# End-To-End Secure Communication using Encryption and Fingerprint Recognition

Salman Mousa
Arab East Colleges
Riyadh, Saudi Arabia

M.A. El-dosuky
Faculty of Computer and Info, Mansoura University, Egypt,
Arab East Colleges, Riyadh, Saudi Arabia

## ABSTRACT
The paper in hand proposes a mobile application for encrypted data communication, due to the increased cases of data leakage. The relation between private and public keys is the basis of public key cryptography. In this way of cryptography, every public key is linked to a private key. Both keys are used in encrypting and decrypting any message sent via the Internet. Many novel approaches provide better data protection. Cryptography service providers are providing on - demand cryptography services. Novel approaches such as homomorphic-encryption help in protecting data. Those approaches are useful compared to other approaches because the former approaches are less expensive. The proposed mobile application is implemented in Flutter. The implemented fingerprint method that has been used in the application is Ateb-Gabor.

## General Terms
Encryption, Cryptography

## Keywords
Encryption, Fingerprint Recognition, End-To-End security

## 1. INTRODUCTION
Data encryption is an operation where plain data is pipelined and transformed into cipher data as shown in Fig. 1. Usually, data is maintained remotely. Users gain benefits from service providers through the Internet. Benefits such as online document storage enabling documents to be accessed anywhere anytime.

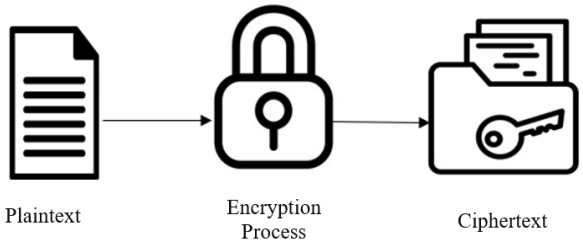


**Fig.1: Methodology of Encryption**

Service providers enable the transfer of online data to the users in a convenient and flexible way, employing encryption subsystems [1]. However, the cost may be excessive in certain cases. Based on a survey, almost 80 percent of organizations that have considerable data loss experience bankruptcy in 2 years of the data loss. The focus in this field is given to data encryption because the data is stored is a secure way in a private or public encrypted data[2].

Many companies are not able to bear the price of a framework that operates under the control of experts. In contemporary days, encoded data is popular because of many factors[3].

Based on certain genre of management, encoded data is transferred to companies via the internet. Storage space is dedicated based on the size of actual data. Encoded data is viewed from diverse viewpoints[4]. Information regarding neighborhood, for instance, is transferred to the encoded data. Encoded data is stored for managerial or any other purpose[5].

Encoded data is used to store sensitive information. Users are directed to the provider of encoded data[6]. Multimedia, such as text, video, and audio undergo streaming while not disturbing the performance of the application which interacts in HTTP protocol. Documents are downloadable from the application with no special requirements[7].

Most of activities regarding encoding and managing documents use REST[8]. Data objects can easily undergo CRUD operations, namely create, read, update and delete[9].

The rest of the paper is as follows. Section 2 is for previous work. Section 3 is for proposed application. Section 4 is for implementation. Section 5 for results. Conclusion and future work are in Section 6.

## 2. PREVIOUS WORK
Encrypting data convert it to a form that the receiver can not understand. Decryption is the reverse process that turns the encrypted data into understandable format.

A recent research study concentrated on using encryption of images[10]. Novel encoding approaches are required for sensitive data such as finance and the like. Multimedia cryptography is crucial in supporting certain web applications[10].

Another recent research study scrutinized Field Development Clusters using Advanced Encryption Standard [11]. Another recent study scrutinized the cryptography performance [12]. This achieved better safety and efficiency[13].

Data encryption structure ensured usability and security[14]. A novel cryptography approach prevented disturbance in communication channel security, assuming that hackers shall find it not easy to guess cryptography secrets [15].

Regarding the security of Internet of Things (IoT), a research paper proposed cryptographic solution[16]. Quantum leaps are witnessed in end-to-end cryptography especially in IoT fields such as remote sensing[16].

In ref. [15], merits of cryptography approaches are scrutinized. Data transferred via the network lose trust over time. Cryptography may be done at-rest or on-the-fly. Cryptography protects data from modification and from being stolen[12].

Despite that a professional technician is able to alter encoded data, data consumers may lose trust in the data. Ref. [17]

argues that cryptography can protect sensitive data. Technology inventions are productive to apply encryption in protecting organizations and users.

Most companies possess strong standards for authorization. This enables the users who own the data to protect their sensitive data.

The major advantage of cryptography is its ability to be employed on devices such as iPhone and Android, either paid or for free[15]. Despite this advantage, cryptography may have some pitfalls[12]. Encoding all files make them secure, but may hinder employees from performing their work to add, move, change and offer data.

The need for specialized cryptography framework increases theoretically speaking[17]. Encoding data is a big issue that faces Information Technology master[14]. Using too much keys to encode the data makes it difficult for Information Technology master to handle those keys. In certain cases, encoding data may become expensive, due to the increase in updating the underlaying data encryption structures.

The merit of decoding is discussed in [11]. It assures adequacy of security of transmitted data. It makes easy for organizations to manage the data effortlessly. It also makes it easy for security technicians to protect data. Difficulties of decryption are scrutinized[16].

## 3. PROPOSED APPLICATION

Most previous work seek to construct a channel for data transfer using an application with powerful encryption and decryption.

Secure communication channel is going to be built to allow users to share data while avoiding cyber attacks such as brute-force and un-authorized access.

The proposed mobile application is programmed in Dart language utilizing the Flutter kit. The used IDE is Microsoft Visual Studio Code to build the user interface and AES approach.

As depicted in fig. 2, AES works by combining the plaintext with the secret key, it can accept keys up to 256 bits, which allow the user to choose a wide variety. Next, it generates the ciphertext; at this stage, the end user can decrypt the cipher easily through the application.

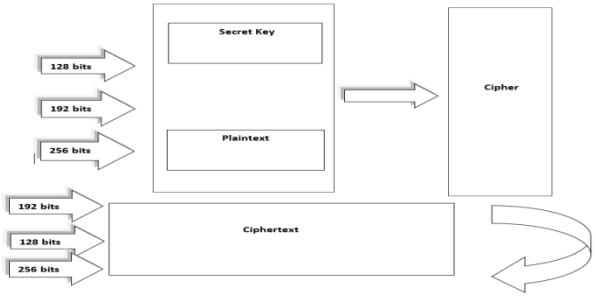


**Fig. 2: AES**

The application will have a security control, such as finger print ID or password to complete the login process by the authorized users. Password or fingerprint is mandatory to identify the identity of the sender who select the document to encrypt in AES. Then the encoded document is received by the recipient via the insecure communication channel using the same application to decode the received document.

As depicted in fig. 3, only authorized persons have the right to access the application by using password or fingerprint.

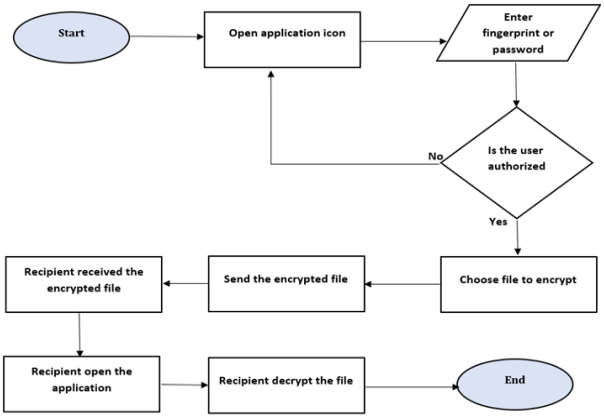


**Fig. 3: Application Flowchart**

Ateb-Gabor approach is implemented in the application. Basically, Gabor performs analysis of the fingerprint in contactless way to produce local and global attributes[18].

**Fig. 4: Before & After Applying Gabor**

Gabor filter is implemented in 5 phases, namely the normalization of the image, image computing, frequencies calculation, binarization of the images, and Gabor design.

Fig. 4 depicts the effect of applying the Ateb-Gabor filter. The normalization of images is the first step. The second step is calculating the O matrix. Then frequencies calculation is performed. After that the B image is calculated. Finally, Gabor function is determined as shown in Eq. 1.

$$\exp\left(-\frac{x'^2+\psi y'^2}{2\sigma^2}\right) ca\left(2pi\frac{x'}{\lambda}+\zeta\right) \quad Eq1$$

$$x' = x\cos(\theta)+y\sin(\theta) \quad Eq2$$

$$y' = -x\sin(\theta)+y\cos(\theta) \quad Eq3$$

Nomenclature is:

$x'$ & $y'$: Gabor rotate mean-square-deviation

$\theta$: orientation of the bandwidth

$\zeta$: lagging regarding the shift of the phase,

$\lambda$: wavelength,

$\psi$: ratio of compression

Fig. 5 shows how the channel of Gabor is stable and is capable of eliminating noise thus enhancing the image.

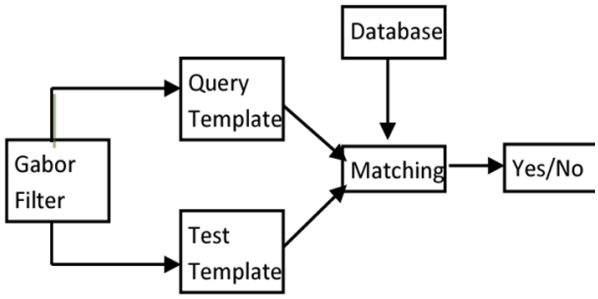


**Fig. 5: Gabor-in-Action**

Fig. 6 shows the fingerprint subsystem. First, the latent fingerprint is pipelined to Gabor filter. Then features are extracted. Classification is performed and matching is done using neural network. Finally, the result is displayed.

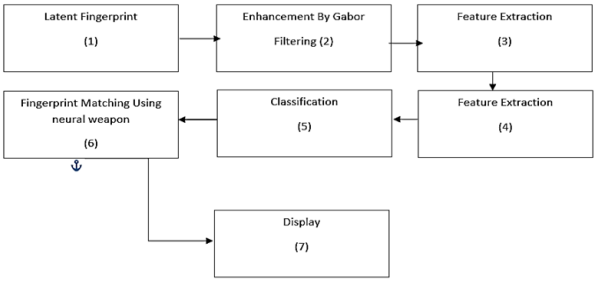


**Fig. 6: Fingerprint Subsystem**

## 4. IMPLEMENTATION

Implementation is done in Dart programming language which transforms into Java to compile for Android platform. The application is decomposed into 4 files. Initially the Main.dart file is where to find main function. The Home Page is listed in Fig. 7.

```
Run | Debug | Profile
void main() => runApp(MyApp());

class MyApp extends StatelessWidget {
  @override
  Widget build(BuildContext context) {
    return MaterialApp(
      debugShowCheckedModeBanner: false,
      title: 'Flutter Demo',
      theme: ThemeData(
        primarySwatch: Colors.blue,
      ), // ThemeData
      home: MyHomePage(),
    ); // MaterialApp
  }
}
```

**Fig. 7: Home Page**

Encryption.dart contains all the required work regarding the encryption of data. Database.dart contains DatabaseHelper class.Libraries are running in pubspec.yaml file.

## 5. RESULTS

The user determines the document then it will be encrypted using AES . the encoded document is stored internally. The user is informed that the encryption process succeeded. To decrypt the encoded document the user selects it first from storage, as shown in Fig. 8


**Fig. 8: Graphical User Interface in Arabic**

Table 1 shows the time interval of encoding and decoding of different document types.

**Table1 Time Interval of Encoding & Decoding**

| Doc. Type | Doc. Size | Encoding | Decoding |
|---|---|---|---|
| docx | 124 – 300 (KB) | 09.11 – 35.12 | 06.33 – 35.12 |
| PDF | 130 – 389 (KB) | 12.01 – 44.14 | 13.33 – 45.19 |
| Audio | 5.95 – 7.10 (MB) | 02.13 – 09.02 | 03.13 – 12.03 |

## 6. CONCLUSIONS & FUTURE WORK

The paper in hand focusses on improving encoding of data transmitted among data consumers. The more the consumers rely on e-commerce and other electronic services, the more the need of cryptography standards.

The paper in hand proposes a mobile application for encrypted data communication, due to the increased cases of data leakage. The proposed mobile application is implemented in Flutter. The implemented fingerprint method that has been used in the application is Ateb-Gabor.

Possible future improvements include the ability to operate on several documents at the same time. Another possible enhancement is to consider face recognition which is expected to achieve user satisfaction and confidentiality.

## 7. REFERENCES

[1] Schillinger F, Schindelhauer C. "End-to-end encryption schemes for online social networks." In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer; 2019. p. 133–46.

[2] Yan F, Xu M, Qiao T, Wu T, Yang X, Zheng N, et al. "Identifying WeChat red packets and fund transfers via analyzing encrypted network traffic." In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE; 2018. p. 1426–32.

[3] Rezaei S, Liu X. "Deep learning for encrypted traffic classification: An overview." IEEE communications magazine. 2019;57(5):76–81.

[4] Patel V. "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus." Health informatics journal. 2019;25(4):1398–411.

[5] Montella R, Ruggieri M, Kosta S. "A fast, secure, reliable, and resilient data transfer framework for pervasive IoT applications." In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE; 2018. p. 710–5.

[6] Lotfollahi M, Siavoshani MJ, Zade RSH, Siberian M. Deep packet: "A novel approach for encrypted traffic classification using deep learning." Soft Computing. 2020;24(3):1999–2012.

[7] Grolman E, Finkelshtein A, Puzis R, Shabtai A, Celniker G, Katzir Z, et al. "Transfer learning for user action identification in mobile apps via encrypted traffic analysis." IEEE Intelligent Systems. 2018;33(2):40–53.

[8] Cho C, Döttling N, Garg S, Gupta D, Miao P, Polychroniadou A. "Laconic oblivious transfer and its applications." In: Annual International Cryptology Conference. Springer; 2017. p. 33–65.

[9] Aceto G, Ciuonzo D, Montieri A, Pescapé A. DISTILLER: "Encrypted traffic classification via multimodal multitask deep learning." Journal of Network and Computer Applications. 2021;183:102985.

[10] Wang C, Wang A, Xu J, Wang Q, Zhou F. "Outsourced privacy-preserving decision tree classification service over encrypted data." Journal of Information Security and Applications. 2020 Aug 1; 53:102517.

[11] Ullah A, Said G, Sher M, Ning H. "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN." Peer-to-Peer Networking and Applications. 2020 Jan;13(1):163-74.

[12] Riazi MS, Laine K, Pelton B, Dai W. Heax: "An architecture for computing on encrypted data." InProceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems 2020 Mar 9 (pp. 1295-1309).

[13] Feng J, Yang LT, Zhu Q, Choo KK. "Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment." IEEE Transactions on Dependable and Secure Computing. 2018 Nov 15;17(4):857-68.

[14] Malche T, Maheshwary P, Kumar R. "Environmental monitoring system for smart city based on secure Internet of Things (IoT) architecture." Wireless Personal Communications. 2019 Aug;107(4):2143-72.

[15] Modak A, Chaudhary SD, Paygude PS, Ldate SR. "Techniques to secure data on cloud: Docker swarm or kubernetes?." In2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT) 2018 Apr 20 (pp. 7-12). IEEE.

[16] Mollah MB, Azad MA, Vasilakos A. "Secure data sharing and searching at the edge of cloud-assisted internet of things." IEEE Cloud Computing. 2017 Mar 15;4(1):34-42.

[17] Chen H, Gilad-Bachrach R, Han K, Huang Z, Jalali A, Laine K, Lauter K. "Logistic regression over encrypted data from fully homomorphic encryption." BMC medical genomics. 2018 Oct;11(4):3-12.

[18] Nazarkevych M, Klyujnyk I, Maslanych I, Havrysh B, Nazarkevych H. "Image filtration using the Ateb-Gabor filter in biometric security systems." In2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH) 2018 Apr 18 (pp.276-279). IEEE.