# TECHNOLOGIES FOR ENHANCED LIVING ENVIRONMENTS

**Gurmeet Kaur, Assistant Professor, Dyal Singh College, Karnal**

***Abstract- Enhanced living environments, supported by optimized algorithms, architectures, and by optimized algorithms, architectures, and by platforms, can help individuals needing platforms, can help individuals needing assistance maintain autonomy and improve quality of life. ELE research aims to create smart and safe environments around people needing assistance, such as the elderly and people with disabilities, to help them maintain an independent lifestyle, reduce health and social care costs, and achieve improved quality of life and advanced autonomy, mobility, social interaction, self-confidence, independence, and social inclusion. This paper describes necesisity of ELE in daily life style , technology used and security challenges for its implementations.***

## I. Introduction

Enhanced living environments (ELEs) support the seamless integration of information and communication technologies (ICT) within context-aware residences and homes. Enhanced living environments (ELEs) encompass all the technology used to support an independent or autonomous lifestyle for people with special needs, such as the elderly and people with disabilities. ELEs use ubiquitous elements to construct safe environments, known as smart infrastructures, such as smart homes. A key element in smart infrastructures is the information exchanged between devices and services to perform the required tasks. For example, wearable medical devices can help monitor a person's wellness by collecting information about the wearer and then sending this information through the network to be processed in the cloud system. Such systems can remotely monitor health, well-being, and resource consumption. Observation of this data leads to the creation of behavioral patterns, where any observed behavioral deviation can be a preliminary indicator of a health issue.[1]

However, building these ELEs requires security measures since cyber attackers can exploit the devices and cloud services, targeting confidentiality, integrity, and/or availability, resulting in the theft of personal information or leading to incorrect medical diagnosis. When maliciously exploited, ELEs can present life-threatening scenarios. Consider, for example, a person is suffering a severe heart attack and can't reach the

phone to call for emergency help. The ELE must be aware of the person's situation and emergency needs and must communicate with the required services successfully while keeping sensitive information secure.

Efforts in this area are supported by optimized algorithms, dependable architectures, and efficient platforms, converging to the realization of ambient assisted living (AAL) systems. AAL systems utilize pervasive devices and ambient intelligence to construct smart and safe ELEs.[2] Important issues relate to the missing interaction of multiple stakeholders needing to collaborate for ELEs, supporting a multitude of AAL services. AAL refers to the use of ICTs in the environments in which users are, so that these spaces are able to interact with people in a natural way, wherever and whenever they are needed, being aware of the context (situational, temporal, emotional, etc.) of the user or the environment, and to act proactively. An AAL environment requires the use of a distributed network of sensors and actuators to create a ubiquitous technological layer, able to interact transparently with the users, observing and interpreting their action and intentions, learning their preferences and adjusting the parameters of the system to improve their quality of life and work. Cloud computing and the Internet of Things (IoT) are significant elements of AAL and the endeavor to produce a ubiquitous, efficient, and cost-effective architecture that will assist targeted individuals to become more independent and to effortlessly perform everyday tasks in their familiar environment. However, gathering all this information into a remote, centralized authority where data is managed and can be accessed by human actors raises security, ethical, social, cost, and user experience issues.

Many fundamental technical issues in the ELE area remain open. Starting with the infrastructure used for data harvesting, a major concern for ELEs is the efficient use of sensors for daily data collection, storage, and mining. Adding human society as another dimension lets us define a new type of system, cyber-physical-social systems, where ICT (cyber), intelligent devices (physical), and human society (social) come together to provide high-quality AAL services to improve users' quality of life. Even if this approach is successfully applied at large scale in smart cities,[3] most current efforts still don't fully take into account the power of human beings and the importance of social connections and societal activities.

AAL establishes a new paradigm of how people use technology. This is due to its holistic and person-centred conception, so that AAL could be usable, acceptable, useful and providing social value. Of course, these AAL technologies and services must be feasible and provide business value for the companies that develop them. In order to fulfil this holistic view of technology, the solutions developed must incorporate in their conception, design and development, the involvement of experts with different backgrounds: technology, health and care, social sciences, etc. What is paramount is users' engagement, in particular of

those groups that may have a greater reliance on technology or who can receive greater support in their daily lives.

**2. Objective of Enhanced living environments (ELEs)**

The objectives of AAL are diverse, as stated by the AAL Joint Programme [4]:

• to extend the time people can live in their preferred environment by increasing their autonomy, self-confidence and mobility;

• to support the preservation of health and functional capabilities of the elderly, promoting a better and healthier lifestyle for individuals at risk;

• to enhance security, preventing social isolation and supporting the preservation of the multifunctional network around the individual;

• to support carers, families and care organizations; and

• to increase the efficiency and productivity of used resources in the ageing societies

**3. Technologies for Enhanced living environments (ELEs)**

In order to provide AAL services in their place of need, such as care centers or personal homes of older people, researchers, engineers and technicians are challenged by the wide scope of involved technological infrastructure. Depending on the sepecfic application, several technological areas and research fields can be involved. However, a common underlying infrastructure usually exists regarding areas as ambient intelligence and ubiquitous computing, that are closely related to sensor and smart home technologies.

This section, provide the required technologies for building resilient and secure cloud services for ELEs including medical devices and the required communication technologies.

In Current State of the Art of Smart Environments and Labs from an AAL Point of View: Critical Analysis, current contributions to the AAL technology development, and more specifically to smart environments and labs, are synthesized to reflect the current state of the field. Crandall & Cook focus on the engineering,

including infrastructure such as sensors and middle wares, and user needs of AAL systems, along two of the major applications of smart homes, namely health care and home automation.[5]

**Wireless Sensors Networks**

A strong approach in building ELEs utilizes implantable and wearable sensors, and wireless sensor networks (WSNs) that are supported by cloud computing.[6] For people with disabilities or for elderly people requiring constant care, the emergence of ubiquitous computing paradigms, empowered by 5G wireless communications, plays an essential role in providing better living environments. Cloud computing has been an empowering force for this endeavor, it raising several ethical, security, and user experience issues. However, the ELE technology and data could be vulnerable to cyber attacks and exploitations, which can lead to life-threatening scenarios such as incorrect medical diagnoses. [7]

A wireless network is the most common means of communication used by an ELE. [6] The Wi-Fi protocol (IEEE 802.11) declares physical and data link layer specifications to use a specific set of frequency bands for wireless local-area networks (WLANs). Even though IEEE 802.11 has been revised and upgraded over the years, it remains vulnerable since the 802.11 MAC headers is sent over the network unprotected. Moreover, it's easy accessibility and wireless nature make it difficult to prevent and/or stop attacks.

Visual sensors can be considered a very special type of sensors, since in most scenarios they are able to provide richer data about the environment than multiple other environmental sensors combined. The chapter Computer Vision for Active and Assisted Living analyses the state of the art of RGB cameras and depth sensors, detailing how pattern recognition and machine learning methods area applied to human motion and activity recognition and tracking. Planinc et al. use the traditional image processing pipeline to illustrate how current AAL projects take advantage of computer vision to approach a variety of applications from human behavior analysis to physiological monitoring. The use of depth sensors, such as the popular Microsoft Kinect, for rehabilitation and robotics among others is reviewed, detailing skeletal pose estimation and tracking techniques, as well as methods based on depth maps, point clouds and plan-view maps. Finally, existing studies are synthesized related to the accuracy of infrared and time-of-flight depth sensors in comparison to stereo cameras and other marker-based tracking systems.

Another in Ambient and Wearable Sensors for Human Health Monitoring, the authors Rodgers etal. Study how monitoring of personal activity, vital signs and physiological measures can be enabled in a manner that minimizes disruption to an individual's daily routine, while protecting their privacy at the same time. Ambient and wearable sensors that make this possible are reviewed, and special emphasis is made on

favoring engagement of individuals to reduce the reliance on health care systems and improve self-care management of chronic conditions

Advances in biomedical sensors, low-power circuits, and wireless communications have led to a new generation of wireless sensor networks, known as body area networks (BANs).[6] These networks are formed by lightweight, low-power, interoperable, and smart wearable nodes, mainly dedicated to healthcare monitoring applications. These applications aim to ensure continuous monitoring of vital parameters, without constraining the wearer's activities, therefore providing higher healthcare quality since existing health-monitoring systems lack the capability of real-time remote diagnosis and on site treatment, and early sensing, monitoring, and diagnosis are essential to delivering high-precision treatments in time.[8] The wearable nodes measure, process, and transmit physiological signals to a hub and then to the Internet so care givers can access the data collected in a health server for real-time diagnosis to trigger the appropriate treatment procedures. BAN technology could potentially revolutionize healthcare delivery by enabling applications such as ubiquitous health monitoring and emergency medical response. Because BAN applications deal with sensitive medical information, they have significant security and safety implications, such as hardware failures, software errors, and cyber attacks that undermine their trustworthiness.[6] To develop and implement reliable healthcare systems, there are several challenges. Because BAN sensors are constrained in terms of computing, storage, and power, communication protocols, fusion algorithms, and BAN control and management methods must be optimized to work with them. In addition, security, privacy, and integrity of BAN resources and information are critical since attackers can maliciously stop the operations of the sensors, change their data, and prevent them from transmitting information. This can mislead caregivers and medical staff and a danger a person's life. Finally, advances in IoT (Internet of Thing), cloud computing, and wearable technologies used to deliver 24/7 remote monitoring, diagnosis, and treatment also introduce in securities.

**Cloud Computing** The US National Institute of Standards and Technology defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, servers, networks, applications, storage, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[9] Thus, cloud computing represents a feasible way for accessing information/computation anywhere and anytime as a utility. Cloud computing provides support for applications, including power grids, mobile communications, transportation, real-time and critical applications (such as medical services), and living environments. Even though cloud computing provides many benefits; it also entails potential threats, especially in healthcare due to the information's sensitivity.

**4. Challenges for Enhanced living environments (ELEs)**

Effective ELE solutions require appropriate ICT algorithms, platforms, and architectures, with a view toward the advancement of science in this area and the development of new and innovative connected solutions (particularly in pervasive and mobile systems). Mobile platforms can now bring the computation power made available by highly advanced datacenters closer to the user. In addition, the actual interconnection between mobile and cloud systems is possible by combining the capabilities of individuals, as they interact with each other, through a well-designed ubiquitous technology. This combination will benefit the platforms of tomorrow through the help of new models for understanding the environment (such as participatory and opportunistic mobile sensing), performing computation (for example, mobile cloud computing), or even exchanging data via mobile ad hoc networks. These issues are supported by inter cloud architectures and progressive integration of sparse, geodistributed resources into big datacenters, where energy-efficient message-exchanging models are already developed.[10] Many ELE applications are used by people with special needs (such as the elderly and people with disabilities), with 24/7 continuous monitoring and control of the environment, and access to care services when needed. One important problem is the expectation and acceptance of new technologies by these populations. The solution is to provide noninvasive and transparent platforms with minimal interaction between the ICT platform and the user. Moreover, ELE applications should be strongly user oriented, involve users at all stages, collect the necessary information anytime, anywhere, and provide feedback to improve quality of service (QoS).

**Security challenges**

The most relevant security requirements for a successful ELE are

• Resiliency: Services must operate correctly even under adverse conditions.

Privacy: Only the people with the right credentials can access confidential information. • Integrity: The information stored in the cloud shouldn't be altered. • Availability: The information must be available at the moment it's required so the right decisions can be made as soon as possible.

Conventional fault-tolerance and information security solutions can't be applied directly to manage ELEs because such solutions are application or domain specific and require a certain amount of computational power that might not be available for small wearable devices. Hence, we require a more general architecture that's open and secure and can tolerate all types of ELR threats.[11]

The increasing number, complexity, heterogeneity, and interoperability of interconnected devices, as well as the increasingly sensitive data transmitted, make ELEs an attractive target for attackers. To better

understand the cyber security implications of ELEs, requires need a threat model to analyze the security problem, design mitigation strategies, and evaluate solutions. The general steps for building a threat model are as follows:

• Identify attackers, assets, threats, and components. • Rank the threats.

• Choose mitigation strategies.

• Build solutions based on the strategies.

ELE threat model for different ELE components to increase our understanding of the security needs is presented here. ELE devices, such as sensors and actuators, can impact human safety, energy, money, time, and so on. Mitigation approaches include lightweight encryption, sensor authentication, intrusion detection and prevention services (IDS/IPS), anti jamming, and behavior analysis. Network failures include router or firewall penetration. Attackers that obtain access to the network can get personal information about users, which can affect their safety, money, and reputations. Counter attacks include strong authentication, encryption, packet filtering, and IDS/IPS. Implantable and wearable medical devices (IWMDs) are another potential point of failure. Attacks on IWMDs, which include cardiac monitors, pacemakers, drug diffusers, fall detectors, and blood pressure monitors, target human safety, money, trustworthiness of medical devices, battery, and so on. Solutions include authentication, encryption, runtime-anomaly detection, and behavior analysis methods. Finally, attacks can be launched against cloud computing and medical application services. Attackers mainly target information on ELE wearable/implantable devices to gather money or threaten safety. Encryption, authentication, session identifiers, IDS/ IPS, selective disclosure, and data distortion should be applied to mitigate such security concerns.

**5. Conclusion**

This paper describes ideas for research in the ELE/AAL field. Enhanced living environments (ELEs) encompass all the technology used to support an independent or autonomous lifestyle for people with special needs, such as the elderly and people with disabilities. Efforts in this area are supported by optimized algorithms, dependable architectures, and efficient platforms, converging to the realization of ambient assisted living (AAL) systems. ELEs use ubiquitous elements to construct safe environments, known as smart infrastructures, such as smart homes. This paper also describes required technologies for building resilient and secure cloud services for ELEs including medical devices and the required communication technologies. To achieve effective ELE solutions for appropriate ICT algorithms, architectures, and platforms, with a view toward the advancement of science and the development of new and innovative connected solutions is challenges. The increasing number, complexity, heterogeneity, and

interoperability of interconnected devices, as well as the increasingly sensitive data transmitted, make ELEs an attractive target for attackers. ELEs, requires need a threat model to analyze the security problem, design mitigation strategies, and evaluate solutions. There are so many things in technologies and security challenges for research in ELE/AAL field in future.

**6. References**

[1]. C. Tunca et al., "Multimodal Wireless Sensor Network-Based Ambient Assisted Living in Real Homes with Multiple Residents," Sensors (Basel), vol. 14, no. 6, 2014, pp. 9692–9719.

[2] N.M. Garcia and J.J.P. Rodrigues, eds., Ambient Assisted Living, CRC Press, 2015.

[3]. A. Costanzo, D. Giordano, and C. Spampinato, "Implementing Cyber Physical Social Systems for Smart Cities: A Semantic Web Perspective," Proc. 13th IEEE Ann. Consumer Comm. and Networking Conf. (CCNC), 2016, pp. 274–275.

[4]AAL Association,"Objectives- Activeand Assisted Living Joint Programme," http://www.aal-europe.eu/about/objectives, (Accessed in March 2016).

[5] A. M. Cook and J. M. Polgar, Assistive technologies: Principles and practice. Elsevier Health Sciences, 2014.

[6]. L. Shi et al., "BANA: Body Area Network Authentication Exploiting Channel Characteristics," IEEE J. Selected Areas in Comm., vol. 31, no. 9, 2013, pp. 1803–1816.

[7] D. He and S. Zeadally, "Authentication Protocol for an Ambient Assisted Living System," IEEE Comm., vol. 53, no. 1, 2015, pp. 71–77.

[8]. A.J. Cheriyan et al., "Pervasive Embedded Real Time Monitoring of EEG & SpO2," Proc. 3rd Int'l Conf. Pervasive Computing Technologies for Healthcare, 2009, pp. 1–4.

[9] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800145, 2011; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[10]. M. Zhang, A. Raghunathan, and N.K. Jha, "Trustworthiness of Medical Devices and Body Area Networks," Proc. IEEE, vol. 102, no. 8, 2014, pp. 1174–1188.

[11] . N. Bessis et al., "Using a Novel Message- Exchanging Optimization (MEO) Model to Reduce Energy Consumption in Distributed Systems," Simulation Modelling Practice and Theory, vol. 39, Dec. 2013, pp. 104–120.

[12] H. Alipour et al., "Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis," IEEE Trans. Information Forensics and Security, vol. 10, no. 10, 2015, pp. 2158–2170.