www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 2 Feb. 2017, Page No. 20202-20205
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i2.06

Survey on Emerging Security Mechanisms for Medical Cyber Physical Systems

Anupama C V [#1]***, Misha Ravi*** [#2]

[#1]PG Scholar, Computer Science and Engineering
Sree Buddha College of Engineering, Ayathil Kerala
[#2]Assistant Professor, Computer Science and Engineering
Sree Buddha College of Engineering, Ayathil Kerala

Abstract

Medical Cyber Physical System (MCPS) is able to transmit and process the data collected from health monitoring systems, which consists of BAN. The acquired data is transmitted to private or public cloud which contains set of algorithms for analysing the patient data. These medical data should be kept secret. After analysing these data, the feedback is given to the doctors to take corrective action. This system includes data acquisition which is capable of acquiring data from body area networks, data aggregation which concentrate the gathered signal information, cloud processing which includes many analysis algorithms and action layer which produce either physical action or decision support. Each of its layer contain hardware such as sensors and cloud computing architectures etc. So, the data should be secured in each layers. So many normal encipher mechanisms are used. Also, emerging encryption technology such as homomorphic encryption standards used in MCPS.

Index Terms—Medical cyber physical systems, medical data privacy, homomorphic encryption, attribute-based encryption

I. INTRODUCTION

Developing MCPSs will needs to avoid the technological hurdles in building the architectural components of the MCPS such as sensors, cloud computing architectures, and fast Internet and cellular phone connections. Additionally, assuring the privacy of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctors' mobile devices will necessitate the development of a sophisticated cryptographic construction for an MCPS. While this design implies only secure storage using conventional encryption schemes, emerging encryption schemes provide options for secure data sharing and secure computation.

II. LITERATURE SURVEY

.

O. Kocabas [1] attempts to analyse the current investigation and development on wearable biosensor system for health observations. WHMS is very important in the research community during the last decade as it is pointed out by the numerous and yearly increasing corresponding research.

As healthcare costs are increasing and the world population is ageing, there has been a need to monitor a patient's health status while he is out of the hospital in his personal environment. To address this demand, a variety of system prototypes and commercial products have been produced in the course of recent years, which aim at providing real-time medical information after analysis is given, either to the patient or to a medical centre or straight to a supervising healthcare professionals, while being able to alert the individual if there is possible imminent health threatening conditions.

Recent years have seen a rising interest in wearable sensors and today several devices are commercially available for personal health care, fitness, and activity awareness. T. Soyata [2] proposed a method along with this these systems in health monitoring uses patient's physiological readings and store it in a private or public cloud for long term. In the normal method, analysing a patient's health status such as body temperature ECG etc.is a time consuming process and may have

some error factors too.. But on current technologies such as wireless wearable sensors, it is very useful and effective to analyse patient's health status. In a hurry world it is more adaptable. Over this technique Body Area Network is capable of capturing the signal from the sensors and keep track a record of patient's health status.

When a person consults doctor for checking his physical health information, the doctor not only have the normal lab tests reports, but also have information that gathered from the wireless wearable sensors. With the help of available information and data collected from system that also have access to a large corpus of observation data for other individuals, the doctor can make a much better prognosis for your health and recommend treatment, early intervention, and life-style choices that are particularly effective in improving the fitness of body. Such a very useful technology can improve the field of medical application and make sure and confident about the patient health status. This may invoke new thoughts in the area of medical science.

There are two adversary models active adversary model and passive adversary model. The MCPS provides data privacy on active adversary model [3] where as it provide both privacy and correctness on passive adversary model. Inn order to analyse the security needs of the MCPS passive adversary is widely used.

In cloud computing the problem related with privacy is based on multi-keyword searching over encrypted data. So it requires set of privacy requirements. It is done by an efficient method called "coordinate matching," . To quantitatively evaluate such similarity measure. The another method used is "inner product similarity" . to achieve various stringent privacy requirements in two different threat models, here first propose a basic idea for the MRSE based on secure inner product computation.

S. Dziembowski proposed encryption mechanisms that pass through rigorous mathematical and theoretical cryptanalysis to provide security and privacy, the system may lost information due to the vulnerabilities in its software and hardware implementations. Attacks based on such leaked information are called side channel attacks. These attacks can be prevented by using leakage resistant cryptography [4].

In search of countermeasures, one can try to prevent side-channel attacks by modifying the implementation or securing hardware. This leads to a trial and error approach where an implementation is made secure against a certain type of attack only before a new more effective attack appears. Leakage Resilient Cryptography adopts a different viewpoint by trying to provide provably secure primitives in the presence of a wide range of side-channel information.

Designing measures are save in the presence of leakage is a difficult but not impossible task. The last few years, the cryptographic community has put a lot of effort in constructing leakage resilient primitives. As the foundations for a theoretical treatment of the subject have been set, we expect that within the next years more and more leakage resilient primitives will be constructed that will tolerate richer and richer families F of leakage functions.

Side channel attacks concentrate on obtaining the secret/ private key by using every layer of the system, rather than just the data that is being processed by the system. While many types of side channel attacks exist for nearly every encryption scheme.

Side-channel attacks[5] are arises due to software or hardware design problems. It is easy-to-implement against powerful attacks, and their targets includes primitives, protocols, modules, and devices to even systems. These attacks are causes Sevier problem to cryptographic sections. To avoid these problems some cryptographic analysis has to be considered. This involves the methods and techniques employed in these attacks, the destructive effects of such attacks, the countermeasures against such attacks and evaluation of their feasibility and applicability; Finally, the most important conclusion from this paper is that it is not only a necessity but also a must, in the coming version of FIPS 140-3 standard, to evaluate cryptographic modules for their prevention towards side channel attacks.

Timing attacks on elliptic curve cryptosystem target the scalar multiplication operation. It is prevented by using Montgomery's multiplication method which is proposed by P. L. Montgomery[6] performs the multiplication independent from the bits of the private key.

This includes an algorithm for calculating elliptic scalar multiplications on non-super singular elliptic curves defined over $GF(2m)$. The algorithm is a small version of method discussed is based on Montgomery's method. The algorithm is easy to implement in both hardware and software. It works for any elliptic curve over $GF(2m)$, and it requires no pre computed multiples of a point, and is faster on average than the addition-subtraction method. In

addition, the method requires less memory than projective schemes and the amount of computation needed for a scalar multiplication is fixed for all multipliers of the same binary length. Therefore, the improved method possesses many desirable features for implementing elliptic curves in restricted environments.

It is an efficient method for computing elliptic scalar multiplications. The method performs exactly 6*b*log2 *kc* + 10 field multiplication for computing *kP* on elliptic curves selected at random, is easy to implement in both hardware and software, requires no pre computations, works for any implementation of *GF*(2*n*), is faster than the addition-subtraction method on average, and uses fewer registers than methods based on projective schemes. Therefore, the method appears useful for applications of elliptic curves in constraint environments such as mobile devices and smart cards.

J. L opez proposed a method for power analysis attacks on AES[7] can be prevented by using randomized masks for AES operations that scramble the relationship between the AES secret key and the intermediate values generated during each AES round. Attacks on implementations are of particular concern to issuers and users of smartcards. Smartcards are becoming a preferred way of securely managing applications in industries such as telecommunications , health care , transportation , pay-TV and internet commerce. Smartcards have also been suggested for use in security applications such as network access and physical access to locations such as automobiles, homes, and businesses. Smartcards, however are potentially vulnerable to implementation attacks.

A smartcard microprocessor has a minimal amount of computing power and memory. Unfortunately, software countermeasures against power analysis attacks can result in significant memory and execution time overhead. The amount of overhead seems to depend on the type and arrangement of the fundamental operations used by an algorithm. Here it examine the fundamental operations used by each of the AES finalist algorithms. Then develop techniques that use random masks to make software implementations of these operations resistant to power analysis attacks. Finally, use these new countermeasures to implement masked versions of each of the remaining AES algorithms. The performance and implementation characteristics of these countermeasures in a 32-bit, ARM-based smartcard are analysed.

Power analysis based attacks on ECC-based encryption schemes can be mitigated by methods proposed that randomize intermediate computations to avoid information leakage about the private key from power consumption patterns.

A lot of attention has been paid to elliptic curves for cryptographic applications and it has become increasingly common to implement public-key protocols on elliptic curves over large finite field. Elliptic curves (EC)[8] provide a group structure, which can be used to translate existing discrete-logarithm cryptosystems into the context of EC.

The implementations of elliptic curve crypto- systems such as El-Gamal type encryption or Diffie-Hellman key exchange are vulnerable to Differential Power Analysis. Here introduced three counter measures that address specifically these attacks. Those countermeasures are easy to implement and do not impact efficiency in a significant way.

In KP-ABE the access policy is encoded into the users' private key and a cipher text is labelled with a set of attributes. KP-ABE schemes [9] place the access policy on the private key of the users and the attributes are associated with the cipher texts.

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). Here develop a new cryptosystem for fine-grained sharing of encrypted data,it is called Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

In an ABE system, a user's keys and cipher texts are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key.

The correctness of the secure computation can be achieved by using techniques from verifiable computing.

In a private database query system, a client issues queries to a database and obtains the results without learning anything else about the database and without the server learning the query. In this work, we show that using a polynomial encoding of the database enables efficient implementations of

conjunction queries using somewhat homomorphic encryption [10].

The basic schemes only require an additively homomorphic system like Paillier, but here showed that significant performance improvements can be obtained using a stronger homomorphic system that supports both homomorphic additions and a few homomorphic multiplications.

CONCLUSION

Here introduce a Medical Cyber Physical System as a four-layer system consisting of data acquisition, data aggregation, cloud, and action layers. It survey conventional and emerging encryption schemes based on their ability to provide secure storage, secure data sharing, and secure computation. Conventional encryptions such as AES and ECIES do not allow any operation other than secure storage, while the emerging Attribute-Based Encryption allows secure data sharing based on the credentials of the sharing parties. Alternatively, secure computation on encrypted data is only feasible using the emerging Fully Homomorphic Encryption schemes. Therefore, analyze six different encryption schemes based on four metrics: i) encryption time, ii) decryption time, iii) cipher text size, and iv) evaluation time. While the first two metrics provide information about the computational intensity of the encryption scheme, the third metric shows the expansion of the amount of data in its encrypted form, determining its storage and transmission characteristics. Clearly, the fourth metric is only relevant to the techniques that provide computation in encrypted format, such as FHE and Paillier.

IV. REFERENCES

[1] A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, "Cloud-based privacy-preserving remote ECG monitoring and surveillance," Ann. Noninvasive Electrocardiol., vol. 20, no. 4, pp. 328–337, 2014.

[2] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. K. Aktas, G. Mateos, B. Kantarci, and S. Andreescu, "Health monitoring and management using internet-of-things (IoT) sensing with cloud-based processing: Opportunities and challenges," in Proc. IEEE Int. Conf. Serv. Comput., Jun. 2015, pp. 285–292.

[3] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, Jan. 2014.

[4] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," in Proc. IEEE 49th Annu. IEEE Symp. Found. Comput. Sci., 2008, pp. 293–302.

[5] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." IACR Cryptol. ePrint Archive, vol. 2005, p. 388, 2005.

[6] P. L. Montgomery, "Speeding the pollard and elliptic curve methods of factorization," Math. Comput., vol. 48, no. 177, pp. 243–264, 1987.

[7] J. L□ opez and R. Dahab, "Fast multiplication on elliptic curves over GF(2m) without precomputation," in Proc. Cryptographic Hardw. Embedded Syst., 1999, pp. 316–327.

[8] T. S. Messerges, "Securing the aes finalists against power analysis attacks," in Proc. Fast Softw. Encryption, 2001, pp. 150–164.

[9] J.-S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in Proc. Cryptographic Hardw. Embedded Syst., 1999, pp. 292–302.

[10] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theor., vol. 22, no. 6, pp. 644–654, Nov. 2006.