International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Review on Medical Secure Systems Using Machine Learning Algorithm

Pragati Hadole[1], Vidya Dhamdhere[2]

[1, 2]Department of Computer Engineering, G. H. Raisoni College of Engineering and Management, Savitribai Phule Pune University, Pune, India

Abstract: ***Behavior-rule specification-based technique is analyzed for intrusion detection of medical devices embedded in a medical secure system (MSS) where patient's safety is of the utmost importance. Medical cyber secure systems (MSS) are used as tool for cyber attacks. This can relatively harm the patient or may even cause a direct or indirect threat to life. Intrusion detection technique helps to detect secret attackers to support safe and secure MSS applications. The present survey gives an idea of the previous work done by several researchers on the medical secure systems related applications and various techniques.***

Keywords: Digital Envelope, medical data privacy, Medical secure systems, encryption

1. Introduction

Our society has been facing considerable challenges in recent years. Increasing traffic congestion, energy scarcity, rising medical costs, climate change and many other issues have taken a turn for the worse and need urgent attention. Technology can play a major role in alleviating these problems through the development of smart-infrastructures.

The idea behind smart-infrastructures is to incorporate intelligence in everyday objects/services in order to improve the efficiency of performing certain rudimentary but crucial tasks. For example, a smart coffee pot can detect the decrease in temperature of its contents (coffee) and alert the user so that the coffee does not have to be unnecessarily re-heated; thereby saving energy. This trend of developing intelligent systems has already begun. A recent survey found that a typical household has at least 100 microprocessors while a typical new model car has more than 100 of its own. In fact, most of microprocessors are now embedded in systems which are not computers. The crucial technology that has made this leap possible are miniature sensing, communication and processing platforms which can be embedded as a part of larger systems/processes for providing real-time monitoring and feedback control services. Such platforms, deeply embedded in physical processes, are called medical secure systems.

The principal goal of Medical secure Systems (MSS) is to monitor the behavior of physical process1 they are a part of, and actuate actions to change its behavior, if needed. CPS platforms are usually designed as an amalgamation of electro-mechanical sensors and actuators, a communication stack, memory and a processing unit. Each of these components can be centralized - in one entity for example, implantable cardiac defibrillators (ICDs) or pacemakers which are embedded inside a person's chest cavity (as a part of the cardiovascular process) to observe its behavior (cardiac cycle) and correct in the event of out of the ordinary behavior (arrhythmia) , or distributed over a group of entities as in the case of an automobile control system, where sensors from the engine provide temperature data to a microprocessor dedicated to manage engine functionality, which then communicates the data through an in-car network to a controller in dashboard which displays this information to the driver.

CPSs, given their environmental coupling, diverse capabilities and lack of isolation are often used for monitoring and controlling mission critical, processes. Therefore any security compromise of the CPS can have profound consequences. Further, the mission critical nature also makes them more susceptible to targeted attacks. The case in point is the pace-makers CPSs which have been targeted to not only reveal a patient's electrocardiogram (EKG) data but also to actuate an untimely shock. Further, CPSs have the ability to monitor the physical process they are embedded in. This makes them privy to detailed and often sensitive information about the process. If this information is available to malicious entities, it can be exploited leading to loss of privacy, abuse and discrimination. For example, unauthorized knowledge of the electricity consumption of a neighborhood from a power-management CPS in the wrong hands can result in socket bombing attacks on households perceived to be using excessive electricity. Finally, CPSs have the ability to actuate changes to the environment they are a part of. Allowing unauthorized parties to actuate untimely changes to the environment can cause harm to the process itself. For example, malicious entities can easily shut-down a CPS controlling an automobile leading to issues ranging from inefficient fuel consumption to break-failure. In a world where we are becoming increasingly dependent upon CPSs to provide us with automated, efficient management of essential services, care has to be taken to ensure that they are protected.

However, before we delve into these details of how to alleviate CPS security issues, we need to understand the typical workflow of CPS. This will provide information on the potential security issues and bottlenecks that have to be tackled.
Section II gives the Literature review for the medical secure systems.

2. Literature Review

In paper [1] authors have talked about the health data interoperability problems occurs in MCPS. It gives the data interoperability issue in terms of medical sensor type, data rate, healthcare standards and other aspects in the context of cloud-based MCPS. In this paper authors also gives a conceptual data interoperability system which highlights the various system entities. Addressing the data interoperability issue for MCPS is beneficial to patient's healthcare and safety.

In this paper [2], a lightweight no-pairing ABE system in view of elliptic curve cryptography (ECC) is develoepd to solve the security and protection problem in IoT. The security of the developed plan depends on the ECDDH assumption rather than bilinear Diffie–Hellman assumption, and is demonstrated in the attribute based selective-set model. By consistently deciding the criteria and characterizing the metrics for measuring the communication overhead and computational overhead, the comparison investigations with the current ABE system are made in detail.

This paper [3] developed a new medicinal cloud computing techniques that disposes of security concerns connected with the cloud supplier. Given technique gains by Fully Homomorphic Encryption (FHE), this empowers calculations on private health data without really watching the underlying information. For a feasibility study, authors introduce a working execution of a long term cardiac health observing application utilizing an entrenched open source FHE library.

This paper [4] depicts a programmer-focused software development approach for cryptographic frameworks. Authors composed and constructed the Charm system to diminish the load on the cryptographer. Low-level mathematical code, regularly an execution bottleneck, is written in C, and is called from the high level Python code. Developers assemble their conventions in Python and appreciate advantages of the implicit components of that high level language, and in addition the system Toolbox and different mechanisms gave by Charm. Charm contains a protocol engine that deals with the communications, serialization and other house-keeping that is necessary to actualizing a multi-party protocol. In this manner, developers are protected from the minutia that is irrelevant to the cryptographic hypothesis in their protocol.

In paper [5] authors developed a technique to establish safety of on demand medical cyber-physical systems which are assembled to treat a patient in a specific clinical scenario. They treat such a system as a virtual medical device (VMD) and propose a model-based framework that includes a modeling language with formal semantics and a medical application platform (MAP) that provides the necessary deployment support for the VMD models.

In paper [6] authors have inspected the present state and projected future directions for incorporation of remote health monitoring advances into the clinical practice of medication. Wearable sensors, especially those furnished with IoT intelligence, offer appealing alternatives for empowering observation and recording of information in home and workplaces, over any longer lengths than are currently done at office and research center visits. This treasure trove of information, when analyzed and displayed to doctors in easy-to-assimilate representations has the potential for fundamentally enhancing healthcare services and decreasing expenses. We highlighted a few of the difficulties in sensing, analytics, and visualization that should be tended to before frameworks can be intended for consistent reconciliation into clinical practice.

In paper [7] authors have developed a framework for outpatients' CDs monitoring by making use of wireless body sensors and based on the SOA and the Cloud environments. Every patient in designee system has a set of sensors, based on his/her CD(s), and a related mobile application. Sensors get readings of different health parameters of the patients and automatically communicate these to the mobile application.

As shown in table 1, literature review of various papers has been listed, giving possibility of research gap.

Table 1: Survey Table

Sr. No.	Paper Details	Techniques	Advantages	Research Gap
1.	A. Alhumud, M. A. Hossain and M. Masud, "Perspective of health data interoperability on cloud-based Medical Cyber-Physical Systems", IEEE 2016	issues that appear in MCPS	proposed a conceptual data interoperability framework	Implementation of the framework is not done
2.	X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things", Future Gener. Comput. Syst 2015	Diffie–Hellman assumption	Reduces a bit of communication overhead	computational overhead can be improved
3.	O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption", IGI Global 2015	Naive Computation	open source FHE library	---
4.	J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems", Journal of Cryptographic Engineering	Attribute-based encryption (ABE)	Charm provides an excellent platform for implementing techniques that automatically translate	examine the possibility of compiling Charm code directly to languages

	2013			
5.	A. L. King, L. Feng, O. Sokolsky and I. Lee, "Assuring the safety of on-demand medical cyber-physical systems" , IEEE 2013	Medical Application Platform (MAP)	Model deal with the nominal behaviors of the devices	VMD is not deployed.
6.	M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges", IEEE 2015	IoT intelligence	highlighted several of the challenges in sensing, analytics, and visualization	System is not designed yet
7.	A. Benharref and M. A. Serhani, "Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors", IEEE 2014	SOA and the Cloud environments	able to detect all anomalies and communicate appropriate messages and data to different stakeholders	All modules are not created also more nodes can be added to improve accuracy, data security not provided

3. Propose Architecture

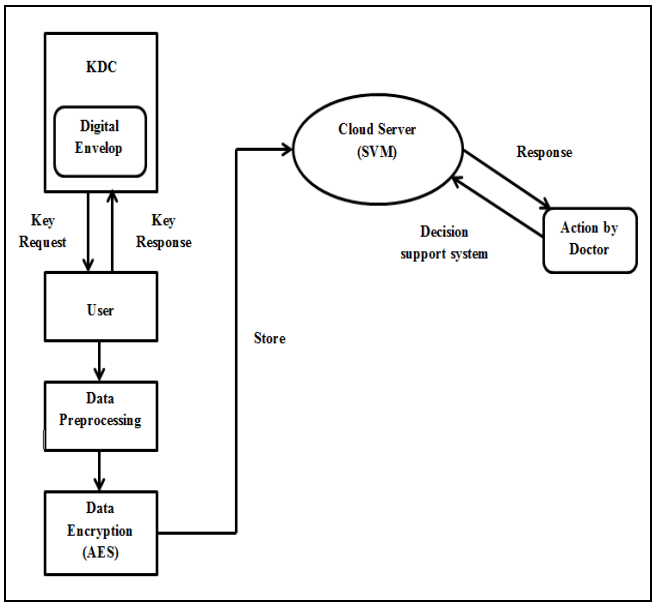

Figure: System Archicture

In propose Medical Secure System as a Seven-layer consisting of KDC and Digital Envelope, data acquisition, data aggregation, AES encryption, cloud processing, action layers. First one is KDC means Key Distribution Center whose have authority to distributed keys to the authenticated users. Here user sends the request to KDC for key and KDC provide key to the server as a response. Second layer is Digital envelope scheme which is used to enhance the security level, Here KDC again generate the keys means for encryption and decryption user need two keys. Third layer is Data acquisition layer which is typically a Body Area Network (BAN) consisting of wireless wearable sensors for specific medical applications such as blood pressure and body temperature monitoring, or data storage for on demand access by doctors. A BAN facilitates the collection of patient medical information and forwards this information to a nearby computationally-capable device. A data aggregation which is fourth layer of system is the most important building block of an IoT-based architecture, since it enables individually-weak devices to have strong overall functionality by concentrating the data from each device and sending the aggregated information to the cloud. The fifth layer is AES Encryption which is used to encrypt and decrypt the data and provide the security from attackers or data modification. For accurate diagnosis requires long-term patient health monitoring information, secure storage is the most important function of the cloud. privacy-preserving processing in a public cloud is only feasible using advanced homomorphic encryption schemes. Sixth layer function of the cloud is data analytics to facilitate decision support for healthcare professionals. The action layer which is seventh layer can provide either "active" or "passive" action. In active action, an actuator is used to turn the results of the algorithms that run in the cloud into the activation of an actuator. In passive action, no physical action is actually taken.

4. Conclusion

This paper analyses various medical secure systems. Also given the advantages and drawbacks present in the different studies performed by various researchers. To deal with drawbacks in present systems we presented a idea of the new system.

References

[1] A. Alhumud, M. A. Hossain and M. Masud, "Perspective of health data interoperability on cloud-based Medical Cyber-Physical Systems," 2016 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), Seattle, WA, 2016, pp. 1-6.
[2] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the internet of things," Future Gener. Comput. Syst., vol. 49, pp. 104–112, 2015.
[3] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," in Enabling Real-Time Mobile Cloud Computing through Emerging Technologies, T. Soyata, Ed. Hershey, PA, USA: IGI Global, 2015, ch. 7, pp. 213–246.
[4] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," J. Cryptographic Eng., vol. 3, no. 2, pp. 111–128, 2013.
[5] A. L. King, L. Feng, O. Sokolsky and I. Lee, "Assuring the safety of on-demand medical cyber-physical systems," 2013 IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), Taipei, 2013, pp. 1-6.
[6] M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing

with Cloud-Based Processing: Opportunities and Challenges," 2015 IEEE International Conference on Services Computing, New York, NY, 2015, pp. 285-292.

[7] A. Benharref and M. A. Serhani, "Novel Cloud and SOA-Based Framework for E-Health Monitoring Using Wireless Biosensors," in IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 1, pp. 46-55, Jan. 2014.

[8] Robert Mitchell, Ing-Ray Chen, Member, IEEE, "Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems", Robert Mitchell, Ing-Ray Chen, Member, IEEE, 2013.

[9] Alhassan Khedr, Member, IEEE, and Glenn Gulak, Senior Member, IEEE, "SecureMed: Secure Medical Computation using GPU-Accelerated Homomorphic Encryption Scheme", 2016.

[10] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," in Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci., 2011, pp. 97–106.

[11] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Process. Mag., vol. 30, no. 1, pp. 82–105, Jan. 2013.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Commun., vol. 17, no. 1, pp. 51–58, Feb. 2010.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[14] G. Nalinipriya and K. R. Aswin, "Extensive medical data storage with prominent symmetric algorithms on cloud - a protected framework," in Proc. IEEE Int. Conf. Smart Struct. Syst., Mar. 2013, pp. 171–177.

[15] Phaneendra Kumar, Dr.S.V.A.V.Prasad , Arvind Patak , "Design and Implementation of M-Health System by Using Cloud Computing", Future Gener. Comput. Syst., Vol. 5, Issue 5, May 2016.