ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Cyber Security for the IOT Based Smart Garbage System

V. Mallikharjuna Rao [1] , Dr. M. SatyaSai Ram [2] , Dr. M N Giriprasad [3] .

Research Scholar, Dept. of Electronics and Communication Engineering, JNTU Anantapur, India[1]

Professor and Head, Dept. of Electronics and Communication Engineering, Chalapathi Institute of Engineering and Technology, Guntur, India [2]

Professor, Dept. of Electronics and Communication Engineering, JNTU Anantapur, India [3]

ABSTRACT: In IOT based smart garbage system many users are uploading and downloading sensitive data to the cloud without any security.In every case Encryption is the great method to protect the information from various assaults. Subsequently numerous people groups and associations are continually sending their touchy information advice regarding encryption to keep up the mystery. There are lotof increasingly ground-breaking encryption and decryptionsystems in the digital world which can give the security to the delicate information. In view of the encryption type the resultant figured information additionally expends high measure of memory. Every single inserted gadgets are poor memory devices subsequently it isn't great to utilize the high memory expending encryption procedures which can influence the cost advancement. It is challenge to secure the delicate information by utilizing encryption strategy which involves less measure of memory.Many authors proposed different encryption techniques listed in this article, but the scope of this research is to propose and apply the encryption and decryption techniques using matrix addition and subtraction with scalar which can protect the sensitive data from the cyberattacks and also consume less code memory.

KEYWORDS: Cloud Computing, Encryption, Decryption, Sensor Node, Security, Cloud, Matrices, Encoding, Decoding, Cyber attack

I. INTRODUCTION

In the era ofIOT based smart garbage systembased data storage system, performing computationally intensive operations on a local machine becomes challenging and inefficient. Relying on powerful distributed servers is desirable for improving efficiency. As clients, users can upload their data onto cloud servers, and let servers perform computationally expensive tasks for them. However, if the servers are untrustworthy and the data contain sensitive information, it raises security concerns. Therefore, designing algorithms to take advantage of the powerful untrusted cloud database servers while keeping them fromlearning anything about input data is of significant interest. Cryptography community has looked at this problem underthe secure multi-party computation framework, also known assecure function computation. In a secure function computationproblem, parties want to jointly compute a function withoutrevealing their respective input to other parties. The basic model of encryption and decryption has given in the **Fig.1.**

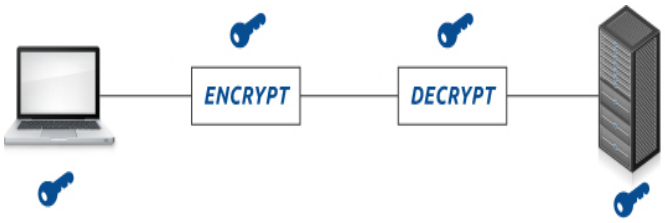

Fig.1:*Basicmodel of encryption and decryption method.*

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A class of encryption schemes called fullyhomomorphicEncryption guarantees that any unencrypted items, including the inputs, any intermediate values and the outputs will notbe leaked to unintended party. Naturally, it is often used asa solution to secure function computation problems and othertypes of security problems [1].Matrix multiplication is a fundamental building block ofmany science and engineering fields, such as machine learning,image and signal processing, wireless communication, andoptimization. In this paper, we focus on the problem of secure distributed matrix multiplication. Secure matrix multiplicationis particularly important in scenarios where one wants totrain a machine learning model distributedusing gradient descent based algorithms while keeping the training data andthe model parameters private. Secure matrix multiplication has been studied in cryptography community, and different approaches have been proposed, including a weaker version offully homomorphic encryption, namely partially homomorphicencryption [2].In contrast to the focus of cryptography community, thereare not many works on distributed matrix multiplication with information-theoretic secrecy constraints. There has been significant recent work [3] in speeding up computation and reducing communication overhead using codes when it comes to distributed matrix multiplication in information theory community. These works speed up matrix multiplication and reduce communication overhead by adding redundancy to the computation using codes. This controlled redundancy introduced by codes allows the distributed system to efficiently tolerate cloud database servers who do not respond in a timely manner and mitigate stragglers. Several other recent works that studied secure distributed computing problems those are similar to ours,which was included in [4].

With the advancement and spread of computation and communication technologies, the amount of data collected and stored by private and public sectors is constantly increasing. Storing and processing such huge amounts of information in local premises becomes very problematic, due to soaring costs of software, hardware, energy and maintenance. In this context, the need emerges to find a fast and cost-effective alternative. An attractive possibility for a data controller is to outsource storage and processing to a cloud [5]. Such outsourcing brings several benefits like elimination of infrastructure costs (no software/hardware investments needed), flexibility (storage and computing power can scale depending on business growth) and energy savings. Unfortunately, storing and processing data in the cloud has also downsides related to security and privacy. A lot of the information being collected is personally identifiable and therefore sensitive. Neither the data controller nor the subjects to whom the data refer want the cloud service provider (CSP) to read, use or sell their data. In this article we discuss several procedures to store and process sensitive data in a privacy-preserving way in untrusted clouds, where processing consists of two basic operations: scalar products and matrix products. These operations are useful in statistics and data analysis (to compute correlations between attributes, contingency tables, etc.), and also in engineering (image encryption, 3D graphics simulation, etc.); which was explained in [6] and references therein. In our solutions, the privacy- protected sensitive data stored in the clouds are not encrypted and preserve some of the utility (that is, some statistical features) of the original data. This allows making the most of the outsourced data, while ensuring that no original records can be re- created from the outsourced records. The outsourced data can be used for purposes other than computing scalar products or matrix products. This is a relevant difference with respect to related work on algebraic computation outsourcing. Specifically, the outsourced data preserve means and standard deviations of attributes for the entire data set and even in sub domains of it. In some of our protocols, we use vertical splitting, so that each cloud stores a clear text fragment on which any statistical analysis can be directly performed by the cloud. In the rest of our protocols, the cloud stores synthetic or anonym zed versions of the original data set that preserve the above mentioned statistics. The goal is that the outsourced version retains some utility for exploratory analysis by any user with direct access to the cloud-stored data (who should however be unable to reconstruct the original data). Note that there are many organizations interested in releasing privacy- protected data for secondary analysis, including but not limited to official statistics [7]. Following the architecture defined in the “CLARUS”European H2020 project [8] (within which this work has been carried out), we will assume a proxy located in a domain trusted by the data controller (e.g., a server in her company’s intranet or a plug-in in her device) that implements security and privacy-enabling features towards the cloud service providers. We will call this trusted proxy CLARUS.

As seen in **Fig. 2**, the growth of WSN(Wireless Sensor Network) is rapid and fast.The projected sales of sensors are going to increase rapidly and listed in the **Table.1**.Similarly **Fig. 3** shows the world revenue forecast andgrowth rate for healthcare, medical and biometrics markets and given in the **Table.2**.From the observation the sensor networks have a great future aheadwith tremendous growth rate.Sensor networks applications in healthcare have potentialfor large impacts [9]. These can be realized through real-time, continuous vital monitoring to give immediate alerts of changes in patient

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

status. The data can also be related to the hospital or correlate with patient records andso on. Home monitoring applications for chronic and elderly patients which can be used to collect periodic or continuous data and be uploaded to a physician and canallow long-term care and trend analysis. It can also reduce length of hospital stay. Manual tracking of patient status isdifficult. Collection of long-term cloud databases of clinical data can be used in future diagnosis.

Table.1:*wearable care unit sales list[10].*

S.No	Year	IOT devices in billion
1	2014	590
2	2015	780
3	2016	890
4	2017	1110
5	2018	1410
6	2019	1680

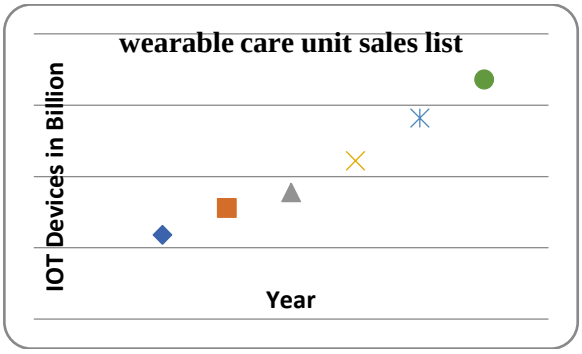

Fig. 2:*Forecasting forwearabledevice unit sales representation [10].*

Table.2:*Wearable unit sales growth and income[11].*

year	Growth %	income in million $
2002	9	12
2003	9.5	13
2004	9.8	14
2005	13	15.5
2006	15	22
2007	21	25
2008	23	27
2009	25	34
2010	33	44
2011	36	57
2012	52	99

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

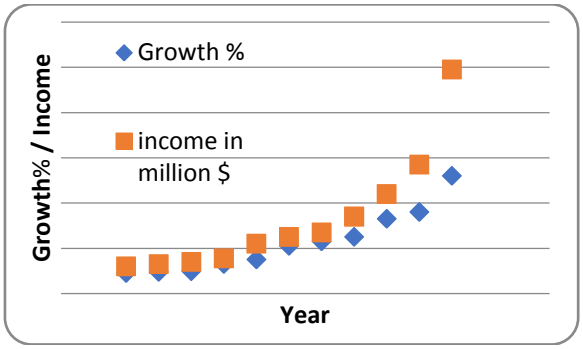

Fig. 3: *Wearable unit sales growth inpercentage and income [11].*

1.1 Types of Keys

Private Key: Private Key cryptography contains the same key for sender and the receiver. The sender sends the key along with the data for receiver to decrypt the data using the same key.

Public Key: Public key cryptography will be used for private and public keys. Public key will be sent to all authorized users which can be enabled for all and one private key which can be known by only receiver. Public key is used for encryption and private key for decryption.

II. RELATED WORK

Ning et al. presented the first CP-ABE construction supporting treebased structure in generic group model [12]. Hur et al. proposed an access control scheme based on CP-ABE in data outsourcing systems such as cloud computing [13]. Wan et al. proposed a fine-grained access control scheme in cloud storage services [14]. However, these schemes only focus on data sharing and cannot support write operation on the stored data. Li et al. proposed a novel patient-centric framework and a suite of mechanism for data access control to personal information records (PHR) stored in semi trusted servers [15]. This scheme encrypted data with access policy based on CP-ABE or with a set of attributes based on key-policy ABE (KP-ABE). Although this scheme supports the write operation, the cloud cannot verify the write permission of user after receiving the re-encrypted modified data. Dong et al. proposed a secure and efficient data collaboration scheme called SECO using multi-level hierarchical identity-based encryption (HIBE), in which users in the same domain can cooperate to complete work [16]. In this scheme, a user encrypts data with multiple recipients' public key, and only these intended recipients can decrypt and modify the data. After performing write operation, the user sends re-encrypted data and ID-based signature (IBS) to cloud. However, the cloud is able to know the identity of user, and it cannot verify whether the user really has the write permission unless it maintains a list of user-permissions values of each data, which will also introduce extra storage cost.

Attribute-Based Encryption (ABE).ABE allows the data owner to share data with others in a more flexible way. At a high level, each potential data recipient is associated with an attribute set Sand given the associated private key generated by a third party. The data provider can encrypt data with a set of function. Anyone with an attribute set can successfully decrypt the cipher text if and only if the set fulfills the function[17]. Later on several variants and improvements have been proposed[18], including cipher text-policy ABE (CP-ABE, where cipher texts are associated with access policies and keys are associated with sets of attributes) and key-policy ABE (where keys are associated with access policies and cipher texts are associated with sets of attributes). Variants of ABE are proposed later, such as [19]for decentralizing the trusted private key generator; [20]for outsourcing computation, [21]for efficient revocation, ABE for circuits [22], online/offline ABE [23], leakage-resilient ABE[24], dual predicates and policies [25]and multi-authority ABE with large universe [26].ABE has been found useful in situations with the requirement of fine-grained control on sensitive data such as PHR. An attribute-based infrastructure for PHR systems was proposed in[27], where each patient'sinformation records are encrypted using a variant of CP-ABE that allows direct revocation. To achieve a flexible control on the encrypted data, a variant of ABE that allows delegation of access rights is proposed in[28]. Unfortunately, none of these proposals allows the doctor to share patient's medical record with other specialists while preserving the patient's privacy.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Proxy Re-Encryption was introduced in [29][30] for the health care cloud system , allows a semi-trusted proxy with a re-encryption key to convert cipher texts computed under Alice's public key into those can be decrypted using Bob's private key [31]. The desirable feature is that the conversion is performed by the proxy without knowing the corresponding plaintexts.

Attribute-based Proxy Re-Encryption (ABPRE).Integrating ABE and PRE is a promising solution for more flexible data sharing. The first cipher text-policy ABPRE scheme was proposed by Wang et al.[32], in which a proxy is allowed to transform a cipher text under a specialized access policy into the one under another access policy (i.e. attribute-based re-encryption). Mizuno and Doi[33]proposed a hybrid PRE scheme (in general) where cipher texts generated in the context of ABE can be converted to the ones which can be decrypted in the IBE setting. Other works on attribute-based proxy re-encryption include [34]. But all aforementioned schemes support access policy with AND gates only. The first construction of a CCA secure CP-ABPRE supporting any monotonic access policy was given in[35]. However, it only supports one single private key generator (PKG) [36] and is not suitable for a large-scale PHR system which needs multiple authorities with different duties (as required in our system).One of the main security issues that arise is that whether the server can be fully trusted by the outsourcer to perform the protocols correctly. In order to solve the above trust problem between the server and the client. In the following, a large amount of research works focused on the subject of verifiable computation [37] inthe past decades. Baharonal. [38] Utilized the fully homomorphic encryption technique to design a verifiable computation scheme for any function. Despite the scheme can provide theoretical privacy guarantees, FHE itself is a computationally intensive operation and large-scale computation needs more expensive encryption overhead. To solve the above heavy verification overhead problem, many researchers has devoted substantial attention to design schemes for efficiently verify the computation results returned by the server. Shen et al. [39] designed an efficient public auditing protocol with global and sampling block less verification, where data dynamics are dramatically more efficiently than that of the previous works. Benabbas et al. [40] firstly proposed a practical verifiable computation scheme for high degree polynomial function. Generally speaking, some solutions keep his own verification secret key, and only the client who submits the input can verify the correctness of the computation result. How- ever, for other proposals [41] , it not only support the public verification which empowers the third party to verify the correctness of the computation result but also support the public delegation which empowers the third party to submit queries to the server and evaluate the outsourced function.

2. Necessity

In case of IOT based smart garbage system,Encryption is necessary thing in the cyber world which keeps our data confidentially. There may be many more hackers to hack our data by retrieving from the cloud or to collect the data by joining between the communication to spoil the organization reputation or which spoils the organization financial strategies. So it is always better to provide the security for that sensitive data to protect from the network security attacks.As per Revision Legal report the confidential affected data of the peoples has given in**Table.3**[42]**,**and the Pie graph analysisis shown in**Fig.4**.

Table.3:*CustomersHacking Information [42].*

Year	Type of information	Info in millions
Jan:2018	Patient information	2.9
Apr:2018	A ride-sharing app	14
June:2018	Customer Email database	92
July:2018	Bithumb Cryptocurrency	31.5

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

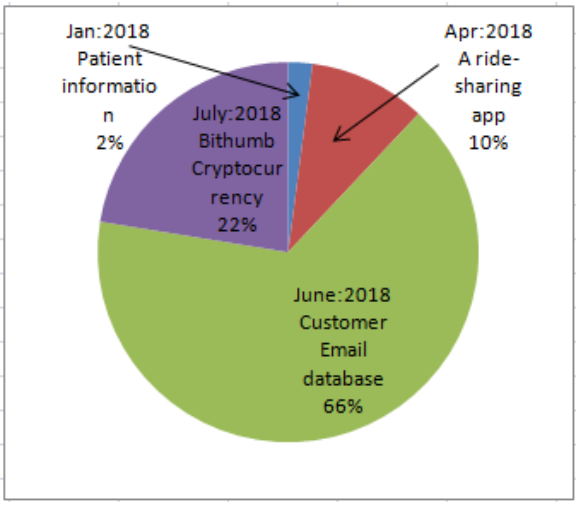

Fig. 4: *Customers hacking information in 2018 [42].*

3. System design Considerations:

The proposed algorithm was applied by considering different parameters which were explained below, though there were much more strong algorithms available in the research world which requires much more memory.

Cost consideration: All cloud communicating devices are wearabledevices,it means they are portable devices hence it is mandatory to select microcontroller for the development. When the microcontroller is entered in the picture, it support less amount of memory .Whenever a developer want to apply stronger encryption algorithms they requires large amount of memory but microcontroller is restricted with less amount of on chip memory ,if anyone want to connect external memory rapidly the cost of the device also increases.

Power source Backup: When theencrypteddata occupies high amount of memorythe encoding and decoding execution time also increases which makes the high power consumption by the microcontroller. But it is necessary to improve the Power source Backup time for the wearable devices which makes the uninterrupted communication between device and cloud.

Latency: When the encryption size increases automatically the device doesn't provideits maximum execution services to the communication devices and sensors, so the device doesn't fed the maximum data to the cloud.

By considering above factors the matrix Addition and subtraction with scalarmethod was proposed which minimize the above explained problems.

III. PROPOSED WORK

Fig.5: Shows the proposed model for the IOT based smart garbage system where the data was uploading to the cloud with the security, in between communication if any cyber attacking is happened it is not possible to get the actual data due to encryption. The basic components which are involved in this project has explained below.

I. **Sensors:** Here the functionality of Sensors is to sense the level of garbage in the bins, once they detect the garbage level, the information can be sent to the CPU.

II. **Display Module:** Here the functionality of the display module is to display the level of garbage in the bins and the connectivity status of the WIFI module.

III. **WIFI:** The functionality of the WIFI module is to send the garbage level to the cloud, which makes easy for monitoring.

It is good to provide the accessibility of information to any person or doctor through the cloud, which can provide the transparent treatment for the patient, at the time it is also necessary to maintain the data security while the data communication is going between the server and the node. Nowa days there should be many more sophisticated hacking

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

techniques to hack such type of sensitive data. Hence it is necessary to protect such type of sensitive data from the hacking. Here the research is proposing one of the lightweight encryption and decryption method for the data which is done by the "Matrix Addition and subtraction with scalar".

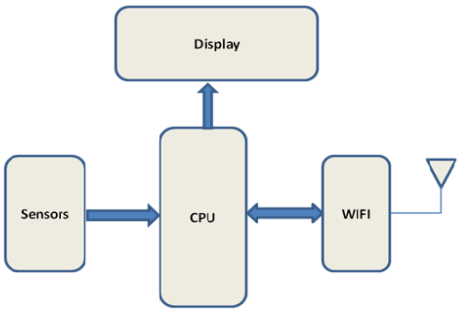

Fig.5 Block diagram of proposed model.

3.1 Methodology& Results

It is always good to send the data from one node to another node with confidentially due to cyber attacks. There are many ways to achieve thisconfidentiality; cryptography provides different techniques to protect the plain text. There are two types of keys are there to protect the data (1) symmetric key and (2) Asymmetric key. In case of symmetric key the plane text is encoded and decoded by the same type of key, whereas asymmetric key the plain text can be decoded and encoded by the different types of keys. In our researchwork we used Scalar symmetric key.

Encoding:

The proposed work completely designed based on the matrix Addition and subtraction. For this purpose let us take *m*x*n* C_{matrix} which contains "*m*" rows and "*n*" columns, here "z" is called scalar encryption element, and C_{matrix} contains elements which are related to data called plain text. Before sending any data to the cloud from the informationunit first it should be necessary to encrypt the C_{matrix} matrix with the help of Scalar encryption element which is "z",Using matrix Addition technique, which are given in the equations (3, 4).The resultant encryption data which was represented by the E_{matrix} with size*m*x*n* given in theequation (2).Here the equation (5) represents the resultant encrypted data element which is prepared for sending to the cloud.

Let us say,

$$C_{matrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad \ldots\ldots (1).$$

$$E_{matrix} = \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ e_{m1} & e_{m2} & \cdots & e_{mn} \end{pmatrix} \quad \ldots\ldots (2).$$

$$E_{matrix} = Z + C_{matrix} \quad \ldots\ldots (3).$$

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

i.e. $E_{matrix} = Z + \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$

$$E_{matrix} = \begin{pmatrix} Z+a_{11} & Z+a_{12} & \cdots & Z+a_{1n} \\ Z+a_{21} & Z+a_{22} & \cdots & Z+a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ Z+a_{m1} & Z+a_{m2} & \cdots & Z+a_{mn} \end{pmatrix} \quad \ldots\ldots\ldots (4).$$

$$e_{11} = Z + a_{11}, e_{12} = Z + a_{12} \ldots\ldots\ldots e_{mn} = Z + a_{mn} \quad \ldots (5).$$

Decoding:

Once the data was reached to the cloud it is necessary to decode the data which was in the encrypted form, for this purpose it is necessary to subtract the resultant encrypted matrix with the scalar element to get the original data. Here the Scalar element (Z) which is used for the encoding is also used as decodekey,

Letus say the resultant decoded matrix is D_{matrix} and resultant matrix is R_{matrix},

$$R_{matrix} = E_{matrix} - Z \quad \ldots. (6).$$

$$\begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix} = \begin{pmatrix} Z+a_{11} & Z+a_{12} & \cdots & Z+a_{1n} \\ Z+a_{21} & Z+a_{22} & \cdots & Z+a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ Z+a_{m1} & Z+a_{m2} & \cdots & Z+a_{mn} \end{pmatrix} - Z$$

Where $r_{11} = a_{11}$, $r_{12} = a_{12} \ldots\ldots\ldots r_{mn} = a_{mn}$ are the decoded data elements.

The above algorithm was implemented on the ARM cortex family and tested with the logic analyzer, which is useful to analyze the execution time of the code. When the plain text size increase automatically the encryption time also increases, which was depicted in the **fig.6,** so the execution time increases when the size of plain text increases

Let us say,

Plain text size is T_{size}.

And Execution time is E_{time}.

$E_{time} \propto T_{size}$ ……. (7).

Fig.6*Encrypted bytes Versus Execution time.*

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Table.4:*Encrypted bytes Versus Execution time.*

data in bytes	1	2	3	4
Execution Time in mSec	0.0009	0.012	0.015	0.018

From the above equation it is very clear that it is necessary to select the high speed processor or microcontroller to get the minimum latency, depending upon the application.

IV. CONCLUSION

TheScalar addition and subtraction technique for the Matrix has been applied for the IOT based smart garbage system, the data was encrypted and decrypted successfully, and the proposed algorithm was tested by the ARM-CORTEX family, which requires less amount of power with high speed. The verified results also emphasizes that the encrypted data requires less amount of memory with high speed. From the results it should be concluded that the algorithm execute with less latency comparing with other algorithms. Finally it should conclude that the Scalar addition and subtraction technique method is better encryption and decryption method for the wearable devices where the cost optimization is considerable. Even though there strong encryption and decryption methods are available in the cyber world which requires more memory and so expensive.

REFERENCES

[1] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018 May 1;82:395-411.
[2] D. H. Duong, P. K. Mishra, and M. Yasuda, "Efficient secure matrix multiplication over LWE-based homomorphic encryption," Tatra Mountains Mathematical Publications, vol. 67, no. 1, pp. 69–83, 2016.
[3] Q. Yu, M. Maddah-Ali, and A. S. Avestimehr, "Polynomial codes: an optimal design for high-dimensional coded matrix multiplication," in Advances in Neural Information Processing Systems 30 (NIPS), 2017, pp. 4403–4413.
[4] R. Bitar, P. Parag, and S. E. Rouayheb, "Minimizing latency for secure distributed computing," in 2017 IEEE International Symposium on Information Theory (ISIT), Jun. 2017, pp. 2900–2904.
[5] Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal. 2018 Jun 15.
[6] X. Lei , X. Liao , T. Huang , F. Heriniaina , Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud, Inf. Sci. 280 (2014) 205–217 .
[7] A. Hundepool , J. Domingo-Ferrer , L. Franconi , S. Giessing , E. Nordholt , K.Spicer , P.deWolf ,StatisticalDisclosureControl,JohnWiley&Sons,2012 .
[8] CLARUS - a framework for user centred privacy and security in the cloud, h2020 project (2015–2017). http://www.clarussecure.eu .
[9] Mahmud R, Koch FL, Buyya R. Cloud-fog interoperability in IoT-enabled healthcare solutions. InProceedings of the 19th International Conference on Distributed Computing and Networking 2018 Jan 4 (p. 32). ACM.
[10]https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#296836011480
[11] Lee YS, Alasaarela E, Lee H. Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. InThe International Conference on Information Networking 2014 (ICOIN2014) 2014 Feb 10 (pp. 453-457). IEEE.
[12] Ning J, Cao Z, Dong X, Wei L. White-box traceable CP-ABE for cloud storage service: how to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing. 2018 Sep 1;15(5):883-97.
[13] J. Hur, D.K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Trans. Parallel Distrib. Syst. 22 (7) (2011) 1214–1221.
[14] Z. Wan, J. Liu, R.H. Deng, HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 743–754.
[15] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Trans. Parallel Distrib. Syst. 24 (1) (2013) 131–143.
[16] X. Dong, J. Yu, Y. Zhu, Y. Chen, Y. Luo, M. Li, SECO: secure and scalable data collaboration services in cloud computing, Compute. Secure. 50 (2015) 91–105.
[17] Koppula V, Waters B. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. IACR Cryptology e-Print Archive, 2018: 847; 2018.
[18] B. Waters, Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, in: Public Key Cryptography, in: LNCS, vol.6571, Springer, 2011, pp.53–70.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 8, Special Issue 1, March 2019*

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

[19] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs, J.A. Manjón, Contributory broadcast encryption with efficient encryption and short ciphertexts, IEEE Trans. Comput. 65(2) (2016) 466–479.
[20] J. Lai, R.H. Deng, C. Guan, J. Weng, Attribute-based encryption with verifiable outsourced decryption, IEEE Trans. Inf. Forensics Secur. 8(8) (2013) 1343–1354.
[21] J. Hur, D.K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Trans. Parallel Distrib. Syst. 22(7) (2011) 1214–1221.
[22] S. Garg, C. Gentry, S. Halevi, A. Sahai, B. Waters, Attribute-based encryption for circuits from multilinear maps, in: CRYPTO 2013, in: LNCS, vol.8043, Springer, 2013, pp.479–499.
[23] S. Hohenberger, B. Waters, Online/offline attribute-based encryption, in: Public-Key Cryptography, in: LNCS, vol.8383, Springer, 2014, pp.293–310.
[24] Z. Yu, M.H. Au, Q. Xu, R. Yang, J. Han, Leakage-resilient functional encryption via pair encodings, in: J.K. Liu, R. Steinfeld (Eds.), Information Security and Privacy – 21st Australasian Conference, Proceedings, Part i, ACISP 2016, Melbourne, VIC, Australia, July 4–6, 2016, in: Lecture Notes in Computer Science, vol.9722, Springer, July 2016, pp.443–460.
[25] N. Attrapadung, S. Yamada, Duality in ABE: converting attribute based encryption for dual predicate and dual policy via computational encodings, in: CT-RSA 2015, in: LNCS, vol.9048, Springer, 2015, pp.87–105.
[26] Y. Rouselakis, B. Waters, Efficient statically-secure large-universe multi-authority attribute-based encryption, in: FC 2015, Springer, Berlin, 2015, pp.315–332.
[27] Liu JK, Yuen TH, Zhang P, Liang K. Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list. InInternational Conference on Applied Cryptography and Network Security 2018 Jul 2 (pp. 516-534). Springer, Cham.
[28] F. Xhafa, J. Wang, X. Chen, J.K. Liu, J. Li, P. Krause, An efficient PHR service system supporting fuzzy keyword search and fine-grained access control, Soft Comput. 18(9) (2014) 1795–1802.
[29] Vijayakumar V, Priyan MK, Ushadevi G, Varatharajan R, Manogaran G, Tarare PV. E-health cloud security using timing enabled proxy re-encryption. Mobile Networks and Applications. 2018:1-2.
[30] Yu Z, Au MH, Yang R, Lai J, Xu Q. Achieving Flexibility for ABE with Outsourcing via Proxy Re-Encryption. InProceedings of the 2018 on Asia Conference on Computer and Communications Security 2018 May 29 (pp. 659-672). ACM.
[31] H. Deng, Q. Wu, B. Qin, W. Susilo, J.K. Liu, W. Shi, Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data, in: ASIACCS, ACM, 2015, pp.393–404.
[32] Wang L, Zhang Z, Dong M, Wang L, Cao Z, Yang Y. Securing Named Data Networking: Attribute-Based Encryption and Beyond. IEEE Communications Magazine. 2018 Nov;56(11):76-81.
[33] H. Deng, Q. Wu, B. Qin, W. Susilo, J.K. Liu, W. Shi, Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data, in: F. Bao, S. Miller, J. Zhou, G. Ahn (Eds.), Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS'15, Singapore, April 14–17, 2015, ACM, 2015, pp.393–404.
[34] Liu JK, Yuen TH, Zhang P, Liang K. Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list. InInternational Conference on Applied Cryptography and Network Security 2018 Jul 2 (pp. 516-534). Springer, Cham.
[35] K. Liang, L. Fang, D.S. Wong, W. Susilo, A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security, Cryptology e-Print archive, report 2013/236, 2013.
[36] Fujioka A, Yoneyama K. Single Private-Key Generator Security Implies Multiple Private-Key Generators Security. InInternational Conference on Provable Security 2018 Oct 25 (pp. 56-74). Springer, Cham.
[37] X. Chen , J. Li , J. Weng , J. Ma , W. Lou , Verifiable computation over large database with incremental updates, IEEE Trans. Compute. 65 (10) (2016) 3184–3195 .
[38] Baharon MR, Shi Q, Abdollah MF, Yassin SW, Idris A. An Improved Fully Homomorphic Encryption Scheme for Cloud Comput.
[39] J. Shen , J. Shen , X. Chen , X. Huang , W. Susilo , An efficient public auditing protocol with novel dynamic structure for cloud data, IEEE Trans. Inf. Forensics Secur. 12 (10) (2017) 2402–2415 .
[40] S. Benabbas , R. Gennaro , Y. Vahlis , Verifiable delegation of computation over large datasets, in: Proceedings of Advances in Cryptology-CRYPTO 2011, 2011, pp. 111–131 .
[41] B. Parno , J. Howell , C. Gentry , M. Raykova , Pinocchio: Nearly practical verifiable computation, in: Proceedings of 2013 IEEE Symposium on Security and Privacy, 2013, pp. 238–252 .
[42]https://revisionlegal.com/data-breach/2018-statistics/