Journal of Autonomous Intelligence (2023) Volume 6 Issue 3
doi: 10.32629/jai.v6i3.695

ORIGINAL RESEARCH ARTICLE

Blowfish based encryption model in real cloud environment

Rubika Walia[1,*], Prachi Garg[2], Manish Kumar[3]

[1] *Department of Computer Science & Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar Institute of Computer Technology & Business Management OR MMICTBM (MCA), Maharishi Markandeshwar (Deemed to be University), Ambala 133001, India*

[2] *Department of Computer Science & Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar (Deemed to be University), Ambala 133001, India*

[3] *Department of Computer Science & Engineering, Chandigarh Engineering College, Chandigarh Group of Colleges (CGC)-Landran, Mohali 140307, India*

*** Corresponding author:** Rubika Walia, ahluwalia.rubika@gmail.com

ABSTRACT

The introduction of the internet has made security a top anxiety. And the preceding of security permits for improved knowledge in the creation of security tools. Several concerns about safekeeping might have arisen just from the way the internet was set up. Many businesses use firewalls and encryption techniques to protect themselves online. Businesses can design an "intranet" that is protected from potential risks while being linked to the internet. For increased security, better encryption techniques are needed to retain data integrity. For better encryption, it is essential to consider into explanation a few of issues, including key size, chunk size, and encoding ratio. Documents transferred to subordinate storage strategies (such as Hard disk or SD card) must be encrypted to provide security and prevent unwanted access. If a key is kept on secondary storage with the document, it is quite simple to decrypt it. It is desirable to create encryption keys from operator passwords when encoding or decoding the folder rather than keeping the key together with the document.

Keywords: advance encryption system; secure hash algorithm; federal information processing standard; national institute of standards and technology

ARTICLE INFO

Received: 8 June 2023
Accepted: 29 June 2023
Available online: 4 September 2023

1. Introduction

1.1. Network security

Network security has become more and more important in recent years since it provides a method for storing contributions that are web-based. Defense is crucial in the effort to restrain recent outbreaks. Relief from breakouts and concerns about cover-up are the only notable unique characteristics of recent attacks. Attacks may be categorized as common individual's interpretation & a technician interpretation. First comprises unlawful, profile-raising & permitted attacks. Those attacks in particular focus on influencing certain components like buying orders, commercial possibilities, and a way to maximize economic advantage[1]. Latter consists of theoretic ideas behind of those attacks and sensible strategies castoff by muggers.

1.2. System security ideologies

There are numerous well-established security concepts that you should be familiar with; the facts protection technological structure is a good place to start for overall information on facts defense. PC protection goals (or requirements) are frequently stated in terms of five regular goals[1].

a) Validation: it proposes data can be swap over among official transmitter and recipient.

b) Privacy: it proposes that the merely the authenticated operator can only contact data of further trustworthy operator.

c) Truthfulness: it recommends that the data is not allowed to somewhat sort of modification among basis and endpoint.

d) Non-Repudiation: it recommends the basis and the addressee will not ever scrap that they must post a pure memorandum.

e) Admission governor: merely the allowable meetings are talented of retrieving the approved archives.

1.3. Cryptography

Data is encoded using encryption, and anyone with the right key can decode it. Encryption makes ensuring that data that is actually associated does not essential to be changed during transfer. Steganography and encryption differ slightly in that the hidden memorandum is continually untraceable in the former while always being visible in the latter since data is contained in plain text. The application of techniques for secure communication in the presence of enemies is known as encryption. Often, it involves developing and analyzing processes that negated an enemy’s impact and were associated to various aspects of data security. Modern encryption combines the self-switches of math, expertise, and electricity. Many different types of encoding exist. Data has a basis, addressee, and intruder, and the use of cryptography prevents invaders from accessing sensitive archives[1–3].

1.4. Uses of encryption

1.4.1. Harmless message transmission by means of substitution-signcryption

The alternate symbol preparations license additional signers to spot transportations on the base of a solitary signer, a business or an administration. It is positioned and decided on the inaccessible logarithm habit. The signcryption is a common significant plain that concomitantly completes the topographies of to each fundamental design and encrypting. Grouping of substitute design and signcryption collective key mock-ups grants comfortable statement. It is loads effective in footholds of functioning out and communication prices. Its unfriendly reject for minor control CPU schemes in which expected technique powers too handover and become grip of memorandums from an arbitrarily massive volume of additional computers[4,5].

1.4.2. Detecting message

Encoding can distribute somewhat robust security; it might mass the management’s resolves to lawfully transmission out automatic examination. Through an opinion to track into this obligation, important is escrowed thru important third congregation. This age licenses the rehearsal of robust encryption, however in adding permits the management while legally permitted to grow deciphering keys detained through escrow dealers. NIST has published the escrowed programming extensive as FIPS 185.

1.4.3. Insignificant recognizing of information

When in a despite the fact dispatcher needs nearly share of the message to be surveyed nonetheless no lengthier all. If so, see-through cryptography is rejected that determines the hole between dense (vigorous converting short of a key escrow) and glowing (no indoctrination or indoctrination by key escrow). Through see-through preparation, the authorities can decipher specific of the transports, but not wholly. Impartial as a see-through arrival on a torrent attitude proposals sure confidentiality, but no extensive has perfect clandestineness, see-through cryptography assumed convinced infrastructures privacy, but no lengthier perfect secluded. In this level of limpidity can be prearranged by altering constraint p.

1.4.4. Conveying records on system

Data that can be transferred between hands need to be protected from nefarious customers and thieves. Symmetric key encoding uses a single key maximum effectively for encoding and decoding. Symmetric solutions are next prearranged using a shared key that is sent along through the folder source to decode the data, and this automatic description is then sent to the addressees. The prearranged typescript implement unit's driving force uses an individual vital which is associated to the addressee to decipher the symmetric strategic substitute used to encrypt the manuscript. The description is subsequently decoded by the prearranged description construction unit teamster using a symmetric strategic.

2. Related work

To enhance security in the suggested scheme, numerous academics and investigators operate in various fields and associated criteria.

According to Kumar et al.[1], security are the maximum tough components within the internet and system packages. Encryption is the one of the principal classes of PC protection that translates data from its ordinary shape into a coded form. The two important traits that categorize and distinguish one cryptography procedures from some other are its capacity to safe the included statistics towards assaults and its pace and performance in doing so. The author provides an honest evaluation among three collective symmetric key encryption procedures: Blowfish and AES on the foundation of constraints: quickness, chunk dimensions and key magnitude. Mock-up platform is carried out the use of java programming.

Goyal[2] provides a concise description of the scrambling process, including how it is carried out and how it is used in various bureaucracies. Using encryption, you can prevent unauthorized access to the crucial information. It appears to be a comfortable way of communicating information. It specifically makes interruptions from third parties shorter. It offers statistical confidentiality, veracity, alphanumeric signals, and creative person verification. The encoding and decoding processes in encryption use mathematics to guard the documents.

According to Mathur[3], encoding is the system of changing text message into the cryptograph manuscript in which text message is the input for the encryption and cipher text is the production of the encoding method. Decoding is the manner of remodeling cipher text into the original message wherein cipher text is the entrance to the decoding method and original message is the outcome of the decoding procedure. There are numerous encoding procedures be labelled as symmetric and uneven encryption procedures. The author presents set of rules for statistics encoding and decoding that is centered totally on ASCII standards of letters in the original message. The proposed procedure is implemented to encode statistics with the aid of the use of ASCII standards of the records to be encoded.

According to Ismil et al.[4], recently, the Rijndael procedure ensures stayed consistent with the aid of the NIST as the progressive encoding well-known. This marks AES a vital and vital information-security appliance for centralized corporations inside the US and other international locations. In AES, spin befalls in strategic extension, ciphering, and decoding. Spin is crucial for misperception and dispersion, which play a vital position in any encryption approach. Mix-up and distribution create infringement the key complex and hard.

According to Dave and Parmar[5], security is the furthermost perplexing worry for system security. Owed to quick development of internet and systems requests, capacity of records swapped among operators is snowballing precise quickly. As a result, information security needs stayed a major issue in the broadcast of statistics. Somewhat harm or threat to statistics can result in serious harm to the firm. Encryption displays a key point in information protection scheme. This author provides an assessment of diverse cryptographic procedures after which discover finest existing one procedure for the system protection.

Pahal and Kumar[6] developed a 200-bit AES technique employing 5 × 5 grounds, then on the foundation of dual parameters—encoding/decoding interval and throughput—compared it to 128, 192, and 256-bit AES processes.

According to Rakholiya and Kathiriya[7], Encryption is the artwork of accomplishing security by encrypting communications to cause them to be inaccessible for unauthorized users. Encryption is the preparation and has a look at of hiding information. Now a day's encryption is reflected a division of arithmetic and computational theory and is associated strictly with facts idea, workstation security and business. Two primary forms of encryption: symmetric key and asymmetric key. Symmetric key procedures are the fastest and efficient generally applied in encryption. Here, an unattached secret is used for both encoding and decoding.

According to Sandhu and Verma[8], masses of cryptography and steganography primarily based techniques were advanced inside the past many years. A number of them are not talented to absolutely guarantee the security of facts from variations, functional via eavesdroppers. Few others employ big key size and complicated methods to encode records for higher security.

According to Sumitra[9], system security has been a major issue in current existences. Information needs stayed calmed through encoding, which is accomplished thru transmitting a private encryption key above certain strategies. With a number of adjustments, encoding makes the transmission unconceivable to unidentified. Data encoding is the process of scrambling data in archives like typescript, photographs, music, and video to make it unreadable or unintelligible during transport. Its primary goal is to safeguard archives from unauthorized contact.

According to Manjesh and Karunavathi[10], cryptography is the observation of mathematical strategies for secured communique within the presence of adversaries and also it offers with the components of records security which include confidentiality, statistics integrity, entity authentication and records foundation authentication. An excessive speed protection set of rules is constantly necessary and essential for stressed out/Wi-Fi communication. The symmetric chunk cryptograph shows a main part in the majority statistics encoding.

Lalitha et al.[11] promote the use of the AES set of principles for statement concealment. Both steganography and encoding are widely used techniques for transferring crucial information in a covert mode. In direction to create comfortable figures, scrambling was introduced. A better security solution can't be provided by encryption only because the viewer can still read the scrambled memorandum. A dearth of evidences is emerging. In order to increase security, the writer pools steganography and encryption. One of the most effective procedures for encrypting data is AES. The writer used a 128-bit strategic in addition to the AES method to encrypt the memorandum. The writer demonstrated that the planned fusion approach offers greater protection than past practices.

According to Acharya et al.[12], cryptography performs a primary function in safeguarding statistics. It is castoff to make certain that the insides of a memo are privately communicated and could not be modified. Community protection is maximum critical thing in statistics security as it mentions to all components and program, features, capabilities, active approaches, duty, entrance manage, and managerial and administration policy. Encryption is imperative to it security demanding situations, because it supports confidentiality, secrecy and identification, which collectively offer the basics for relied on e-trade and comfy message.

According to Al Hamid et al.[13], attentive is considered to work a fog management workplace to safe community assurance set aside data in the cloud. To attain this, a tri-party one-round verified significant pronouncement preparation is prearranged in the essence of the bilinear corresponding encryption, which can yield and communicate a conference key securely amid the members. Concluded revisions, the journalist established by what means untruthful strategies may be realized to grow and steadily supply isolated and community assurance statistics.

According to Qadir and Varol[14], now, the knowledge of cryptography were discovered sideways with its past, ever-changing procedure necessities, and standing to ordinal security. At this time, early procedures such as the Caesar cryptograph, up-front replacement cryptographs, reversal cryptographs, tributary cryptographs, and modern hash procedures were likewise enclosed.

According to Gupta[15], now, we saw the numerous individualities and physiognomies of some hashing approaches. We observed at the DES, RSA, MD, and SHA families. Moreover, we observed at the basics of cryptography and the several types of solutions which are active in encoding. This artefact likewise enclosed the weaknesses or limitations of definite procedures, such as in what way DES is not appropriate for encoding complex statistics and in what way selecting big p and q in RSA can be puzzling.

According to Verma et al.[16], to encode operator statistics (imageries, videotapes, auditory, word documents, and several files) on the operator arrangement, it is recommended to use the additional up-to-date and harmless Hashing Procedure (SHA-512). The 512-tads prearranged cryptograph formed by SHA-512 is incredible to crash. As of Sheltered Hashing Technique (SHA-512), robust encoding is no extended maintained in a numeral of sites, comprising (BTS), LBRT Recognitions (LBC), and Android Studio. Though, nearly websites, such as cloud flash, are nowadays proposing SHA programmed transmission dealings in direction to expand operator security[17].

3. Proposed work

3.1. Operator entered keywords

Through deciding that keys shouldn’t be saved with leaflets, however rather should be generated using keywords given by operators, we want to increase security. We improved the standard blowfish technique to produce encryption keys from user-provided keywords, enabling it to encode and decode any kind of folder (typescript, image), by way of top-secret code sequences cannot be castoff as symmetric encoding keys, necessitating some kind of precise transformation[18,19]. By means of Cryptool 2.0, the yield of the cypher will be evaluated.

a) Key production: stock keyword as an organizer in UTF-16 arrangement, blowfish Vault then customs this categorizer.

b) Key folder: declaim the keyword from the listed key categorizer. Yield the extent of the top-secret expression or an undesirable worth if there was a fault.

c) Policy self-governing 32-bit numeral operation.

3.2. Evaluation parameter

Hardness of the key

Hardness of information is understood to be the catalogue of statistics. Hardness is calculated in terms of moments per letter. The numbers in the current surround can be viewed as a message basis from the perspective of information viewpoint. About examine the possibilities of the improper dispersal in direction to calculate the measurements. It is anticipated that the numerous infrastructures (writing in the manuscript or text) will all be moved over the immoral with a constant probability and will be stochastically unbiased of all together.

In **Figure 1**, Planned Encoding Decoding Procedures are applied.

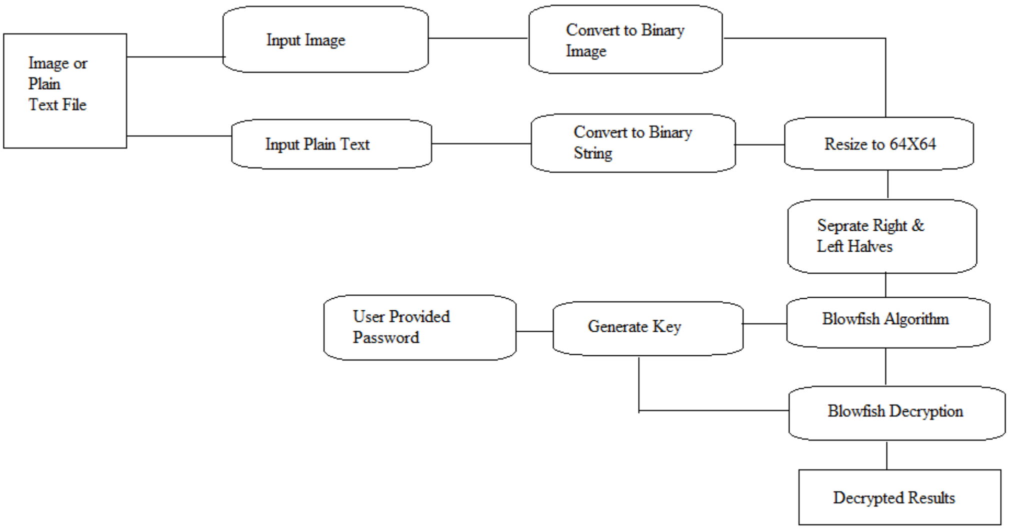

Figure 1. Planned encoding decoding procedures.

3.3. Tools used

3.3.1. Ubuntu

Ubuntu is an open-source operational structure based on Unix OS with an additional adjustable Graphical User Interface. It is widely used in colleges and research associations.

3.3.2. Virtual box

Virtual Box is undefended basis package and it is simply available and attains as a computer-generated device. The computer-generated container lodger embellishments are software design packages which can be hosted inside maintained guest agendas to improve their implementation and to provide additional grouping and communication through the host background.

3.3.3. GCC compiler

GCC is a key component of the GNU toolchain, GNU C++ compiler is used for compilation.

4. Results and discussion

Validating truthfulness of data:

Table 1. Confirming truthfulness.

Files names before encryption	Original file size (MB)	Files names after encryption	Encrypted file size (MB)	Files names after decryption	Size after decryption (MB)
F-1	710	F-1e	710.8	F-1d	710
F-2	945	F-2e	945.9	F-2d	945
F-3	1045	F-3e	1046.5	F-3d	1045
F-4	1245	F-4e	1247.8	F-4d	1245
F-5	1450	F-5e	1452.6	F-5d	1450

According to **Figure 2** and **Table 1**, all the Encrypted files have different sizes as the original ones.

According to **Figure 3**, all the decrypted files have the same sizes as the original ones.

As seen in **Table 3**, **Figure 5**, modified blowfish offers a larger entropy value when compared to the currently used encryption methods (DES, 3-DES and AES).

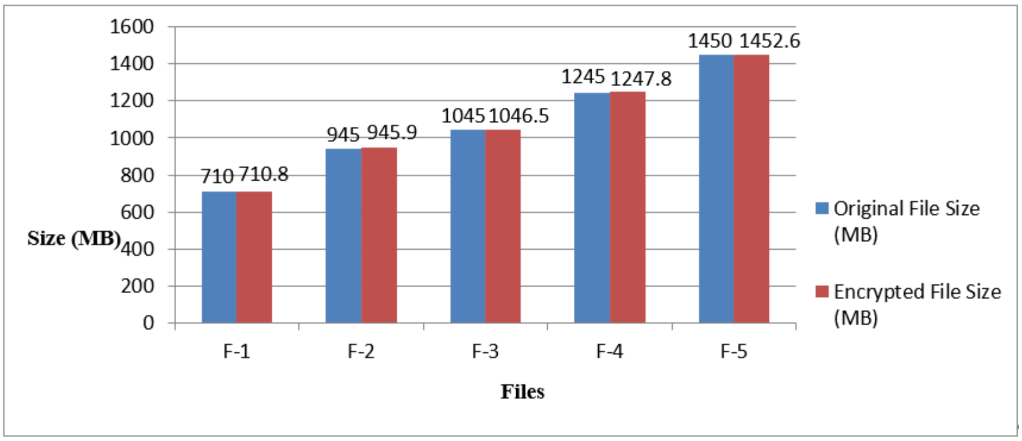

Figure 2. Encrypted vs. original file sizes (MB).

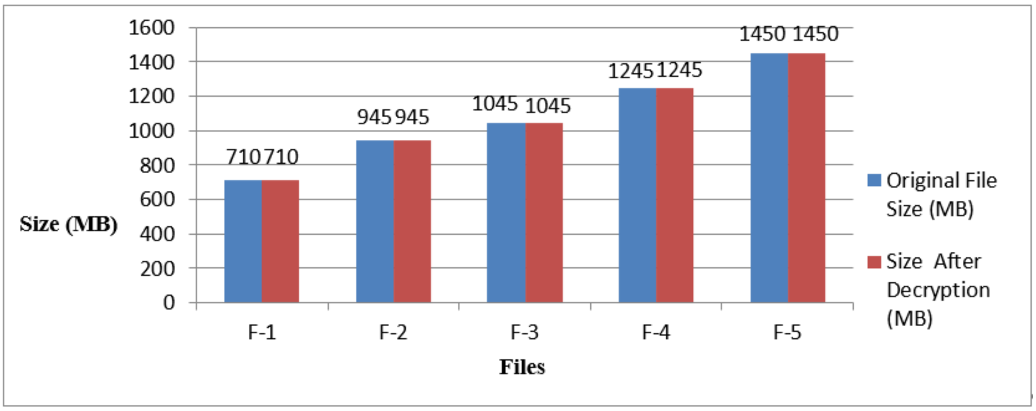

Figure 3. Decrypted vs. original file sizes (MB).

Computing firmness of the key:

Table 2. Cryptool examination of encrypted files.

Files names after encryption	Encrypted files size (MB)	Hardness of key
F-1e	710.8	7.85
F-2e	945.9	7.78
F-3e	1046.5	7.67
F-4e	1247.8	7.61
F-5e	1452.6	7.58

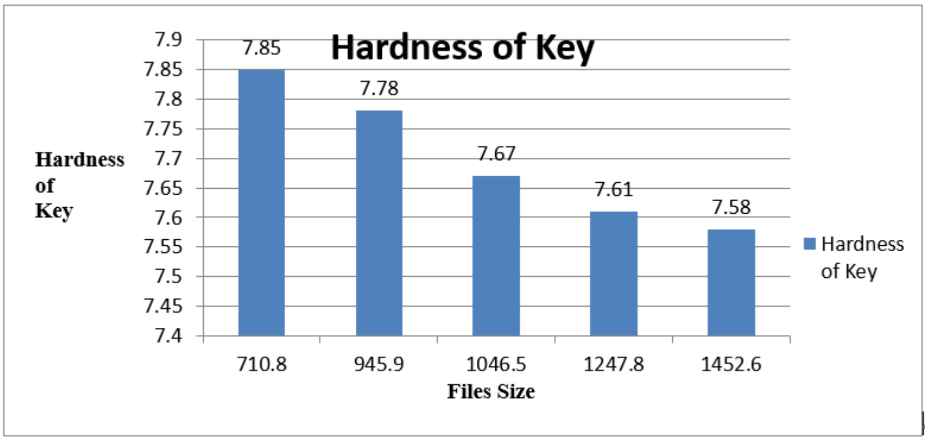

Figure 4. Hardness of key of encrypted files.

Assessment with present encryption procedures:

Table 3. Cryptool investigation of cryptography procedures.

Encryption method	Hardness of the key
Data Encryption Standard (DES)	7.82
3-Data Encryption Standard (3-DES)	7.81
Advance Encryption System (AES)	6.47
Modified Blowfish	7.85

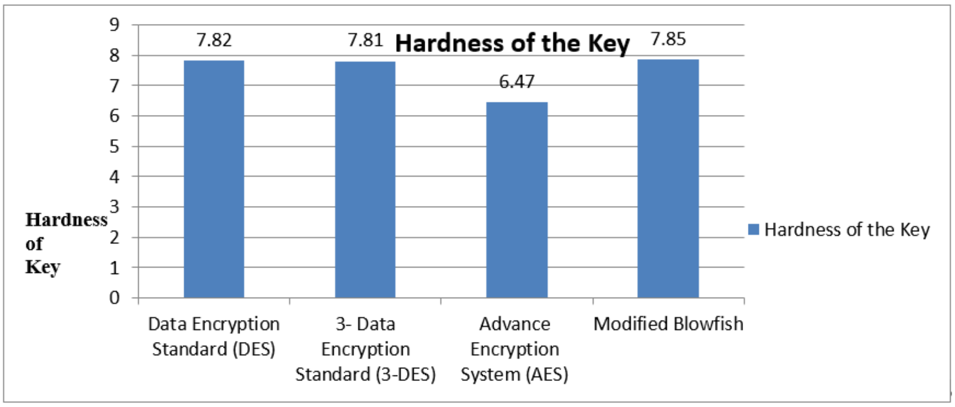

Figure 5. Cryptool investigation of cryptography procedures.

5. Conclusion and future scope

Presently, Blowfish is reflected doubtful for a number of applications. So, it was essential to toughen the procedure’s security through comprising novel security essentials in direction to create it further useful and suitable for communication systems. Blowfish has been transformed so that, once matched to existing schemes, it supports typescript, image, and mass media archives and has a platform-independent strategy. An improved sort of the blowfish procedure is used for encoding and decoding. The projected better-quality blowfish deals superior security than present encryption approaches due to its advanced hardness of the key, safeguarding that the leaflets cannot be delivered among the cradle and the receiver. To propose roughly slight attentions for the programming and deciphering phases, assessment of enhanced Blowfish and present cryptographic methods is showed. Steadfastness of the key (entropy) is a mark of the rebuilt blowfish process’s capability. Blowfish is suitable for IoT and is speedy, memory-saving, safe, and effective. The planned Blowfish procedure uses a single key for all of its expansion. The present procedure’s power can be improved by take on dissimilar keys at each rotation.

Author contributions

Conceptualization, RW and PG; methodology, RW; software, MK; validation, RW, PG and MK; formal analysis, RW; investigation, MK; writing—original draft preparation, RW; writing—review and editing, RW, MK; visualization, PG; supervision, PG.

Conflict of interest

The authors declare no conflict of interest.

References

1. Kumar N, Thakur J, Kalia A. Performance analysis of symmetric key cryptography algorithms: DES, AES and Blowfish. *An International Journal of Engineering Sciences* 2011; 4: 28–37.

2. Goyal S. A survey on the applications of cryptography. *International Journal of Science and Technology* 2012; 2(3): 352–355.
3. Mathur A. A research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. *International Journal on Computer Science and Engineering (IJCSE)* 2012; 4(9): 1650–1657.
4. Ismil IA, Galal-Edeen GH, Khattab S, et al. Performance examination of AES encryption algorithm with constant and dynamic rotation. *International Journal of Reviews in Computing* 2012; 12: 18–29.
5. Dave KC, Parmar SK. A review on various most common symmetric encryptions algorithms. *International Journal for Scientific Research & Development* 2013; 1(4): 1015–1018.
6. Pahal R, Kumar V. Efficient implementation of AES. *International Journal of Advanced Research in Computer Science and Software Engineering* 2013; 3(7): 290–295.
7. Rakholiya KR, Kathiriya D. Efficient black-box collision search in cryptanalysis. *Paripex-Indian Journal of Research* 2013; 2(1): 30–31.
8. Sandhu GS, Verma V. Comparing popular symmetric key algorithms using various performance metrics. *International Journal of Advance Research in Computer Science and Management Studies* 2013; 1(7): 394–399.
9. Sumitra. Comparative analysis of AES and DES security algorithms. *International Journal of Scientific and Research Publications* 2013; 3(1): 1–5.
10. Manjesh KN, Karunavathi RK. Secured high throughput implementation of AES Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering* 2013; 3(5): 1193–1198.
11. Lalitha N, Manimegalai P, Muthukumar VP, Santha M. Efficient data hiding by using AES & advance hill cipher algorithm. *International Journal of Research in Computer Applications and Robotics* 2014; 2(1): 1–13.
12. Acharya K, Sajwan M, Bhargava S. Analysis of cryptographic algorithms for network security. *International Journal of Computer Applications Technology and Research* 2014; 3(2): 130–135.
13. Al Hamid HA, Rahman SMM, Hossain MS, et al. A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access* 2017; 5: 22313–22328. doi: 10.1109/ACCESS.2017.2757844
14. Qadir AM, Varol N. A review paper on cryptography. In: 2019 7th International Symposium on Digital Forensics and Security (ISDFS); 10–12 June 2019; Barcelos, Portugal.
15. Gupta RK. A review paper on concepts of cryptography and cryptographic hash function. *European Journal of Molecular & Clinical Medicine* 2020; 7(7): 3397–3408.
16. Verma J, Shahrukh M, Krishna M, Goel R. A critical review on cryptography and hashing algorithm SHA-512. *International Research Journal of Modernization in Engineering Technology and Science* 2021; 3(12): 1760–1764.
17. Oberoi N, Sachdeva S, Garg P, Walia R. Dynamic extraction and analytics of big data from cloud and social media integrated platforms. *Advances in Mathematics: Scientific Journal* 2020; 9(6): 3703–3711. doi: 10.37418/amsj.9.6.48
18. Walia R, Garg P. Cryptography: Analysis of SYN and UDP attacks using wire shark. In: 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST); 17–18 December 2021; Mohali, India.
19. Walia R, Garg P. Key management scheme for cloud integrated Internet of Things. In: 2023 International Conference on Artificial Intelligence and Smart Communication (AISC); 27–29 January 2023; Greater Noida, India. pp. 1067–1071.