Dr. K.Kavitha, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 219-229
ISSN: 2321-8363
Impact Factor: 5.515

Performance Analysis of Modified Blowfish Algorithm towards Cloud Security

Dr. K.Kavitha
Assistant Professor, Department of Computer Science, Mother Teresa Women's University, Kodaikanal

Abstract— The accessing of sensitive information from the cloud database is done through the internet. To avoid the hacking number of privacy preservation mechanisms such as cryptography, attribute-based models are employed. The existing systems suffer from the linear increase in time complexity with respect to increasing in cipher text size, lack of scalability, improper security. To overwhelm this difficulty, a novel Blowfish algorithm is introduced in this paper. Advanced Encryption Standard (AES) technique used to encrypt and decrypts data to provide an enhanced security. This work provides better encryption rate in software, not providing effective cryptanalysis, provides security and flexibility and same key used for both encryption and decryption process. Whenever the user download the data, the key is essential to match for encryption key. If the key is unmatched the user can't download the data. The experimental results evaluate the performance of the proposed blowfish algorithm in terms of security, efficiency, performance values and encryption.

Index Terms— information-centric networking, attribute-based encryption, blowfish algorithm, advanced encryption technique.

I. INTRODUCTION

IN existing networking schemes, the network routing protocols provided from the following server that has to locate and connect, and access some information content. The position of the server associate tightly with the information is the required results. Therefore, the important factors of the network are to the connection status and that overall network is centered between the content providers and content consumers. The focus of the ICN architecture changed to consumer-content connections from the consumer-server connections. Thus, identify the authentic content copies from the network changes, and identified the content owner's address. From where the content locates are not known by the consumers, i.e. the IP statement of the content owner. Then, the consumer can be directed by using the content name from a content copy. Using network caches, the content owners published the content owing to the network since the network has copied and stored documents. Therefore, the consumer obtained efficiently from the contents being enabled. This is due to an ICN architecture because the consumers and content owners are not directly connected.

The distributed network collections are not accessed the content owners because have no control. Therefore, suggested several frameworks for admittance control to the content have been enforced. Authenticate each content consumer in the network, supreme of them required secure communication channels or additional authorities. In the traditional control schemes, produce sound schemes, high reliance, and inefficient schemes.

ISSN: 2321-8363
Impact Factor: 5.515

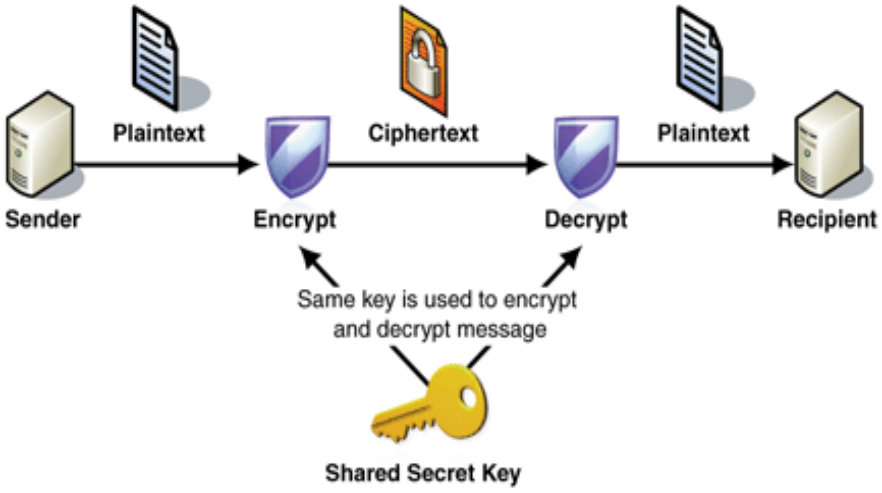

Fig 1 System Architecture

In this work, a novel attribute based access control approach is proposed for ICN naming scheme. There are classified into two levels of the proposed scheme. They are the upper level and lower level. In the first upper-level, addressed the attribute management problem. Then, managed the distributed attributes in the ICN network by using ontology-based attribute management solution attribute management solution. Paralleled with prevailing approaches, more efficiently synchronized the different authority's attributes. Does not obtain the request contents from other authorities, their attribute keys are negotiated. The second level of the planned method is the lower level that suggests ABE-based naming scheme and it is motivated. Trusted Third Party (TTP) with their real identities were utilized in each network entity for assigned a set of attributes. According to their content names replaced with the contents required by the access control policy. Besides, content access policies attained from the privacy-preservation. They distributed in public domain from the ICN data and is greatly improved the privacy protection by this features. Previously retrieving the data content, the encrypted names used to identify the user eligibility of the contents. Figure 1 represents the system architecture for secure sharing. The planned scheme qualifies the support for attribute management ontology. According to that attributes, the different privileges are associated and the rank attributes are provided. The major involvement of the investigation work listed as follows,

- In distributed deployment, the attribute management reduced the price of the planned ontology-based attribute management,
- In the actual world, the data access policy have constructed from the enabled attribute rankings that access control policies have flexible attribute combination operations in the projected schemes and confidentially preserved the content access policy. If collude composed that cannot derive the data access policies by the ineligible consumers.
- Then, combined the privacy preserving access policy and flexible attribute management solution create a naming scheme called ICN network,
- A potential consumer access the content efficiently with eligibility and expressively reduces the provided from the communication and computation overhead.

The content privacy and content are never addressed in the access control that focuses on the security and efficiency of these ICN solutions. The needs of the ICN are supported by the suggested independent access control system. Through a Relaying Party (RP) component, the ICN structure connected to this system. Then the consumer's credentials enforced from the policies and access policies created from the Access Control Provider (ACP) in additional to that. It requires abundant new network interactions because the ICN systems obtain from incorporates access control systems. This scheme is able to produce high security and required files. Based on this description, a novel improving and featuring matching method known as the Adaptive matching framework is designed to improve the performance.

The remaining sections of this paper are structuralized as follows: Section II reviews some of the existing works related to cloud security and significance in attribute based encryption technique. Section III provides the detailed description of the proposed Blowfish algorithm for improving privacy and security in the ABE technique. Section IV benevolences the comparative investigation of the future with the existing technique. Lastly, concluded the overall process of the proposed section in Section V.

ISSN: 2321-8363
Impact Factor: 5.515

II. RELATED WORKS

This segment deals with the mechanism connected to the robust cloud environment for upload and download the files and to augment the presentation of the ABE technique.

Arora, et al. [1]surveyed the cloud computing security, the mechanisms and challenges. The user data in the cloud environment. It described numerous safety problems during transformation and listed some solutions to overcome. They studied some encryption procedures such as AES and DES, blowfish and RSA for providing the security to the cloud data. Then compared the evaluation performance of the encryption algorithms. It has the big issue in the confidentiality defense and data security.

Lai, et al. [2]recommended the Attribute based encryption (ABE) technique for certified that the outsourced decryption processes. This technique efficiently proved that transformation of the outsourced data has been verified. They applied concrete ABE scheme with verifiable subcontracted decryption for obtaining the secure and verified data. The proposed technique does not trust the random oracles. They produced heavy computational cost and increased cipher text size.

Hur [3]implemented a chipertext-policy attribute based encryption technique for secured data sharing. This process resolved two major problems in data sharing system. They are removed the key escrow difficult during key generation and implemented user revocation for access on each attribute level. This method provides an alternative solution for data sharing scenarios because of the decryption and revocation. Therefore, the proposed outline achieved fine grained pieces of informations admittance control in data sharing system. The effectiveness of the method was not satisfied.

Kaur and Mahajan [4]proposed four different Encryption algorithm improved the security level of records in the cloud. The AES, DES, and Blowfish algorithms were symmetric key algorithms, which utilized the single key for both encryption and decryption whereas RSA was an asymmetric key algorithm, which utilized the public key cryptography. The proposed work does not require any third party to encrypt the data on client side. Every bit of the data read and write through an encryption process. The user authorized by password to access the data in the cloud. The proposed encryption keys were generated instantly and it was deposited in the cloud. The user could select the encryption algorithm needed the service.

Li, et al. [5]implementedDekey approach for secure the deduplication process with high proficient and consistent key management system. The Ramp secret sharing scheme used in the Dekey approach for network overhead problem of regular upload and download operations. It needed more memory space for storage and high bandwidth.

Fernandes, et al. [6]analyzed the cloud security issues and challenges. This reviewed the comprehensive problems of threats, attacks, taxonomy classification and vulnerabilities. This survey results utilized for coming directions and resolved challenges.

Chu, et al. [7]analyzed the cloud storage for sharing a data with scalable way suggested a key aggregate cryptosystem (KAC). This technique provided high security rather than existing because most powerful decryption key utilized for multiple cipher texts without increased its size. They required more cipher texts classes that were the major effects.

Li, et al. [8]hired a hybrid cloud approach to achieve the secured authorize deduplication. In this work, insider and outsider attacks were avoided and effective results obtained. It is the minimal overhead of the secured duplicate checks and it's compared with network transfer and convergent encryption technique. They provide high communication cost.

Wang, et al. [9] projected a Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE) system in the cloud computing was provided efficient and secured access process. From the data users and owners, the computation overhead and resource constrained was reduced effectively. This framework enhanced to ECCP-CABE for access different attribute domains produced high efficiency. The foremost problems in this technique improper security. Wang, et al. [10] recommended the confidentiality protective mechanism for achieved high efficient user revocation in the shared cloud data. Inspecting the reliability of the mutual data in the cloud environment the author recommended the Homomorphic Authenticable Ring Signature (HARS) scheme. In this approach, the signer in the each block of mutual data was kept confidential to the group. The Third Party Auditor (TPA) acted as the semi trusted TPA and verified.The proposed TPA has detected the despoiled wedges presented in the shared data, which were suitable for public auditing. The ring autograph was generated by the group members, which enclosed three algorithms such as KeyGen, RingSign and RingVerify. The KeyGen algorithm was generated both community key and remote key. In RingSign algorithm, the operator in the cluster was signed on the block with either private key or the group member's public keyThe TPA improved the proficiency of verification through batch auditing process.

Liu, et al. [11] introduced a new mechanism, namely, Ciphertext –PolicyAttribute Based Signcryption (CP-ABSC) technique for fine grained access control and secured sharing of signcrypted data. The main intention of this paper was to provide authenticity, anonymity, unforgeability, confidentiality and collusion resistance. However, it has the foremost weaknesses of increased computational complexity and execution time.

Selvamani and Jayanthi [12] surveyed about various isolation and security issues occurred during public auditing in the cloud. In suggested work, the data and the user's traceability were supported based on the signature mechanism. The multiple auditing tasks has performed simultaneously and the proposed TPA was spotted the data error location to the user. The user sent the

ISSN: 2321-8363
Impact Factor: 5.515

request to the TPA and the TPA sent the auditing challenge to the Cloud Server (CS). The CS generated the proof based on the verification of the signature and passed to the TPA. The TPA was validated the auditing proof and the report was sent to the user.
Almorsy, et al. [13] analysed the cloud computing security issues and traditional challenges. The cloud models weak points were identified and highlighted their root cause for each weak points. This helped security vendors, cloud providers and also researchers for identified the existing problems.
Sun, et al. [14]presented scalable fine grained search authorization by using an attribute-based keyword search scheme (ABK-UR) for achieved high efficient user revocation. This scheme utilized multiple data users, multiple data contributors and less computational time and secured for chosen-keyword attack. Very big issues not supported the Boolean functions and computation.
Pancholi and Patel [15]proposed the symmetric cryptographic algorithm known as Advanced Encryption Standard (AES) for the security of data. The proposed AES was used to decrypt the confidential data stored in the cloud. The encrypted data blocks were outsourced into the cloud. The receiver requested the user to access the cloud data and decrypted the message through the same secret key to obtain the original information. The AES algorithm has the high level of security because it utilized the 128, 192 or 252 bit keys. The user data was divided into the number of blocks and broadcast into the cloud hence, the storage space was reduced through this proposed algorithm.

III. PROPOSED WORK

This section illustrates the comprehensive explanation of the projected Blowfish algorithm for improving the privacy and security issues in the existing attribute based encryption (ABE) technique. The overall flow of the projected scheme is shown in Fig 2. At first, the proposed blow fish algorithm used to generate the key for security. Then, generating a symmetric key block used for encryption and decryption of both of them technique. Freely available in the network for anyone to access the blowfish key, any new users cannot access the files. Since, one of the most secure block ciphers is the blowfish key algorithm. In the cryptographic software, benefitted the popularity has the contribution of this work and securely stored the file in the cloud environment. By its name, the consumer can get the content if they need this file. If they want the content, then process this way for getting the required file. To decrypt the name by used the assigned attributes.

The random data-encrypting key protected in the name by getting from the hidden policy of the name with satisfied his attributes. Using the random key to retrieve the original file from the decryption process taken in the data content. If unauthorized used cannot access the file, then the file has been protected in the proper way. It implied that the consumer is not allowed to access the original file due to the consumer cannot effectively decrypt the content name. Thus, the unauthorized user cannot download the content because does not have rights to decrypt the content.

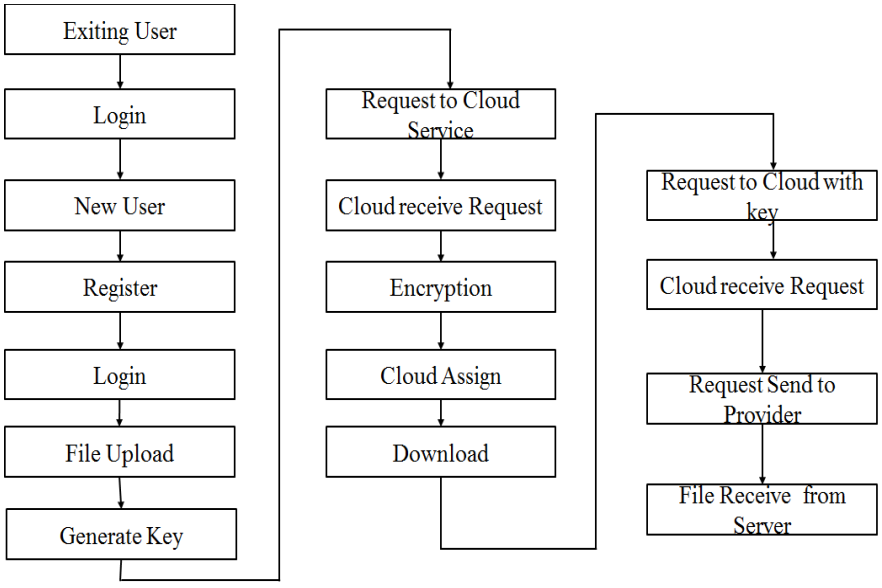

Fig 2. Overall flow of the proposed system

ISSN: 2321-8363
Impact Factor: 5.515

The user login process can perform under two categorize section that authorized and unauthorized users.

Fig 3. Attribute Based Access Control for ICN

If the authorized user can access the file by simply login the page with the corresponding user identity number and password are required to get the access control of the attribute for ICN in the cloud environment. If the user is new means, the registration process held on the login page and the user will register their own information into the database. After that get the user id and password to access the database. Then, displayed login page for entering the corresponding user id and password. Then, the file will be stored in a proper way. Fig 3 shows the attribute based access control for ICN. It shows four important processes for uploading the files. They are the secret key, request cloud server, the key to file and upload. These are the process involved to upload the new user file. The file upload based on the user's condition. The file can be upload into the cloud environment by generating a secured key for accessing only authorized users.

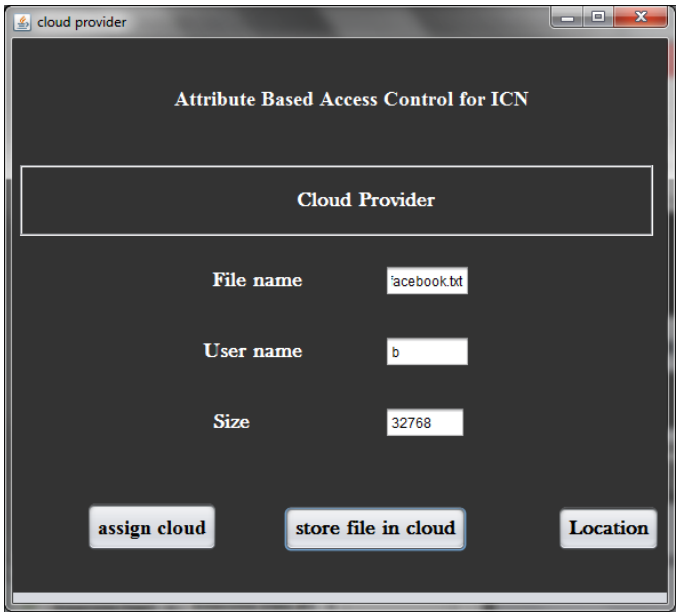

Fig 4 Cloud Provider

ISSN: 2321-8363
Impact Factor: 5.515

The data can be uploaded related to the certain choosing of cloud providers to the users. Cloud service provider stores data and acts as a main component in the system. The highest detached cloud service providers are to hide the location details of the virtual servers from the users. Fig 4 shows the cloud service provider. They get the related key from the cloud service provider and then access to secure store and transmit the required files. Then, secure the data in the cloud that includes the three important following stages:

- Key Generation
- Encryption
- Decryption

A. Key Generation

The key generation process based on the Blowfish algorithm creates a secure key for both encoding and decoding process are used. Blowfish is a symmetric block cipher that can effectively use for safeguarding the data and same key used for both encryption and decryption function. Benefits of using blowfish algorithm,

- Large blocks data are manipulated,
- 64-bit block size,
- Scalable key from 32 bits to least 256 bits,
- Efficient algorithm,
- Perform simple operations.

Hence, Blowfish algorithm used in this proposed work. It is also called variable length key block cipher. This is suitable for many applications because the key does not change and is faster than most encryption algorithms.

B. Encryption

After providing the access control, the Advanced Encryption Standard (AES) mechanism is implemented to encode the data, which is a symmetric encryption algorithm that has a key length of 128 bits. The main reason for using this technique is, the cloud users can decide their needed services. It has some major advantages that include,

- It has the increased setup time and better key agility,
- Required minimum amount of memory and can support any key size as well as block size,
- Provided high performance.

C. Decryption

The development of renovating the cryptograph text into natural text format is termed as decryption. This step is executed by the user who has the decryption authorities. The encrypted data is decrypted by the user by implementing the AES decryption mechanism. It is defined as the reverse process of inverse sub bytes, inverse shift rows, and inverse mix columns and inverse round operations, which are performed to get the original data. Figure 5 shows the get access from the cloud service provider to access the file that can choose.

Dr. K.Kavitha, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 219-229
ISSN: 2321-8363
Impact Factor: 5.515

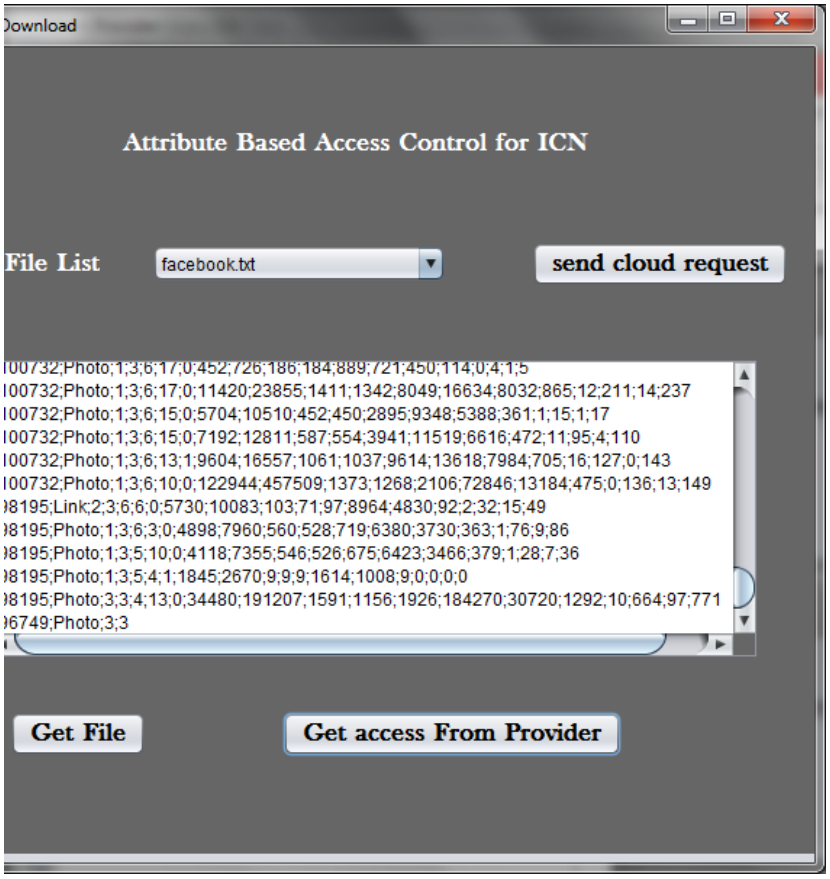

Fig 5 Access from Cloud Provider

IV. PERFORMANCE ANALYSIS

This section presents the results of the proposed blow fish algorithm. Here, the results are analyzed and evaluated in terms of efficiency, security, and encryption process and performance results. To implement this system, a Net Beans (JAVA) simulation tool is utilized in this work. It is a high-level visualization tool that provides a powerful support for both encryption and decryption techniques.

A. Performance Review of the Proposed System

Performance analysis is defined as the calculating the resources that required by an algorithm to perform its task. This can be calculated by using the required time to perform and complete its task. It performed under the two processes. They are,

- Space complexity,
- Time complexity.

The space complexity is referred in this section for given the space for efficiently worked and time complexity refers to complete the task in particular time. In this work, the proposed blowfish algorithm is compared with the existing Attribute Based Encryption (ABE) technique.

Dr. K.Kavitha, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 219-229
ISSN: 2321-8363
Impact Factor: 5.515

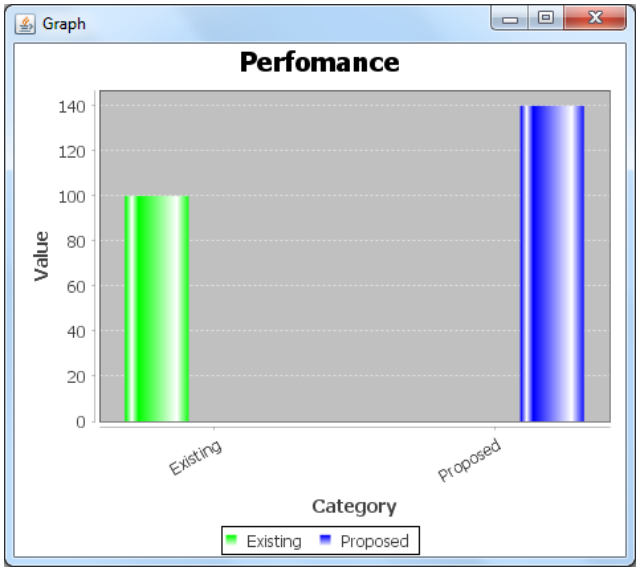

Fig 6 Performance of the Proposed System

Fig 6 shows the performance values of the proposed blowfish algorithm, where the x-axis represents the measures of existing and proposed technique and the y-axis represents the performance values value of the mentioned techniques. From the analysis, it is analyzed that the proposed blowfish algorithm provides the best results by accurately extracting the features. It obtained 100% review of the performance analysis.

B. Efficiency

Typically, efficiency is the basic measures that are widely used to evaluate the performance of the proposed technique. Efficiency is defined as a measure of the output accuracy and is compared with the existing techniques, which is calculated as follows:

$$\text{Efficiency} = \frac{Output\ \ accuracy\ value}{Existing\ accuracy\ value}\ X\ 100 \qquad (1)$$

Fig 7 shows the comparative analysis of the proposed with existing efficiency values. Where the x-axis indicate the existing and proposed techniques and the y-axis indicate the performance values of the efficiency. From the results, it is observed that the proposed Blowfish algorithm provides the better results. This technique provides 100% efficient than existing technique.

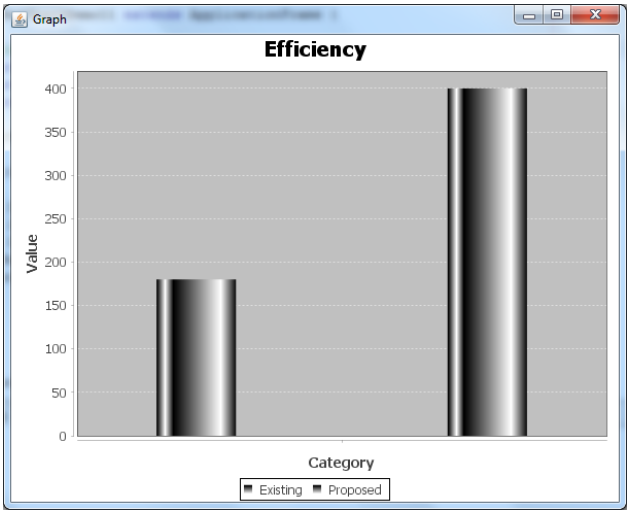

Fig 7. Efficiency of the Proposed System

ISSN: 2321-8363
Impact Factor: 5.515

C. Encrypting Technique

Encryption is the development of transforming of normal plain text into cipher text format. This takes some more time for converting the process that can be compared with the existing ABE technique. Fig 8 shows the presentation of the encryption process for proposed blowfish algorithm and existing ABE technique. The graphical representation of x-axis denotes the compared techniques and the y-axis denotes the performance values of the encryption process. From the analysis, it is analyzed that the proposed blowfish algorithm provides the best results. The proposed work shows that 4 times greater than the existing technique.

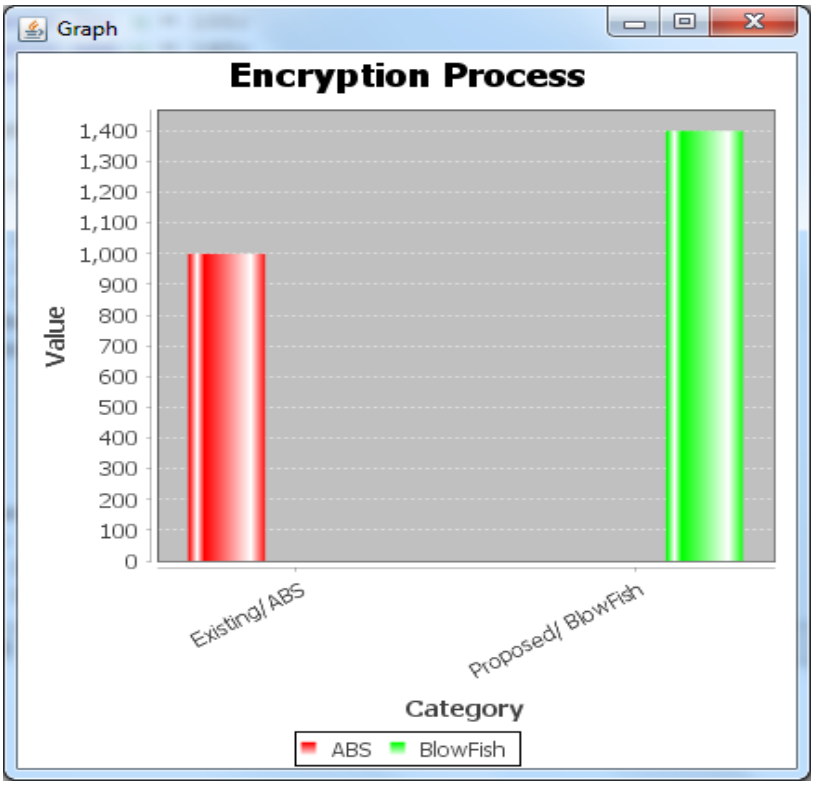

Fig 8 Encryption Process

D. Security Analysis

From the presentation scrutiny of the proposed algorithm is confirmed under the security perspective. The security examination is derived from the information usage of the work. In this criteria, the proposed system security compared with the existing technique. Figure 9 shows the security analysis of the proposed Blowfish algorithm with existing technique. The graphical representation of x-axis symbolizes the existing and proposed technique and the y-axis symbolizes the security analysis values. From the results, it is detected that the projected Blowfish algorithm provides the better results. This proposed algorithm provides 5 times more than the existing technique.

ISSN: 2321-8363
Impact Factor: 5.515

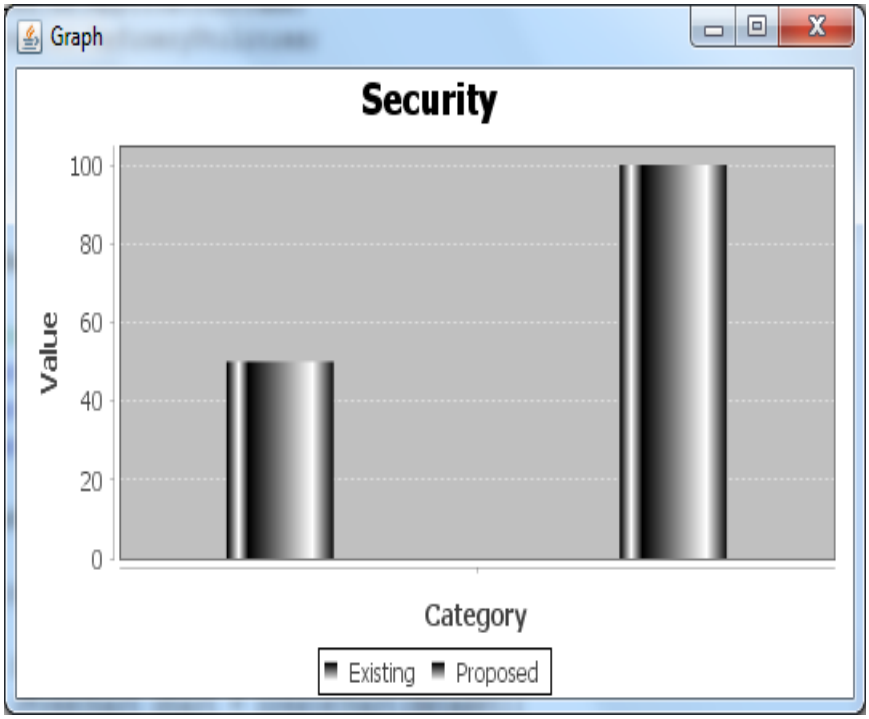

Fig 9. Security Process

V. CONCLUSION AND FUTURE WORK

This paper recommends a blowfish algorithm aimed to generate the key generation. Initially, create the symmetric key for both encryption and decryption. Then, the data stored proper and safe by the user. This solution is based on a privacy-preserving ABE-based naming scheme and ontology-based attribute management scheme. The ontology-based scheme supports flexible attribute management with significant performance gains in term of time consumption, storage costs, and throughput improvement. From the security and privacy perspective, the ABE-based naming scheme achieves high security level as CP-ABE, but with attribute anonymity protection for policy privacy and flexible attribute rankings. In experiments, the grades of the projected methodology appraised in rapports of encryption, efficiency, performance and security achieved high results than the existing ABE technique. In future, enhance the same process with the usage of the different algorithm. Then experiment and analyzed the performance to confirm the efficacy of our schemes and design.

REFERENCES

[1] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," *International journal of engineering research and applications*, vol. 3, pp. 1922-1926, 2013.

[2] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 1343-1354, 2013.

[3] J. Hur, "Improving security and efficiency in attribute-based data sharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, pp. 2271-2282, 2013.

[4] M. Kaur and M. Mahajan, "Using encryption algorithms to enhance the data security in cloud computing," *International journal of communication and computer technologies*, vol. 1, pp. 56-59, 2013.

[5] J. Li, X. Chen, M. Li, J. Li, P. P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE transactions on parallel and distributed systems*, vol. 25, pp. 1615-1625, 2014.

[6] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13, pp. 113-170, 2014.

[7] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 468-477, 2014.

ISSN: 2321-8363
Impact Factor: 5.515

[8] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 1206-1216, 2015.

[9] Z. Wang, D. Huang, Y. Zhu, B. Li, and C.-J. Chung, "Efficient attribute-based comparable data access control," *IEEE Transactions on computers*, vol. 64, pp. 3430-3443, 2015.

[10] B. Wang, B. Li, and H. Li, "Panda: public auditing for shared data with efficient user revocation in the cloud," *IEEE Transactions on services computing*, vol. 8, pp. 92-106, 2015.

[11] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67-76, 2015.

[12] K. Selvamani and S. Jayanthi, "A Review on Cloud Data Security and its Mitigation Techniques," *Procedia Computer Science*, vol. 48, pp. 347-352, 2015.

[13] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *arXiv preprint arXiv:1609.01107*, 2016.

[14] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, pp. 1187-1198, 2016.

[15] V. R. Pancholi and B. P. Patel, "Enhancement of cloud computing security with secure data storage using AES," *International Journal for Innovative Research in Science & Technology*, vol. 2, 2016.

