Khargharia, B & Chen, H & Yang, J & Zhang, Y & Parashar, M & Liu, H (2006) 'The Autonomic Computing Paradigm' Cluster Computing 9, 5–17

[12] Ross Ashby, W (1960) Design for a brain (Second Edition Revised 1960). Chapman & Hall Ltd, London.

[13] IBM (2001) 'Autonomic Computing: IBM's Perspective on the State of Information Technology' http://www.research.ibm.com/autonomic/ (24 May 2011)

[14] Grishikashvili-Pereira, E & Pereira, R & Taleb-Bendiab, A (2006) Performance evaluation for self-healing distributed services and fault detection mechanisms. Journal of Computer and System Sciences 72 1172–1182

[15] Abernathy, W & Tien, L (2003) 'Biometrics: Who's Watching You?' Electronic Frontier Foundation http://www.eff.org/ (28 April 2011)

[16] Ratha NK, Connell JH, Bolle RM (2001) 'Enhancing security and privacy in biometrics-based authentication systems' IBM Systems Journal (3) http://domino.research.ibm.com/ (14 March 2011)

[17] Chandra A & Calderon T (2005) 'Challenges and constraints to the diffusion of biometrics in information systems' Communications of the ACM Volume 48 , Issue 12 pp 101 - 106

[18] Kakadiaris I.A, Passalis G, Toderici G, Perakis T, Theoharis, T (2009) 3D Face Recognition," in Encyclopaedia of Biometrics

[19] Weiser M (1991) 'The computer for the 21st Century'. 265(3) p.94–104

[20] Satyanarayanan M (1996) 'Fundamental Challenges in Mobile Computing' *ACM Symposium on Principles of Distributed Computing.* Philadelphia. 1(1)

