Received: 03 November 2022 | Revised: 09 December 2022 | Accepted: 10 December 2022
DOI: 10.37917/ijeee.19.1.12 Vol. 19| Issue 1| June 2023

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access

# Securing a Web-Based Hospital Management System Using a Combination of AES and HMAC

**Alaa B. Baban *[1], Safa A. Hameed [2]**

[1] Department of Communication and Computer Engineering, Faculty of Engineering, Cihan University-Erbil, Kurdistan Region, Iraq.

[2] Peoples' Friendship University of Russia (RUDN University), Moscow, Russian Federation.

**Correspondence**
*Alaa B. Baban
Department of Communication and Computer Engineering,
Faculty of Engineering, Cihan University-Erbil,
Kurdistan Region, Iraq.
Email: alaa.ali@ cihanuniversity.edu.iq

***Abstract***

***The demand for a secured web storage system is increasing daily for its reliability which ensures data privacy and confidentiality. The proposed paper aims to find the most secure ways to maintain integrity and protect privacy and security in healthcare management systems. The Advanced Encryption Standard (AES) algorithm is used to encrypt data transferred by providing a means to check the integrity of information transmitted and make it more immune to cyberattack techniques, this was implemented by using Keyed-Hash Message Authentication Code (HMAC) and Secured Hash Algorithm-256 (SHA-256). The risk of exposure to attackers can be avoided by using honeypot systems combined with Intrusion detection systems (IDSs) as a firewall system is not effective against such attacks alone. The experimental results evaluate the proposed security health information management system by comparing the performance of the encryption algorithm based on encryption time, memory and CPU usage, and entropy for different plaintext lengths. In addition, it can be seen that when changing the AES key size, more memory and time are required the longer the key size is used. The 128 bits AES key is therefore advised if the system must operate in hard real-time.***

***KEYWORDS: Management System, Database security, database encryption, Encryption Algorithms and*** **Keyed_Hash_Message_Authentication_Code (HMAC).**

## I. Introduction

The Healthcare Management System (HMS) is essential to manage health organizations accurately and efficiently. Previously, it was hard to hold the right real-time activity records for hospitals, patient information, and maintaining equipment. Hospital information systems may help in various ways with quality assurance activities for instance; assessing the quality of primary care, checking quality indications, supporting medical care assessment studies, and verifying the continuing process of care using reminders or decision support techniques [1]. Essential parts of the process of any HMS include; the acquisition, management, and timely retrieval of large amounts of data. This information usually involves; patient personal information and medical history, staff information, and payment receipts, this sensitive information is vulnerable, therefore database systems should be protected from any attacks. To achieve the security management of the HMS the encryption algorithms are utilized to encrypt and securely send personal health information. Protecting data security in cloud databases has become a crucial issue in the field of information security where protecting the privacy of patients should be the highest priority that should be practiced by HMS, keeping in mind that this information is usually shared between different untrusted entities [2]. This study evaluates the encryption algorithm AES with a variable key length of 128, 192, and 256 bits; combined with the HMAC-SHA-256 algorithm as part of the suggested security model. This combination was evaluated to determine its effectiveness and efficiency by calculating many performance measurements. Additionally, Intrusion Detection System (IDS) with honeypot system, which is a security system that was used to detect network security breaches, were implemented.

## II. Related Work

The cloud database has a serious data security problem that was solved by encrypting the database. Even though the

database was hacked, the attackers could only get the encrypted data which is invaluable. At present, the research work mainly focuses on the confidentiality of stored data, security checks and access control, and so on. Fenghua Z.et al. [3] developed the AES algorithm by P-AES algorithm. The P-AES algorithm is combined with the RSA algorithm, named a hybrid algorithm, the obtained results demonstrate the hybrid encryption algorithm has the benefits of fast encryption and decryption. Additionally, Yitao C. et al. [2] in their research project developed a health information management system based on the Java platform to realize the duties of the system, most of the hierarchical structure of the system was enhanced according to the health information management module, also they used the Data Encryption Standard (DES) algorithm to encrypt and protect personal healthcare information, the system was developed to evaluate health information confidence, information security, and system response time.

In another study, Pramila M. Chawan [4] implemented multiple layers of security measures containing JWT, CORS, SHA-256, AES Algorithms, and, IDEA and compared the two algorithms AES, and IDEA in terms of data privacy. In [5], the authors suggest adopting the Advanced Encryption Standard (AES) algorithm for the encryption of the user information before storing it in the database as well as using an authentication approach for valid user verification and protection of unauthorized access to all system functionalities. In the project work of Owusu N. et al. [6], the AES algorithm can use multiple cryptographic key lengths of 128, 192, and 256 bits created by C# programming language as a front-end client machine and MS SQL used for the database as a back-end machine. Mondal, S. et al. [7], present a method for safer and more economical encryption system, which randomizes the key of the AES algorithm and covers the key data into the encrypted digital image by applying the basic concepts of cryptography and digital watermarking. W Xing-hui and M Xiu-jun [8] proposed a hybrid encryption method in databases, they adopted RSA and IDEA algorithms which are public key and symmetric key respectively. Firstly, the database is encrypted by RSA algorithm and then these keys were used to encrypt the plain data using the IDEA algorithm. This hybrid system enhances the security of data and make it more immune against attacks. Furthermore, the authors in [9] present a system that provides password encryption using hashing functions such as MD5, SHA, etc., they also proposed a novel modification that enhanced the security using a hashing function. Min-Shiang Hwang and Wei-Pang [10] proposed two methods of encryption techniques depending on the concept of sub keys that gives some security; moreover, solves key management problem which allows multiple users to right access. Table III shows a comparative study.

## III. Description of AES Algorithm

Joan Daemen and Vincent Rijmen created the AES block cipher, which is also known as the Rijndael algorithm. The method runs smoothly on a wide range of computer processors and hardware [11]. AES is based on a design concept known as a substitution-permutation network, which is a combination of substitution and permutation, and is fast in both software and hardware. AES does not employ a Feistel network, unlike its predecessor DES. The thorough AES development process, as well as its complex internal structures, ensuring that the algorithm is extremely safe and has no known flaws. Rijndael's key length can be 128, 192, or 256 bits, depending on the AES requirements. The Rijndael algorithm has variable block sizes, which can range from 128, 192, or 256 bits. This means that a Rijndael method with key sizes of 128, 192, and 256 bits gives nearly the same amount of security [12]. The round transformations used in this encryption technique serve as a framework for its iterative structure[13].

AES is one of the most up-to-date algorithms of the four currently certified for federal use in the United Statuses uses a four-by-four (4 x 4) column-major-order byte matrix called the state, while certain Rijndael variants use a larger block size and have more columns inside the state. AES composition and building blocks were created based on a standard known as a substitution-transformation arrangement with a set block size of 128 bits and a key size of 128, 192, or 256 bits, and has a high-speed in both software and hardware (see Figure 1). The AES technique encodes 10 cycles for 128-bit keys during encryption and decryption. To get the last encoded message, go through 12 rounds for 192-bit keys and 14 rounds for 256-bit keys [14]. The encryption begins with a "Add round key stage" for encoding and decoding. However, shortly before the final round, the output is subjected to nine fundamental rounds, each of which includes four transformations: 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, and 4) Add round Key. Mix column transformation is not accessible in the ninth round [15-17].Decryption is the inverse procedure, with the following stages [18]:

1. Substitute Byte Transformation: AES is made up of 128-bit data blocks, which means that each database item comprises 16 bytes. By implementing an 8-bit substitution box known as the Rijndael s-box, every bite of a data item is turned into another piece in sub-byte transformation.
2. Shift Rows transformation: This transformation is simple; the bytes in the state's last three lines, which are dependent.
3. On row position, are moved in a cycle. The second line does a 1-byte circular left shift. Two bytes and three bytes left circular shifts are performed in the third and fourth rows, respectively.
4. Mix columns transformation: This is the inverse of a multiplication set of each state's column. Every is multiplied by a stable matrix. Bytes are treated as multi-names in this procedure.
5. Include a round key transformation: a bit-like XOR between the current state's 128 bits and the round key's 128 bits. This is the polar opposite of transformation.

The Table I shows a comparison of cryptography symmetric algorithms based on common factors.

TABLE I
COMPARISON BETWEEN SOME SYMMETRIC ALGORITHMS [18, 19]

| | Symmetric Cryptography | | | | |
|---|---|---|---|---|---|
| Algorithm | Key Size (bits) | Block Size (bits) | Round | Security level | Speed |
| DES | 64 | 64 | 16 | Less secure | Slow, but speed depends on key |
| RC2 | 40 | 64 | 16 (Mixing) +2 (Mashing) | Less secure | Fast |
| AES | 128,192 and 256 | 128 | 10,12 ,14 | Secure | Fast, but speed depends on key |

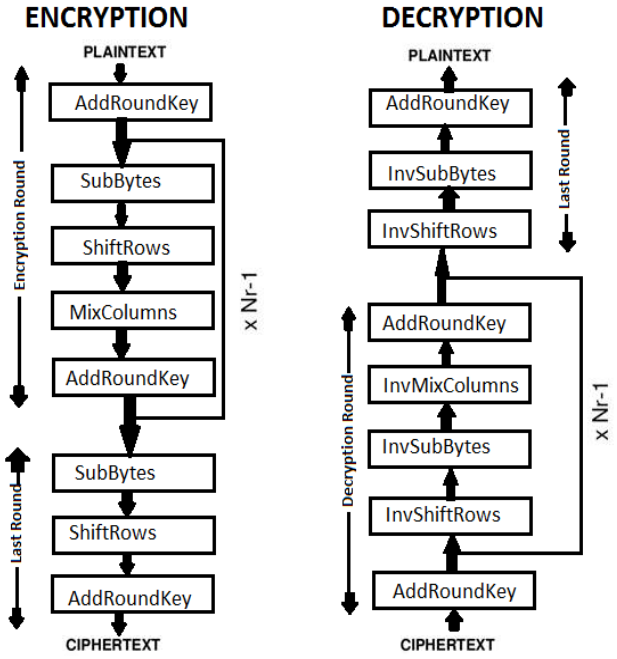


Fig. 1: The AES Algorithm's General Structure [7]

## IV. THE KEYED-HASH MESSAGE AUTHENTICATION CODE (HMAC)

HMAC is used to check the integrity of data transmitted over or stored in an unreliable medium it is considered an essential requirement in open computing and communications. Procedures that give integrity checks based on a private key are generally named message authentication codes (MACs). Usually, message authentication codes are used between two sides that share a private key to authenticate information transmitted always the is MAC used with a hash function together with a private key whereas the HMAC uses the private key for the calculation and verification of the MACs[20].The HMAC gives two types of keys one of them is a private key that only known in specific client and servers and the other is a public key[21]. Since encryption ensures just the confidentiality of the information being sent, a digital signature which is another security technique ensures other security goals such as non-repudiation, data authentication, and data integrity as shown in figure 2. One–way-hash function (SHA256) is used in the digital process which creates compressed data or digest which is often unique and smaller than the plaintext and if any change made to the massage can be discovered from a different hash result even if the same hash is used [22]. Definition of HMAC-SHA256 as:

$$HMAC(K,m) = H(K \oplus opad) \parallel H(K \oplus ipad \parallel m)) \quad (1)$$

which uses the following parameters:
H = cryptographic hash function = SHA256
K = secret key
m = message
$\parallel$ = concatenation
$\oplus$ = exclusive OR
opad = outer padding
ipad = inner padding

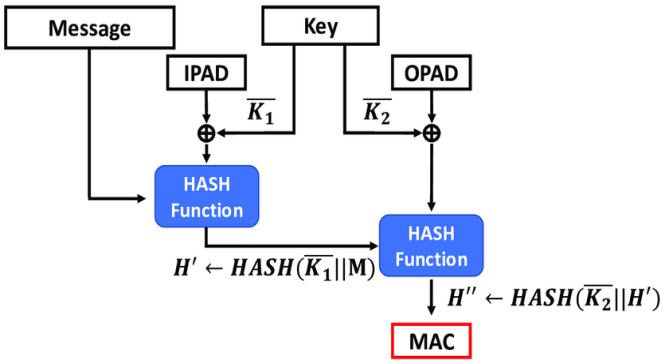


Fig. 2: HMAC structure with Multi-Hash [23]

## V. INTRUSION DETECTION SYSTEM (IDS)

The intrusion can be described as group of activities that attempt to hack the confidentiality, integrity or availability of a resource where the monitoring the events occurring in a computer system or network and analyzing them for signatures any of intrusions and virulent attacks named by Intrusion detection. Intrusion Detection System (IDS) is a software or hardware system to ensure the intrusion detection process automatically [24]. IDS is classified based on many various criteria to the present day. A common criterion is the intrusion detection method and IDS is divided into two groups according to intrusion detection method "anomaly detection" and " Pattern matching or misuse detection"[25].

## VI. MISUSE DETECTION

The misuse detection process is also known as signature-based detection. Signature based methodology works by matching observed signatures to the signatures on record which is can be a database or a list of known attack signatures. Every signature seen on the monitored system which matches the signatures on record is flagged as a breaking of the security policy or as an attack. The signature-

based IDS recognizes the network traffic or activity only in the known signatures in the database or file [26]. The most important job of these systems is to compare activities with pre-generated signatures. Signatures are usually a set of characteristic features that assign to the specific attack or pattern of attacks. Typically, there is no need for highly skilled administration to detect the attacker when misuse detection techniques are used. In addition above mentioned advantages, misuse-based IDSs operate efficiently and quickly[27]. Otherwise the anomaly-based methodology, the signature-based methodology system is easy to set up because it does not need to learn the environment [28].

## VII. Anomaly Detection

The anomaly detection approach includes two phases: firstly, a training phase which is based on the identification of behavior and normal traffic by creating profiles of users, network connections, and servers; and a testing phase where the learned profile is applied to new data [25].

## VIII. Honeypot System

The Honeypot systems are based on attracting intruders. These systems are used as a trap for unauthorized interaction in networks. Also, honeypot systems are used to learn about stranger behavior. They are not used to solve specific problems such as firewalls or IDSs. Honeypot systems are used as a part of security systems with other equipment. When using the honeypots, network administrators can calculate the number of attacker succeeded prevent subsequent attacks, and identify security vulnerabilities in the network.[29].Honeypots get their strength from their assailable options to attract the hackers [30]. A honeypot is considered an isolated resource that looks like a real database used to attract the attackers to them allowing explorers to analyze any pattern of aggressive or violation behavior[31]. Honeypots gathered with IDS system's main usage purposes specify below like;

*1)* Get more information on security weak points and intruder's behavior.
*2)* Discovering the intruders and all unwanted traffic by using setting up a trap system.
3) Detecting malicious activities that are interior the network, and attacks from outside of the network.
4) Hiding the real systems, which are created within the honeypots.
5) Increasing the system security [32].

## IX. CLOUD COMPUTING

A form of Internet-based computing known as "cloud computing" makes data and shared computing resources available instantly to computers and other devices. In cloud computing, users are provided with resources based on their need, and resources are simply assigned and released based on user demand. Data management and storage may both be facilitated by cloud computing, making it more convenient for businesses to access their data. By implementing cloud computing technologies, can make it possible for the healthcare sector to store data effectively and cheaply without using physical servers. The huge data issue can be solved via cloud computing. It provides endless storage capacity and makes the procedure of transferring patient data across healthcare facilities simpler.

## X. The Proposed Security Model

The proposed security model, shown in Figure 3, uses the combination of AES and HMAC algorithms to produce a strong system protection encrypted by a symmetric key that ensures a secure transmission between server-client or client-client through encrypting the exchanged data and makes. While the message integrity and authentication can be guaranteed by using HMAC.
The procedure of the proposed security model is as follows:

1) The client uses the AES algorithm to encrypt its data using cipher keys of 128,192 and 256 bits.
2) HMAC algorithm is used to ensure message integrity and the source of origin using hash function (SHA-256).
3) The data on the cloud is vulnerable to attackers thus a honeypot system that represents a real computer system, is used as a trap for unauthorized communications in the network. Besides Honeypot technologies, other security tools are implemented such as the Intrusion Detection System (IDS) which provides two functions; first, the information required for an attack, i.e signature, in order to develop a fast and appropriate response in real-time, and second, the time required to execute that response. When the attack occurs, a honeypot can be used in analyzing an attacker's activity by comparing the observed signature with the known list of attack signatures, and if they match then it will be classified as a breach of the security policy or as an attack.

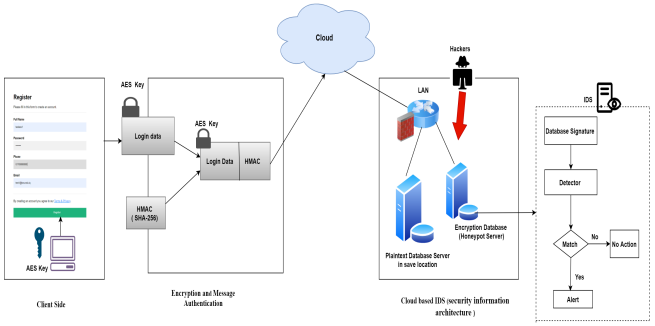


Fig. 3: Architecture of Proposed Security Model.

## XI. System Implementation and Results

### *A. System Implementation*

A web application with login details of the patients was developed to collect raw data in plaintext to be encrypted by the AES and combined with HMAC-SHA256 for integrity and message authentication. The testing of the outcome of the

implementation is done by using different sizes key128,192 and 256 bits, AES algorithms as shown in the figure 4 below:

| fullname | password | phone | email |
|---|---|---|---|
| testaeshmac1 | knKmTt2zgEZWoC4jJ3MgPaBzDiu5PjiAEBMIveR+owDwYz15v... | 0776543322 | test1@bnu.edu.iq |
| testaeshmac1 | mYSc1utPLoVhZuL8CptRAjyAyks+fVI+BUMWINhTKYuRCWRDW... | 0776543322 | testmac1@bnu.edu.iq |
| testmac1 | oXZtox9CWVa2N4e2HLFDhAhNgWxQvMdPmtCpqwoTa6kFEZNuO... | 0776543322 | test1@bnu.edu.iq |
| testmac1 | 2ijs5dmK3Np6ADoqOBFGlaBpJSX8PzozXIXwiB9zg1nl9mQND... | 0776543322 | testmac1@bnu.edu.iq |
| testmac2 | StA9UmdAuX9Qyt3zO0mgbSMfWJEYYUAwtz5FD6b6Dd63get8h... | 0776543322 | testmac2@bnu.edu.iq |
| testmac3 | h2xU8TieVJI2pOm/XS4Ry/4W7x70Aq2OgKT7NwVcVA/LHc4AJ... | 0776543322 | testmac3@bnu.edu.iq |
| testmac4 | j4bTCQwfBuoKOZ5P/CRdfXrgiCjt/YLQYc0hJhS9AGK6iVskY... | 0776543322 | testmac4@bnu.edu.iq |

Fig.4: User Database Table of AES- HMAC-SHA256 Security System.

*B. Experimental Results*

All experiments were done on a laptop hp Elitebook 2.6 GHz Intel processor with 16GB memory and 512GB hard disk. The operating system which was used is 64bit Windows 10. The results were executed based on the database XAMPP phpMYAdmin Server and the programming language is PHP, HTML, CSS, and JAVASCRIPT. Performance comparison of symmetric encryption algorithm AES based on the execution time of Encryption with different types of keys length 128,192 and 256 bits and study is performed on the effect of changing plaintext length 2,4,8 and 16 respectively on encryption time, CPU workload and amount of the memory usage.

Figure 5, shows the execution time in the encrypting process for three types of AES keys over different lengths of plaintext. The units of encryption time were measured in milliseconds. Overall, the consumption time of encryption using AES-256 is higher than the rest of the AES types.

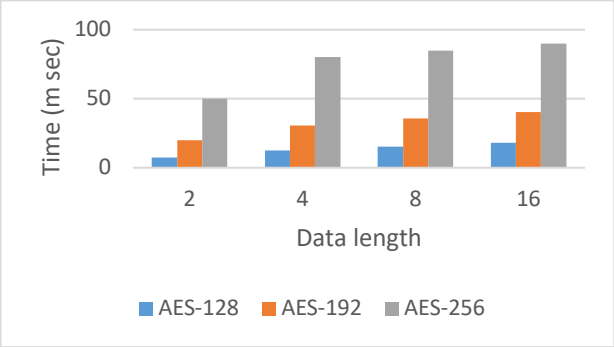


Fig. 5: Time consumption for encrypt different length of text transmission (millisecond).

Results of the experiment for measuring the percent of CPU used are presented in Figure 6. As one can see, the average value is just above 7% when encrypted the message by the AES-256 algorithm.

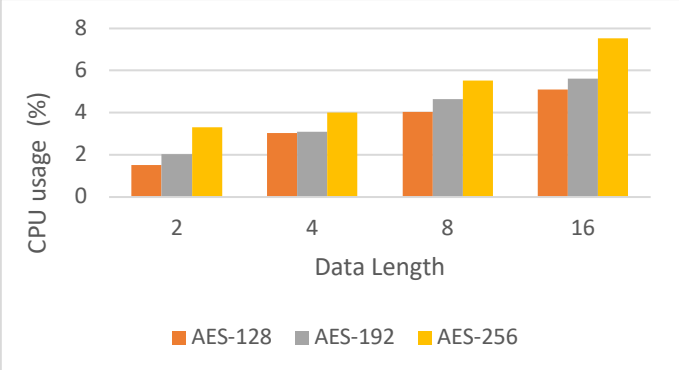


Fig. 6: Percentage of CPU used (%)

Meanwhile, the performance evaluation of the AES is based also on the memory parameter and effect on Intel-Core i7-6600U Processor (8M Cache, up to 2.6 GHz) with RAM 64GB. The results in Figure 7 demonstrate that the AES-256 need more space of memory to encrypt the data.

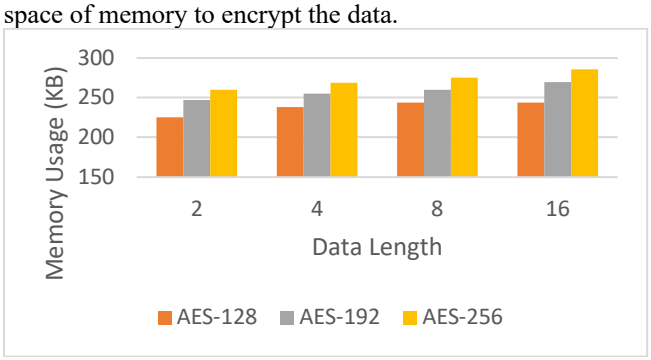


Fig. 7: Reserved Memory (KB)

As the entropy test, a famous measure of uncertainty in the theory of knowledge was described in 1948 by (Shannon, 1948) [33]. Shannon proposed that entropy H(X) could be calculated by the average amount of information of a discrete random variable X

$$H(X) = \sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \qquad (2)$$

on the following terms:

X consists of a finite of a sample space $x_1, x_2, x_3, .., x_n$;

P(xi) probability distribution, $x_i \geq X$;

• And $\sum_{i}^{n} 1p(x_i)$

Entropy analysis measures the complexity of encrypted data [34]. As the proposed security system consists of encrypted massage using AES combined with HMAC -256 that lead the optimum entropy value is 5. 580.Thus, a value that is close to 5.580 corresponds to the high complexity of encrypted data. Table II shows that combination of AES and HMAC algorithms records the highest average entropy per byte in contrast if using only AES algorithm. increasing entropy leads to making the data less susceptible to attack.

TABLE II
AVERAGE ENTROPY VALUES

| Data Length | Average entropy per byte | Average entropy per byte |
|---|---|---|
| | Type of Algorithm / AES | Type of Algorithm / AES with HMAC |
| 2 | 3.2743 | 5.4321 |
| 4 | 3.6321 | 5.4725 |
| 8 | 3.8439 | 5.41665 |
| 16 | 4.1673 | 5.5707 |

TABLE III
COMPARISON BETWEEN THE RELATED MENTIONED WORKS.

| Ref. | Algorithm Used | Description | Processing Time | Memory Usage | Encryption | Message Authentication |
|---|---|---|---|---|---|---|
| [2] | Developed the AES algorithm named by (P-AES) | A hybrid encryption algorithm can provide security protection | ✓ | × | ✓ | × |
| [3] | Data Encryption Standard (DES) | Symmetric key cipher of Encryption | ✓ | × | ✓ | × |
| [4] | International Data Encryption Algorithm (IDEA) | Symmetric key cipher of Encryption and Decryption | × | × | ✓ | × |
| [5] | AES | Symmetric block cipher with a block length of 128 bits. | ✓ | × | ✓ | × |
| [6] | AES | Symmetric key cipher with length 256bits | ✓ | × | ✓ | × |
| [7] | AES | AES algorithm gives more security with a little encryption time used to encrypt using 128-bit key. | × | × | ✓ | × |
| [8] | RSA+ IDEA | Added Security by use of 2 encryption algorithms | × | × | ✓ | × |
| [9] | Hashing | MD5(Message-Digest Algorithm | ✓ | × | × | × |
| [10] | Data Encryption Standard (DES) | Security is guaranteed by the use of two-phase encryption. | × | × | ✓ | × |
| The current work | AES +HMAC | Symmetric key cipher with three different key lengths: 128, 192, or 256 bits. | ✓ | ✓ | ✓ | ✓ |

## XII. CONCLUSIONS

In this paper, we successfully ensured the privacy and integrity of healthcare data by implementing secured model that included AES and HMAC-SHA-256 algorithms and demonstrated the addition of an extra layer of security for data authentication and integrity using an intrusion detection system to prevent the misuse by intruders who may bypass the common access control mechanisms and have direct access to the database. Finally, in the case of changing AES key size, it can be observed that the longer the key size used the more memory and time is needed. For 2bit data, it can be noticed that when changing the AES key length from 128-bit to 256-bit (100% key size increase), the memory usage will be affected the least by an increase of only 13%, while the CPU utilization is increment by 90%, However a dramatic increase in time is observed by about 1366%, which indicates the mathematical complexity of the AES algorithm. Therefore, if the system needs to operate in hard real-time manner, then the 128 bits AES key is recommended.

## CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

## REFERENCES

[1] A. Jayawardena, "The electronic hospital information system implemented at the district general hospital trincomalee-an experience of business process re-engineering" J Community Med Health Educ S, Vol. 2, 2014.

[2] Y. Chen, and L. Wan, "Towards Designing Personal Health Information Management System Based on Java", Mobile Information Systems, 2021.

[3] F. Zhang, et al., "Hybrid encryption algorithms for medical data storage security in cloud database", International Journal of Database Management Systems (IJDMS), Vol. 11, 2019.

[4] K. Deshmukh and P.M. Chawan, "Data Integrity and Privacy in Healthcare Management System: A Survey", International Research Journal of Engineering and Technology (IRJET), Vol. 7, No. 11, 2020.

[5] R. Amrutha, P. Perumal, S. Balaganesh, D. Ishwarya, "Secured Data Migration using AES Algorithm and Authentication Techniques in Cloud Environment", International Journal of Research in Engineering, Science and Management, Vol. 2, Issue 3, pp. 853-856, March-2019.
[6] I. Nti, E. Gymfi, and O. Nyarko, "Implementation of advanced encryption standard algorithm with key length of 256 bits for preventing data loss in an organization", Int. J. Adv. Technol, Vol. 8, No. 02, pp. 1-5, 2017.
[7] S. Mondal, S. and S. Maitra, "Data security-modified AES algorithm and its applications", ACM SIGARCH Computer Architecture News, Vol. 42, No. 2, pp. 1-8, 2014.
[8] X. h.Wu, X. j. Ming, "Research of the Database Encryption Technique Based on Hybrid Cryptography" In 2010 International Symposium on Computational Intelligence and Design, 2010.
[9] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, "Security analysis of MD5 algorithm in password storage", In Applied Mechanics and Materials. 2013.
[10] M. S. Hwang, and W. P. Yang, "A two-phase encryption scheme for enhancing database security", Journal of Systems and Software, Vol. 31, No. 3, pp. 257-265, 1995.
[11] B. Schneier, et al., "The Twofish team's final comments on AES Selection", AES round, Vol. 2, No. 1, pp. 1-13, 2000.
[12] W. M. Tatun, "The Advanced Encryption System (AES) Development Effort: Overview and Update", SANS Institute, 2001.
[13] H. A. Younis, A. Y. Abdalla, and T. Y. Abdalla, "Partial encryption of compressed image using threshold quantization and AES cipher", Iraq J. Electrical and Electronic Engineering, Vol. 8, No. 1, 2012.
[14] M. G. Singh, M. A. Singla, and M. K. Sandha, "Cryptography algorithm comparison for security enhancement in wireless intrusion detection system", International Journal of Multidisciplinary Research, Vol.1, No. 4, pp. 143-151, 2011.
[15] S. William, "Cryptography and Network Security: for VTU", Pearson education india, 2006.
[16] Z. J. Chowdhury, D. Pishva, and G. Nishantha, "AES and Confidentiality from the Inside Out", in 2010 The 12th International Conference on Advanced Communication Technology (ICACT), 2010.
[17] K. F. Jasim, et al, "Analysis the Structures of Some Symmetric Cipher Algorithms Suitable for the Security of IoT Devices", Cihan University-Erbil Scientific Journal, Vol. 5, No. 2, pp. 13-19, 2021.
[18] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES", in 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012.
[19] M. F. Mushtaq, et al, "A survey on the cryptographic encryption algorithms", International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.
[20] J. M. Turner, "The keyed-hash message authentication code (hmac)", Federal Information Processing Standards Publication, Vol. 198, No. 1, pp. 1-13, 2008.
[21] E. S. I. Harba, "Secure data encryption through a combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research, Vol. 7, No. 4, pp. 1781-1785, 2017.
[22] N. A. Azeez, and O.J. Chinazo, Achieving Data Authentication With Hmac-Sha256 Algorithm", Computer Science & Telecommunications, Vol. 54, No. 2, 2018.
[23] B. Park, J. Song, and S. C. Seo, "Efficient Implementation of a Crypto Library Using Web Assembly", Electronics, Vol. 9, No. 11, 2020.
[24] Benmoussa, H., A. Abou El Kalam, and A.A. Ouahman. Towards a new intelligent generation of intrusion detection system. in Proceedings of the 4th Edition of National Security Days (JNS4). 2014. IEEE.
[25] M. Baykara, and R. Daş, "A survey on potential applications of honeypot technology in intrusion detection systems", International Journal of Computer Networks and Applications (IJCNA), Vo. 2, No. 5, pp. 203-211, 2015.
[26] D. Mudzingwa, and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (IDPS)", in 2012 Proceedings of IEEE Southeastcon, 2012.
[27] E. Cole, "Network security bible", John Wiley & Sons, 2011.
[28] A. Valdes, and K. Skinner, "Probabilistic alert correlation," in International Workshop on Recent Advances in Intrusion Detection. Springer, pp. 54–68, 2001.
[29] S. Li, Q. Zou, and W. Huang, "A new type of intrusion prevention system", in 2014 international conference on information science, electronics and electrical engineering, 2014.
[30] I. Koniaris, et al., "Honeypots deployment for the analysis and visualization of malware activity and malicious connections", in 2014 IEEE international conference on communications (ICC), 2014.
[31] J. Wang, and J. Zeng, "Construction of large-scale honeynet Based on Honeyd", Procedia Engineering, Vol. 15, pp. 3260-3264, 2011.
[32] Y. Gökırmak, et al, "IPv6 Balküpü Tasarımı", Tübitak Ulakbim, Ankara, 2011.
[33] N. Shaji, and P. Bonifus, "Design of AES architecture with area and speed tradeoff", Procedia Technology, Vol. 24, pp. 1135-1140, 2016.
[34] B. Latinović, Z. Ž. Avramović, and M. Zajmović, "Safety Analysis Of Reverse Algorithm Encryption In Databases", Journal of Information Technology & Applications, Vol. 9, No. 1, 2019.