AES-PRESENT: A NEW SECURE IOT-BASED SCHEME FOR TELEMEDICINE AND E-HEALTH SYSTEMS

Abdellaoui Abderrahim, Fdili Ibtissam, Chaoui Habiba, El Achgar Hicham and Hmina Nabil
Systems Engineering Lab, ADSI Team, ENSA Kénitra, Ibn Tofail University, Morocco
E-Mail:abderrahim90@gmail.com

ABSTRACT

Over the last few years, the Internet of things has gained more and more space in various activities sectors, including the health sector. In fact, the Telemedicine has benefited from this new concept by using its various kinds of special devices and tools which facilitate to provide distance healthcare services, and thus, solve many problems notably for the elderly or person in remote areas. However, the transfer of sensitive medical data is threatened by falsification, while its security and privacy are crucial in healthcare. The main contribution of this paper is to propose a secure telemedicine scheme that supports different types of medical data. The scheme ensures, on the one hand, communication confidentiality by means of a combination between heavyweight and lightweight cryptography, and on the other hand, data integrity by using network steganography and the cryptographic hash function RIPMD160.

Keywords: Internet of things, telemedicine, e-health security, cryptography, steganography.

1. INTRODUCTION

In recent years, there has been an increasing interest in the Internet of Things concept thanks to the development of different kind of intelligent tools. This paradigm enables to interconnect various devices by means of the internet. According to Gartner, the market of Internet of Things devices will continue on its growth and will reach nearly 21 billion connected devices by 2020 [1]. Thus, due to the broad nature of these devices, they may cover any activities sectors. For example, when it comes to the health sector and particularly telemedicine, the use of these devices is mandatory.

In other words the telemedicine has benefited from the advantages provided by the devices characterized by many features[2] including self-configuration, interoperability, self-adaptation, facility of integration and the ability to communicate with each other, all of these devices are integrated in a network that allows creating a remote link between the patient and a doctor to benefit from consultation, surveillance, assistance, expertise (for instance, in ambulatory surgery and many other services)in order to reduce serious events, and provide access to healthcare services in isolated areas.

At this level, we can say that Telemedicine technology can be considered as a human performance before being a technical solution owing to its benefits offered to the population. However, regarding the technical level, the IoT and the telemedicine present some security challenges that could impact the patient's privacy, indeed in a doctor-patient relationship dominated by technology it is essential to ensure data confidentiality.

In this paper, we propose a new robust architecture, allowing a secure exchange of different forms of medical data (Figure-1) such as medical imaging [4] or patient's personal information in text format by implementing a hybrid cryptographic technique. It uses the lightweight cryptography at the perception layer, precisely at the biosensors level and the heavyweight cryptography, which is applied in the network layer coupled with the implementation of a cryptographic hash function in order to ensure data integrity. The transmission of the encrypted data will be through an overt channel, whereas the transfer of a special control data will be through a secret channel which will be created using network steganography. The remainder of the paper is organized as follows. Section 2 and 3summarizes related works by discussing the important existing security approaches for an IoT environment based Healthcare. The different security mechanisms implemented in our proposed architecture are the subject of section 4, while the presentation of our contribution is addressed in section 5, we discuss and analyze the security requirements of our proposal in section 6.Conclusion and future research visions are given in section 7.

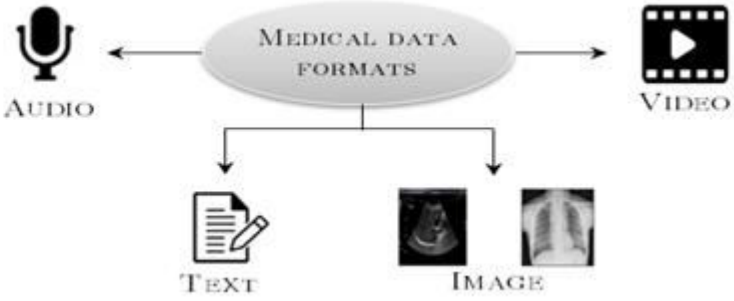


Figure-1. Different types of medical data.

2. PRELIMINARIES

In this section, we present a summary of related security approaches and the existing threats that can impact the healthcare information systems.

2.1 Information security challenges in telemedicine technology

In recent years, the number of threats in healthcare information system has increased [5],such threats might be an illegal access to medical data, unauthorized activity or the loss of sensitive information that can negatively impact the patient's privacy.

In 2007, more than 1.5 million names have exposed during data breaches [6] in hospitals alone. In addition, Healthcare Information and Management Systems society Security Survey in 2010 declared that the report of more than 110 healthcare organizations has shown the loss of sensitive medical data [7] affected over 5 300 000 patients, due to virus attacks, malicious insiders, system hacks and web explosion. Another study [8] has shown that accident event and deliberated action threats are two parameters that can severely impact the continuity of Telemedicine technology.

3. RELATED WORKS

Various methods and approaches have been proposed to ensure healthcare data security. In this section, we briefly present some of the existing contributions.

In [9] the authors presented an authentication framework composed of three phases to prevent the misuse of the remote patient monitoring in e-health, based on Radio fingerprint technique. Whereas in [10] the authors introduced an end to end mobility scheme for the Internet of Things environment based healthcare, it consists of a secure and efficient end-user authentication and authorization architecture.

In [11] the authors presented Code Blue as a wireless infrastructure intended for deployment in emergency medical care, by ensuring seamless transfer of data among caregivers and facilitate efficient allocation of hospital resources. However, the security aspects of Code Blue are still left as a future work.

Meanwhile, the authors in [12] presented an image-based authentication scheme, to improve authentication in the telemedicine information system, their contribution overcomes different security issues, but it was not implemented in an IoT environment.

In the same context, in [13] the authors introduced a system able to remotely control health by using RFID tags. However, their contribution doesn't take into account data security. In [14] the authors presented an open secure and flexible platform based on IoT and Cloud Computing for the healthcare domain, their contribution is mainly focused on authentication by giving importance in decision making related to the privacy of patients.

TheBSN-care scheme, a secure IoT based healthcare system using body sensor network, was proposed in [15]. It enables patients to be monitored using a collection of lightweight sensor nodes. In this regard, SEA was presented in [16] as an architecture for IoT-based healthcare by using smart getaways, in order to perform a remote authentication and authorization of end-user securely and efficiently and to support different wireless protocols and inter-device communication.

4. THEORETICAL WORK

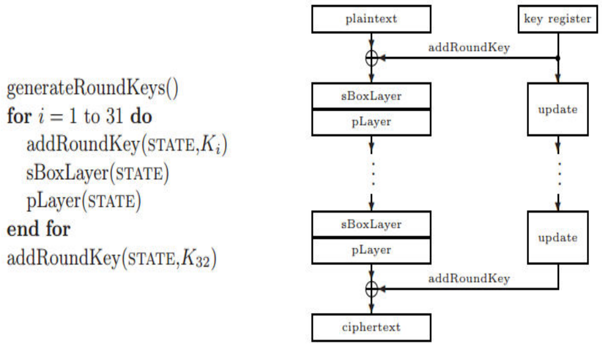
It is worth mentioning that during the phase of data transmission from the patient to the medical server, there is a risk of data interception which may impact the patient's confidentiality and integrity. Ensuring security in an IoT based healthcare environment is considered as one of the most important research challenges. In contrast with the existing techniques, our proposed architecture implements robust security mechanisms, to deal with different threats that can impact data integrity and confidentiality.

4.1 Cryptographic techniques

Cryptography is the science of protecting information from malicious acts to ensure that the transmitted data remains confidential and to provide assurance on the integrity and authenticity of the information. Mainly used to ensure the security of communications and access control. In this direction, the application of a cryptographic technique in an intelligent environment has to be developed in order to support heterogeneity, interoperability, key size, low energy consumption, limited resources of IoT devices and to keep patient's anonymity and protect the personal data.

In our contribution, a hybrid cryptographic technique (Figure-5) was implemented by using both the heavyweight and lightweight cryptography.

Lightweight encryption algorithms: this technique is deployed on devices that haven't sufficient resources (memory, power, size). PRESENT is an example of a lightweight encryption algorithm which is considered an ultra-lightweight block cipher [17].It consists of 32 rounds, the block length is 64 bits and two supported key lengths of 80 and 128 bits (Figure-2).



```
generateRoundKeys()
for $i = 1$ to 31 do
    addRoundKey(STATE,$K_i$)
    sBoxLayer(STATE)
    pLayer(STATE)
end for
addRoundKey(STATE,$K_{32}$)
```

Figure-2.A description of present algorithm [17]

Heavyweight encryption algorithms: These algorithms need more memory due to the huge amount of computation involved. But, they are more secure when compared to lightweight algorithms [18]. Figure-3 illustrates the common computational steps involved in heavyweight encryption algorithms.

The advanced encryption standard AES algorithm (also known as Rijndael) is one of the most important and most used heavyweight encryption algorithms because of its simplicity and high efficiency.It is a symmetric encryption algorithm which can support different key size particularly 128, 160, 192, 224, 256bits.

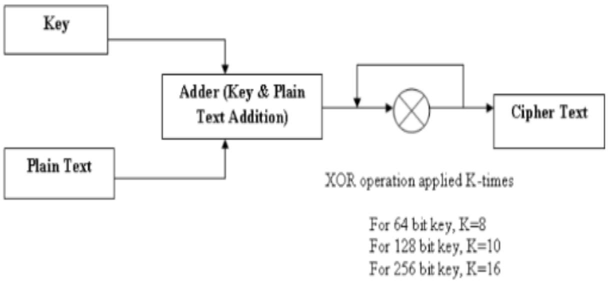


Figure-3. Steps used in heavyweight encryption.

4.2 Network Steganography

All of the information hiding techniques that can be used to exchange secret data in telecommunication networks is called network steganography [19].Our proposed architecture comprises two kinds of channels: an overt and a covert channel.

Covert channel: the aim of this technique is to hide the existence of the communication. Typically, covert channels use means of communication not normally intended to be used [20].It is an escape technique, which will allow us to exchange some special data in a secret way without being detected. The implementation of this mechanism in our architecture is for the purpose of exchanging data integrity information.

Overt channel: The overt channel is the regular network that links the patients and the healthcare server which is used as carriers for the covert channel.

4.3 Cryptographic hash function

The aim of the cryptographic hash functions is to verify the authenticity and integrity of the data. In the proposed scheme, we implemented the RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) which is a fast cryptographic hash function that is tuned towards software implementations on 32-bit architectures [21].

It is considered as a very advanced security method which offers a very high level of data compliance. The purpose of its implementation in our security architecture is to overcome the problem of falsification of patient's data to limit the risk of errors and any unlawful disclosure.

4.4 Biosensors

A biosensor is a tool that merges the biological sensing element with a transducer in order to create a signal proportional to the analyte concentration such as blood glucose level, antibodies, receptors, and microorganisms [24]. The goal of biosensors is to collect information from the patient and detect early markers characteristic of diseases. The field of medical diagnostics is a pioneer in the development of biosensors [22] owing to their higher sensitivity and their ability to perform multiplex analysis.

5. PROPOSED WORK

This part of the article will be devoted to a detailed study of the contribution. It consists to propose a security scheme for the telemedicine technology, in order to ensure an encrypted data exchange between the patient entity and the telemedical server and to overcome different types of attacks. The proposed architecture is divided into three layers: the perception layer ,the intermediate layer and the treatment layer (Figure-4):

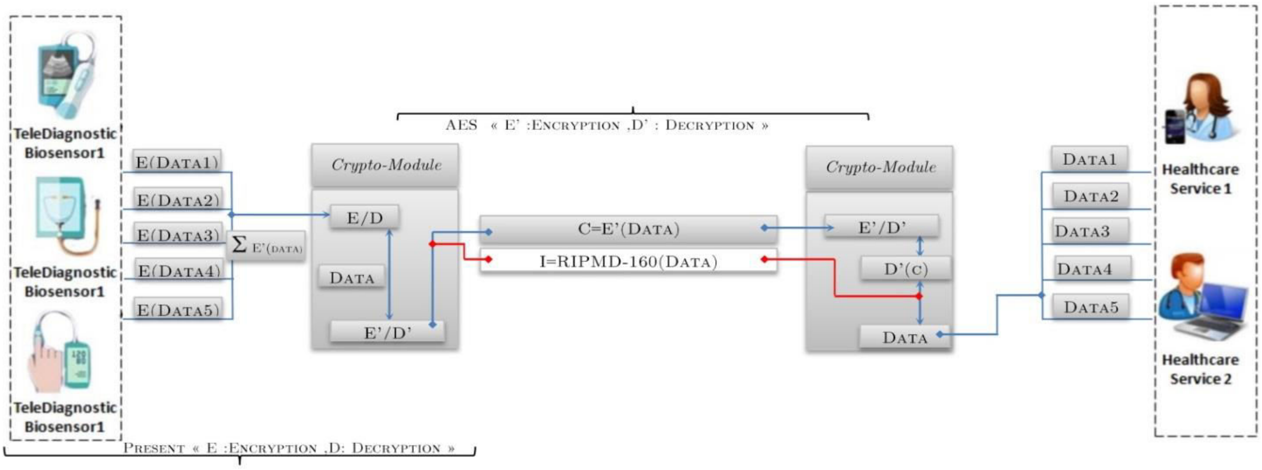


Figure-4. The proposed scheme.

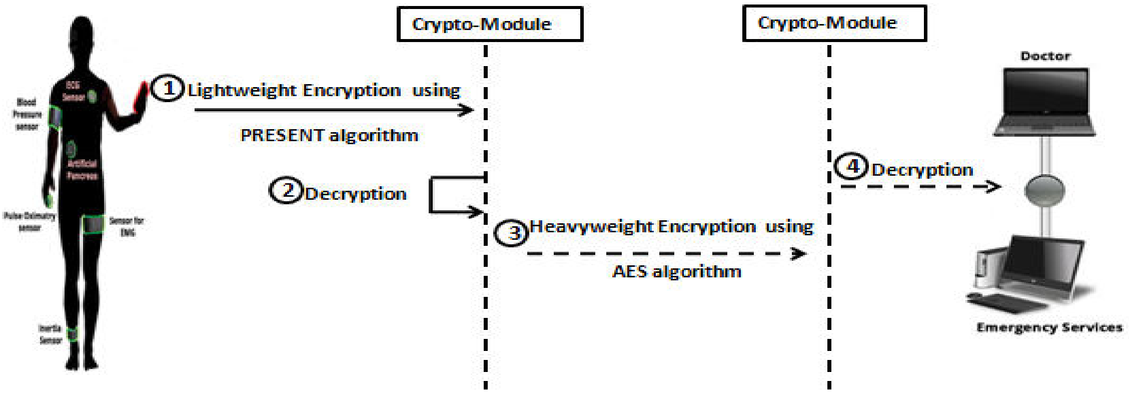


Figure-5. Hybrid encryption present-AES.

5.1 Perception layer

The perception layer includes all of the smart physical medical tools with built-in sensors for identification. These devices use the lightweight cryptography mechanism. They can be used at home or in a health center. This layer essentially allows the collection of information, depending on the type of sensors diagnosis, radiology, temperature measurement, pressure, or heart rate...The collected data is then transmitted to the intermediate layer to ensure a secure transmission to the final processing layer.

5.2 Intermediate layer

This layer is responsible for the data transmission from the perception layer to the final processing layer, at this level, different security mechanisms are applied in order to ensure a secure and a secret data transmission, based on a Crypto-Module entity (CRE). This entity is responsible for the encryption and decryption of the patients' data using the PRESENT algorithm at the perception layer, and the AES algorithm at the intermediate layer. The Crypto-Module is responsible for the creation of two main channels: the overt channel and a covert channel. The overt channel is the normal network in which the patient's data are exchanged in an encrypted manner. It is also used as carriers for the covert channel which is a hidden network created by means of network watermarking. Its principal aim is the transmission of a special control data between crypto-modules in order to verify the integrity of the patient's sensitive data (personal information, Image Dicom, MRI, CT, PET ...) using the RIPMD-160 hash function.

5.3 Treatment layer

This layer is responsible for the management, data processing and decision-making of the received data from the perception layer. It usually provides all the medical assistance and various medical equipment that can analyze, diagnose and treat the situation of the patient.

These three layers can ensure a secure exchange of medical data taking into account the constraints of an intelligent environment with limited resources and low energy consumption.

6. DISCUSSION AND ANALYSIS

The IoT medical devices, like most of the devices, are vulnerable to different types of attacks that can impact negatively the exchange of sensitive medical data and can disturb the good practices of telemedicine technology. In this section, we demonstrate that our

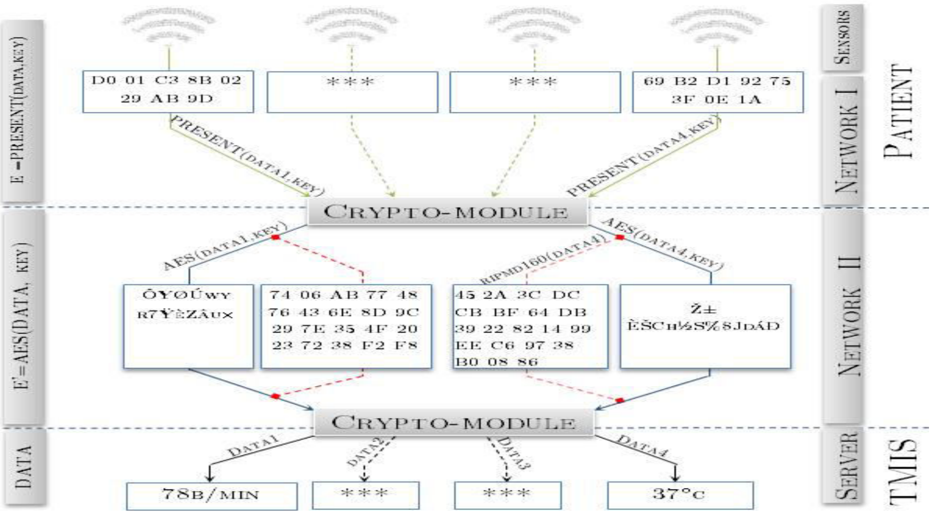


Figure-6. Communications in the proposed

proposed architecture can satisfy the majority of security requirements particularly, confidentiality, integrity and availability.

6.1 Man in the middle (MITM)/eavesdropping attacks

The MITM attack is considered as one of the most dangerous attacks that allow intercepting the communication between medical devices, without being able to suspect that the communication channel has been compromised. The proposed architecture is based on a hybrid cryptography technique which implements PRESENT as a lightweight encryption algorithm and AES as a heavyweight technique. The combination between the lightweight and heavy weight cryptography makes our approach resist to such attacks (Figure-6).

6.2 Replay/ playback attacks

The Replay attack is a form of attacks based on the network properties where an adversary replays existing messages which increase confusion and misleads innocent entities [23]. To settle such a problem. We verify data integrity using the cryptographic hash function (RIPMD160).Table-1compares the proposed scheme with some existing solutions. With the confidentiality and integrity, the proposed solution ensures that the received medical data has not been compromised or altered during the transmission, which makes our security scheme resist to common types of network attacks that can disrupt the exchange of medical data, including, DoS attacks, Eavesdropping, Man in the middle and the playback attacks.

Table-1. Comparison between the proposed solution and some existing frameworks.

	Attacks			Security issues		
	EV	MITM	PB	I	C	A
Our Contribution	✓	✓	✓	✓	✓	✓
[9]	✗	✓	✗	✗	✓	✗
[10]	✓	✓	✗	✗	✓	✗
[11]	✗	✗	✗	✗	✗	✓
[12]	✗	✓	✗	✓	✓	✗
[13]	✗	✗	✗	✗	✗	✗
[14]	✗	✗	✓	✗	✓	✗
[15]	✓	✗	✓	✗	✗	✗
[16]	✗	✓	✗	✗	✓	✗

EV	→ Eavesdropping	PB	→PlayBack
MITM	→ Man in the middle	I	→ Integrity
C	→ Confidentiality	A	→ Availability

7. CONCLUSIONS

In this paper, we've proposed a new robust security architecture for the Telemedicine systems. This contribution allows controlling the integrity and the confidentiality of the patient's data and ensures that the information has not been altered or falsified during its exchange, relying on some security mechanisms that provide a very high level of security by implementing a hybrid cryptographic technique to protect the personal medical data.

As future work, we will further investigate the critical features of smart objects in telemedicine in order to implement other security mechanisms to build and strengthen the proposed architecture and test it in a real environment.

REFERENCES

[1] Lee, In, and Kyoochun Lee. 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 58.4: 431-440.

[2] Ray P. P. 2016. A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences.

[3] Saeed A., Ahmadinia A., Javed A. & Larijani H. 2016. Intelligent intrusion detection in low-power IoTs. ACM Transactions on Internet Technology (TOIT). 16(4): 27.

[4] McInerney T. & Terzopoulos D. 1996. Deformable models in medical image analysis: a survey. Medical image analysis. 1(2): 91-108.

[5] Shahri A. B. & Ismail Z. 201). A tree model for identification of threats as the first stage of risk assessment in HIS. Journal of Information Security. 3(02): 169.

[6] HIMSS. 2008. Kroll-HIMSS Analytics 2008 Report on Security of Patient Data.

[7] HIMSS. 2010. Kroll-HIMSS Analytics 2010 Report on Security of Patient Data.

[8] Kahn S. & Sheshadri V. 2008. Medical record privacy and security in a digital environment. IT professional. 10(2).

[9] Habib K., Torjusen A. & Leister W. 2014. A novel authentication framework based on bio-metric and radio fingerprinting for the IoT in eHealth. In Proceedings of International Conference on Smart

Systems, Devices and Technologies (SMART) (pp. 32-37).

[10] Moosavi S. R., Gia T. N., Nigussie E., Rahmani A. M., Virtanen S., Tenhunen H. & Isoaho J. 2016. End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Generation Computer Systems. 64, 108-124.

[11] Lorincz K., Malan D. J., Fulford-Jones T. R., Nawoj A., Clavel A., Shnayder V.& Moulton S. 2004) Sensor networks for emergency response: challenges and opportunities. IEEE pervasive Computing. 3(4) : 16-23.

[12] Abdellaoui A., Khamlichi Y. I. & Chaoui H. 2016. A Robust Authentication Scheme for Telecare Medicine Information System. Procedia Computer Science. 98, 584-589.

[13] J. M. Lina, C. H. Linb. 2013. RFID- based Wireless Health Monitoring System Design, 7thAsian-Pacific Conference on Aerospace Technology and Science, 7th APCATS.

[14] Zhang X. M. & Zhang N. 2011 May. An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. In Computer and Management (CAMAN), 2011 International Conference on (pp. 1-4). IEEE.

[15] Gope P. & Hwang T. 2016. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. IEEE Sensors Journal. 16(5): 1368-1376.

[16] Moosavi S. R., Gia T. N., Rahmani A. M., Nigussie E., Virtanen S., Isoaho J.& Tenhunen H. 2015. SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science. 52, 452-459.

[17] Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. & Vikkelsoe C. 2007, September. PRESENT: An ultra-lightweight block cipher. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 450-466). Springer, Berlin, Heidelberg.

[18] Singh K. J. & Manimegalai R. 2011. Fast random bit encryption technique for video data. European Journal of Scientific Research. 64(3): 437-445.

[19] Frączek W., Mazurczyk W. & Szczypiorski K. 201). Multi-level steganography: Improving hidden communication in networks. Journal of Universal Computer Science (J. UCS). 18(14): 1967-1986.

[20] Zander S., Armitage G. &Branch P. 2007. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys & Tutorials. 9(3): 44-57.

[21] Bart Preneel, Hans Dobbertin, Antoon Bosselaers. 1997. The Cryptographic Hash Function RIPEMD-160. CryptoBytes. 3(2): 9-14.

[22] Benny P.L. Lo, Surapa Thiemjarus, Rachel King and Guang-Zhong Yang. 2005. Body Sensor Network - A Wireless Sensor Platform For Pervasive Healthcare Monitoring.

[23] S. M. R. Islam *et al*. 2015. Internet of Things for Health Care: A Comprehensive Survey IEEE Access.

[24] Nikolelis D, Krull U, Wang J, Mascini M. 1998. Biosensors for direct monitoring of environmental pollutants in field. Kluwer Academic, London.