International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 03 | March -2019 e-ISSN: 2395-0126

SECURE MEDICAL COMPUTATION USING VIRTUAL ID

Mrs.v.Ezhilarasi[1],M.Mohamed Manaas[2].
A.V.C College of Engineering& IT& Anna University& Mayiladuthurai, Tamil Nadu

1. Mrs.V.Ezhilarasi Professor , A.V.C College Of Engineering, Mayiladuthurai.
2. M.Mohamed Manaas IV Year, B.Tech(IT), A.V.C College Of Engineering, Mayiladuthurai.

ABSTRACT:

PHR provides users with a great deal in leakage of sensitive information. However, securing the sensitive medical data also brings very serious security problems, especially for enterprise data security stored in the medical cloud data. Once the data is outsourced to a third party, the data privacy has become a major problem, such as user authentication, integrity of data etc. and needs to be addressed very effectively. A mutual authentication scheme based on virtual smartcard using hashing function for medical data is proposed to solve the problem of which the illegal users access the resources of servers**.**

INTRODUCTION:

Healthcare data security is an important element of Health Insurance Portability and Accountability Act Rules. The HIPAA Security Rule requires covered entities to assess data security controls by conducting a risk assessment, and implement a risk management program to address any vulnerabilities that are identified.HIPAA-covered entities must also implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information. With cyberattacks on healthcare organizations on the rise and cybercriminals developing increasingly sophisticated tools and methods to attack healthcare organizations, healthcare data security has never been more important.

EXISTING SYSTEM:

In existing system GPU-Accelerated Homomorphic Encryption scheme has been implemented for decrypt the stored data in cloud server.This system used to generate the signatures to verify the integrity of this encrypted file, finally upload this encrypted file and its corresponding signatures to the cloud. The flatten operation in the GPU-Accelerated Homomorphic Encryption scheme which leads to large memory usage and cloud maintenance.They are also able to decrypt only a single bit from one polynomial and discard the remaining polynomials.

PROPOSEDSYSYEM:

The medical data generated by the medical personnel in laboratories and by patients using their devices will then be encrypted by the public key and uploaded to the cloud.The data's will encrypted first then it uploaded to cloud. So even the cloud Server also don't have the original data's.All patient medical data can be stored on the cloud servers safely as the Homomorphic encryption scheme with File swapping is provably secure against attacks.Proposes the Homomorphic encryption with file swapping algorithm for securely stored the patient details.The proposed system contains the virtual id the. The doctor need to access the EHR. They need to login to the server using their unique virtual id.In order to finally decrypt the encrypted experiment results, the researchers will need to gain access to the virtual id.After decrypting, the file location is changed by file Swapping concept which ensure great security in cloud storage.When the researchers trying to login or trying to

read the health report the notification will send to the admin.

LITERATURE SURVEY:

1. Title:Factor Graphs and the Sum-Product Algorithm

Authors: Frank R. Kschischang,Hans-Andrea Loeliger

Description:

Algorithms that must deal with complicated global functions of many variables often exploit the manner in which the given functions factor as a product of "local" functions, each of which depends on a subset of the variables. Such a factorization can be visualized with a bipartite graph that we call a factor graph. In this tutorial paper, we present a generic message-passing algorithm, the sum-product algorithm that operates in a factor graph. Following a single, simple computational rule, the sum-product algorithm computes—either exactly or approximately—various marginal functions derived from the global function. A wide variety of algorithms developed in artificial intelligence, signal processing, and digital communications can be derived as specific instances of the sum-product algorithm, including the forward/backward algorithm, the Viterbi algorithm, the iterative "turbo" decoding algorithm, Pearl's belief propagation algorithm for Bayesian networks, the Kalman filter, and certain fast Fourier Transform(FFT).

2.Title:Fully Homomorphic Encryption over the Integers

Authors: Marten van Dijk, Craig Gentry, Shai Halevi

Description:

We describe a very simple "somewhat homomorphic" encryption scheme using only elemen- tary modular arithmetic, and use Gentry's techniques to convert it into a fully homomorphic scheme. Compared to Gentry's construction, our somewhat homomorphic scheme merely uses addition and multiplication over the integers rather than working with ideal lattices over a polynomial ring. The main appeal of our approach is the conceptual simplicity.

We reduce the security of our somewhat homomorphic scheme to finding an approximate integer gcd – i.e., given a list of integers that are near-multiples of a hidden integer, output that hidden integer. We investigate the hardness of this task, building on earlier work of Howgrave- Graham.

3.Title:Private Predictive Analysis on Encrypted Medical Data

Authors: Joppe W. Bos, Kristin Lauter, and Michael Naehrig

Description:

Increasingly, confidential medical records are being stored in data centers hosted by hospitals or large companies. As sophisticated algorithms for predictive analysis on medical data continue to be developed, it is likely that, in the future, more and more computation will be done on private patient data. While encryption provides a tool for assuring the privacy of medical information, it limits the functionality for operating on such data. Conventional encryption methods used today provide only very restricted possibilities or none at all to operate on encrypted data without decrypting it first. Homomorphic encryption provides a tool for handling such computations on encrypted data, without decrypting the data, and without even needing the decryption key.In this paper, we discuss possible application scenarios for homomorphic encryption in order to ensure privacy of sensitive medical data. We describe how to privately conduct predictive analysis tasks on encrypted data using homomorphic encryption. As a proof of concept, we present a working implementation of a prediction service running in the cloud (hosted on Microsoft's Windows Azure), which takes as input private encrypted health

data, and returns the probability for suffering cardiovascular disease in encrypted form. Since the cloud service uses homomorphic encryption, it makes this prediction while handling only encrypted data, learning nothing about the submitted confidential medical data.

4.Title:A Virtual Machine Introspection Based Architecture for Intrusion Detection

Authors: Tal Garfinkel, Mendel Rosenblum

Description:

Today's architectures for intrusion detection force the IDS designer to make a difficult choice. If the IDS re- sides on the host, it has an excellent view of what is happening in that host's software, but is highly susceptible to attack. On the other hand, if the IDS resides in the net- work, it is more resistant to attack, but has a poor view of what is happening inside the host, making it more susceptible to evasion. In this paper we present an architecture that retains the visibility of a host-based IDS, but pulls the IDS outside of the host for greater attack resistance. We achieve this through the use of a virtual machine monitor. Using this approach allows us to isolate the IDS from the monitored host but still retain excellent visibility into the host's state. The VMM also offers us the unique ability to completely mediate interactions between the host soft- ware and the underlying hardware. We present a detailed study of our architecture, including Livewire, a prototype implementation. We demonstrate Livewire by implementing a suite of simple intrusion detection policies and using them to detect real attacks.

IMPLEMENTATION:

1. MODULE

- Registration and Login
- Cloudlet
- Doctor
- Patient
- Health Device

1.1. REGISTRATION AND LOGIN

- Doctor can view the patient details by using their login name and password.
- The patient can view their details only their details only.
- The patient need to enter their using password and username..After entering the login details the patient need to enter the virtual id that use send to the mail id when register to the cloud.

1.2. CLOUDLET

- The cloudlet is working as central authority.
- If the new patient or doctor registered on the cloud the cloudlet need to enable the login permission.
- The cloudlet has the control over the cloud.

1.3. DOCTOR

- The doctor can view the patient details.
- The doctor can give advice to the patient based on the patient problems.The doctor can view only their patient details

1.3.1.PATIENT

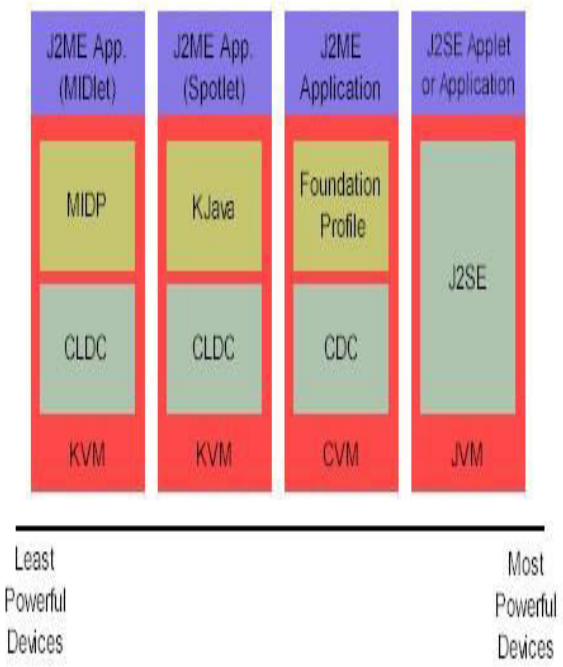
- The patient can view their health report. Before that the patient need to get the access permission.
- The patient can request the cloudlet the give access to the doctor for their records.

1.4. HEALTH DEVICE

- The health devices are used to continuously monitoring the patient health.

The health devices are used to upload the patient health details.

ARCHITECTURE:



CONCLUSION:

We formulated, optimized, and implemented an NTRU- based variant of the HE scheme of which achieves much slower growth of noise, and thus much better parameters than previous HE schemes. Compared to the work in, our GPU implementation (GM204 Maxwell architecture) achieves a speedup of 6085xin Ctxt multiplication, which represents the bottleneck for most HE schemes. Representative medical applications, namely Pearson Goodness-of-fit test, Cochran-Armitage test for trend (CATT), predictive analysis, and relational operations were implemented and scored speedups of 160.9x, 162.9x, 80000x, and 12.2x, respectively.

REFERENCE:

[1] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in Proceedings of the 41st Annual ACM Symposium on Theory of Computing, ser. STOC '09, New York, NY, USA, 2009, pp.169178.[Online].Available:doi.acm.org/10.1145/1536414.153644

[2] ——, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, crypto.stanford.edu/craig.

[3] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," in Advances in Cryptology – CRYPTO 2011, ser. Lecture Notes in Computer Science, P. Rogaway, Ed. Springer Berlin Heidelberg, 2011, vol. 6841, pp. 487–504. [Online]. Available: dx.doi.org/10.1007/978-3-642-22792-9 28

[4] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully Homomorphic Encryption over the Integers," in Advances in Cryptology– EUROCRYPT 2010, ser. Lecture Notes in Computer Science,H. Gilbert, Ed. Springer Berlin Heidelberg, 2010, vol. 6110, pp. 24–43. [Online]. Available: dx.doi.org/10.1007/978-3-642-13190-5 2

[5] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(Leveled) Fully Homomorphic Encryption Without Bootstrapping," in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ser. ITCS '12, New York, NY, USA, 2012, pp. 309–325. [Online]. Available: doi.acm.org/10.1145/2090236.2090262

[6] Z. Brakerski and V. Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard) LWE," in Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, 2011, pp. 97–106.

[7] C. Gentry, A. Sahai, and B. Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based," in Advances in Cryptology – CRYPTO 2013, ser. Lecture Notes in Computer Science, R. Canetti and J. Garay, Eds.

Springer Berlin Heidelberg, 2013, vol. 8042, pp. 75–92. [Online]. Available: dx.doi.org/10.1007/978-3-642-40041-4 5

[8] Z. Brakerski and V. Vaikuntanathan, "Lattice-based FHE As Secure As PKE," in Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, ser. ITCS '14, New York, NY, USA, 2014, pp. 1–12. [Online]. Available: doi.acm.org/10.1145/2554797. 2554799

[9] ——, "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages," in Advances in Cryptology – CRYPTO 2011, ser. Lecture Notes in Computer Science, P. Rogaway, Ed. Springer Berlin Heidelberg, 2011, vol. 6841, pp. 505–524. [Online]. Available: dx.doi.org/10.1007/978-3-642-22792-9 29

[10] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can Homomorphic Encryption Be Practical?," in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, ser. CCSW '11, New York, NY, USA, 2011, pp. 113–124. [Online]. Available: doi.acm.org/10. 1145/20466 .