Minimizing the Effect of Brute Force Attack using Hybridization of Encryption Algorithms

Lalit Kumar
Kamla Nehru Institute of Technology
Sultanpur, Uttar Pradesh
India- 228118

Neelendra Badal, PhD
Kamla Nehru Institute of Technology
Sultanpur, Uttar Pradesh
India- 228118

ABSTRACT
Encryption is a process to hide the data into a secure manner. It helps the people to provide security and protect the data from unauthenticated people. For Encryption process, user uses many algorithms but all algorithm has some pitfalls i.e. a single encryption algorithm is not efficient to provide security to the data. For removing this disadvantages user uses more than one encryption algorithm in sequence to achieve high security encryption method. This process is called Hybrid Encryption Method. Sometimes MD5 hash function identified using Brute Force Attack. So user uses two encryption algorithms i.e. MD5 and Transposition Reverse String Algorithm. Here Transposition Reverse String Algorithm reverse the hash function due to this user cannot easily identify the hash function. This approach has fast Execution time in comparison to another hybrid approaches, so it is an optimize Hybrid Encryption Method.

General Terms
Hybridization of Encryption Algorithms

Keywords
Hybrid Encryption, MD5, Transposition Reverse String Algorithm, AES, Brute Force Attack

1. INTRODUCTION
Hybrid encryption procedure consolidates more than one encryption frameworks. It fuses two encryption methods for example symmetric and asymmetric encryption [3].

In hybrid encryption at the sender site first Data is encrypted by symmetric key that is secret key. A similar key is utilized for encryption and decryption both. When information is encoded by the secret key, information is stores in encryption block [1].

To improve the security, secret key is additionally encrypted by open key for example here framework utilizes asymmetric encryption system. This total encoded block which contains encrypted information and secret key is decrypted key is send to the collector site. When recipient gets this encoded block previously secret key is decrypted key by utilizing private key. Presently decrypted secret key is utilized to decrypt encrypted data block [5].

Hybrid encryption is viewed as an exceedingly secure sort of encryption as long as people in general and private keys are completely secure. A hybrid encryption plot is one that mixes the accommodations of an unbalanced encryption conspire with the viability of a symmetric encryption conspire [14].

If your paper is intended for a conference, please contact your conference editor concerning acceptable word processor formats for your particular conference.

In the present encryption frameworks, singular algorithms are utilized to verify information. For example, Window frameworks use MD5 encryption algorithm while some others use possibly AES or DES algorithms to encrypt their passwords.

In any case, every one of these referenced algorithms has been split a few or the other time, which implies they are not strong and can be broken by a talented hand. In this way the security of the information (passwords much of the time) is very and threateningly traded off. Every one of these algorithms are extremely acclaimed all around the world and are utilized by many, some are even open source [6].

This implies the algorithm's blemishes are notable to all and now and again, even the source code is outstanding to many. This indicates the security burdens of these algorithms. In this manner there should be a framework which beats these disadvantages while maintaining the positive parts of these broadly known algorithms [3].

2. REVIEW ON RELATED WORK
Hybrid encryption techniques consolidate more than one encryption frameworks. It joins two encryption methods, symmetric and asymmetric encryption. In hybrid encryption at the sender site first Data is encrypted by symmetric key that is secret key [1]. In this equivalent key is utilized for encryption and decryption both. When information is encrypted by secret key, information is stores in encryption square. To improve the security, secret key is additionally encoded by open key for example here framework utilizes uneven encryption method [3]. This total encoded square which contains scrambled information and scrambled mystery key is send to the beneficiary site. When collector gets this encrypted square initially scrambled mystery key is decoded by utilizing private key. Presently decrypted secret symmetric key is utilized to unscramble scrambled information square [13].

Gaurav R. Patel, Prof. Krunal Panchal [1], “Hybrid Encryption Algorithm”, So as to forestall some undesirable clients or individuals to gain admittance to the information cryptography is required. This paper presents hybrid approaches by consolidating two most significant algorithm RSA algorithm and Diffie Hellman algorithm. This “hybrid encryption algorithm”, gives greater security as contrast with RSA algorithm. The execution and result is additionally inferred in the paper.

Ms. Priyanka Deore, Mr. Tushar Chaudhari [2], “Hybrid Encryption for Database Security”, Database is an accumulation of sorted out data. Information is sorted out in lines and sections group. User can perform “insert”, “update”, and “delete” task on database. Database is utilized by different regions like medical clinic, protection, school, school, government office, web based life and so on to store the delicate data. As databases contain the delicate data, security of such databases is an essential concern. Hybrid encryption technique is increasingly secure as compare to previous techniques. It joins the mix of asymmetric and symmetric

encryption. To verify information in databases hybrid encryption technique assumes significant job."

Prachi More, Shubham Chandugade [3], "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud", This work demonstrates a security structure that can give a "protection" and "uprightness" to exchanging sensitive information through the cloud or the correspondence frameworks, in perspective on the use of the blend of Attribute-Based Encryption and Byte Rotation Encryption Algorithm. The embodiment of the work is to develop a clear stage that can get "protection", "integrity", and execution for the information trade from shared. The proposed structure uses symmetric cryptography system. Information trade must offer end-to-end perceivability, security, and consistency.

Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi et. all [4], "Hybrid Encryption/Decryption Technique Using NewPublic Key and Symmetric Key Algorithm", this research contemplate proposes Hybrid Encryption System utilizing the new ("open or Public") key algorithm and private key algorithm. A hybrid cryptosystem is one which consolidates the accommodation of an open key cryptosystem with the proficiency of a symmetric key cryptosystem. Here, user proposes a provably two way verified information encryption framework, which tends to the worries of client's security, verification, and precision. This framework has two diverse encryption algorithms have been utilized both in the Encryption and decryption algorithms. One is open key cryptography dependent on linear block cipher another is private key cryptography dependent on a basic symmetric algorithm. This cryptography algorithm gives greater security just as validation contrasting with other existing hybrid encryption algorithm.

Sourabh Shivaji Kumbhar, Young Lee, Jeong Yang [5], "Hybrid Encryption for Securing Shared Preferences of Android applications", Most mobile applications produce "local data on internal memory" with Shared Preference interface of an Android operating system. Along these lines, numerous potential provisos can get to the private data, for example, passwords. User propose a Hybrid Encryption approach for Shared Preferences to secure the releasing private data through the source code. User build up an Android application and store some information utilizing Shared Preference. User produce various trials with which this information could be gotten too. User apply Hybrid Encryption approach joining encryption approach with Android Key store framework, for giving better encryption algorithm to conceal delicate information.

Sushant Susarla , Gautam Borkar [6], "Hybrid Encryption System", Encryption algorithm have been utilized for quite a while to guard mystery information from gatecrashers. These algorithms are for the most part improved dependent on downsides of prior algorithm. Be that as it may, every encryption algorithm has a downside that is misused very well by the interlopers. These algorithms are so very much published that their system gets known to everybody and along these lines the escape clauses are effectively misused. So as to defeat these downsides and in an offer to take out the best viewpoints from the celebrated algorithms and covering their imperfections, in this overview, a system of utilizing numerous algorithms in a predefined request on a similar arrangement of information is recommended. That is, the algorithm security is enormously improved, through looking into a few well known information encryption algorithm, and improving a few information encryption algorithms, and organizing encryption algorithm in some request.

P.Chinnasamy, P.Deepalakshmi [7], "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography", "In recent years all the medical data is stored as well as managed in online worldwide. The data can be utilized by medical professional, patients for their understanding, government authorities and insurance companies etc. The medical related data can be protected in the form of Electronic Health Records (EHR) which is available online at any time. It contains data like ray x images, scan images, therapy procedure, medical prescription, patient information. All of this kind of sensitive records facing the problem is where it can be stored securely and who can access as well as view the data. To resolve this, user design secure cloud storage for healthcare data by using a Hybrid cryptographic technique. Within this, the data are encrypted through symmetric algorithm and keys are encrypted using an asymmetric algorithm. The performance evaluation, as well as security of proposed method, was measured and compared to an existing technique. The results clearly show that our method provides better security than any other hybrid algorithms".

N. Thirupathi Rao, J. Anitha, Debnath Bhattacharyya and Tai-Hoon Kim [8], "Secure E-Commerce Model uses Hybrid Encryption for Financial Transactions", as people and organizations increment data sharing, a worry with respect to the trading of cash safely and helpfully finished the web increments. An internet business framework is an exchanging stage which gives clients day in and day out access so they can shop at whatever point they have a couple of minutes. It additionally gives the capacity to window shop, which empowers value touchy customers to think about costs, assortment and extent of items. The prime necessities for any internet business exchanges are Privacy, Authentication, Integrity support and Non-Repudiation. Half and half Cryptography encourages us in accomplishing these prime prerequisites. Half breed cryptography in view of AES symmetric calculations and RSA Asymmetric calculation for internet business application is as a rule; the harder to find the key, the more secure the component.

3. BACKGROUND

In this section user describe hybrid encryption preliminaries related to proposed model, along with current encryption algorithms i.e. MD5 (Message Digest-5) and Transposition Reverse String Algorithm. Here user especially discuss two encryption algorithms with Brute Force Attack.

3.1 Md5 Algorithm

MD5 is one of the widely used hashing algorithms developed by Ronald Rivest in 1991. MD5 is a successor version of MD4. MD-5 is broken in regard to collisions, but not in regard of pre-images or second-pre-images [19]. It produces 128 bits a fixed length hash values. MD5 is very collision resistant. In 1996 attacks on MD-5 were published [16].

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is used in each round which is nonlinear function. Mi denotes the message input of 32 bit, and Key which is different for each operation and is 32-bit constant. s is a left bit rotation by s [1],[12]. The main algorithm MD5 is divided into A, B, C and D which operates on 128 bit where each carry 32 bits. These are constants which are initialized into [17],

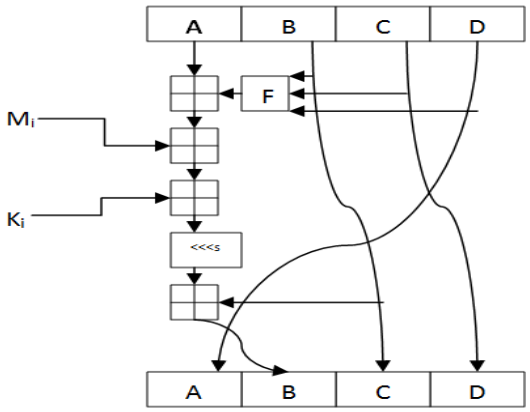

Fig 1: MD5 Hash Generation

A = 0x67452301
B = 0xEFCDAB89

C = 0x98BADCFE

D = 0x10325376

The processing consists of four same stages and each stage is composed of similar 16 operations. The figure denotes one such kind of operation.

F (B, C, D) = (B AND C) OR (NOT B AND D)

G (B, C, D) = (B AND D) OR (C AND NOT D)

H (B, C, D) = B XOR C XOR D

I (B, C, D) = C XOR (B OR NOT D)

The output is called a hash value, a fingerprint or a message digest.

3.2 Transposition Reverse String Algorithm (Trsa)

Transposition cipher is a simple data encryption scheme. In transposition Cipher, the plaintext characters are shifted in some regular pattern to form cipher text. In Transposition Encryption Method, user can use various techniques.

Here user uses the transposition reverse string algorithm which is easy to implement. Transposition Cipher contains all the plain text Alphabet but into a specific manner which is not understandable without Key. Here Key is used to assign or placed to alphabet at a specific place.

Here user only changes the place of the character for plain text.

For example, if a Text is "computer" then after applying reverse string Transposition method. It will be "retupmoc".

The Basic Algorithm of this method is

1.) If there is a word which is consist of 'n' alphabets

i.e. a(1), a(2), a(3), a(4) ---------- a(n)

2.) Then after Converting it into the cipher text it will be

a(n), a(n-1), a(n-2)----------a(3), a(2), a(1).

3.3 Brute Force Attack

A typical danger Web designers face is a password-guessing attack known as brute-force attack is an endeavor to find a secret word by methodically attempting each conceivable blend of letters, numbers, and images until you find the one right mix that works. On the off chance that your Web website requires client verification, you are a decent focus for a brute-force attack.

An attacker can generally find a secret phrase through a brute-force attack, yet the drawback is that it could take a long time to discover it. Contingent upon the secret word's length and unpredictability, there could be trillions of potential mixes.

Hackers can endeavor to get into client's framework utilizing a couple of various techniques. Techniques are talked about beneath –

1.) Manual login endeavors: In this methodology, they will attempt to type in a couple usernames and passwords

2.) Dictionary based assaults: In this methodology, robotized contents and projects will have a go at speculating a great many usernames and passwords from a word reference record, some of the time a document for usernames and another record for passwords.

3.) Generated logins: A splitting system will produce arbitrary usernames set by the client. They could produce numbers just, a mix of numbers and letters or different mixes.

4. PROPOSED SYSTEM

With the advancements in computer technology, providing security becomes more important task due to the increase of information. So consider this issue to propose a new group hash function based to enhanced and maintain integrity and security of entire data security. Here user basically uses a hash encryption algorithm that is used to convert the plain password into hash function and it is not reversible into plain text. But attackers uses brute force attack to crack the password and they succeeded after some iteration [1].

4.1 Flow Chart

Working Process of this existing system are described by using flow chart, which are shown below [6]-

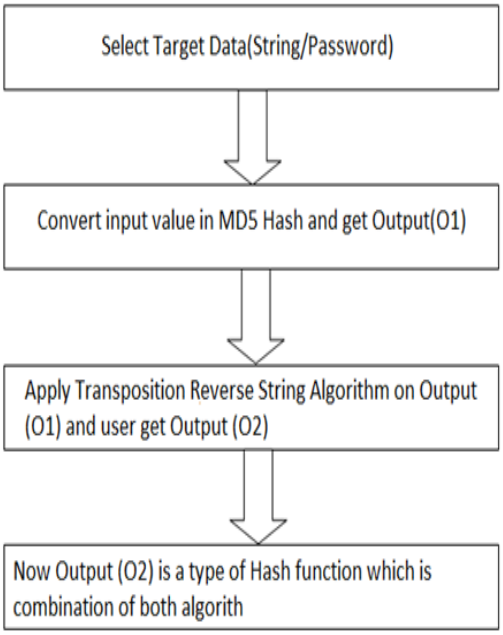

Figure 2: Flow Chart for Proposed Model

4.2 Algorithm

Algorithm for the proposed method is:

1.) Select the Target Data (Input String/Password);

2.) Convert the Input using MD5 algorithm and get Output O1;

3.) Apply Transposition reverse String Algorithm on Output O1 and get Output O2;

4.) Now O2 is the Final Hash Function after applying both algorithms.

5. RESULT AND ANALYSIS

5.1 Existing Model

AES and MD5, both is hash algorithm i.e. used to encrypt a plain text into hash function. Both have great security feature to hide the data but due to removing some disadvantages of these this work used it together. This approach is called Hybrid Encryption. This is the existing work, for this the execution time for encryption of Table is:

Table 1: Table for execution time and cipher text of Some Input String/ Password using AES+MD5 Hash Algorithm

S. No.	Input String/Password (Plain Text)	Execution Time (AES + MD5)	Respected Hash Function (Cipher Text)
1	Roman	426	75f70cf4c54fa493940a4d859d39ca54
2	Qwerty	427	8194d3c2c1ff6be10526756c028af6bc
3	Airline	427	92dd5f6a8de93738b40195c90a19a913
4	Computer	428	2b592363e88225bde7b9f18bd0557915
5	LifeCycle	429	c3e73f1989086c30fafc5f0a554c63d7
6	Encryption	429	8f8c87b5c81f7254d450956ea2805b80
7	Publication	430	40cebe7afe0811179dc9ed29560c6d3c
8	HelloWorld	430	3efbd6899a164110649ce5b4c1925ceb
9	785@KNIT	431	42822de9dba4c57aa96aec1fbfcba68c
10	Knit@123456	432	32467da1e84c3e82aec2855b35bee730
11	Harsh@#9568	432	c3f9def0a0489b8281510cc81dd47c87

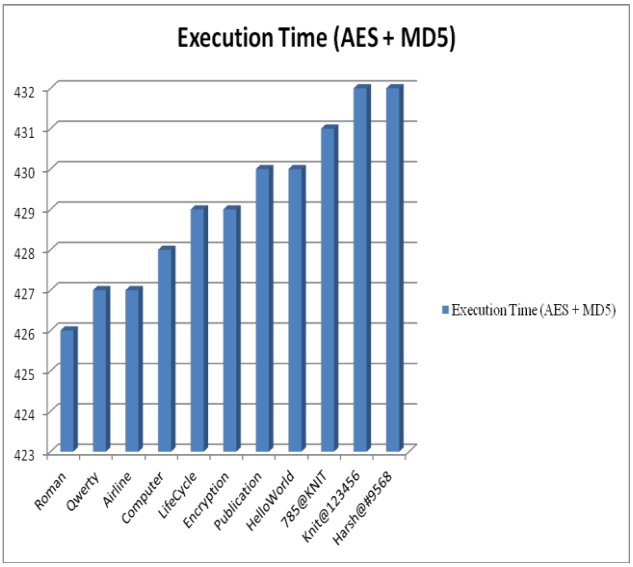

Fig 3: Execution time Chart for AES+MD5 (Existing Model)

According to the execution time of this hybrid Approach, This work can say it takes more computational time as expected. This approach has great level of security. But the main drawback of this algorithm is its execution time.

5.2 Proposed Model

Here both MD5 and Transposition Reverse String Algorithm are used together. MD5 is a hash algorithm and Transposition Reverse String Algorithm is used to convert plain text into cipher text. If it uses alone in encryption process, then it can't provide great security. So this work uses it together to remove the drawback of MD5. This approach is called Hybrid Encryption. This is the proposed model, for this the execution time Table is:

Table 2: Execution Time for some String with their respected hash function using proposed model

S. No.	Input String/Password	Execution Time (MD5 + Transposition Algorithm)	Respected Hash Function
1	Roman	30	0887da5e9b234bff1936aa97ca63fd5b
2	Qwerty	31	1a645614528f1925f3aeb86f2ba9dbca
3	Airline	31	b0f832af7a1b9378d5799fdd3eed0c0a
4	Computer	31	7464ff0e4c35f43bcceb069dad009181
5	LifeCycle	31	7290d6ec956bb599c843f7d1c0e60911
6	Encryption	32	aea0ed7f7a3fc31cc7651a17c5162f7d
7	Publication	32	c430ab4197b3c9a2d2b67ad1caeb6db6

8	HelloWorld	33	6e8f68722cc50e51a27ac04f0f901e86
9	785@KNIT	33	6564f7c077252e0e3a2cfde07a36debf
10	Knit@123456	33	9ee8673c30af51890b2c385e8fc61beb
11	Harsh@#9568	34	c7674175e16a0973d5be9404e518cb6d

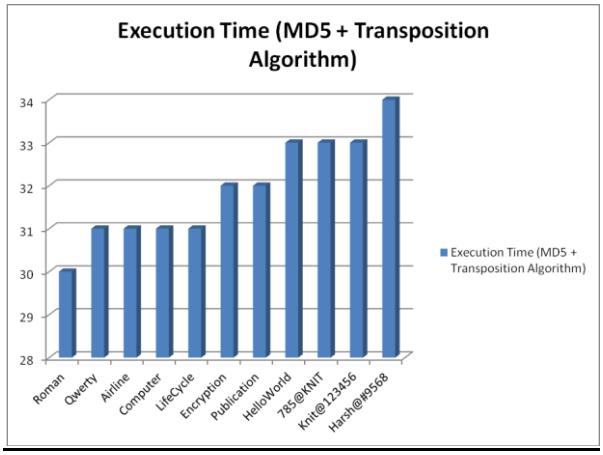

Fig 4: Execution time Chart for AES+Transposition Reverse String Algorithm (Existing Model)

5.3 Comparison Between Existing And Proposed Model

Here is the comparison graph (figure 5.6), that shows a big difference between existing and proposed model. The proposed model takes 10x times more execution time in comparison of proposed model. So according to this comparison chart these things can be said:

- It is better and optimize hybrid Encryption Algorithm
- It can be used for safe and secure authentication channel.
- This works help to keep data into a secure manner.
- This work shows a great encryption scheme with fast execution time.

Table 3: Comparison between Execution time of Existing and Proposed Work

S. No.	Input String/Password	Execution Time (AES + MD5)	Execution Time (MD5 + Transposition Algorithm)
1	Roman	426	30
2	Qwerty	427	31
3	Airline	427	31
4	Computer	428	31
5	LifeCycle	429	31
6	Encryption	429	32
7	Publication	430	32
8	HelloWorld	430	33
9	785@KNIT	431	33
10	Knit@123456	432	33
11	Harsh@#9568	432	34

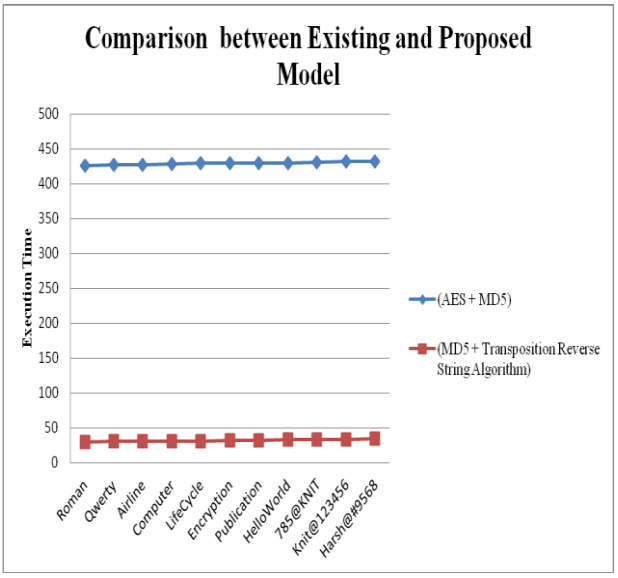

Fig 5: Chart for Comparison between Existing and Proposed Model

Here in the comparison chart execution time for Existing system (AES+MD5) is indicated by Red line whereas the Blue line shows the execution time for Proposed System i.e. combination of MD5 and Transposition Reverse String Algorithm.

6. CONCLUSION

This Proposed work helps to create optimize and safe channel for better communication and authentication purpose. This work takes only 10% execution times of Existing work's Execution Time.

By using the Proposed Hybrid Encryption This work can remove the pitfalls of MD5 algorithm. This work is done by using Transposition Reverse String Algorithm which helps to change the pattern of MD5 hash function. Due to this attacker cannot easily deduct pattern of MD5 hash function.

Hybrid Encryption is also helps to make a safe and secure authentication channel because combination of algorithm helps to hide the identity of both algorithms. Due to this it cannot be cracked easily.

Hiding identity of both algorithms is also help to keep data into a secure manner, because deduction of both algorithms on a single hash is not easy.

This approach comes with the great combination because it takes less time for execution time for encryption of data into a secure manner.

At last, this approach also carries a better optimize encryption algorithm on the basis of the execution time of encryption. Using a single hash algorithm with a simple cipher text conversion algorithm is helps to create a strong hybrid encryption method.

7. FUTURE SCOPE

This dissertation is implemented with the consideration of hybrid encryption by using MD5 and Transposition Reverse String Algorithm. Further it may be extended to use more than two algorithm to create another more optimize hybrid encryption.

Therefore, future study should gain by examining the properties of Hybrid Encryption, specifically the number of the algorithm used in the work and how it reduces the effect of various types of attacks.

8. REFERENCES

[1] Gaurav R. Patel, Prof. Krunal Panchal, "Hybrid Encryption Algorithm", International Journal of Engineering Development and Research, Volume 2, Issue 2, ISSN: 2321-9939, 2014.

[2] Ms. Priyanka Deore, Mr. Tushar Chaudhari, "Hybrid Encryption for Database Security", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 11, Nov 2017.

[3] Prachi More, Shubham Chandugade, "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems over Cloud", 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), Feb 8-9, 2018.

[4] Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using NewPublic Key and Symmetric Key Algorithm", 2014 Department of Management Information Systems, College of Commerce National Chengchi University & Airiti Press Inc., 2 March 2014.

[5] Sourabh Shivaji Kumbhar, Young Lee, Jeong Yang, "Hybrid Encryption for Securing Shared Preferences of Android applications", 1st International Conference on Data Intelligence and Security, 2018.

[6] Sushant Susarla , Gautam Borkar, "Hybrid Encryption System", International Journal of Computer Science and Information Technologies (IJCSIT), 2014.

[7] P.Chinnasamy, P.Deepalakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography", 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT) IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN: 978-1-5386-1974-2, 2018.

[8] N. Thirupathi Rao, J. Anitha, Debnath Bhattacharyya and Tai-Hoon Kim, "Secure E-Commerce Model using Hybrid Encryption for Financial Transactions", Advanced Science and Technology Letters Vol.147 (SMART DSC-2017), pp.367-373, 2017.

[9] Mrinal Kanti Sarkar; Sanjay Kumar, "Ensuring data storage security in cloud computing based on hybrid encryption schemes", Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on 22-24 Dec. 2016.

[10] Neha, Mandeep Kaur, "Enhanced Security using Hybrid Encryption Algorithm", International Journal of Innovative Research in Computer and Communication Engineering; Vol. 4, Issue 7, July 2016.

[11] Atewologun Olumide, Abeer Alsadoon, P. W. C. Prasad, Linh Pham, "A hybrid encryption model for secure cloud computing", ICT and Knowledge Engineering on (ICT & Knowledge Engineering 2015).

[12] Kaur, Khushdeep, and Er Seema, "Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices", International Journal of Engineering Research and Applications (IJERA) 2.5 (2012): 914-917, 2012.

[13] Gupta, R.K. and Parvinder, S., 'A new way to design and implementation of hybrid crypto system for security of the information in public network', International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 8, pp. 108-115.

[14] Ramaraj, E., Karthikeyan, S. and Hemalatha, M., 'A design of security protocol using hybrid encryption technique', International Journal of the Computer, the Internet and Management, Vol. 17, No. 1, pp. 78-86, 2009.

[15] Shaar, M., Saeb, M., Elmessiery, M. and Badawi, U. (2003), 'A hybrid hiding encryption algorithm (HHEA) for data communication security', Proceedings of IEEE 46th Midwest Symposium on Circuits and Systems, Cairo, Egypt, pp. 476-478, 2013.

[16] Research for the Application and Safety of MD5 Algorithm in Password Authentication-9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2012.

[17] Priyanka Walia and Vivek Thapar, "Implementation of New Modified MD5-512 bit Algorithm for Cryptography", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349- 2163 Volume 1 Issue 6, July 2014.

[18] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider " A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication" in Comsats Institute of Information Technology, Wah Cantt ., 47040, Pakistan.

[19] Xiaoling Zheng, JiDong Jin, Research for the Application and Safety of MD5 Algorithm in Password Authentication, 9th International Conference on Fuzzy Systems and Knowledge Discovery, 2012.

[20] Tanvi Gautam, Anurag Jain," Analysis of Brute Force Attack using TG – Dataset", SAI Intelligent Systems Conference 2015, November 10-11, 2015.

[21] MD5hashgeneratorhttp://www.md5hashgenerator.com/index.php