The 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220609

Secure Electronic Medical Records Using Lattice Cryptography and Fog Computing Techniques

Fatokun Yemi Tunrayo[1], Arome Junior Gabriel[2,*][0000-0001-6665-9308] and Alowolodu Olufunso Dayo[2]

[1] Osun State University Osogbo, Nigeria yemi.fatokun@uniosun.edu.ng
[2] Department of Cyber Security, Federal University of Technology, Akure, Nigeria ajgabriel@futa.edu.ng

odalowolodu@futa.edu.ng

Abstract. The usage of Information Technologies (IT), as well as data has increased over the years to improve businesses and human life generally thereby increasing productivity. In the health sector, Electronic Health Records (EHR) has helped in collecting demographic medical data which helps healthcare practitioners to provide quality health care. The EHR generates lots of medical data and are analyzed and processed to form big health data and sent to Agencies, Government to influence decisions in improving quality of life and to predict or prevent premature deaths and disease development. In this research work, we propose a model using lattice-based cryptography to encrypt health big data and deploy a decoy model which will be coined in fog computing facility to serve as honeypot or trap machine to attract attackers.

Keywords: cloud computing, information security, fog computing, medical health records, post quantum cryptography.

1. Introduction

Data and its transformation to information undergo several processes for it to be meaningful to the end users. Some of the processes involved in processing include retrieving/extracting, storing, and sending information from one end to another. The use of technology to transform the data digitally has increased tremendously over the years making computers to take over the key activities in our day-to-day lives [1][2]. Computers and other transmitting devices play key roles in transmitting data over secured channels [3]. Security of data from one node to another node during transmission would have been guaranteed, but with the emergence of internet and the need to make data accessible to all, has raised security concerns [4]. As a result, many new technologies evolved to improve the security of data where it is stored so that users can generally access data over secured public domains. The Health Sector play primary key role in profiling patients' personal data to properly discharge quality health care. In view of this, the sector also joined the trend and is currently undergoing a dramatic and fundamental shift by digitizing health and patient data to predict disease outbreak and make better decisions.

DOI: 10.54254/2755-2721/2/20220609

2. Related works

There exist several published researches that use the adoption of cloud computing as a solution to explore healthcare industry. [5] pointed out that EMR-based hospitals have little relevance because just about 10% of Nigerian hospitals can afford them, and most of these EMRs are remotely placed in the hospital's infrastructure rather than being moved to the cloud. Electronic Medical Records must be migrated to the cloud in order for consumers to have quick access to health care. Because human life is valuable and medical resources are limited, cloud-based healthcare services match a cost-effective concept in which patients and health organizations benefit from this new technology by improving patient quality of service through a distributed high-integrated platform, coordinating medical processes, and lowering IT infrastructure investment or maintenance costs, resulting in improved healthcare outcomes [6].

[7] developed fine-grained encryption to safeguard individual info within an EMR, and with the proliferation of smart mobile devices, more patients and healthcare givers are turning to mobile devices to access EMRs for faster record access. Each node, XML-based EMR, was exported to partially-trusted cloud storage locations, or the patient's mobile device was used, according to an encryption engine. To make available self-protecting EMRs for mobile platforms using recent breakthroughs in attribute-based encryption, provider personnel acquire their ABE decryption keys with an online key server. The keys are manually provided and configured on hospital equipment.

[3] carried out the development of an EMR system to help medical professionals in a typical Nigerian hospital automate their tasks. The design process entailed breaking down the system into modules and establishing the relationships between them. The goal of the research was to address the problems associated with paper-based records, such as insufficient physical storage space for cards in cases of a large number of patients, inconsistency in individual handwriting, and vulnerability to termite or other attacks. It is necessary to continue to use both as instruments for delivering high-quality, secure healthcare services.

[8] carried out the development of a cloud-based EMR system that may be utilized to efficiently handle medical information sharing. A Central Database Server for all medical centers, a Unifier Interface Middleware, and an Authentication Server make up this new system, which was built with capacity for reducing administrative bottlenecks, as well as, lowering the cost of healthcare delivery. The security of both EMR access and medical data sharing was not taken into account.

[9] presented a secure EMR system that includes a cloud server, an ECC connection module, a smart card, as well as, portable devices. The ECC-based secured EMR provides increased security while reducing the amount of computation required on terminal devices. When security demands grow, the massive amount of processing required for encryption and decoding will use significantly more hardware resources.

[10] presented a user authentication system based on location and biometrics, as well as a steganography-based technique for embedding EHR data. The focus of future work will be on ensuring a secure key exchange between all parties involved.

[11] proposed fine-grained access control, taking into account, extra security factors, such as encryption and digital signature, to safeguard the public from the danger of privacy violations by supplying only the necessary information from the desired patient medical documents to authorized users using ABAC, a XACML, XML security measures for encryption and digital signature. Additional privacy-preserving features will be required for the model.

[12] suggested an attribute-based access procedure for healthcare systems that ensures, only permitted users have access to the system's requested resources by implementing policies and rules. In addition, we deal with emergency situations within this framework. The researcher showed how an emergency could be handled while maintaining patient privacy.

[13] suggested a privacy-aware authentication scheme to protect patients' privacy, as well as a probabilistic strategy for detecting and blocking inference channels to prevent indirect data access. By computing the credibility of medical data using the beta and dirichlet reputation systems, the study addressed the weak status of privacy and trust control in EHR systems. For the preservation of medical

DOI: 10.54254/2755-2721/2/20220609

data in storage, no cryptographic scheme was explored. Besides, the suggested access control approach requires the implementation of a prototype.

[14] presented a trust framework for information exchange in health care, particularly in mobile health care, with the goal of providing high-quality as well as efficient patient care. The designed model has two parts: the first calculates the amount of trust required for each user to share a given piece of information, and the second determines the (contextual) present level of trust. A comparison of the components would be used to make a decision about sharing information. This model, on the other hand, is just focused on access control regulations and cannot serve as a decision-making tool for the user.

3. Background to lattice cryptography

To guarantee patients' data availability, integrity and confidentiality, some researchers proposed so many measures in ensuring security and privacy of medical data. Some of the measures include Access Control, Data Masking, Authentication, Monitoring, Auditing and Cryptography [15].

The use of cryptography has been proven over the years to be most effective in securing data over public networks. Cryptography is defined to be the art of transforming information into something unintelligible for anyone but the intended recipient [16]. This has been used for diplomatic, military, commercial and private communication, and historically for disguising religious texts. By scrambling the information in a given medical file/record, the original text, or plaintext, is converted into a coded equivalent, called cipher-text, which can only be deciphered (decrypted) by those who have a secret key [16][17].

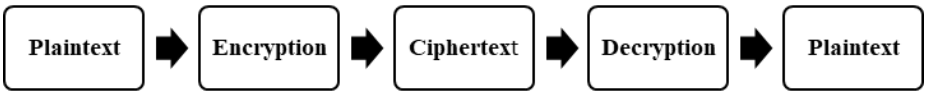

Figure 1. Simple illustration of the cryptography process.

A cryptosystem is an aggregation of protocols, algorithms and/or keys, which is capable of providing encryption, decryption, and related services. The algorithm, also known as a Cipher, is a collection of rules that governs the process of encrypting and decrypting, while the key is in essence, the secret value/piece of information required to encrypt and decrypt. A key is a sequence of random bits that the algorithm will utilize to increase the unpredictability of the encryption procedure. In order to communicate using encryption, two entities have to make use of the same algorithm and, in many cases, the same key [18]. Various crypto algorithms have been developed and deployed relatively well and can be broadly classified as Symmetric, Asymmetric and Hash Functions [19].

Symmetric (Private Key) Cryptography techniques (such as DES, 3DES, AES, or even Blowfish) encrypt and decrypt data using two copies of the same key. Asymmetric (public-key) cryptography schemes (such as RSA or ECC), on the other hand, employs public/private keys for encrypting and decrypting secret messages respectively. one-way hash-function that takes a variable-length message and returns a fixed-length string as the input message's hashed value. To produce a certificate with some kind of digital signature for confirming that the content of such an input message has not been altered, hashing techniques (such as MD5, SHA-1, SHA-2, or even SHA-256) are utilized. However, all these crypto algorithms are susceptible to post-quantum attacks. This current paper utilizes a public key cryptography scheme (lattice crypto) that works based on the difficulty of solving difficult problems in lattice mathematics.

Among all research areas of post-quantum cryptography, lattice-based cryptography attracts the greatest interest. Because it operates across very small integers, it ensures great security and efficiency, making it ideal for IoT applications [20]. Simple manipulations involving matrices and vectors in certain rings or fields of short order are used in the computations. A lattice is a subsequence with a

DOI: 10.54254/2755-2721/2/20220609

pattern in an n-dimensional space. It is a set of points in an n-dimensional space with a periodic pattern.

This is easy to solve in a two-dimensional grid, but as the number of dimensions is increased, even a quantum computer cannot efficiently solve the problem. Given n linearly independent vectors b_1, b_2 , …, b_n $\in$ R_n , the Lattice L is defined as: $L = \{a_1b_1 + \cdots + a_nb_n \mid a_i \in Z\}$ where the set $(b_1, b_2, \ldots, b_n)$ is called a basis of the lattice. This can be written in a compact form [3]:

$$L(B) = \{B_x \mid x \in Z_n\}$$

Where:

n - dimension, q – prime, P(x) – Polynomial, Ring, Rq $\coloneqq$ Zq[x]/P(x), $Z_q^n \equiv$ The additive group of n-dimensional integer vectors mod q.

This current paper proposes a framework that integrates lattice-based cryptography in preserving privacy of medical data in cloud repositories/channels or fog nodes.

4. Design of the proposed fog-based system for secure medical health records

The proposed fog computing based medical data security system has two (2) major units; the first unit (cloud facility) contains the OMD in Cloud facility [21-22]. The second unit contains the decoy medical data storage facility, which is like (but it is not) the mirror image of the Original (actual) users' Medical Data (OMD). The design of the second module (fog facility) will involve, the setting up and configuration of a virtual local server on a HP Laptop with iCore7 on Ubuntu Linux Operating System (OS) to serve as the Fog Computing facility [20][23]. Necessary or required configurations would be made and tested. Some data would be uploaded to compute the communication overhead and computational cost using these parameters (Memory Requirement, Latency, Bandwidth usage).

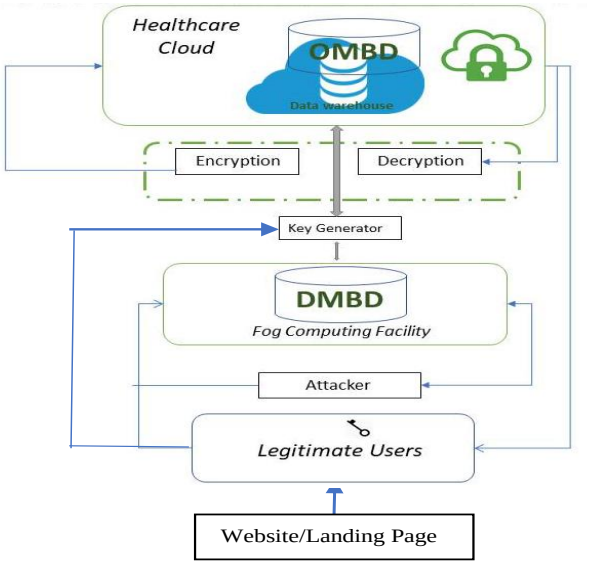

Figure 2. Conceptual view of the proposed system.

Users would be granted access according to their requests by their virtue of job functions. Privileges would be assigned to users for authentication and access to data according to their rights or specific roles. There will be room for users to choose from available options whether they want to classify documents (sensitive or non-sensitive). Using the fog computing as well as the decoy/honeypot concepts/techniques, a Decoy MBD, which contains fake copies of medical data is created inside the first module.

DOI: 10.54254/2755-2721/2/20220609

To cater for the design of the Cloud Computing facility where the OMBD will reside, users will be prompted to choose from these three major categories of Cloud Computing Service Models, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), or Platform-as-a-Service (PaaS). This choice of category will determine the kind of Cloud Storage Provider (pCloud, Google Drive, Dropbox, Microsoft Onebox, or Amazon Drive) to be recommended [24-27].

The design of a user-friendly platform that will serve as interface for data administrators, medical researchers and other related paramedical personnel for easy access to load data to fog or cloud storage. The platform will be web-based hosted on localhost/live server (bluehost) for a period time for the purpose of the research. A content management system, Joomla 3.9.15 was used to manage the contents of the website.

A computer interface that defines interactions involving multiple software intermediaries is known as an application programming interface (API). Google Sign-in API, Crypto API and Google Cloud API on Google Cloud Platform will be integrated on the website. Google Sign-in API uses OAuth 2.0 for authentication and authorization. This will enforce users to login to the platform using authentic email accounts. The Crypto API will be designed using php and this is where our algorithms will be configured and installed. The Google Cloud API is a free platform that enables users to create, manage and migrate databases to the cloud. The Google Cloud API will be used to manage our databases in the cloud. These APIs except the Crypto API only work when hosted on a live server. Then verification of the user takes place. As soon as a user is confirmed a legitimate user (by providing correct answers to security questions or supplying a confirmation code), such user will be allowed to access his/her Original Medical Data (OMD).

User privileges will be set up according to job roles and users will be categorized according to the use of the database they intended to work with. Users will be categorized into Primary Users, Secondary Users and Third-Party Users. Every other user will be treated as Guests. The Primary Users will be issued full access to the platform, and they will be referred to as Authors. The Secondary Users will be referred to as Editors while the Third-Party Users will be referred to as Managers. The user termed administrator is the IT personnel managing the site, its sole responsibility is to manage users and check the activities of all users. They have privileges to keep the system running and manage access keys; design models to secure data over secured transmission. The Author is the originator of the medical data. Personnel include Medical Doctors/Practitioners in custodian of the health record. The Editor is like a government agency or researcher given access to work or analyze the original data. The User category entails the users of the analyzed data to make decisions. Insurance agency, Social Security agency, patients belong to this category. The Manager is the owner of the hospital or healthcare facility. All other users not registered are categorized as Guest.

Also, Hybrid User Profiling (Explicit and Implicit Profiles) is adopted to improve the strategy used for monitoring cloud access and detecting any unconventional/strange data access pattern by reducing the weaknesses and enhancing the strengths. Once unusual data access pattern is discovered from any user, such user is checked for possible blacklisting. Likewise, as a second security mechanism, the medical data in the OMD are encrypted. The legitimate user must supply a cryptographic key to decrypt. To minimize or even eliminate performance issues, a lightweight (based on lattice cryptography) selective encryption approach is used. This selective encryption protocol is robust in security since it is resistant to common classical and quantum attacks [28-30]. Furthermore, not all data will be encrypted, as a result, just the information that requires additional protection is encrypted. This is accomplished by offering the user the option of encrypting his or her data completely, selectively, or not at all.

The second module caters for configuration of the fog facility as a honeypot. This technique is classified as an illusion technique because it leads the attacker to believe that he or she has gained access to the user's Medical Data (MD), when in fact it is only a decoy (and unimportant) piece of medical data. Once a user interacts with his/her account, the Decoy MD is first shown to him/her. This really means that, all users (authorized/unauthorized) are first directed to the Decoy MD at every attempt. Furthermore, for every file uploaded in the OMD, a replica of the file would be created in the DMD

DOI: 10.54254/2755-2721/2/20220609

using an algorithm that will add some bogus information to the decoy file which will serve as honey-pot. Non-sensitive data will remain within the fog server while sensitive data would be sent to Health Cloud Server. A port will remain open on the Fog server so that attackers can have access to the decoy file to observe the behavioral pattern using these parameters (IP Address, bandwidth usage, Access time and date, Memory Usage, Power Consumption etc.).

5. Setup for the experiment

The proposed system was built using .net framework, C# programming language, angular JS, with every unit built as a containerized application using docker, HTML 5, CSS, MSSQL, as well as Azure Cloud Service Provider to model a user-friendly EHR software with capacity for guaranteeing multi-level privacy/security utilizing lattice crypto and user access control to patients' personal info. The website was able to get several hits (the clicks on one of the webpages) between 15th November 2020 and 15th December 2020 due to the COVID-19 pandemic. It was observed that, about 1,800 hits were recorded within a week, out of which about 741 (41%) download of the decoy files were made. 481 (27%) attempts at reading and accepting the terms and conditions were made. Similarly, about 67% followed the correct user-registration procedure. More significantly, no unauthorized user was able to download the original file that was encrypted using the crypto-scheme. To allow for the testing and appraisal of the performance characteristics of the proposed privacy model, we independently developed cryptographic systems based on the ECC and lattice crypto algorithms. Tests were then conducted based on some standard metrics (such as, computation time, output size, throughput, and bandwidth consumption. It was observed that Lattice-based do confirm our speculations about being faster in terms of speed of encrypting and decrypting and does not involve complex mathematical calculations. However, our proposed system seems to handle large files better than the ECC-based system. This is probably because of the fact that, in lattice-based systems, calculations are performed using matrices as against the ECC-based systems where complexity of computation becomes exponential due to the number of hops it takes to compute the private keys. Therefore, lattice-based cryptosystem seems to be more efficient when dealing with big data.

6. Conclusion and recommendation

Various systems have been developed for ensuring the security/privacy of communication over enterprise networks or even between client systems and cloud servers. Almost all of these have shortcomings like inefficiencies and susceptibility to highly technical classical or even quantum threats/attacks [5][18]. Post-Quantum Cryptography is somewhat a new and interesting topic for researchers and the lattice cryptography scheme in particular offers desirable qualities like efficiency and resistance to common classical/quantum attacks with respect to communication or cloud computing security. This research has proposed a lightweight security system (cryptosystem) that will guarantee privacy of data and communication in both Classical and Post Quantum Computing era.

References

[1] Gabriel A. J., BK Alese, AO Adetunmbi, OS Adewale, (2015). "Post-quantum crystography based security framework for cloud computing", Journal of Internet Technology and Secured Transactions (JITST), Pages 351-357.

[2] Quek Kia Fatt and Amutha Ramadas (2018) "The Usefulness and Challenges of Big Data in Healthcare", Journal of Healthcare Communications, ISSN 2472-1654 Vol.3 No.2:21

[3] Ajala F., Awokola J., and Emuoyibofarhe O.(2015) Development Of An Electronic Medical Record (EMR) System For A Typical Nigerian Hospital. Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 3159- 0040 Vol. 2 Issue 6.

[4] Abouelmehdi Karim, Beni-Hessane Abderrahim, Khaloufi Hayat (2018), "Big Healthcare data: preserving security and privacy", Journal of Big Data, https://doi.org/10.1186/s40537-017-0110-7.

[5] Asonganyi Jeffrey Nkwetta Matricule No: CT14A019 Degree for which submitted: B.Tech Department: Computer Engineering Project Title: Honey-System: Design, Implementation and Attack Analysis Project Supervisor: Dr. Sone Ekonde Michael Date: July, 2018.
[6] Wang X. (2010) Application of Cloud Computing in the Health Information System, International Conference on Computer Application and System Modeling (ICCASM).
[7] Akinyele J., Pagano M, Green M, Rubin A, Lehmann C , Peterson Z, (2011) Securing electronic medical records using attribute-based encryption on mobile devices DOI: 10.1145/2046614.2046628.
[8] Boyinbode O. and Toriola G. (2015) CloudeMR: A Cloud Based Electronic Medical Record System. International Journal of Hybrid Information Technology Vol.8, No.4 (2015), pp. 201-212.
[9] Tsai K., Leu F., Tien-Han W., Chiou S., Liu Y., and Liu.H (2014) Secure ECC based Electronic Medical Record System. Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 47-57.
[10] Premarathne U., Abuadbba A., Alabdulatif A., Khalil I., Tari Z., Zomaya A., and Buyya, R. (2015) Hybrid Cryptographic Access Control for Cloud-Based EHR Systems. IEEE Cloud Computing, 3(4), 58–64. doi:10.1109/mcc.2016.76.
[11] Kwangsoo et al. (2018) Privacy-preserving Attribute-based Access Control Model for XML-based Electronic Health Record System. IEEE Access PP (99):1-1 DOI: 10.1109/ACCESS.2018.2800288.
[12] Afshar M., Samet S., and Hu T. (2018) an Attribute Based Access Control Framework for Healthcare System IOP Conf. Series: Journal of Physics: Conf. Series 933 (2018) 012020 doi :10.1088/1742-6596/933/1/012020.
[13] Bandar S Alhaqbani. (2010) Privacy and Trust Management for Electronic Health Records. Queensland University of Technology, Brisbane, Australia.
[14] Saghar B. and Stephen M. (2017) Trust-based framework for Information Sharing in Health care. University of Ontario Institute of Technology.
[15] Suraj Shukla, Detailed Review of Different Security Techniques for Data Protection in Cloud Computing (April 20, 2020). Available at https://ssrn.com/abstract=3580863 or http://dx.doi.org/10.2139/ssrn.3580863.
[16] Gabriel, A., Alese, B. K., Adetunmbi, A. O., & Adewale, O. S. (2013).” Post-Quantum Crystography: A combination of Post- Quantum Cryptography and Steganography”, 8th International Conference for Internet Technology and Secured Transactions (ICITST 2013) doi:10.1109/icitst.2013.6750240.
[17] Alowolodu O.D., Alese B.K., Adetunmbi A.O., Ogundele O.S. (2013). “Elliptic Curve Cryptography for Securing Cloud Computing Applications”, International Journal of Computer Applications, Volume 66 Issue 23.
[18] Gabriel, A. J. (2021). Secure Storage and Sharing of COVID-19 Data in Health Facilities using AES-Cryptography and Audio Steganography. Journal of Information technology and Secure Transactions (JITST), 9(1):735-740. Infornomics Society. DOI: 10.20533/jitst.2046.3723.2021.0090.
[19] Thompson, A., Abayomi, A., Gabriel, A.J. (2022). Multifactor IoT Authentication System for Smart Homes Using Visual Cryptography, Digital Memory, and Blockchain Technologies. In: Misra, S., Kumar Tyagi, A. (eds) Blockchain Applications in the Smart Era. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-89546-4_14.
[20] Bowen B. M., Shlomo Hershkop, Angelos D. Keromytis, Salvatore J. Stolfo (2009) “Baiting Inside Attackers using Decoy Documents”, Department of Computer Science Columbia University New York, NY 10027.
[21] Hamid, H. Rahman, S M., Hossain, M. S., Ahmad A., Alamri, A. (2017). A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing

Facility With Pairing-Based Cryptography. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2757844.

[22] Alowolodu, Olufunso Dayo, Gabriel Kayode Adelaja, Boniface Kayode Alese, Olufunke Catherine Olayemi (2018) “Medical Image Security Using Quantum Cryptography”, Issues in Informing Science & Information Technology, Informing Science Institute, Pages 57-68.

[23] Spitzner, Lance (2003). Honeypots: Sticking it to hackers. 18. 48-51.

[24] David R.Matos, Migue lL.Pardal, PedroAd˜ao Ant´onio RitoSilva, Miguel Correia (2018) Securing Electronic Health Records in the Cloud INESCID, Instituto Superior T´ecnico, Universidade de Lisboa, Portugal 2 Instituto de Telecomunica¸c˜oes, Lisboa, Portugal.

[25] Sriram M., Vaibhav Patel, Harishma D., Nachammai Lakshmanan, (2014), “A Hybrid Protocol to Secure the Cloud from Insider Threats”, DOI: 10.1109/CCEM.2014.7015476.

[26] Wang, Lidong & Alexander, Cheryl. (2013). “Medical Applications and Healthcare Based on Cloud Computing”, International Journal of Cloud Computing and Services Science (IJ-CLOSER). 2. 10.11591/closer.v2i4.3452.

[27] Thavamani S., M.Rajakumar (2019) Privacy Preserving Healthcare Data using Cloud Computing International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-10S.

[28] Hey T. (1999) Quantum computing: An introduction. Computing & Control Engineering Journal, 10(3):105–112.

[29] Kraemer Frank Alexander, Anders Eivind Bråten, Lindner, R., & Peikert, C. (2011). Better Key Sizes (and Attacks) for LWE-Based Encryption. IACR Cryptol. ePrint Arch., 2010, 592.

[30] Yuan Y.et. al. (2016) Portable implementation of lattice-based cryptography using javascript. InCANDAR.