Technium Vol. 4, Issue 6 pp.18-28 (2022)
ISSN: 2668-778X
www.techniumscience.com

Survey of Blowfish Algorithm for Cloud

Shamil Ezadeen [1]
alaojanshamil@gmail.com

Auday H. Alwattar [1]
Ahsa.alwattar@uomosul.edu.iq

[1] Computer Science Department, University of Mosul

Abstract. Security is the study of encryption and decryption, data hiding, potential attacks, and performance evaluation. Many algorithms perform this purpose. Blowfish is a symmetric block cipher that uses the Feistel network. Although several works employed the Blowfish algorithm for the security of the cloud, there is still no article that lists previous studies. Cloud computing is the transmission of computer services such as servers, storage, databases, networking, software, analytics, and intelligence through the Internet ("the cloud") in order to provide faster innovation, more flexible resources, and cost savings. The most common issue with cloud computing is information security, privacy, confidentiality, and how the cloud provider ensures these services. This paper includes a survey of most previous works that were concerned with using the Blowfish algorithm in achieving cloud security

Keywords. Blowfish, cloud , security.

1. Introduction:

Encryption is the way to protect valuable information, such as documents, images, or electronic transactions on the Internet, from unwelcome people. Today, this science plays a prominent place among sciences, as its practical applications have diversified to include multiple fields, such as the diplomatic, military, security, commercial, economic, media, banking, and informational fields[20].
Blowfish algorithm (BA) is a symmetric block cipher with a 64-bit block size and variable key lengths from 32 bits up to 448 bits[18].

Cloud computing is the deployment of computer services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet in order to provide faster innovation, more flexible resources, and economies of scale[22]. Cloud computing is becoming more significant, and it is gaining traction in the academic and technical worlds. According to a Gartner survey, Cloud Computing is the first among the top ten most significant technologies, with a bright future for businesses and organizations in the next years[24].

Cloud computing mainly depends on the modern technologies of virtual servers - Virtual Machines, as these technologies allow for ease and flexibility in increasing or decreasing the available resources as needed. This service is offered by companies providing cloud computing services in return for a fee that is determined based on usage[21].

Because vital services are frequently outsourced to a third party, maintaining data security and privacy is more difficult with cloud computing[19]. Although there are numerous advantages to using Cloud Computing, there are also some substantial obstacles. Security is one of the most major impediments to adoption, followed by concerns about compliance, privacy, and legal difficulties [21]. Because Cloud Computing is such a novel computing model, there is a lot of confusion regarding how to ensure security at all levels (e.g., network, host, application, and data) and how to migrate programs to Cloud Computing [20]. Because of this uncertainty, information executives have frequently stated that security is their top concern with Cloud Computing[19].

External data storage, reliance on the "public" internet, lack of control, multi-tenancy, and integration with internal security are all security concerns. The cloud differs from previous technologies in several ways, including its massive scale and the fact that cloud provider resources are completely distributed, diverse, and virtualized. Traditional security procedures like identity, authentication, and authorization are no longer sufficient for cloud computing in its current state[23].

Moving key apps and sensitive data to public cloud settings is a major worry for companies that are expanding their network beyond their data center's management[25]. To allay these fears, a cloud solution provider must ensure that customers retain the same security and privacy controls over their applications and services, demonstrate to customers that their organization is secure and capable of meeting service-level agreements, and demonstrate compliance to auditors[19].

This research paper includes the Abstract, followed by the Introduction, then the Literature Review, and finally, the Conclusion.

2. Literature Review

There are many scholars and researchers who have written on this topic, including Abdelrahman Shawki and Mohamed Qadri Sharouda, where cryptographic algorithms have been proposed to make cloud data more secure and fragile as well as pay attention to security issues and challenges. Comparisons were made between the following algorithms AES, DES, Blowfish and RSA to find the best algorithm to use in cloud computing to make cloud data secure and inaccessible to attackers[1]. So did researchers E.Dinesh & S.M.Ramesh where they presented a research paper providing statistical testing of randomness on Blowfish block blades. where the tests were performed on the parts of the Blowfish algorithm in (ECB) mode with all types of data[2]. Researcher Venkata Koti Reddy Gangireddy et al. also provided performance metrics such as confidentiality, reliability, and other identified resources. With cloud monitoring, processing time is lower and timely data delivery is guaranteed.[3] Researcher Venkata Koti Reddy Gangireddy also presented a paper that converts data into an unintelligible format using the Blowfish cipher system by expanding the input key into several sub-arrays of 4168 bytes. An array P consisting of eighteen 32-bit boxes, along with the S-boxes, are four 32-bit arrays with 256 entries each[4]. In this thesis, researcher Mohamed Khaled ElBeltagy presents double-layer security using Wolfram Mathematica® steganography and encryption techniques on 3D objects. At the first layer, in the encryption part, the data is encrypted using Blowfish technology with a key length of 256-bit. In the second layer, in the steganography part, the LSB . variable a technique was used to embed data in the wrapper object[5]. In this paper, researcher Ashwak Alabaichi introduces the process of security analysis. Security analysis is divided into two phases. The first stage is to check the entire RAF output, including the avalanche text and correlation coefficient. The second stage is to check the quality of the 3D dynamic s-square generated by RAF using the strict collapse criterion and the bit-independence criterion (BIC). In addition, the RAF algorithm is compared with the Blowfish algorithm[6]. As for Reynaldo R. Corpuz, he relied in his research on the (FYS) algorithm, also called (KS), to replace and

modify the S-Box, and the function F was used to improve the BF algorithm to address this problem[7]. Here researcher Reynaldo R. Corpuz introduced the implementation and testing of a modified Blowfish algorithm using the Shuffle algorithm for encryption, decryption, and throughput.This study presented an application of a modified blowfish algorithm in cloud computing, Isabella State University, using the proposed system architecture as well as using an interface that adds security to the shared file through cloud computing[8]. Researchers K.Mohana Prabha and Dr.P.Vidhya Saraswathi have also developed the TH-KBBA mechanism for secure data access. At the registration stage, user information is entered and stored on the server. Then AS checks the user ID and password to select AU and Unauthorized user. Then install AS to CS by creating tickets. The ticket is encrypted using Blowfish cipher with a symmetric key. Then CS decrypts with a symmetric key that are shared by AS. Finally, CS verifies the user ID and provides the required data to CS[9]. Researchers Salma, Rashidah Funke Olanrewaju and others have proposed a structure that encrypts the file using a file of mixed algorithms such as AES (DAES) and Blowfish before serving the file in the cloud. This proposal can solve significant file security risks such as various attacks such as brute force and forced attack because it provides an authentication structure to verify file access from the cloud. Thus if it is used safely, it will provide a great advantage and overcome the disadvantages of security risks[10]. The researcher Shafi'i Muhammad Abdulhamid has also designed an application that ensures that no party can have the same unique identifier and each user must keep the secret of the unique identifier along with the secret key chosen by the user. The unique identifier helps the user to access and decrypt the stored data upon retrieval[11]. Researcher Srinivas Mudepalli also wrote a paper looking at ciphertext retrieval via cloud storage using some effective privacy techniques. To efficiently search ciphertext content, a derivation-based Porter Index and data stored on the cloud was created as an cryptographic model. Here Blowfish cipher and elliptic curve keys are used for secure data transmission[12]. Researchers V.Saranya and K.Kavitha also wrote a paper recommending a Blowfish algorithm aimed at key generation. At first, create the symmetric key for both encryption and decryption. After that, the data is stored correctly and securely by the user. This solution is based on the ABE-based naming system for privacy preservation and the ontology-based trait management system[13]. Researcher Mohaned Abduallah Elshaikh conducted research aimed at evaluating the performance of Blowfish by modifying the structure of the F function. The modified Blowfish will use only two S-boxes in the F function instead of the four used in Blowfish to compare encryption time and security. Encoding time and decoding time were calculated to compare between Blowfish and modified Blowfish[14]. In this paper, Adviti Chauhan and Jyoti Gupta researchers propose a new parallel cipher algorithm, which mixes and mutates from MD5 and Blowfish cipher schemes, which can upgrade security. The MD5-Blowfish hybrid cipher computation is created to overcome the shortcomings of symmetric cryptographic and hash function systems[15]. As well as a study by researcher Ashwak alabaichi, the study includes three phases: Design, implementation and verification In the first phase, 3D Dynamic S-Box, Dynamic P-box and F-Function were designed. The second stage is to implement a key to expand, encrypt and decrypt the data, as for verification, it includes evaluating the output of the new design using a random statistical test and coding analysis[16]. The aim of this research by researchers Vaibhav Poonia and Dr. Narendra Singh Yadav aims to improve and evaluate the Blowfish algorithm based on various parameters such as encryption quality, correlation coefficients, key sensitivity testing, and output file size. The 'f' function is modified by mixing XOR and the addition used in the original algorithm. Four cases are generated and analyzed[17]. The aim of this research by Ashwak alabaichi is to enhance the Blowfish algorithm. The research included three phases, algorithm design, implementation and evaluation. At the design stage, the dynamic 3D S-Box, the Dynamic Flip Box (P-Box), and the Festal (F-Function) function have been improved. The optimization included the integration of a cylindrical coordinate system (CCS) and a dynamic P-Box[18]. In this paper by researchers Rachna Arora and Anshu Parashar Cryptographic algorithms have been proposed to make cloud data secure, fragile, and given attention to security issues and challenges, and comparisons are

made between AES, DES, Blowfish and RSA to find the single best security algorithm, which should be used in computing Cloud to make cloud data secure and not hacked by attackers[20]. This paper by Ashwak alabaichi et al. presents the statistical test of randomness on Blowfish mass blades [21].

Table 1 . The table above shows all the theses and research papers that were previously published r Blowfish algorithm as well as the cloud, which we have collected in this table.

Seq.	Paper title	Paper Authors	year	contribute
1-	Medical image Encryption Employing Blowfish	Abdelrahman Shawki Mohamed Qadri Sharouda	2021	This thesis employs the Blowfish algorithm, which is suited for such situations because it is patented–free and has never been subjected to cryptanalysis since its inception, demonstrating that it provides a high level of security for the protection of patient data. The key size of the Blowfish algorithm employed is 256 bits. After encrypting an X–ray medical image, it appears that it is no longer recognizable, and the human visual system (HVS) was unable to distinguish any aspects of the encrypted image. This demonstrates that the algorithm in use is capable of maintaining patient and hospital confidentiality.
2-	Security aware data transaction using optimized blowfish algorithm in cloud environment	E.Dinesh & S.M.Ramesh	2020	The blowfish algorithm (BA) is used to propose security-aware data transactions in the cloud in this research. To increase the system's security, the proposed approach first checks the user's authentication. The uploaded data is initially separated using a pattern-matching algorithm after the authentication process. After that, BA is used to encrypt the separated data. Finally, the data is encrypted and saved in the cloud at the most appropriate location. This solution is safer since the data is column-separated and optimized in the cloud, making it harder to hack. Because the user cannot recover the document without authentication, this method is highly secure.
3-	Implementation of enhanced blowfish algorithm in cloud environment	Venkata Koti Reddy Gangireddy and etc…	2020	Data security is primarily concerned with safeguarding confidential information on the cloud. This section identifies and specifies performance measures such as confidentiality, authenticity, and other resources. The Cloud monitor reduces processing time and ensures that data is delivered on time. The Enhanced Blowfish Algorithm is a meta heuristic algorithm in which the optimal key is chosen. More security is achieved with the suggested Enhanced Blowfish Algorithm.
4-	Implementation of enhanced blowfish algorithm	Venkata Koti Reddy Gangireddy and….etc	2019	The main focus of this study is on converting data into an incomprehensible format using the blowfish encryption method. Key-expansion The input key is divided into many sub arrays, totaling 4168 bytes, at this phase. The P array

	in cloud environment			is made up of eighteen 32-bit boxes, while the S-boxes are made up of four 32-bit arrays with 256 items each. The initial 32 bits of the key are XORed with P1 in the next phase (the first 32-bit box in the P-array). The second 32 bits of the key are XORed with P2, and so on until all 448 bits are used. F function and data encryption It sends four 32-bit S-boxes, each with 256 entries apiece. The underlying 32 bit left halves are partitioned in the Enhanced blowfish approach.
5-	StegoCrypt3D: 3D Object and Blowfish	Mohamed Khaled ElBeltagy	2019	In this thesis, steganography and cryptography techniques were used to accomplish double layer security on 3D objects in Wolfram Mathematica®. Data is encrypted using the Blowfish technique with a key length of 256 bits in the first layer's cryptography section. The LSB variation technique was used to embed the data in the cover object in the second layer, in the steganography component. This algorithm was created using Wolfram Mathematica® code. When the numerical findings were compared to those of other similar works that used a similar technique but used a different encrypting algorithm, the numerical results showed that the values were the most significant.
6-	Evaluation of a dynamic 3D S-box based on cylindrical corrdinate system for Blowfish algorithm.	Ashwak Alabaichi	2018	The process of security analysis is carried out in this work. There are two steps to the security analysis. The first step is to double-check the RAF's whole output, including the Avalanche text and correlation coefficient. The quality of the dynamic 3D s-box formed by RAF is checked in the second step using the rigorous avalanche criterion and the bit independence criterion (BIC). In addition, the Blowfish algorithm and the RAF method are contrasted.
7-	A modified Approach of Blowfish Algorithm Based On S-Box Permutation using Shuffle Algorithm.	Reynaldo R. Corpuz……etc	2018	(FYS), also known as (KS), was used to replace and modify the S-Box in this paper. To solve this problem, function F was employed to improve the BF method. The modified BF outperforms the original Blowfish(BF) in terms of encryption, decoding, and throughput, according to the results. It also suggests that modifying the BF algorithm with the Shell algorithm is a good idea because it enhances the BF method's performance by reducing processing time.
8-	Using A Modified Approach Of Blowfish Algorithm For Data Security	Reynaldo R. Corpuz……etc	2018	The Shuffle method was used to test a modified Blowfish algorithm for encryption, decryption, and throughput in this paper.This research demonstrated a use of the modified blowfish method in cloud computing at Isabella State University, with the proposed system

	In Cloud Computing.			architecture and an interface that adds security to the shared file via cloud computing. The application demonstrates that the modified Blowfish method improves file encryption and decryption efficiency in cloud computing. The test was undertaken to determine the modified Blowfish algorithm's quality and efficiency. The results showed that the modified Blowfish method is 440 percent effective in encryption for all files and 308 percent effective in decryption.
9-	Tiger hash kerberos biometric blowfish user authentication for secured data access in cloud	K.Mohana Prabha & Dr.P.Vidhya Saraswathi	2018	The TH-KBBA Mechanism was created to allow for secure data access. User information is entered and kept in the server during the registration step. Then AS checks the user ID and password to see if the user is AU or an unauthorized user. The AS then proves to the CS by generating tickets. The ticket is encrypted with symmetric key blowfish encryption. The CS then decrypts the data using a symmetric key shared by the AS. Finally, the CS confirms the user ID and gives the CS the necessary data. This makes it easier for AU to access cloud data. Using an Amazon access sample dataset, the proposed TH-KBBA Mechanism and existing approaches are evaluated experimentally. The TH-KBBA Mechanism's experimental results show that it improves authentication accuracy, confidentiality, and authentication time.
10-	Enhancing Cloud Data Security using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms	Salma , Rashidah Funke Olanrewaju …..etc	2018	Before presenting the content in the cloud, a structure has been developed that encrypts it using a file from Hybrid algorithms such as AES (DAES) and Blowfish. Because it provides validation Authentication framework for file access from the cloud, this proposal can solve a substantial security risk on the file, such as diverse attacks like brute force and forced assault. As a result, if it is used safely, it will deliver a terrific function while also overcoming security dangers.
11-	Development of Blowfish Encryption Scheme for Secure Data Storage in Public and Commercial Cloud Computing Environment	Shafi'i Muhammad Abdulhamid ….etc	2018	The blowfish algorithm assists the user in generating a unique Id for encrypting messages (m) and retrieving data from the cloud using the same key. The unique Id is utilized for data retrieval as a kind of authentication. The application ensures that no two parties have the same unique identifier, and each user must maintain the unique identifier as well as the secret key chosen by the user confidential. The unique Id also aids a user in gaining access to stored data and decrypting it once it is retrieved.

12-	An efficient data retrieval approach using blowfish encryption on cloud	Srinivas Mudepalli….etc	2017	This research looks into ciphertext retrieval through cloud storage, as well as some effective privacy techniques. Porter stemming-based index has been created to effectively search ciphertext content, and the data has been stored in encrypted form on the cloud. Here For safe data transmission, Blowfish encryption and elliptic curve keys are used. When an authorized user sends a query to the cloud, the relevant files are encrypted and provided to the user. The user then provides the private key for the decryption process, and the files are decrypted by blowfish. When compared to traditional methods, our proposed solution outperforms them in terms of retrieval efficiency and time consumption.
13-	A Modified Blowfish Algorithm for Improving the Cloud Security	V.Saranya1 and K.Kavitha	2017	The blowfish algorithm is recommended in this study for key generation. To begin, construct a symmetric key that can be used for both encryption and decryption. The data is then properly and securely kept by the user. This method is built on an ontology-based attribute management scheme and a privacy-preserving ABE-based name strategy. The ontology-based method allows for customizable attribute management while also reducing time consumption, storage costs, and increasing throughput. The ABE-based naming system provides the same high security level as CP-ABE in terms of security and privacy, but with attribute anonymity protection for policy privacy and adjustable attribute ranks. Experiments showed that the proposed methodology scored higher than the existing ABE technique in terms of encryption, efficiency, performance, and security.
14-	Performance Evaluation of Blowfish Encryption Algorithm	Mohaned Abduallah Elshaikh	2017	The goal of this study is to see how well Blowfish performs by changing the structure of the F function. To compare encryption time and security, the modified Blowfish will use only two S-boxes in the F function instead of the four used in Blowfish. Encryption and decryption times were calculated to compare Blowfish to modified Blowfish, with the findings indicating that the modified Blowfish performs better. The results of the Diehard Battery, which was used to test randomness, demonstrate that Blowfish algorithm has a higher level of security than the modified Blowfish, hence it is better to encrypt data and applications that require a high level of security with Blowfish algorithm.

15-	A Novel Technique of Cloud Security Based on Hybrid Encryption by Blowfish and MD5	Adviti Chauhan & Jyoti Gupta	2017	This study offers a new parallel cryptographic algorithm that improves security by combining and altering MD5 and Blowfish encryption algorithms. To overcome the shortcomings of symmetric block cryptography and hash function techniques, a hybrid MD5-Blowfish cryptographic calculation was developed. The suggested technique's performance is compared to the hybrid RSA and MD5 algorithm on the basis of two parameters: storage and time. In comparison to the hybrid RSA-MD5 algorithm, the hybrid Blowfish-MD5 algorithm takes less time to execute. In compared to the generated parameter output, simulation results show more efficient results (i.e., storage and time). Because the blowfish algorithm encrypts data by generating S-boxes, and because of their parallel processing, the execution time is reduced, the execution becomes faster. As a result, blowfish-MD5 has shown to be more efficient than the previous approach.
16-	A Dynamic 3D S-Box Based On Cylindrical Coordinate System For Blowfish Algorithm.	Ashwak alabaichi	2015	Design, implementation, and verification were the three phases of the research. The 3D Dynamic S-Box, Dynamic P-Box, and F-Function were designed in the initial phase. The execution of key expansion, data encryption, and decryption is the second stage
17-	Analysis of modified Blowfish Algorithm in different cases with various parameters	Vaibhav Poonia & Dr. Narendra Singh Yadav	2015	The goal of this work is to improve and assess the Blowfish method using various metrics such as encryption quality, correlation coefficients, key sensitivity testing, and output file size. By combining the XOR and addition utilized in the original technique, the 'f' function is updated. Four different scenarios are generated and assessed. The findings of all of the tests conducted on these scenarios all point to the same conclusion: the updated algorithm's security in various cases makes the original Blowfish method more compact and secure than before.
18-	An enhanced blowfish algorithm based on cylindrical coordinate system and dynamic permutation box	Ashwak mahmood alabaichi	2014	The goal of this study is to improve the BA's ability to deal with these issues. Algorithm design, implementation, and evaluation were the three steps of the study. A dynamic 3D S-Box, a dynamic permutation box (P-Box), and a Festal Function (F-Function) were improved during the design phase. Integration of the Cylindrical Coordinate System (CCS) and dynamic P-Box was part of the enhancement. The Ramlan Ashwak Faudziah (RAF) algorithm is the upgraded BA. Performing key

				expansion, data encryption, and data decryption were all part of the implementation process. The algorithm was tested in terms of memory and security throughout the evaluation phase.
19-	Secure User Data in Cloud Computing Using Encryption Algorithms	Rachna Arora , Anshu Parashar	2013	In this paper, encryption algorithms were proposed to make cloud data secure, and vulnerable, and to give concern to security issues, challenges, and comparisons between AES, DES, Blowfish, and RSA algorithms to find the best security algorithm that should be used in cloud computing to keep cloud data secure and not be hacked by attackers. Encryption algorithms are vital for cloud data security, and a study of several parameters used in algorithms revealed that the AES algorithm takes the least amount of time to process cloud data. The Blowfish algorithm uses the least amount of memory. The DES algorithm takes the shortest amount of time to encrypt data. RSA uses the most memory and takes the longest to encrypt.
20-	Randomness Analysis On Blowfish Block Cipher.	Ashwak alabaichi and…..etc	2013	The statistical test of randomness on the Blowfish Block Cipher is presented in this study. The results also revealed that the ECB mode of the Blowfish method is ineffective for images and text files with long sequences of identical bytes.

3. Conclusion

In this research, all the theses and research papers dealing with the bloating fish algorithm and its relationship to cloud computing were collected, as no research paper was previously published that collects all previous studies on this topic, where a table was made that summarizes all these works and provides a brief summary of each work. In our future work we will modify the Blowfish algorithm to suit the security of cloud computing.

References

[1] Sharouda, A. S. M. Q. (2021). Medical Image Encryption Employing Blowfish.

[2] Dinesh, E., & Ramesh, S. M. (2021). Security aware data transaction using optimized blowfish algorithm in cloud environment. Journal of Circuits, Systems and Computers, 30(01), 2150004.

[3] Gangireddy, V. K. R., Kannan, S., & Subburathinam, K. (2021). Implementation of enhanced blowfish algorithm in cloud environment. Journal of Ambient Intelligence and Humanized Computing, 12(3), 3999-4005.

[4] ElBeltagy, M. K. (2019). StegoCrypt3D: 3D Object and Blowfish.

[5] ALabaichi, A. (2018). Evaluation of A dynamic 3D S-Box based on Cylindrical Coordinate System for Blowfish Algorithm. Life Science Journal, 15(10).

[6]Sadiq, N. A., Abdullahi, M., Rana, N., Chiroma, H., & Dada, E. G. (2018). Development of blowfish encryption scheme for secure data storage in public and commercial cloud computing environment. i-Manag J Cloud Comput, 5, 1.

[7]Olanrewaju, R. F., Abdullah, K., & Darwis, H. (2018, November). Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms. In 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT) (pp. 18-23). IEEE.

[8]Corpuz, R. R., Gerardo, B. D., & Medina, R. P. (2018, December). Using a modified approach of blowfish algorithm for data security in cloud computing. In Proceedings of the 6th International Conference on Information Technology: IoT and Smart City (pp. 157-162).

[9]Corpuz, R. R., Gerardo, B. D., & Medina, R. P. (2018, December). A modified approach of Blowfish algorithm based on S-box permutation using shuffle algorithm. In Proceedings of the 2018 VII International Conference on Network, Communication and Computing (pp. 140-145).

[10]Olanrewaju, R. F., Abdullah, K., & Darwis, H. (2018, November). Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms. In 2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT) (pp. 18-23). IEEE.

[11] Prabha, K. M., & Saraswathi, P. V. (2018, August). Tiger hash kerberos biometric blowfish user authentication for secured data access in cloud. In 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on (pp. 145-151). IEEE.

[12]Mudepalli, S., Rao, V. S., & Kumar, R. K. (2017, June). An efficient data retrieval approach using blowfish encryption on cloud ciphertext retrieval in cloud computing. In 2017 International conference on intelligent computing and control systems (ICICCS) (pp. 267-271). IEEE.

[13] Elshaikh, M. A. (2017). Performance Evaluation of Blowfish Encryption Algorithm (Doctoral dissertation, Sudan University of Science & Technology).

[14]Chauhan, A., & Gupta, J. (2017, September). A novel technique of cloud security based on hybrid encryption by Blowfish and MD5. In 2017 4th International conference on signal processing, computing and control (ISPCC) (pp. 349-355). IEEE.

[15] Saranya, V., & Kavitha, K. (2017). A modified blowfish algorithm for improving the cloud security. Elsiyum J, 4(3), 1-6.

[16] Alabaichi, A. M. (2015). A dynamic 3D S-box based on cylindrical coordinate system for blowfish algorithm. Indian Journal of Science and Technology, 8(30).

[17] Poonia, V., & Yadav, N. S. (2015, January). Analysis of modified Blowfish Algorithm in different cases with various parameters. In 2015 International Conference on Advanced Computing and Communication Systems (pp. 1-5). IEEE.

[18] Alabaichi, A. M. (2014). An enhanced Blowfish Algorithm based on cylindrical coordinate system and dynamic permutation box (Doctoral dissertation, Universiti Utara Malaysia).

[19] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of internet services and applications, 4(1), 1-13.

[20] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487

[21] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

[22] Fontaine, C., & Galand, F. (2007). A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security, 2007, 1-10.

[23] Qarkaxhija, J. (2020). Using Cloud Computing as an Infrastructure Case Study-Microsoft Azure.

[24] Basi, H. (2021). Improving the Availability of the Education Sector in Iraq over the Cloud Computing.

[25] Ali, A. I. M. (2021). E-Governance System Challenges and Cloud Computing Benefits in E-Governance.