www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 9 September 2018, Page No. 24311-24318
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i9.04

Analysis of Encryption Techniques to Enhance Secure Data Transmission

P. Rajesh Kannan[1], **Dr. R. Mala**[2]

[1]Research Scholar, Dept. Of Computer Science, MarudhuPandiyar College,Thanjavur, Tamilnadu, India.
[2]Assistant Professor, Dept. Of Computer Science, Alagappa University College of Arts and Science, Paramakudi, India

Abstract

with the rapid increase of technology, the data stored and transmitted among the client and server has been increased tremendously. In order to provide high security for the confidential data, there is a need for proper encryption techniques that are to be followed by the concerns. This paper presents an analysis of the various encryption algorithms and their performance on handling the private data with authentication, access control, secure configuration and data encryption. Document oriented databases such as MongoDB, Cassandra, CouchDB, Redis and Hypertable are compared on the basis of their security aspects since they manipulate the huge amount of unstructured data in their databases. It is proposed that each database has its own security breaches and emphasises the need for proper encryption methods to secure the data stored in them.

Keywords—: Encryption algorithms, data transmission, data security, NoSQL databases

I. Introduction

In the era of fifth generation technologies, data transmission is speed and popular in almost all the fields of communication. People exchange lots of data through internet and mobile technologies. Confidential and private data are shared among them via different channels. Since every information processing has become online, there is an important need to secure the data and the details of the users in the digital media. In the recent history of communication technology, there are lots of security breaches on the personal and official data that are stored on the databases during transmit of the data or at the rest [1]. So data security has become one of the key requirements for all the users who share their data on any media.

The technology behind information security in various fields such as computer science, information technology and e-commerce is cryptography. Cryptography is the art of combining some input data, called the plain text with a user defined password or key to generate an encrypted output, called the cipher text. The key is a sequence of symbols that controls the cryptographic operations such as encryption, decryption and signature generation or verification [2].

1.1 Encryption Algorithms

In order to provide secure data transmission, various security algorithms are used along with the information that is transferred. Encryption is the process of converting plain text into unreadable cipher text format by applying some mathematical transformation techniques. The real security exists on the secrecy of the key rather than the encryption algorithm used according to the Kircchoff's statement. In this paper, we have analyzed the various encryption algorithms available to establish a confidential data transmission such as DES, triple DES, RSA, AES, ECC, BLOWFISH AND RC5 algorithms. Among these encryption algorithms RSA and ECC are asymmetric key algorithms and the remaining are symmetric key cryptographic algorithms. In symmetric algorithms, both sender and receiver share the same key for encryption and decryption whereas in asymmetric key algorithms, two keys are used, public key for encryption and private key for decryption. Figure.1 depicts the various classification of ciphers.

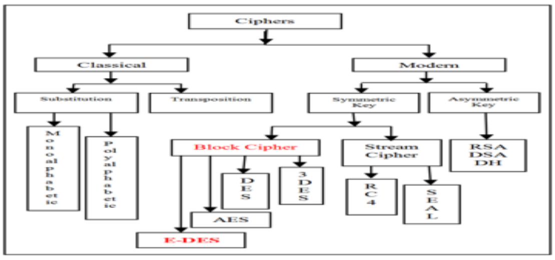

Figure 1. Classification of Ciphers

Encryption was used by military and government to facilitate secure communication among the authorized persons. Nowadays encryption methods are used to protect the data in transit, since they are susceptible to various kinds of security attacks. The encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) are widely used to solve the problem of communication over an insecure channel [3]. The method of encryption and decryption are simpler and provide high security due to the substitution mapping and transposition operations.

1.2 Secure data Transmission

For secure transmission of data both authentication and encryption are important to ensure the computers at each end are ensured [4]. The secure data transmission on transit depends on the encryption methods used in the communication. To secure the confidential data that are transmitted must be ensured with the proper methods of encryption techniques.

There are certain best practices are suggested to secure the private data by applying centrally managed encryption, multiple key recovery options, data loss prevention integration SSL specific requirements [5]. Some encryption solutions are offered to keep the digital interactions safe with the protection of the confidential customer data, intellectual property and private data with the help of some security solutions like Symantec [6]. While using these techniques, some special training and practices to be followed by the concerns to have a highly secured environment.

The emerging need for data transmission by various Medias leads to the important security measures that are adopted to secure the data at rest or in transit. This paper also focus on the data security provided by the various open source NOSQL databases.

II. Related Work

2.1 Various Encryption Methods

Rajdeep Bhanot et al.[1] compared the various encryption algorithms and suggested the best one related to parameters of security. They compared ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA etc.

They have found that each algorithm has its own benefits according to different parameters and they observed that the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption that will lead to more heat dissipation. So, it is not advisable to use short data sequence and key lengths. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. From their analysis they have found that ECC and Blowfish, these two encryption algorithms are leading with the security level that they provide and faster encryption speed. ECC is having some attacks on it but on Blowfish, no attack is successful yet. These two encryption algorithms are more secure and fast to work with and in future, there is wide scope of improvement in these both encryption algorithms as suggested by the authors.

2.2 Integrated Techniques of Encryption

Gurpreet Singh et al.[2] integrated the three encryption algorithms namely, DES, AES and 3-DES and found that AES algorithm takes less time to encrypt and decrypt files. They also suggested that when these algorithms are used in parallel, the time taken is comparatively less. They concluded that the application of multiple algorithms increase the time and space complexity of the system. In order to have secure transmission, they have suggested including some compression techniques to ensure more security.

Jaishree Singh et al. [3] proposed a technique to secure data or message with authenticity and integrity. In their work, the secret message is encrypted before the actual embedding process starts. The hidden message is encrypted using tiny algorithm using secret key and DCT technique is used for embedding and extracting file.

Er. ManpreetKauret al. [6] discussed on the different encryption algorithms like RSA (Rivest Shamir and Adleman) Algorithm, Digital Signature Algorithm, Diffie–Hellman Algorithm, Data

Encryption Standard and AES (Advanced Encryption Standard). The main security goals like confidentiality, integrity, authentication and non-repudiation are achieved by following some real time encryption techniques. Each technique has its own applications and might be suitable for the particular environment in order to have high rate of security.

Arpit Agrawalet al[7] proposed a combined symmetric and asymmetric key cryptographic algorithm to increase the strength of encryption process and suggested that RSA will help to achieve authentication about sender and SHA-1 algorithm can be used to ensure integrity of content.

Gurpreet Singh et al[8], studied the popular encryption algorithms AES, DES and 3DES and concluded that AES algorithm takes less time compared to the other algorithms. They also suggested that using multiple algorithms may increase the security while time and space complexity is increased. They have also suggested that encryption algorithms can be combined with compression techniques to improve data security with reduced memory requirements.

Nikita D. Dongare et al.[9] Proposed a combined technique namely, encryption and compression to provide high security and reduced overhead problems. This method is achieved by incorporating pattern recognition, data encryption and data compression. They also concluded that their method maximizes data security during data transmission by making the output file small in size with compression technique and thereby decreasing the channel overhead.

Prateek Kumar Singh et al [10] proposed a method of using both cryptography and steganography. In cryptography they used a three level encryption with AES, DES and Blowfish algorithms and in steganography, the data file is embedded with any audio, video or image with the use of LSB, DWT and DCT techniques. They concluded that this combined technique will increase the security of the data at the receiver end and suggested that in future the encryption process can be increased multiple times and the steganography technique can be optimized to increase the secure transmission of data.

Gurpreet Singh et al. [11] emphasize the importance of securing data during transmission and studied the encryption algorithms like, RSA, DES, 3DES and AES. They described that each algorithm is unique in its own way and may be suitable for different applications. They compared these algorithms in terms of speed, time, and throughput and avalanche effect; found that AES algorithm is most efficient and also suggested to use more than one algorithm to have secure transmission of data. For the future work, they recommend a combination of algorithms in sequential or parallel in order to have more secure environment for data storage and retrieval.

NoSQL databases/ Access Criteria	MongoDB	Redis	Couch DB	Cassandra	HBase	Couch Base Server
Authentication	Medium	Low	Medium	Low	Medium	Medium
Access Control	High	Low	Low	Low	Medium	Low
Secure configuration	Medium	Low	Medium	Low	Low	Low
data encryption	Medium	Low	Low	Medium	Medium	Low
auditing	Low	Low	Medium	Low	Medium	Medium

III COMPARISION OF ENCRYPTION ALGORITHMS IN NoSQL DATABASES

3.1 Introduction to NoSQL databases

For every individual or an enterprise, the data transmitted between their users become very important and need more security. Data in rest or in motion must be safe and should not be tampered with any intrusions that are possible by the hackers or due to some unexpected security breaches. Nowadays open source databases are available to store and retrieve the data of every individual in an organization called as NoSQL databases. NoSQL databases are flexible and support for BASE (Basically Available, Soft State and Eventually Consistent) properties with sharding which is considered as the key feature in providing faster reads and writes to the database. But securing data which is sharded over various distributed servers is a challenging task since the data is processed and transmitted over the unsecured network [12].

3.2 Comparison of NoSQL databases

Anam Zahid et al. Analysed the various security features offered by NoSQL databases and proposes an assessment criterion which comprises of various security features. To improve security controls of various NoSQL databases, the sharding architecture of various existing databases namely, MongoDB, Redis, HBase, Cassandra, CouchDB and Couch base were compared on the basis of defined assessment criteria.

They discussed from their findings that improving security is a continuous process and there is no complete solution to secure the data at rest or in motion or transit. The authors compared the NoSQL databases on the assessment criteria based on authentication, Access Control, Secure configuration, data encryption and auditing. They found from their analysis that all the assessment criteria provides low and medium support except access control is the only high factor that is provided by MongoDB database as depicted in Table 1. The emphasized the serious need for the security of data on various aspects on these sharded databases.

Table 1. COMPARATIVE ANALYSIS OF SHARDING SECURITY IN VARIOUS NoSQL DATABASES

3.3 Security aspects of MongoDB

Charmi Pariawala et al [13] discussed the lack of encryption in MongoDB databases and proposed an encryption security features at application level. They suggested to encrypt the data at application level since encryption of data is not followed in database level and the sensitive data can be secured.

Saurabh Singh et al [14] discussed on the security vulnerabilities of Mongo DB databases and proposed some cryptographic techniques using elliptic curve and RSA for data encryption and decryption to reduce the security breaches. They introduced a hybrid protocol architecture, in which the client requests server authentication, then SSH protocol uses RSA for authentication and in parallel it uses ECC to provide integrity and confidentiality for the transaction of the data. Performance of ECC depends on efficient computation which is known as elliptic curve discrete logarithm problem or scalar multiplication. Linear RSA and EAMRSA perform better in encryption and decryption respectively. The new security protocol has been designed for better security. It is a combination of both the symmetric and asymmetric cryptographic techniques. The protocol provides three cryptographic primitives such as Integrity, Confidentiality and Authentication. These three primitives can be achieved with the help of ECC, Dual-RSA and Message Digest MD5 and from their results; the time required for encryption/decryption of ECC is less than RSA and its improved version.

They have also used the ECC technique to create the secure shell while transmission of data in communication channel. ECC also provide confidentiality and integrity. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. Comparative analysis in this thesis illustrates the appeal of elliptic curve cryptography especially for applications that need high security. So in future the ECC algorithm is applied in SSL/SSH to provide digital certificate called “passport” to in order to achieve good security level and remove the flaws in NoSQL database as shown in Figure 2. We can also improve the ECC algorithm to achieve the time and the power in a cost effective manner The hybrid protocol architecture can also be used in Internet-based application, for example, online banking or e-business where large volume of online transactions or web server request is on demand.

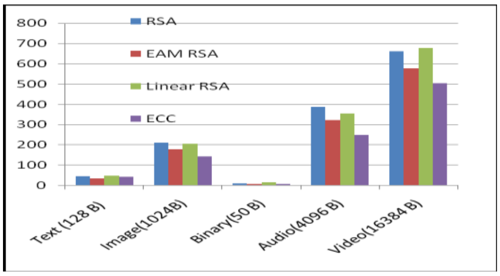

Fig 2. Decryption time of ECC and RSA with its improved version [13]

3.4 Security Methods in Open Source Databases

Preecha Noiumkar et al [15] compared the security level of the top 5 open source databases namely, MongoDB, Cassandra, CouchDB, Redis and Hypertable. They were compared on the security issues namely; data file encryption, client/server authentication/encryption, inter cluster encryption, and script injection and Denial of Service attacks. They found from their research that MongoDB, CouchDB and Cassandra were the databases that are safe from data capturing and sniffing during the communication from the servers and Redis and Hypertables are safe from attacks that are launched by internet users as shown in Table 2. The researchers found that all these databases do not perform data file encryption and have suggested some useful methods like encrypting sensitive data in the application level by creating stunnels for making safer communication.

3.5 Mongo DB Encryption methods

Mongo DB is one of the best open source NoSQL database which does not have data file encryption techniques followed. According to the table 2, the client server authentication/encryption, inter cluster encryption and script injection are weak and vulnerable in Mongo DB and Denial of Service (DoS) attacks are the only attacks that are not possible in the database. It is suggested that before recoding the sensitive data like passwords and credit card numbers, the application must perform data encryption at the application level itself in order to protect the data from hacking. Running MongoDB in standalone mode or replica-set mode is more secured than in shared mode because the authentication with pre-shared secret is activated.

Security Issues	Databases				
MongoDB		Cassandra	CouchDB	Hypertable	Redis
Data files encryption	No encrypt	No encrypt	No encrypt	No encrypt	No encrypt
Client/ Server Authentication /Encryption	weak	weak	SSL	No authen / No encrypt	No authen / No encrypt
Inter-cluster Authentication /Encryption	weak	weak	SSL	No authen / No encrypt	No authen / No encrypt
Script Injection	Vulnerable	Not vulnerable	Vulnerable	Not vulnerable	Not vulnerable
Denial of service attack	Not vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable

Table 2. The Security Comparison of the Top 5 Open Source NoSQL Databases[14]

However, hackers with an access to the system files can crack the pre-shard secret. Thus, to make the key file more secured, permission in an OS level should be determined to suit the key file (e.g. using chmod command). In the same way, as per the author’s statement, we can prevent this kind of attack on MongoDB by terminating the following symbols: (:), ({), and (}), in order to stop the attacking input from getting into the web server, which is the frontage of the database server. For these reasons, the developers should write an extra script to detect and delete these extra symbols before they can get into the database.

Matthew Trudeau et al [16] discussed the probability of hacking in NoSQL database technologies. They focus on Mongo DB database and their security features that are built in including authorization, authentication and TLS/SSL encryption. They insisted the importance of using the built in security features otherwise major security risks will be attempted on the confidential data as attacked in January 2017. The authors also added the future security measures to be undertaken to the current open source framework.

Mongo DB (version 3.4) has built in features in order to provide authentication, authorization, encryption, auditing, network exposure, injection prevention etc., but all these features are not effective when they decrease the speed of database [17].

Mongo DB supports two type of encryption standards namely, AES256-CBC, which is the Advanced Encryption Standard running in Cipher Block Chaining mode. Additionally, MongoDB supports AES256-GCM, which is known as Galois/Counter Mode. Master keys and database keys are used to encrypt, The data within the database is encrypted using the database keys, and the database keys are in turn encrypted with the master key. The authors have also analyzed that MongoDB does not offer any in-house features for application level encryption. To encrypt each field or document, MongoDB documentation suggests writing a custom encryption/decryption methods or using solutions created by one of their partners [18]. MongoDB also supports transport encryption, such as TLS/SSL, to encrypt network traffic. The implementation of TLS/SSL makes use of Open SSL libraries, only using SSL ciphers that use a key that is at least 128-bit in length.

Kusum Kakwani et al [19], in their work presented an enforcement monitor called Mem(MongoDB enforcement monitor) to implement security by acting as a proxy between the MongoDB user and server and enforce access control. P.R.Hariharan et al [20] proposed a survey on various schemes for database encryption and the future need for the complete solution of providing better secured environment for the data transmit.

IV Results and Discussion

In the digital era of data transmission via media, the security becomes an important requirement for the users who are working individually or in a group. The data at rest or in motion must be kept with proper security environment so that the data is never tampered with the unknown users. Private data may be lost in transit due to planned attacks from external devices or leakage of data during transit. Traditional relational databases handle the structured data that are difficult to handle with. There is huge demand for secure transmission of data among the clients and servers by following some cryptographic techniques.

With the large scale distributed computing due to the development of internet web technology, there is a great demand for secure databases. In recent days, NoSQL databases are becoming popular to accomplish availability and scalability factors in order to handle the unstructured data which are available in the form of documents, E-mails, multimedia and social media. These document oriented databases have many security vulnerabilities that can be mitigated by adapting suitable encryption techniques.

In this paper, the various encryption algorithms are analyzed in detail and compared with one another based on various security parameters like time required to encrypt/decrypt, key length required and space required in the memory, in order to satisfy the security requirements such as authentication, access control, confidentiality and integrity. There are various related works available that suggests some hybrid technologies that allow encryption algorithms with compression techniques to minimize the overheads. The various popular encryption algorithms such as DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA were compared and few of them were suggested to be adapted in a particular environment according to their need. According to our survey, each algorithm has its own advantages and flaws as they are reported in the papers and the authors suggested some combined techniques that are to be adapted in parallel while following encryption/decryption.

This paper also analyzes the various NoSQL databases like MongoDB, Cassandra, Redis, CouchDB, Hypertable etc. Since they follow unstructured format of data which are available in the form of documents, emails etc. Most of the NoSQL databases are susceptible to external security attacks by the intended or unintended intruders and found to be weak in some aspects like authentication, script injection, DoS attacks etc. Almost all the NoSQL databases do not follow proper encryption/decryption techniques to authenticate the user data which is at rest or in transit. From the survey, it is clear that there is a serious need to handle the confidential data safely without any loss in transit or susceptible to sniffing or injection attacks by providing a suitable secured environment by following encryption and compression techniques. Many hybrid methods are suggested by various authors and the future work of all the authors demand for combined parallel encryption methods that provide optimized solution for time delay and memory overhead and speed.

There is a need for one complete solution that provide great security for the confidential data of the users while in transit or at rest. At application level the data must be properly encrypted before the database is communicated by the users at both the end. There are some techniques that are suggested to partially encrypt the most confidential data like passwords, credit card numbers etc. While talking about the various document oriented, NoSQL databases that are used by the growing organizations where huge amount of unstructured data are manipulated, there is a great demand for open source databases like MongoDB, Cassanra etc., each of the databases do not adapt proper encryption techniques. So, there is a great demand for following proper encryption algorithms along with the open source document oriented databases to provide integrity, confidentiality and access control to the users.

When using MongoDB database, implementing SHA-3 algorithm or using enterprise edition are possible options to avoid hacking. Application level encryption must be implemented to avoid interception of data. There are certain suggestions to encrypt all the fields and follow the best practices in order to provide safe environment to the database users and implementing all built-in security features is a must for any successful database. Security attacks that are occurred in early 2017 are due to questionable selection of default settings and not following the best practices like opt-out instead of opt-in.

III. Conclusion and Future Scope

Enhancing data security is one of the important aspects of the transmission of data among the users. While the usage of data in unstructured format has been increased in various fields, there is a significant need for providing access criteria such as authentication, access control, data encryption, secure configuration and auditing. Data security is provided by proper encryption methods of various important fields of data without affecting the performance of the database in the aspects of speed and memory usage. Since the usage of document oriented, unstructured data are often handled by the NoSQL databases such as MongoDB, Cassandra, CouchDB, Redis, Hypertable etc. Due to their open source nature, there is a serious requirement in providing high security and safeguard the user's confidential data without any tampering during at rest or in transit. The various encryption algorithms were compared and it is identified that some hybrid techniques of using more than one encryption algorithm along with compression techniques are recommended along with the proper usage of best practices in handling the private data.

There is a demand for a single solution to enhance the secure transmission of data by providing improved encryption method that minimizes the process delay and memory usage in handling databases.

References

1. Rajdeep Bhanot1 and Rahul Hans2, "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications, Vol. 9, No. 4 (2015), pp. 289-306.
2. Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013, pp- 2058-62
3. Jaishree Singh, Dr. J.S. Sodhi ,"Secure Data Transmission using Encrypted Secret Message", International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, pp-522-525.
4. Jennifer Vesperman, "Introduction to Securing Data in Transit", International **Journal** of Innovative Technology and Exploring Engineering (IJITEE) ,**Volume** 13 Issue 15 Version 1.0 Year 2013
5. Symmantec, "White paper: Keeping your private data secure", http://www.symantec.com/encryption.
6. Er. ManpreetKaur , Er. Jasjeet Kaur, "Data Encryption Using Different Techniques: A Review", International Journal of Advanced Research in Computer Science, Volume 8, No. 4, May 2017 (Special Issue),pp-252-255.
7. ArpitAgrawal, Gunjan Patankar , "Design of Hybrid Cryptography Algorithm for Secure Communication", International Research Journal of Engineering and Technology (IRJET, Volume: 03 Issue: 01 pp- 1323-28.
8. Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013,pp-2058-62.

9. Nikita D. Dongare, Prof. V. T. Gaikwad, Prof. H. N. Datir, “Secure Data Transmission Scheme by Using Encryption Based Technique: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 3, March 2016 pp-25-28
10. Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar, ” Secure Data Transmission”, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 04,| Apr -2017, pp-217-222.
11. Gurpreet Singh, Supriya, “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, *International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013, pp-33-38*
12. Anam Zahid, Rahat Masood, Muhammad Awais Shibli, “Security of Sharded NoSQL Databases:***A Comparative Analysis”,*** Conference on Information Assurance and Cyber Security (CIACS), 2014 IEEE
13. Charmi Pariawala, and Ravi Sheth, “Encrypting Data of MongoDB at Application Level”, Advances in Computational Sciences and Technology,Volume 10, Number 5 (2017) pp. 1199-1205
14. Saurabh Singh, Karamjit Kaur ,”Comparative analysis of ECC and RSA for Document-oriented database MongoDB”, International Journal of Computer Technology & Applications,Vol 5 (4), April 2014, pp-1555-1560
15. Preecha Noiumkar, and Tawatchai Chomsiri, “A Comparison the Level of Security on Top 5 Open Source NoSQL Databases”, The 9th International Conference on Information Technology and Applications (ICITA2014), At Sydney, Australia
16. Matthew Trudeau, Joshua Kolodny “An Analysis and Overview of MongoDB Security,51st Hawaii International Conference on System Sciences (HICSS 2018), Waikoloa Village, Hawaii, USA, 2 - 6 January 2018, Volume 1 of 8, ISBN: 978-1-5108-5655-4.
17. Hou, Boyu, et al. “Towards Analyzing MongoDB NoSQL Security and Designing Injection Defense Solution.” *2017 IEEE 3rd International Conference on Big Data Security on Cloud*, July 2017.
18. Sahafizadeh, Ebrahim, and Mohammad Nematbakhsh. “A Survey on Security Issues in Big Data and NoSQL.” *Advances in Computer Science: an International Journal* , vol. 4, no. 4, July 2015, pp. 68–72.
19. Kusum Kakwani1, Naziya Pathan2 , Shyam Dubey3, I.C. Mehta, “Data Management and Privacy Preservation in Mongo DB”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 5, Issue VII, July 201, pp-2044-2049.
20. P.R.Hariharan & Dr. K.P. Thooyamani , “Various Schemes for Database Encryption - A Survey”, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8763-8769.