M^{3}HP: An Efficient Secured Data Transmission using the Human Password Generation Solution

Amarnath J L, Pritam Gajakumar Shah

Abstract*—One of the most important and essential tasks in all kinds of online information transmission system is security. In recent days mutual authentication and authorization are used for secured communication and data transmission. Most of the public and private networks are insecure networks. Various existing researchers proposed various secured protocols using various key cryptographic methods, whereas the computational, time and cost, complexity is more and utilize more memory space. Hence, the existing security protocols cannot be used as fast and efficient internet-based applications. To overcome the above-said issues, this paper proposed a Multi-Stage Multi-Model Human Password (MMMHP-M3HP) generation framework to provide a highly secured data transmission in online applications. The M3HP framework generates a human password is by combining various data models like numerical, alphabets, alpha-numerical and images for authorizing the end users in various stages of the applications. This is so-called Multi-stage and Multi-Model security. Each time user enters into the application, the password is regenerated and cross verified to increase the security level.

***Index Terms*—Human Password Generation, Security in Cloud, Data security, Multi-level security, Authentication, Authorization**

1. INTRODUCTION

In recent days internet becomes a most important technique used for multipurpose computing. Today cloud computing is involved on the internet. Since clouds don't have security, a secured communication is a crucial task. Most of the recent research works used cryptographic methodologies, authentication & authorization methodologies and data integrity to provide secure communication on the internet. These kinds of securities are not successful in case of a multi-tenant environment. One of the secured communications is provided using novel methodologies like human password generation. But there are some issues faced in terms of comparison, time and cost complexities. Hence this research work aimed to provide a successfully secured data transmission methodology for online applications. A multi-stage multi-model human password generation framework is proposed to increase the success level of the security provision for online applications.

The Internet is one of the global systems which interconnect a huge number of computer networks with the help of internet protocols. The internet protocols are used to link various devices throughout the world. It is also called as a network of the network. Private, academic, public, wired, wireless, ad-hoc and optical networks are some of the networks interconnected with the internet. Internet carryout a huge amount of information and provide very good services like hypertext and various applications based on www. In order to integrate parallel processing in a distributed environment, cloud computing is introduced. It is a fast, efficient, world connecting information technology method which makes ubiquitous access to sharing resources. Resources are sharable under various types such as software, platform, and infrastructure. A third party cloud facilitates the business people to focus their business on core business. The expenses of any core business are reduced with the help of cloud. Totally cloud provides a typical method of cloud usage called as Pay-n-Use. Cloud reduces investment cost of a core business, only operating cost they have to spend.

Due to the parallel and distribution procedure, anyone can connect to cloud at anytime from anywhere. This makes a critical situation and creates one of the big issues as security. Cloud means "Security-less". In recent days, several research people are trying to provide security in various points of view such as user-level security, data level security, routing level security and maintenance level security. Some of the earlier research works provide security using privacy preservation method. Few of the research people encrypt and decrypt their data using AES [26], DES [26], MD5 [27], PKE [28], KP-ABE [28], RSA [29] and DSA [29] algorithms.

There are two different stages is carried out while providing a secured communication in the cloud. One is authentication and other is authorization. Authentication is the process making a user to prove them as true or valid by showing something like Identity. Once the user proved himself as valid then he becomes an authorized person, can participate in the network functionalities. Here the author aimed to authenticate a cloud user to provide authorization for data sharing.

Human password generation means, generating a password using a Human Body Information (HBI) using the Metadata of internal or external features. Facial Features such as eyes, nose, forehead, mouth, fingerprint, Irish and other biometric information are considered as external features. DNA pattern, blood cell information, RNA pattern and other inside human body information is considered as internal features. Using certain image features like (eye, nose, face, etc.,) will mean the biometric authentication based security provision which had been discussed already by several earlier research works. In order to avoid confusion, and tightened the security level authentication process, this paper generates

Revised Version Manuscript Received on July 18, 2019.

Amarnath J L, Assistant professor,Computer Engineering, Research scholar at Vishveswaraya Technological University Belagavi, India. (E-mail: amarnath.jl@gmail.com)

Pritam Gajakumar Shah,Chief Editor Australian journal of wireless technology mobility and security Canberra Australia, University of Canberra. (E-mail: wsnpgs@gmail.com)

equivalent digital information for all the HBI and used for creating Human Passwords. This paper aimed to use the external features of the Human body and generate the password. The entire contribution of the proposed framework is

- Application Assignment
- Password Generation
- Authentication and Authorization based data transmission

The novelty of this paper is, **M^{3}HP** has no arduous proof of security. The memory utilized, the number of comparisons handled and execution time taken by **M^{3}HP** is comparatively lesser than other existing approaches. Since user authentication process is very similar to the user creation process the false rate is very less and tights the security. Through ethical hacking and other hackers cannot trace out or destroy the password. In case of re-entering the user info, the server makes the user provide the last entries in terms of HBI where it cannot be given as duplicate.

2. MOTIVATION AND BACKGROUND STUDY

There are various research works are focused on human password generation method for secured communication and data transmission. Like conventional approaches, the human password generation method is also used prime number generation for the private key and public key generation, key distribution. Additionally, a cryptographic process such as encryption and decryption is applied on the key as well as on the data where it takes more time and makes data loss when data recovery. In order to avoid such kind of problems, make a password easy, quick and involved on the end user who needs the security. Any user associated with any online applications they need to answer some form of authentication credentials. Most of the users are struggling to remember their password due to the passwords is still prevailing. In this kind of scenarios, users adopt insecure password practices [1-4] like always reset the password and fail to recall their passwords finally. Some of the earlier research works focus the essentiality of solving these problems [5-16]. One of the main objectives of the research work is to design and implement usable and secure password generation and management where it helps the users to remember the password even if it is multiple. Authors in [17] and in [18] anticipated a novel method for password generation where it conserves some security assurances after a small constant number of fissures.

Most of the researchers used Identity Based Encryption (IBE) [19-23] 6where it encrypts the messages before transmission in the network. It needs to share two different keys such as public and private where the public key is distributed and still the performance of the IBE mechanisms is less and to be improved better. The existing approaches [24-25] used too many functions and notations which makes more complexity in terms of generation and validation. Sensor nodes are considered as client nodes in the existing system but in this paper Personal computer, laptops are considered as the client nodes connected to the network. In order to reduce the comparison complexity and memory usage, this paper provides an efficient human password generation method. Hence, this study aimed to develop a fast efficient and easy understanding human password generation and management to increase the security level after several breaches. In this method the user no need to reconstruct password, since all the credentials and the answers to the credentials are the personal information about the user. The motivation of the paper increases the security involving less complexity in terms of password generation, comparison, and computation and authorizing the user to access the data.

From the above discussion, it is noted that ethical-hacking is also one of the emerging research areas in recent days. Since security and ethical-hacking are growing parallel; it is very difficult to tighten the security in the cloud. Sybil, sink, data forwarding, and wormhole are the various attacks function seriously in the cloud and destroy the online data. In order to avoid this, the first level called user-level security is tightened by generating a human password-based access control provision is applied in the cloud.

3. APPLICATION ASSIGNMENT

In this paper, to verify the efficiency and evaluate the performance of the proposed **M^{3}HP,** a user pairwise communication model is considered as the application. Any user in the cloud is transmitting their secret data to any other user in the cloud over a common application like money transfer, data transmission about the company and etc.

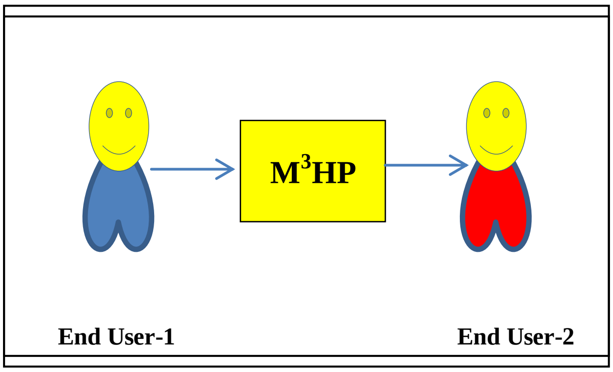
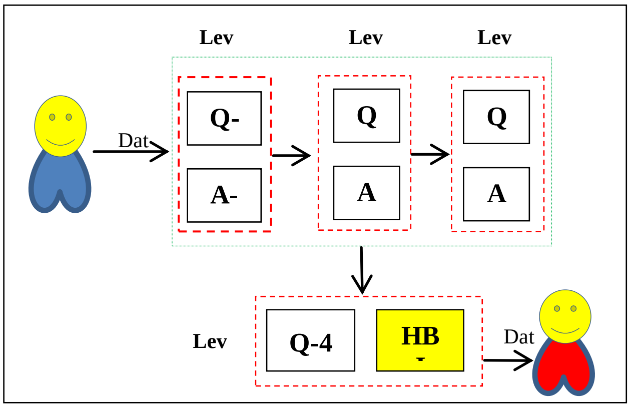


Figure-1: Overall System of M^{3}HP

In this scenario, the proposed approach **M^{3}HP** is deployed in the cloud on a specific application where it authenticates and authorizes the users by comparing the credentials and the password generated based on the user credentials. The overall system model of **M^{3}HP** and the level by level authentication verification process is illustrated in Figure-1 and Figure-2. Figure-1 illustrates any two end users can communicate with one another through **M^{3}HP**. Means M^{3}HP watch, intake, validate and permit the end users to share their information. The main advantage of M^{3}HP is, it only validates and permits the users in the network. M^{3}HP do not know about the data shared by the end users in the network.



*HBI – Human Bodv Identification

Figure-2: Multi-Level and Multi-Model Human Password Generation

When a user tries to transmit a data to the other end user, **M^{3}HP** framework verifies the trustiness of the user level by level. In this paper, it is assumed that a user **A** transmitting a data to user **B** at the time **T**. A restriction is provided for each stage to map the request and the response. A request is always considered as question and response is always considered as the answer. This scenario is applicable for any kind of applications where two end-users are sharing their secret data like online money transfer. The entire framework comprises of four levels to be carried out within a stipulated interval of time (T). If the request response mapping is not completed within T then the system quit the process. Among the four levels, the first level is asking a question related to the user personal information where the answer cannot be provided by other users. In the second level is asking a question related to financial status (like net salary) which where the answer cannot be provided by other users. The third level is asking a question related to the user family information where the answer cannot be provided by other users. The fourth level is asking a question related to Human Body Identification (HBI) where the answer cannot be provided by other users.

Whereas, HBI represents the human facial features Irish, Fingerprint and facial features. All of these information's such as personal information, financial information, family information and human body information are stored in the main database of the cloud server while user registration. The time T is divided intot_1,t_2, t_3, and t_4 as a time interval assigned for answering Q1, Q2, Q3 and Q4 respectively. If and only if the correct answer of the Q1 is provided by the user A within T1 (i.e 0 to T1) A is allowed to enter to the second level. Similarly, Q2 is answered by A within T2 (i.e T1 to T2) is allowed to enter to the third level and vice versa. This framework is very simple and only the private information of the user A is assigned as the answers. Also, these answers cannot be shared with anybody and hence the security is increased. For example, the following Table-1 illustrates the way of user password creating using the four answers given by the user.

Table-1: User Password Generation

User ID	Q1	A1	Q2	A2	Q3	A3	Q4	A4	User Password
0011-00-11-1019	Name of the first lover	XXX19 (Anil)	Present Take home salary	YYY19 (43252)	Name of the great-grandfather name	ZZZ19 (Govindarajulu)	What is the facial feature is your ID	Image (LEFT EYE)	***AN43GOLE***
:	:	:	:	:	:	:	:	:	:
:	:	:	:	:	:	:	:	:	:
0011-00-11-1044	Name of the first school	XXX44 (Little John)	Name of the first affair	YYY44 (ramya)	Age of the grandfather/grandmother/father	ZZZ44 (74)	What is the facial feature is your ID	Image NOSE	***LJRA74NO***

Table-2: Facial Feature Values

Facial Features	Values	Digital Information	Binary
Left Eye	LE	6	110
Right Eye	RE	4	100
NOSE	NO	5	101
MOUTH	MO	8	1000
FOREHEAD	FH	7	111
FACE	FA	9	1001

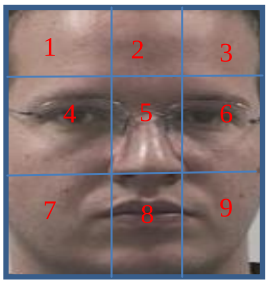


Figure-1: Facial Features with Digital Information

Password Generation

The user ID given in Table-1 is generated sequentially like enrollment number. But the password is generated by integrating the first three answers given by the user.

$$\boldsymbol{if} \begin{cases} \boldsymbol{A1} = \text{"}\boldsymbol{ANIL}\text{"} \\ \boldsymbol{A2} = \text{"}\mathbf{43252}\text{"} \\ \boldsymbol{A3} = \textbf{Govindarajulu} \\ \boldsymbol{A4} = \text{"}\mathbf{110}\text{"} \end{cases}$$

$$then$$

$$\boldsymbol{Password} = \text{"}\boldsymbol{AN43GO}\mathbf{110}\text{"}$$

That is the first two characters from A1, A2, A3, and type of A4 is concatenated as a password. Similarly, in the last row, the generated password is "***LJRA74101".*** The set of facial features are assigned by the values, which are given in table-1. But, during registering the user information, the facial features are stored as images including the values given in Table-2. Storing an image as a password is suitable in a static computing world, but nowadays users are roaming the world. Hence providing an image as a password at all the time of cloud entry is high, not possible. In order to avoid these kinds of issues, this paper provides digital information which is equal to the image. Converting an external facial feature into digital information is demonstrated in Figure-1 and in Table-2. The formula for this password generation is

$$\boldsymbol{HuPwd} = \text{“}\boldsymbol{word}\text{”} + \text{”}\boldsymbol{digit}\text{”} + \text{”}\boldsymbol{word}\text{”} + \text{”}\boldsymbol{digit}\text{”} + \text{”}\boldsymbol{word}\text{”}$$

In any case of online applications, the number of users **N** is considered as a set **U={U$_1$, U$_2$, U$_3$,…, U$_i$,…, U$_n$},** where each user **U$_i$** is registered. It is restricted that the total length of the password is 8 characters. The password is a combination of characters and numerals without any special characters. The number of alphabets is 6 and the number of digits is 2.

This above-described algorithm and the functionalities of the proposed framework is implemented in DOTNET software and the results are verified.

Authentication and Authorization based data transmission

Let **N** be the number of users, where it depends on the application. The set of questions **Qi** is stored in the question pool. The set of all answers **Ai** is stored in the answer pool. In order to help the user **Ui**, to register should answer the questions $1, Q2, . . , Qm$, where the security variable m=4. The value of m varies in accordance with the application. When a user **Ui** enter into the application, the first challenge Q1 is displayed to the user. After receiving the answer a mapping function $f(Q1, A1)$ store it in the main database. There is no additional database is required for the authentication process. Similarly, the values of $(Q1, A1), (Q2, A2), (Q3, A3)\ and\ (Q4, A4)$ are stored sequentially in accordance with the user number in the database.

Each time the user enters into the application, the first challenge Q1 is displayed to the user and waits for $t_1$seconds. After receiving the answer A1 from the user, the mapping function $f(Q1, A1)$ is called to map the first question and the answer from the user values with the database values. The user is permitted to answer the next credential Q2 if the answer given by $f(Q1, A1)$ is “1” and it will display the second question Q2 automatically to the user and waiting for A2. As discussed above, after A2 given by the user F(Q2, A2) should provide "1" for moving to the next level else, the user cannot permit to the next level of meeting the credential Q3. In addition to the above process, the user answering time t_i is calculated for each A_i. That is $T = t_1 + t_2 + t_3 + t_4$ and $f(Q1, A1) = f(Q2, A2) = f(Q3, A3) = f(Q4, A4)$ =1, since m=4. The main database available in the server consists of all the user answers according to their credentials. The memory required to store the question and answers is not more comparing with the other approaches. Also, the mapping function $\boldsymbol{f}$takes considerably very less time than the other approaches. Authenticating a user is very similar to the account creation and it helps the user to recall the password associated with the answers effectively and speedily. Since the credentials are user privacy information, it is very easy to recall the answers and enter the password. In case of the genuine user, the **M^{3}HP** helps the user to remind the answers by providing Qi and Ai alternatively retrieved by the mapping function f(Qi, Ai). One of the main advantages of the **M^{3}HP** is easy two remember, very fewer chances to hack.

Algorithm_ M3HP ( )

```
{
    T=0
    start time
    T = T +1
    Q1 passed to User
    Used pass A1
    If (A1 is correct and T ≤ δ1 )then Q2 passed to user else user forced to quit
    user pass A2
    if (A2 is correct and T ≤ δ2 )then Q3 passed to user else user forced to quit
    user pass A3
    if (A3 is correct and T ≤ δ3 )then Q4 passed to user else user forced to quit
    user pass A4
    If (A4 is correct and T ≤ δ4 ) then user-1 can do data transmission
    else user forced to quit
    stop timer
    T =0
}
```

Algorithm _ Authentication-Process ( )

{

$$\boldsymbol{Input}: Q_1, \dots, Q_m, b, d\ \ and\ |\ f_{ij}\ \ for\ i\ \in [m], j \in \{0, \dots, d-1\}$$

$$Where, j \in \{0, \dots, d-1\}\ andi \in \{1, \dots, m\} f_{ij}\ is\ a\ function\ map\ the\ application\ request\ and\ the\ user\ response\ including\ the\ biometric\ image\ Ii\ associated\ with\ Ui.\ d = 1\ to\ m, here\ m = 4,$$

$$that\ is\ the\ credential\ number.\ Where\ b\ is\ 1\ or\ 0,\ generated\ by$$

```
$f_{ij}$ in accordance with $Qi$ and $Ai$ relation.
for $i \leftarrow 1$ to $m$ do
            $\sigma_i \leftarrow f_i(Q_i, A_i)$ as 0 or 1
    $f_i \leftarrow f_{i,\sigma_i}$
    $U_i$
$\leftarrow$ next level, using $f_i$, associated wit(h $A_i, \sigma_i$) for $i$
$\in [n]$
end i
  }
```

The entire functionalities of **M^{3}HP** are implemented in DOTNET software and the results are verified. The application is considered as two or more end users under a mutual bind are transmitting their secret data (like money transmission).

4. EXPERIMENTAL SETUP & RESULTS

To experiment and evaluate the performance of the proposed approach the implementation of **M^{3}HP** is installed in the server of a 50 computer connected computer laboratory. The lab is at Vellore Institute of Technology, Vellore, India. Other than server machine all computers are considered as the client machine where any client can operate, input and process in **M^{3}HP**. Since **M^{3}HP** is authentication software it verifies the registered users working in the network. It occupies a less amount of memory to store the user profile with ID. Since less memory, the time taken to access the data is very less. Due to less complexity and less time it is cost effective. C#.Net is used for implementing the routines and C++ based binary libraries used for fetch the log file whereas this log file is distributed to the network. The entire simulation and experiments are executed in Personal computers, Laptops interconnected in the LAB. The minimum RAM capacity of the systems is 4 G.B RAM running on Windows OS build using SQL database manager. In order to evaluate the performance of the proposed approach, it is compared with SPPDA scheme [19] followed and implemented from Charm-Framework [20]. It was proved that SPPDA is better than Charm-Framework in terms of various performance parameters. It is considered that the network size always to be $1 \geq k \geq 50$. In the experiment, user registration, user password generation and user authentication are the three main routines. Theoretically is it understand that the comparison and computational time complexity is very less since there is no encryption -decryption, less memory storage and less comparison.

The performance of the proposed approach is evaluated by calculating the computational complexity, CPU time, and cost. It is calculated by changing the number of clients involved in the application (decide the network scale) as 2, 4, 6, 8, and 10 in each time of the experiment, but the network size is fixed at 50.

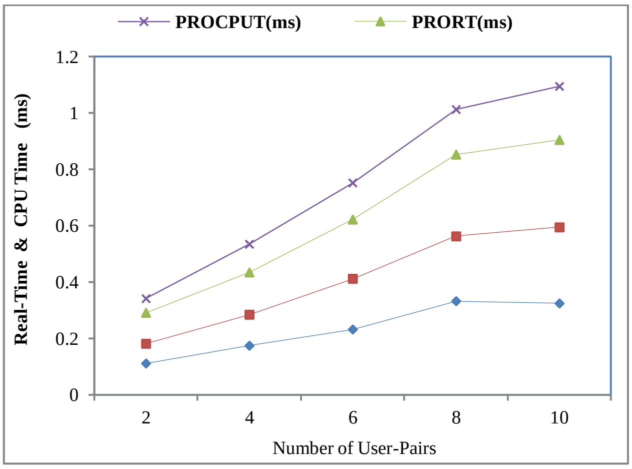


Figure-3: Real-Time, CPU Time Comparison

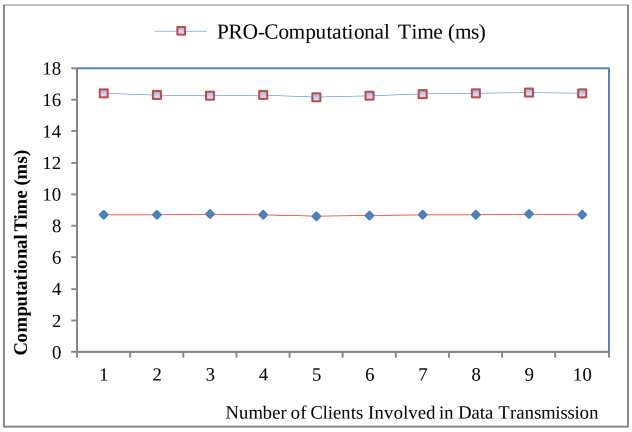


Figure-4: Computational Time Comparison

The obtained results are given in Figure-1 and 2 illustrate the real-time computations and CPU computation time based on the number of clients. From the output, it is clear and noticed that the proposed **M^{3}HP** is better than the SPPDA approach. When the number of nodes increases the compilation, comparison, and computational time increases and it is shown in Figure-3 and in Figure-4.

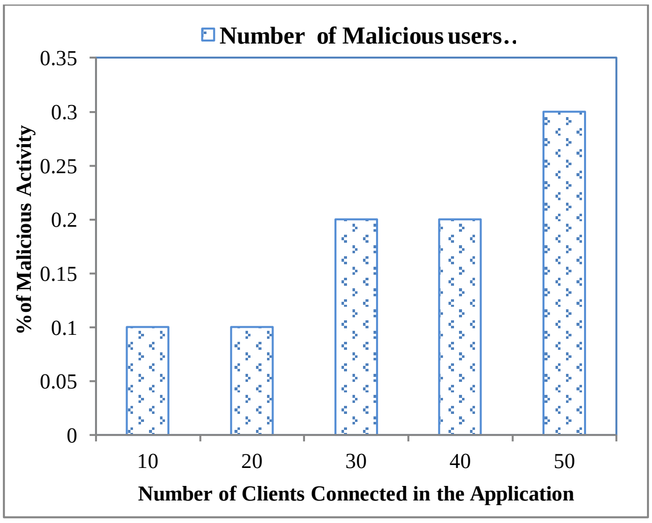


Figure-5: % Malicious Activity Detection

The time is taken for the real world and the CPU time taken is experimented and compared. From the comparison, it is obtained that the real and CPU time taken by the proposed approach is considerably lesser than the existing approach. Similarly, the complete computational time taken by the proposed approach is less than the existing system. The computational cost depends on the computational time. Since the computational time is very less, the computational cost is also very less and it is implicitly noticed.

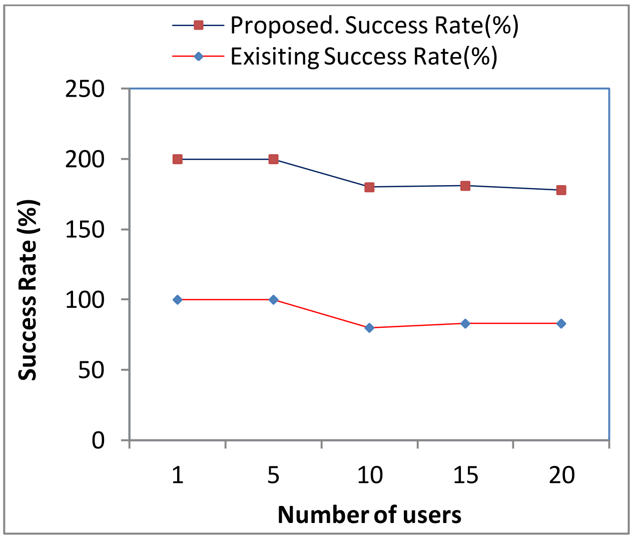


Figure-6: Number Human Password Secured Data Transmission

The main objective of security provision using various kinds of password generation methods is used to identify and detect the malicious activities. In this paper, the malicious activities can be detected by comparing the answers (A1 to A4), and the time interval t1 to t4 ∈ T. If the answers are not given in in-time or the interval t_i is not correct at any level then the user who tries to login into **M^{3}HP** is considered as malicious and there will be an intimation is generated to the server and the particular users' through mail or message to the mobile. In this paper, the number of malicious activity generation is assumed as 0.5% and the malicious activity is generated and the obtained result is given in Figure-5. From the result, it is clear and noticed that the % of malicious activities is less and it can be reduced further. Also, the number of success rate is calculated by changing the number of users at each round of operation. Each user in the cloud is asked to enter into a common application by human password and verified. The success rate is calculated before and after deploying the **M^{3}HP** algorithm and compared the performance. The obtained result is given in Figure-6. From the Figure-6, the **M^{3}HP** approach is proved as better in using human password generation method. Also, it is identified that the human password can bring universal uniqueness in security applications.

In future internal feature based human password generation is created and compared with the external feature based and the performance is evaluated.

CONCLUSION

The main objective of this paper is to provide a high security in terms of user authentication. To make security high, human body identification based password generation is applied. The password generation does not meet any high complexity, comparison, and more storage. The way of password generation is unique, not able to hack, less comparison, less memory usage and less computational time taken. Hence this password generation method is more effective and takes very less cost. This method is implemented and the results are verified. From the obtained results it is obtained that the **M^{3}HP** approach is more efficient and provides high security. In future, this approach is deployed in real cloud application and the results will be verified.

REFERENCES

1. D. Florencio and C. Herley. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web, pages 657-666. ACM, 2007.
2. I.A.D. Center. Consumer password worst practices. Imperva (White Paper), 2010.
3. H. Kruger, T. Steyn, B. Medlin, and L. Drevin, "An empirical assessment of factors impeding effective password management", Journal of Information Privacy and Security, 4(4):45-59, 2008.
4. J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords", In Security and Privacy (SP), 2012 IEEE Symposium on, pages 538-552.
5. Cert incident note in-98.03: Password cracking activity. http://www.cert.org/incident_notes/IN-98.03.html, July 1998. Retrieved 8/16/2011.
6. I.A.D. Center. Consumer password worst practices. Imperva (White Paper), 2010.
7. Sam. Biddle. Anonymous leaks 90,000 military email accounts in the latest antisec attack. http://gizmodo.com/5820049/anonymous-leaks-90000-military-email-accounts-in-latest-antisec-attack, July 2011. Retrieved 8/16/2011.
8. Nato site hacked. http://www.theregister.co.uk/2011/06/24/nato_hack_attack/, June-2011. Retrieved 8/16/2011.
9. Abe. Singer. No plaintext passwords. ; login: THE MAGAZINE OF USENIX & SAGE, 26(7), November 2001. Retrieved 8/16/2011.
10. Zappos customer accounts breached. http://www.usatoday.com/tech/news/story/ 2012-01-16/mark-smith-Zappos-breach-tips/52593484/1, January 2012. Retrieved 5/22/2012.
11. Oh man, what a day! an update on our security breach. http://blogs.atlassian.com/news/ 2010/04/oh_man_what_a_day_an_update_on_our_security_breach.html, April 2010. Retrieved 8/18/2011.
12. Apple security blunder exposes lion login passwords in clear text. http://www.zdnet.com/ blog/security/apple-security-blunder-exposes-lion-login-passwords-in-clear-text/ 11963, May 2012. Retrieved 5/22/2012.
13. Update on play station network/Qriocity services. http://blog.us.playstation.com/2011/ 04/22/update-on-play station-network-Qriocity-services/, April 2011. Retrieved 5/22/2012.
14. An update on linked to member passwords compromised. http://blog.linkedin.com/2012/ 06/06/linkedin-member-passwords-compromised/, June 2012. Retrieved 9/27/2012.
15. The data breach at ieee.org: 100k plaintext passwords. http://ieeelog.com/, September 2012. Retrieved 9/27/2012.
16. Important customer security announcement. http://blogs.adobe.com/conversations/ 2013/10/important-customer-security-announcement.html, October 2013. Retrieved 2/10/2014.

17. Jeremiah Blocki, Manuel Blum, and Anupam Datta. Naturally rehearsing passwords. In Kazue Sako and Palash Sarkar, editors, Advances in Cryptology - ASIACRYPT 2013, volume 8270 of Lecture Notes in Computer Science, pages 361{380. Springer Berlin Heidelberg, 2013.
18. Manuel Blum and Santosh Vempala. Publishable humanly usable secure password creation schemas. Proc. of HCOMP, 2015.
19. Anees Ara, Mznah Al-Rodhaan, Yuan Tian and Abdullah Al-Dhelaan, (2016), “A Secure Privacy-Preserving Data Aggregation Scheme based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems”, IEEE, Translations and content mining, Vol. 5, No. 1, PP. 12601 – 12617.
20. J. A. Akinyele et al., (2013), “Charm: A framework for rapidly prototyping cryptosystems,” Journal of Cryptography Engineering, vol. 3, no. 2, pp. 111–128.
21. M. Bellare, B. Waters, and S. Yilek, “Identity-based encryption secure against selective opening attack,” in Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, Springer, Heidelberg, 2011, pp. 235-252.
22. Adi Shamir, “Identity-based Cryptosystems and Signature Schemes”, Adv. in Cryptology, CRYPTO’84, vol. 196, LNCS, New York, USA, Springer Berlin, 1985, pp. 47-53.
23. Dan Boneh and Matt Franklin, “Identity-Based Encryption from the Weil Pairing,” CRYPTO’01. Int. Cryptology Conf. on Advances in Cryptology, London, UK, August 19-23, Springer, Vol. 2139, 2001, pp. 213-229.
24. R Canetti, S Halevi, and J Katz, “A forward-secure public-key encryption scheme,” EUROCRYPT'03. Int. conf. in TACT, Springer, 2003, pp. 255-271.
25. Jongkil Kim, Willy Susilo, Man Ho Au, and Jennifer Seberry, "Adaptively Secure Identity-Based Broadcast Encryption With a Constant-Sized Ciphertext", IEEE Transactions On Information Forensics And Security, vol. 10, no. 3, Mar. 2015.
26. Nie TY, Song C, Zhi X. Performance Evaluation of DES and Blowfish Algorithms, 2010 International Conference on Biomedical Engineering and Computer Science, ICBECS, Wuhan. 2010; 1−4.
27. Arora R, Parashar A. Secure user data in cloud computing using encryption algorithms, International Journal of Engineering Research and Applications. 2013 Jul-Aug; 3(4):1922−26.
28. Boneh D, DiCrescenzo G, Persona G, Ostrovsky R. Public key encryption with a keyword search. In Advances in Cryptology-Eurocrypt, Springer-Verlag: Berlin Heidelberg. 2004; 506-22.
29. Blessed Prince P, Krishnamoorthy K, Anandaraj R, Jeno Lovesome SP. RSA-DABE: A Novel Approach for Secure Health Data Sharing in Ubiquitous Computing Environment. Indian Journal of Science and Technology. 2015 Aug; 8(17): 1−9.