iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1397

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

An Efficient Encryption Scheme for Small Arbitrary Length Domains

Dr.Vidhya[1],
[1]*Associate Professor, Department of Information Technology, KG College of Arts and Science, Coimbatore, Tamilnadu, India*

Abstract: ***Encryption in an important evolving technology, used to protect private data in computers, over private and public network. Encryption is the method of transforming information in order to secure it from intruders. Encrypting entire database can be inefficient because it is challenging to selectively access a part of the encrypted data in an encrypted file. It would be desirable to apply cryptographic techniques specifically on the selected fields in the database. Conventional encryption scheme changes the database structure and applications related to the database. It requires re-engineering of databases and applications in order to store the modified data size and formats.***

In order to overcome the drawbacks of the conventional database encryption schemes, a new secure and efficient Format preserving encryption scheme is proposed. In format preserving encryption the data type, length and format of the plaintext is conserved during the encryption process. The structure of the database, applications and the existing queries never modify by the encrypted data.

Index Terms: Deterministic Encryption, Format preserving encryption,

I. INTRODUCTION

Encryption at rest should be compulsory for any media that can possibly leave the physical limits of the infrastructure. Cryptography can be implemented on the physical storage the databases are stored. Data encryption keys should be updated frequently. Data in transit is data being accessed over the network, and therefore could be disturbed by someone else on the network or with access to the physical media the network uses. Encryption can take place in three different levels such as physical storage, database, and application. The lowest level of encryption is encryption of physical storage. It encrypts disk and tape storage that is data stored gets encrypted while anything retrieved from storage gets decrypted. The stored data is protected from unauthorized access. Encrypt the entire database, so that any data in the database are encrypted and any data fetch from the database are decrypted. When encrypting sensitive data within database tables one should consider the difference between encrypting at the column level versus encrypting an entire database file. File encryption schemes apply to entire files and provide access control and auditing capabilities on the entire file only. Column-level encryption solutions provide much more granularity and enable access control, auditing, and security policies for particular columns within a database. It is more flexible in selecting a particular field to encrypt. Applications can be written to control when, where, by whom, and how data is viewed[1]. Different columns (and even different rows) can be encrypted with different keys. The top level of the data encryption is the application level. At this level, individual applications protect data that they use. The data used by the application is get encrypted and after the completion of application it is decrypted.

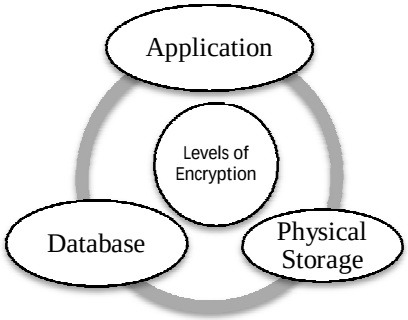


Figure 1: Levels of Encryption

Column-level encryption is preferable and best one, but there are some drawbacks in the column level encryption. In Most of the block cipher, N-bit block is mapped into another N-bit block. For a few AES modes, the other modes require padding to make the

size of the input block at least 128 bit as the base rate. The primitive DES also has a minimum value of 64 bit. The cipher text is in the form of hexadecimal digits or Base64 value. The encrypted column size is expanded and data type is also changed. An existing database structure does not support the encrypted column. After completing all the encryptions, the database structure will change to store the encrypted value. The related queries that handle the credit card number will also differ. Cryptographic operations require a huge amount of arithmetic calculations. The encrypted data decreases the system performance enormously. To avoid such drawbacks, this work introduces format preserving encryption to calculate cipher text similar to plaintext in length and format[2].

II. FORMAT PRESERVING ENCRYPTION

Format Preserving Encryption means the format of the cipher text is the same as the format of the plaintext. It is mainly used for finite domains such as Credit Card Number, Social Security Number, IP address etc. When the FPE encrypts the N digits plaintext, the output is also N digits cipher text.

Credit Card
1234 5678 8765 4321

Tax-Id
123-45-6789

FPE	6745 2390 8765 1290	673-50-2691
AES	C889F1C15035F8A1 37DF6DF94E096009	E40D86C04D723AFF EDEBE51A722D0162

Figure 2 : Format preserving Encryption

Most of the encrypted columns are used as an index of the table to speed up the searching operation. FPE does not change the index. Referential integrity of the database is also retained. Use of FPE enables improving database security in a transparent manner to many applications[3].

III. FORMAT PRESERVING ENCRYPTION WITH DATA INTEGRITY

An existing FPE ciphers ensures only confidentiality. They never ensure data integrity. Encryption may not guarantee integrity. Most block cipher modes allow the attacker to induce some targeted changes into the decrypted plaintext. Especially in Format Preserving Encryption, an attacker definitely knows the format of the cipher text and there is a possibility to make changes to the cipher text. Hence, data integrity must be implemented along with encryption.

IV. ARCHITECTURE OF PROPOSED SYSTEM

The proposed Format Preserving Encryption with Authentication algorithm consists of four main processes such as key derivation, mapping, encryption and authentication. In key derivation process, we generate separate encryption key and authentication key from the master key since using a single key for both encryption and authentication is not secure[4]. The mapping is performed before and after encryption.

Each and every character in the plain text is mapped into integer value since the proposed system handles only integer domain. Actual encryption is based on AES-CTR mode which supports arbitrary length text. An encryption is followed by authentication[5]. HMAC-SHA1 algorithm is used for data integrity. The final cipher text is applied to HMAC algorithm to produce tag. The cipher text along with tag is sent to the destination. Again the tag is calculated for the cipher text in the receiving side. The equality of receiving thetag and calculated tag ensures that the cipher text is not changed by an attacker.

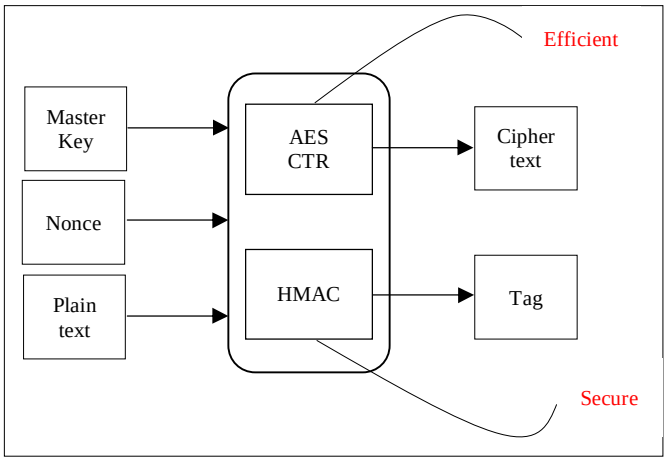


Figure 3 : Format Preserving Encryption with authentication

If the hash values do not match, simply reject the cipher text and the decryption function is cancelled. If the hash values match then the decryption function is carried out[6].

V. PROPERTIES AND RATIONALE

The existing FPE methods ensure only confidentiality while the proposed FPE ensures confidentiality, authentication and integrity. It is used for both data at rest and data at transmit.

A. Substitution Permutation Network

The proposed FPE is based on substitution permutation network (SPN) instead of a Feistel network. SPN is fast both in hardware and software. Feistel structure cannot support parallel operations[7].

B. Stream Cipher

The proposed Algorithm is based on AES-CTR mode. AES-CTR uses the AES block cipher to create a stream cipher. It can accept plaintext of arbitrary length. Stream ciphers are especially important where data must be processed in real-time or where data comes in quantities of unknown length and padding or buffering must be avoided[8].

C. AES-CTR Mode

AES-CTR mode can handle message of arbitrary length. With CTR mode, both encryption and decryption depends only on E—while it does not depend on the inverse map, $D = E^{-1}$. So D need not be implemented.

D. AES-CTR + HMAC

The main drawback in CTR mode is that it is malleable. HMAC must always be added to confirm that the encrypted data has not been tampered with. In some situations it could be preferable for performance reasons to use a cipher mode such as GCM which combines encryption and authentication. HMACs are fast and easy to implement.

Property	Value
Confidentiality	Encryption
Data Integrity	HMAC Authentication
Message Length	Arbitrary Length
Key	Only One Master Key
Parallelism	Partially parallel. Only encryption is parallel. Authentication is not parallel.
Nonce & Counter	16 byte Nonce is required

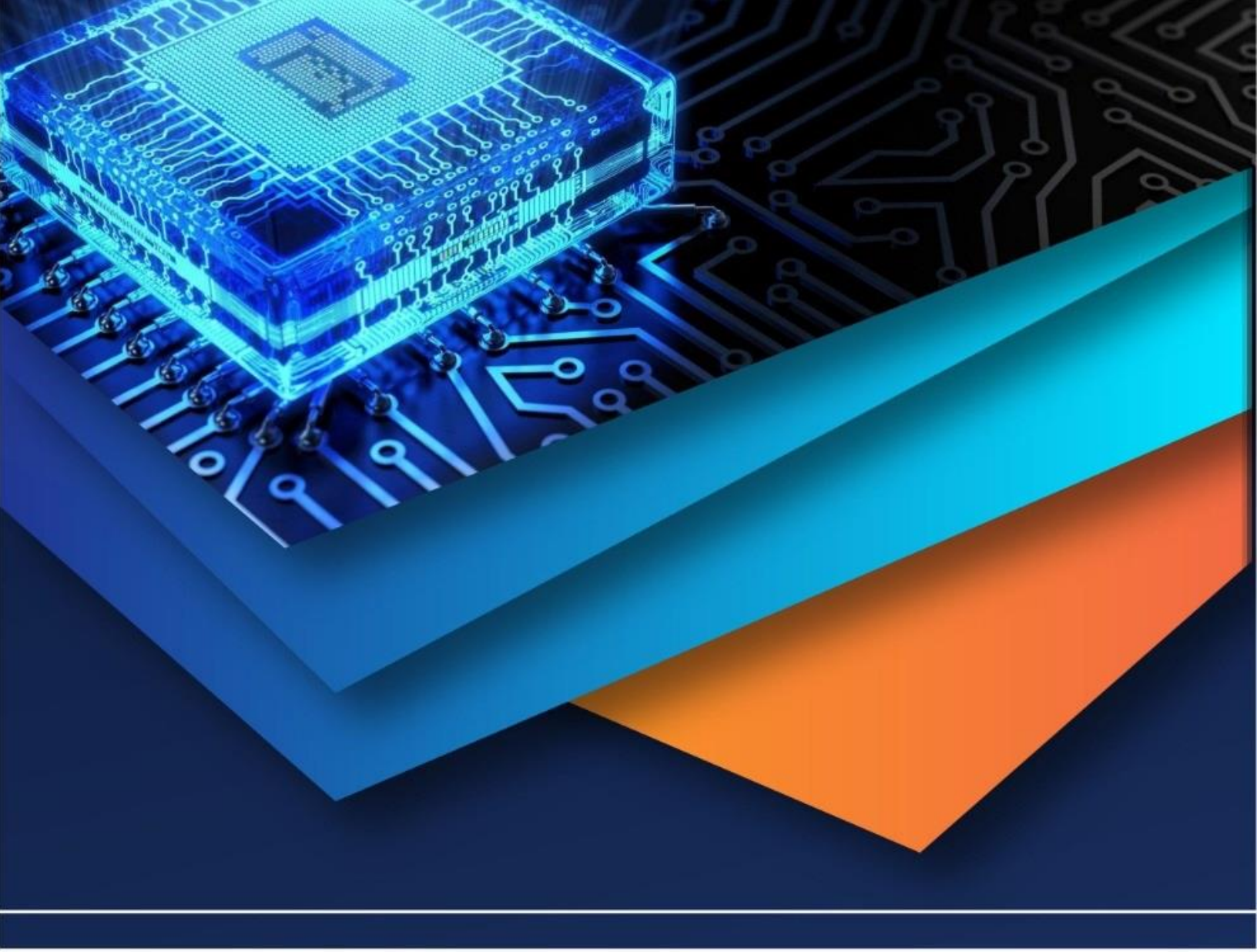
Table 1: Properties of FPE with authentication

VI. CONCLUSION

The proposed FPE algorithm achieves confidentiality, integrity and authentication. Confidentiality is implemented without data expansion. The key stream can be pre-computed. It does not depend on the plaintext. Utmost care should be taken to design the HMAC algorithm and generating unique nonce for encryption. The proposed algorithm can be applied for any data type at any arbitrary length.

REFERENCES

[1] Prakruti.C, Sashank Dara, V.N.Muralidhara. 'Efficient Format Preserving Encrypted Databases'. International Association for Cryptologic Research (IACR), 2015
[2] S.Vidhya, Dr.K.Chitra. 'Enhancement of Prefix Cipher in Format Preserving Encryption'. International Journal of Engineering Inventions. Volume 2, Issue 5 (March 2013) pp:12-15
[3] Joshua E. Hil. 'Block Ciphers Modes of Use, DES and AES'. October 2012
[4] Shikha Gupta, Priyanka Bhutani, Ridhi Nim. 'Format Preserving Encryption Technique to Strengthen Data Warehouse Security'. International Journal of Computer Science and Network. Volume 3 , Issue 4 , .August 2014. Pp:171-17
[5] Shawn Fitzgerald. 'An introduction to authenticated encryption. iSEC Partners', Inc. March 7, 2013
[6] William Stallings, 'Format preserving Encryption : Overview and NIST Specification', Cryptologia, Volume 41, Issue 2, June 2016, Pp:137-152
[7] Kamalam K, 'Rounting Protocols in Authentication way for Data Transmission in Wireless Sensor Networks, International journal for Trends in Engineering and Technology, Volume-10, No. 1., October 2015.
[8] Keonwoo Kim&Ku-Young Chang, 'Performance analysis of Format Preserving Encryption based on Unbalanced Fiestel structure', Advances in Computer Science and Ubiquitous Computing, December 2015, Pp:425-430.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY