International Journal of Grid and Distributed Computing
Vol. 14, No. 1, (2021), pp. 1494–1500

# Fully Homomorphic Secure Internet of Things Framework Over Untrusted Cloud

Idris Afzal Shah[1*], Adil Bashir[2] , Sheikh Moeen ul Haque[3] , Dr. Mohammad Ahsan Chishti[4], Dr. Shaima Qureshi[5]

[1,2,3]*Department of Computer Science and Engineering, School of Engineering and Technology, Islamic University of Science and Technology,Awantipora, J&K, India*

[4,5]*Department of Computer Science and Engineering, National Institute of Technology, Srinagar, J&K, India*

[1]*idrisshah@yahoo.com,*[2]*adilbashir.445@gmail.com,*[3]*sheikhmoin41@gmail.com,*
[4]*ahsan@nitsri.net,*[5]*shaima@nitsri.net*

***Abstract***

*Leveraging the cloud support has proven critical and pivotal in storing/managing the data being generated at an exponential rate by Internet of Things (IoT) devices. The data sensed by IoT devices is private mostly and needs to be protected from unauthorized users during its transit where symmetric/ asymmetric cryptography like RSA, AES work well. However, these cryptosystems fail as they need to access plaintext for performing data analytics thus revealing data to cloud owners. The proposed model mitigates this concern by employing fully homomorphic encryption (FHE) for enciphering of data collected from the sensor for privacy preserving and providing confidentiality services before sending it to the cloud for analytics. FHE allows direct computation on encrypted data. Moreover, the model performs error detection / correction using Reed Solomon Codes (RS Codes) at edge/fog nodes and at cloud also as an additional security measure keeping in mind the sensitivity of the data obtained for IoT system. It is a unique model combining power of FHE and RS codes for IoT objects.*

***Keywords:*** *Cloud; Fully Homomorphic Encryption (FHE); IoT; Reed Solomon Codes ;Security.*

## 1. Introduction

Any physical object equipped with communication portion can connect to the Internet and be a part of the loT infrastructure. It includes almost everything you would consider including wearable's, bulbs, TV , etc. The number of loT-enabled devices is now 22 billion as per the Strategy Analytics Report, and the study estimates that 38.6 billion devices will be connected by 2025 and 50 billion by 2030[1]. [1]

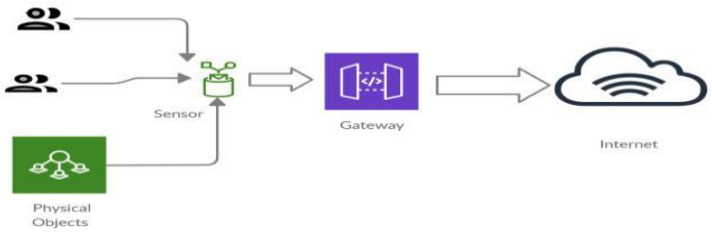



**Figure 1. IoT architecture**

### 1.1. Home Automation



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

In our homes, IoT can be used to monitor various appliances such as lighting, heating, air conditioning, entertainment gadgets and other home protection equipment in order to enhance comfort and reduce energy usage as well.

### 1.2. Healthcare

IoT can be used in the healthcare sector for patient surveillance, early identification of diseases that will ensure timely medical treatment in emergencies.

### 1.3. Environment Monitoring

IoT has become a focal point in our world because of its diverse applications. Our environmental experts may use loT with the help of sensor based technologies to track air, water quality, atmospheric or soil conditions.

### 1.4. Smart Wearables

Smart devices such as medical health monitoring devices are worn by patients for their continuous observation of health parameters. Similarly, the fitness gadgets are also used by people in order to track their daily fitness activities.

### 1.5. Smart City

Smart city includes a diverse use cases ranging from waste management to traffic management to water supply management to smart parking. The objective behind this important application of IoT is to lessen the real troubles faced by people living in cities by managing pollutions, traffic congestion and time of the dwellers [2][3][4]. Cloud-IoT designs have been proposed in [5–7] and an examination of properties for IoT cloud suppliers has been performed in [8].Taking computation to cloud might prove pivotal for resource constrained devices in an IoT environment for performing analytics over data. However, the untrustworthiness of cloud seems to be a major concern when designing a safe and secure cloud based IoT framework. Cloud provides different required services to IoT environment; however, the security of sensitive data in-transit and at cloud needs to be ensured. Analytics of the data at cloud needs to be performed in encrypted form and computed results shall be shared only to intended users, possessing secret key, in encrypted form [9].

### 1.6. Background

**1.6.1. Fully Homomorphic Encryption:** Fully Homomorphic Encryption (FHE) was given by Craig Gentry in the year 2009 and has been considered as a major breakthrough in the field of cryptography [10]. Using this scheme, it is plausible to directly perform arbitrary computations over the encrypted data. We have what we call as Partially Homomorphic Encryption (PHE) cryptosystems such as RSA, Paillier systems. RSA is multiplication homomorphic. If the RSA public key is modulus and exponent , then the encryption of a message is given by ( ) = .

In this case, the homomorphic property is,

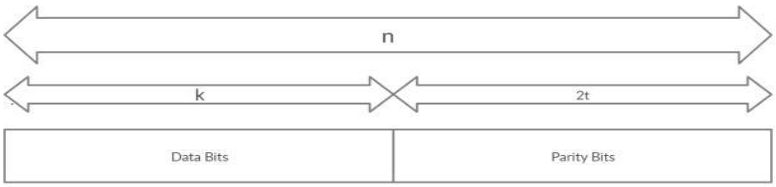
$$(\quad).(\quad)==(\quad)=(\quad.) \tag{1}$$

Similarly Paillier cryptosystem is additively homomorphic. In the Paillier cryptosystem, if the public key is the modulus $m$ and the base $g$, then the encryption of a message $x$ is$(\ ) = {}^{2}$ , for some random $\in \{0, \dots \dots, -1\}$.The homomorphic property is then

$$(\quad)(\quad)=(\ {}^{1}\ )(\ {}^{2}\quad)=1+2\quad(\ )\quad=(\quad+\quad) \tag{2}$$

**1.6.2. Reed Solomon Codes :** RS codes are used to correct errors in communication channels caused by noise and other external interferences in a data repository due to factors such as dust, scratches, etc. RS codes are block-based codes .The format of reed Solomon code is ( , ) where the symbol length is s-bits. The RS encoder takes k data symbols of s bits each and then applies parity symbols to

it. Each of the s bits have n-k parity symbols. At the other hand, an RS decoder will correct errors up to t symbols which have errors in a codeword. $2 = -$ gives the relation between the number of symbols and the codeword.






ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

Figure 2. Reed Solomon codeword

RS encoder/decoder may be implemented both in software and hardware [11][12].

The contribution of this paper is to put forth a model which can serve as a basis for cloud based IoT systems in future keeping in mind the promising impact that FHE will have with advancement at both hardware and algorithm/software level. The paper is further divided into sections with sequence as related work, proposed framework, process flow diagram, results/discussions, conclusion and references.

## 2. Related Work

Stergiou et al.[13] have studied the integration benefits of cloud and IoT technologies. They have proposed a security model based on AES and RSA for improving the security resulting from the integration. Aazam et al.[14] focuses on some of the main CloudIoT problems and the communication strategy focused on smart gateways. Cloud of Things requires a smart gateway to perform the rich tasks and pre-processing which sensors and light IoT's can't accomplish. Ammar et al.[15] have done a detailed survey of some of the main IoT frameworks including their architecture, hardware and security details. As one of the most critical contemporary issues facing the Internet of Things, they have concentrated on the security measures of every network and protection from attacks. In [16], attacks on IoT systems have been shown to be both easy and highly capable of building powerful botnets, a network of remote-controlled systems ready to work together. With the combined amount of resources, Distributed Denial of Service (DDoS) attacks can then be launched. Andrea et al.[17] did an IoT attack report. IoT attacks are classified into four key categories: human, computer, network, and encryption. The physical assault occurs when the attacker is close to the IoT device. The network attacks occur when the attacker accesses the IoT network, and they manipulate a certain device to inflict damage. The software attack is exploited through bugs in system. Finally encryption attack is caused by breaking the security system. Saeed et al. [18] have put forward a security architecture using random neural networks for detecting any kind of intrusion in an IoT system. Experiments have successfully detected a malicious sensor node in the operating range with an accuracy of 97.23 per cent. Sharaf et al. [19] proposed an authentication solution in IoT wherein they have used specific fingerprints. For IoT, the fingerprint can include features such as physical state and position. Although each system had different features due to the same working environment, the proposed solution offered a technique for transmission learning by which devices with different environments could be authenticated. Wu et al.[20] have carried out studies that seek to determine Cloud Service Providers 'trust-worthiness' by using Cloud Service Customers feedback ratings, namely the rating-based credibility assessment, which is widely adopted in web service-based applications. Wazid et al. [21] have stressed upon the need of secure authentication of cloud driven IoT system between a user and a sensor. They addressed the problems facing CloudIoT framework in developing the authentication schemes and other security protocols. Li et al. [22] have proposed a framework that enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context by integrating security- and reputation-based trust assessment methods. They have carried out experiment to demonstrate the effectiveness of their model on sample data sets. Ray in [23] has made an analysis of some popular cloud based IoT platforms and given a comparison in areas such as management of a devices, system, heterogeneity, data and application development. Ferretti et al. [24] suggested a lightweight proxy re-encryption scheme to ensure that messages exchanged between less trusted fog nodes in an IoT network are kept confidential. They proved the feasibility through experiments on microcontrollers and architectures based on ARM.

None of the above work has focused on how to safeguard data being generated by sensors from untrustworthy cloud providers for data analytics. In view of this, our proposed model overcomes this crowning issue by employing FHE which is considered as the "holy grail" of cryptography. We have also incorporated RS codes as an additional security layer.



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

## 3. Proposed Framework

Integration of various modules in building the proposed model is as follows:

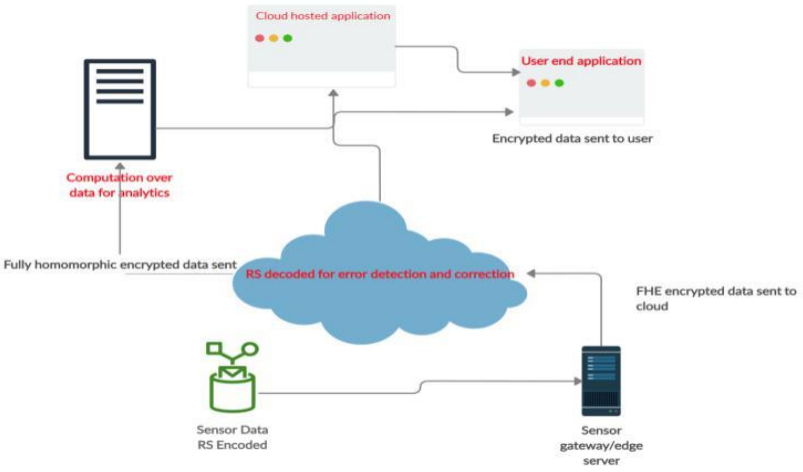



Figure 3. Proposed cloud based IoT framework

## 4. Process Flow Diagram

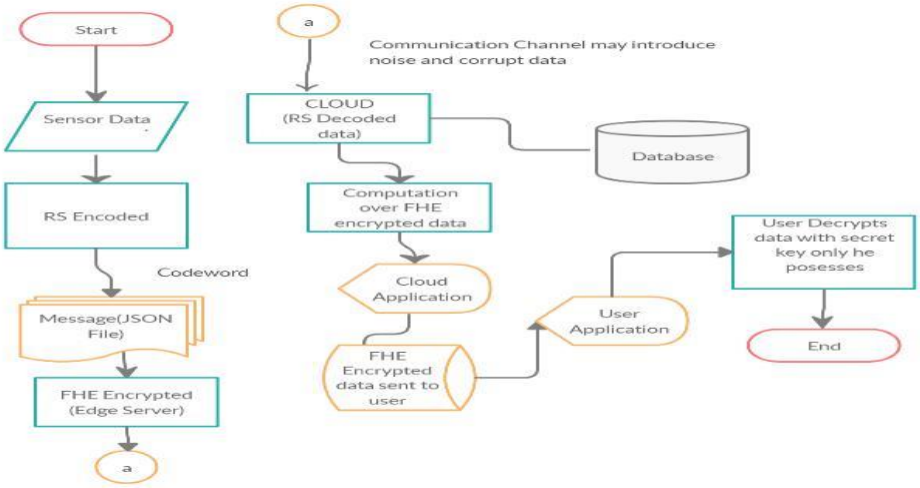



Figure 4. Flow Diagram of proposed design



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

## 5. Results/Discussion

**5.1.** User generated data collected by sensors is RS encoded and sent in a structured format (such as a JSON file) to the sensor gateway/edge server.
**5.2**. At the fog server, the user encrypts the codeword using FHE and forwards the data over the network to cloud.
**5.3.** Error detection/correction is performed at the cloud as the communication channel is noisy and may corrupt the bit stream.
**5.4.** After this, computation is performed over the encrypted data directly for analytics.
**5.5.** Once the results are obtained, the cloud application forwards the encrypted results to the user application.
**5.6.** Finally the user decrypts the encrypted results with the secret key which only he/she possesses.

The table 1 presents the specific technologies that will be used to build a prototype model based on our proposed design such as the devices, processors and system software.

**Table 1. Platform And Its Specifications**

| | |
|---|---|
| **Wireless Sensor Gateway** | ZigBee protocol based. Frequency Band of 2.4 GHz; Range of 100 m; USB , RS- 232, Ethernet. |
| **Wireless (Wi-Fi) Router** | Works in frequency band of 2.4 GHz Wi-Fi; Outdoor Range of 300 feet. |
| **Zigbee Smart Sensor** | Transmission upto 100 m; Frequency band of 2.4 GHz; ARM Cortex M0. |
| **Communication Protocol: ZigBee** | Protocol designed for low cost, Low power etc. |
| **Communication Protocol: 802.11 Wi-Fi** | Protocol for wireless LAN(WLAN) such as handling communication between IP based devices and wireless routers. |

FHE is relatively new cryptosystem. However, owing to its bright future and with advancement both at hardware/ software level, we firmly believe that it will become the de facto standard for cloud/IoT systems in future. So in this context, our model will serve as a basis for further research in this domain.

## 6. Conclusion

To the best of our knowledge, this is a unique framework for securing sensitive data in-transit and the data in storage at cloud. The future work will focus on implementing the system and then analyzing its performance with respect to various metrics like latency, memory, space, time etc. We will also focus on accelerating the fully homomorphic encryption both in terms of hardware and software by translating algorithms and exploiting parallelism.

## 7. Acknowledgements

This work was funded by NPIU (Unit of MoE) Govt. of India under TEQIP III project.



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

**References**

[1]https://www.strategyanalytics.com/strategyanalytics/news/strategy-analytics-pressreleases/2017/10/26/smart-home-will-drive-internet-of-things-to-50-billion-devices-says-strategy-analytics.

[2] Stankovic, John A. "Research directions for the internet of things." IEEE Internet of Things Journal 1, no. 1 (2019): 3-9.

[3] Holler, Jan, Vlasios Tsiatsis, Catherine Mulligan, Stamatis Karnouskos, Stefan Avesand, and David Boyle. Internet of Things.Academic Press, 2020.

[4] Kortuem, Gerd, Fahim Kawsar, Vasughi Sundramoorthy, and Daniel Fitton. "Smart objects as building blocks for the internet of things." IEEE Internet Computing 14, no. 1 (2009): 44-51.

[5] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future generation computer systems 56 (2018): 684-700.

[6]Rogers, Ethan A., and Eric Junga. "Using Intelligent Efficiency to Collect and Analyze Nonenergy Benefits Information." Report IE1702 of the American Council for an Energy-Efficient Economy (ACEEE) (2017).

[7] Fortino, Giancarlo, Antonio Guerrieri, Wilma Russo, and Claudio Savaglio. "Integration of agent-based and cloud computing for the smart objects-oriented IoT." In Proceedings of the 2014 IEEE 18th international conference on computer supported cooperative work in design (CSCWD), pp. 493-498. IEEE, 2019.

[8] Pflanzner, Tamas, and Attila Kertész. "A survey of IoT cloud providers." In 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 730-735. IEEE, 2016.

[9] Dobre, Ciprian, and FatosXhafa. "Intelligent services for big data science." Future generation computer systems 37 (2014): 267-281.

[10] Gentry, Craig. "Fully homomorphic encryption using ideal lattices."Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009.

[11] Gorenstein, Daniel, and Neal Zierler. "A Class of Error-Correcting Codes in p^m Symbols." Journal of the Society for Industrial and Applied Mathematics 9.2 (1961): 207-214.

[12] Shao, H., T. Truong, L. Deutsch, J. Yuen, and I. Reed. "A VLSI design of a pipeline Reed-Solomon decoder." In ICASSP'85. IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 10, pp. 1404-1407. IEEE, 1985.

[13] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78 (2018): 964-975.

[14] Aazam, Mohammad, Pham Phuoc Hung, and Eui-Nam Huh. "Smart gateway based communication for cloud of things." In 2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP), pp. 1-6.IEEE, 2014.

[15] Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." Journal of Information Security and Applications 38 (2018): 8-27.



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC

[16] The Guardian “DDoS attack that disrupted internet was largest of its kind in history, experts say”.October2016.[online].Availablehttps://www.theguardian.com/technology/2016/oct/26/ddos-attack-dynmirai-botnet.

[17] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." In 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187.IEEE, 2015.

[18] Saeed, Ahmed, Ali Ahmadinia, Abbas Javed, and HadiLarijani. "Intelligent intrusion detection in low-power IoTs." ACM Transactions on Internet Technology (TOIT) 16, no. 4 (2016): 1-25.

[19] Sharaf-Dabbagh, Yaman, and WalidSaad. "On the authentication of devices in the Internet of Things." In 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-3. IEEE, 2016.

[20] Wu, Qingtao, Xulong Zhang, Mingchuan Zhang, Ying Lou, RuijuanZheng, and Wangyang Wei. "Reputation revision method for selecting cloud services based on prior knowledge and a market mechanism."The Scientific World Journal 2014 (2014).

[21] Wazid, Mohammad, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel JPC Rodrigues. "Authentication in cloud-driven IoT-based big data environment: Survey and outlook." Journal of Systems Architecture 97 (2019): 185-196.

[22] Li, Xiang, Qixu Wang, Xiao Lan, Xingshu Chen, Ning Zhang, and Dajiang Chen. "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach." IEEE Access 7 (2019): 9368-9383.

[23] Ray, ParthaPratim. "A survey of IoT cloud platforms." Future Computing and Informatics Journal 1, no. 1-2 (2016): 35-46.

[24] Ferretti, Luca, MircoMarchetti, and Michele Colajanni. "Fog-based secure communications for low-power IoT devices." ACM Transactions on Internet Technology (TOIT) 19, no. 2 (2019): 1-21.



ISSN: 2005-4262IJGDC
Copyright ⓒ2021SERSC