AUTHENTICATION METHOD FOR PASSWORD ENCRYPTION

BY

MD KHALIDUR RAHMAN
ID: 161-15-7131

SOVAN ROY
ID: 161-15-6958

AND

MEHEDI HASAN EMON
ID: 161-15-6741

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Shah Md Tanvir Siddiquee
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised By

Narayan Ranjan Chakraborty
Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

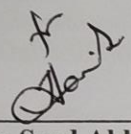
DHAKA, BANGLADESH

DECEMBER 2019

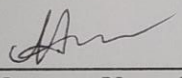
APPROVAL

This project titled "**AUTHENTICATION METHOD FOR PASSWORD ENCRYPTION**", submitted by MD KHALIDUR RAHMAN, ID No: 161-15-7131, SOVAN ROY, ID No: 161-15-6958 and MEHEDI HASAN EMON, ID No: 161-15-6741 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering (B.Sc.) and approved as to its style and contents. The presentation has been held on 7th December 2019.

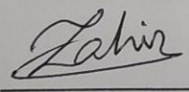
BOARD OF EXAMINERS



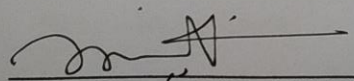
Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Nazmun Nessa Moon — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Gazi Zahirul Islam — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Mohammad Shorif Uddin — **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

©Daffodil International University

DECLARATION

We hereby declare that; this project has been done by us under the supervision of **MR. SHAH MD TANVIR SIDDIQUEE, Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Shah Md Tanvir Siddiquee
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised by:

Narayan Ranjan Chakraborty
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

Md. Khalidur Rahman

Md Khalidur Rahman
ID: 161-15-7131
Department of CSE
Daffodil International University

Sovan Roy

Sovan Roy
ID: 161-15-6958
Department of CSE
Daffodil International University

Mehedi Hasan Emon

Mehedi Hasan Emon
ID: 161-15-6741
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We really grateful and wish our profound our indebtedness to **Shah Md Tanvir Siddiquee, Assistant Professor,** Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Cryptography*" to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Dr. Syed Akhter Hossain, Professor and Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This the 21st century where each and everything are becoming digitalized. Everyone makes his life comfortable with the benefits of technology. As a result various kinds of data like personal, business and so on are stored in the online platform. To access the data the users need to create account and have to use password in the system to get authenticated. Sometimes the sensitive information like password of a user has stolen from the database by the hacker. Without using the traditional method we design a methodology named "**AUTHENTICATION METHOD FOR PASSWORD ENCRYPTION"** to encrypt the password of the user. In our methodology we make a conversion of user inputted password and date of birth during the time of registration. According to the methodology which we design, a calculation will happen and finally the output result will save into the database against password without saving the raw password. When the user login to the system and input his raw password then according to the methodology it will calculate again and match the calculated value with the database value. If the database access goes to any third party, they will not get the exact password of any users. Our encryption method secure the users password into database as well as secure them to leak their personal sensitive data

TABLE OF CONTENT

List of Figures

List of Tables

TABLES **PAGE**

CHAPTER 1

INTRODUCTION

1.1 Introduction

In our daily life, we are now familiar with online platforms. We are used to use it in our daily basis to make our life more comfortable. The number of online platforms are increasing day by day. Everyone shares a lot of important staffs by using the medium of various kinds of web application. To keep secure the sensitive information of the users as well as to secure them different organization have different rules or technique. But the users have a headache about losing the sensitive information as like as password.

Every time, the web application developer or the owner of that web application do not think how the password of the users will store into the database. As a result many of the web application have the traditional method to store the login information into database as a raw input of the users.

So, we think about the problem and define a method which will convert the raw password and stores it into the database. During the signup process the users have to input the personal information as well as password which is required to get login into the system. From the inputted birthday and password during the signup process, we make a binary conversion of the password which is inputted by the users and calculate a base value from the birthday and finally make a calculation and generates a unique value for the unique users and stores it into database. As a result, after having the database access they can't get the actual password of any users.

1.2 Motivation

The word is moving towards digital system in every sector. Personal to business, social to governmental information are available on online platform. But due to proper security information are disclosed to the third party. It impacts on daily life, spoils the image of an organization and so on. The numbers of new technology are increasing daily in a numerous quantity. The use of password in every online platform is a mandatory phenomenon. As a result the numbers of third party has increased whose main focus is to ransack the confidential information and sell it to the black market.

It's estimated that people will have to manage as many as 300 billion passwords by the year 2020 and some estimates say that nearly 100 password are stolen in every second, that's more than 8 million password per day[9]. The concern is to leak the confidential information and availability to the blackmailer.

Nowadays, building up online platform is a tradition and it's playing an important role for a person, an organization. Most of the users have no idea about the backend process of the system. They never know the reliability how much their information are secured. Many of the online platform owner don't follow any encryption methodology to store the sensitive data of the users. Sometimes it's cost high so they neglect it.

Who takes the responsibility to secure the password of the users from the third parties?
There has been a lot of methodology to encrypt password. But at this time many of them are easily breakable and the others are not cost efficient.

So, we want to introduce a methodology where the developer can easily use the method to secure the password of their users into their database. Coming out from the traditional method if it use, the secret key will be encrypted within a time.

1.3 Rationale of the Study

A crucial moment is created when the secret information is disclosed publicly. It can be personal or important information about any organization. Nowadays it's a common news that secret information like login information of users are stolen from the central database of a web application or platform. Every year a lots of secret information are selling to the grey market. In 2019, around 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords was posted on the web for sale [10].

Most of the cases, million numbers of password are stolen by the hacker. The hacker just find out the fault of the system and make them happy by stealing the secret information. Most of the times, the owner or the developer do not apply any encryption methodology to protect the users. As per the result the hackers can easily get the raw information from the database. On the other hand, because of using traditional method of the encryption the information are also lost. Nowadays, the traditional encryption has easy or available decryption method. Perhaps, to minimize the cost of that platform they don't apply any paid or secret method to protect the data.

1.4 Research Questions

- What is the definition of encryption and why it is important?
- What are the common benefits of encryption?
- What types of algorithm is used to do this encryption?
- What the base value in the calculation for the algorithm?
- What types of value will generate after encryption?
- What are the benefits of this methodology?
- Is it possible to get login with the encrypted value stored into the database?
- Is it tested with guess attacking or dictionary attacking?
- What will be the final value format of password which will be saved into the database?
- Is it possible to get the exact password by converting the database value into text?
- Do the authentication process of signup and login are time consuming?
- Which platform is used to test the method?
- Is it possible to applicable in any platform?

1.5 Expected Outcome

The numbers of people of online dependency are increasing daily. They are creating new accounts on different platform and using password to get authenticated on that platform. Our main target is to introduce a methodology which will encrypt the inputted raw password of the users and according to the methodology a calculation will give a different value based on the user.

Our main focus is to keep secure the password into the database. According to our method the calculation for each unique users will generate unique values based on the define condition. As a result, if anyone have the database access, they will not get the raw password and also can’t login with the value which is saved into the database.

1.6 Report Layout

Chapter 1: Introduction

In this chapter, we have reviewed the introduction, motivation of the work, rationale of the study, research questions and expected outcome of the research work and the report layout.

Chapter 2: Background

We discussed the background elements of our work. We also delivered the literature review, research summary, and scope of the problem and the difficulties of the system.

Chapter 3: Research methodology

In this chapter, we have introduction of our research subject and instruments. Here we showed how we collected the data and also the statistical analysis of the collected data. This things we needed to complete the research are described here.

Chapter 4: Experimental results and discussion

Here in this chapter all the experimental result that has been achieved by the proposed method is explained along with the performance judgment and a version of the result is covered.

Chapter 5: Summary, Conclusion, recommendation and implication for future research

In this chapter we have the summary and conclusion of the research study. We also have some recommendations and suggestions for the further study of this research.

CHAPTER 2

BACKGROUND

2.1 Introduction

Nowadays information is increasing exponentially day by day in the online world. In together, the risk of leaking sensitive data (like -personal data) is increasing. It is almost vice-versa to the advancement of technology. Data hacking is the most anxiety issue in this era. Therefore, we have to prevent this illegal data hacking, theft at any cost.

Following the above circumstances, we have decided to develop an innovative methodology that will be helpful, fruitful to secure anyone's sensitive data. We have completed sufficient study behind our methodology. For ensuring data integrity, there are many methods including backups, encryption, pseudonymization,access control etc. We have studied numerous numbers of algorithms, different types of possible attacks for data hacking.

Hence, we think our proposal will be convenient to secure sensitive data from unexpected attacks. In our project, we have tried initially to change data format using the encryption-method. A user's password saving process in any database is so valuable. Because, if any invader hacks the database, he will find the password of a user. We can say, user's password is all and it is most worthy. So, we have designed our password storing process in the database in which if a cracker breaks down our database anyhow, he cannot log in to the user's profile. Hence, the hacker's efforts will be valueless.

2.2 Related Works

This is neither an original nor a new concept. There are many existing implementations like our proposal system after the introduction of **Authentication Method for Password Encryption.** However, this is a new plan for adding a new era for securing a user's password with proper secure strengthen.

The paper [1], has proposed an innovative explication that generates a true random number from an image of 25*25 pixels (black and white). A user can easily create this image from ms-point software. The proposed method of producing a true random number is cheap and useful for users. It is also a cost-effective and good method for cryptographic applications. In this paper, two value p and g are taken from an image by concatenating columns or rows of

the selected image. Before that 625 numbers generating by using pixel value by a function from .NET. This function converts all pixel values into string value and then these string values are converted into a binary format. Here checking the RGB value of each and every pixel is an important role. XOR, mapping, discarding, etc. many methods can apply for creating random numbers.

$$R_1 = g^x \ mod \ p$$

$$R_2 = g^y \ mod \ p$$

$$K_1 = (R_2)^x \ mod \ p$$

$$K2 = (R_1)^y \ mod \ p$$

Here, if K_1 and K_2 will be the same, then any secure transactions will be occurred. Otherwise, the transaction does not happen.

The paper [2], has introduced a method in which 3d objects are created with the aid of unity 3d software. Then hardware named epic motion track theses selected/chosen objects by user's hand or finger. After that, those selected objects have been transferred to the algorithm that they have used and afterward the algorithm generates a unique password for the client.

The paper [3], they have proposed a method in which they have modernized the play fair method into a new stage, where they have encrypted and decrypted text file. In their proposal, they have made promotions for encrypting messages multiple times which is not easy to play fair method. The pattern of the key matrix will depend on the initial text key provided by the user.

After calculation the randomization number, encryption number, and the shift parameter from the user's given text key, they have performed different functions like,

cycling(),upshift(),downshift(),leftshift(),rightshift(),random(),random_diagonal_right(),rand om_diagonal_left()

After all procedures, they have encrypted a text file and decrypted that (decrypted file from text file provided by the user) again. Their method operates superbly. The decrypted message (text) is the same as the original text. They have formed a fruitful result. It is very tough to match the three parameters (randomization number, encryption number, the shift parameter) for 2 different text-key. As a result, if an intruder desires to break the encryption method, he has to affirm the exact pattern of the text key. Even if anyone implements the BFS method,

then he has to give trail for 256! Times which is ridiculous. Because the encryption key matrix is 16*16.As a result, the total elements of the matrices are 16*16=256.

The Paper [4], has proposed a two-stage verification technique for user authentication in a smartphone. Firstly, the normal graphical text password. Secondly, a session-based 3d image where some objects are driving as a password. To the approach of making a password more secure, they have added 3d image environment and movement in extra stage for avoiding guessing attack, dictionary attack which are drawbacks of normal text-based authentication.

2.3 Research Summary

In our study, we are aimed to find a worthwhile solution for data encryption system. We have done sufficient study behind our works. We have studied AES algorithm, DES algorithm, RSA algorithm, Diffie-Helman algorithm, play fair method, discrete algorithm attack, Man-in-middle attack, Guess attack, Dictionary attack, Random sequences, etc. We have studied several numbers of articles, thesis papers, documents related to encryption, tutorials, videos related to our works.

For example [5] [6] [7] [8], Discrete algorithm attack and man-in-middle attack are two significant weaknesses of Diffie-Helman algorithm. Pseudo random numbers are less secured than True random numbers because it is created from non-deterministic resources. Random sequences are categorized into two classes: PRNGs (pseudo random numbers) and TRNGs (true random numbers). Pseudo random sequences can de be produced from deterministic source BBS methods, ANSI X9.17, FIPS 186 generator, etc. [6]. True random numbers are formed from hardware, software, and de-skewing methods [6]. It is more secure, compared to pseudo random numbers. But it requires extra devices which makes inconvenient for normal users.

True random number generator method based on image for key exchange algorithm [1] is a very economical and cost-effective. No supplementary device is wanted for producing true random numbers from this recommended method and the speed is high. It generates 256 bits key or higher bits from a small image.

In the paper, they have applied the maximum randomization number=128 and maximum encryption number=64.In the existing work, the key matrix may be created in 256! ways. The proposed work is a substitution method. It can be employed to replace a character by any of

the 256 characters. Hence in principle, it will be challenging for any to decrypt the encrypted text without identifying the exact key matrix. This method is basically stream cipher method. If the file size is long, then it takes a huge amount of time. Another significant site of this methodology is that anyone alters the key text a little bit then the entire encryption and decryption process will change. This method can be applied in many sensitive sectors where data is important to be secure. Like: in ATM, railway reservation systems, banks, in sensor nodes, in defense [3].

In all papers motivated the different types of security of data in different ways. They have applied 3d image movement for generating passwords in the final stage, epic motion hardware for selecting objects by user's hands/fingers, unity 3d software for creating 3d objects for further calculation through the algorithm for generating a unique password for a user. Moreover, MS-point software for creating 2d objects. Some functions, methods have been acquainted with us.

In our efforts, we are going to introduce a new, innovative, less time consuming, easier, effective method for encrypting user's password to the aim of protecting these sensitive data from unexpected authentication.

2.4 Scope of the problem

This study concentrates on gaining a way to develop a smart encryption system to diminish the risk of hacking data as well as more trustworthy performance.

In true random number generator method based on image for key exchange algorithm, calculationR_1,R_2 depends on p and g. Those are rows or columns respectively of the source image. But accomplishing transactions between two users, two users should have the same image. We want to point that image has to transfer through some medium like messenger, email, google drive another transferring medium. But we know, pixels of the image are lessened in transferring through messenger, WhatsApp. Some medium is not convenient to hold image pixels genuine. This is one of the pointed issues of this method. Because p and g should be fixed, immutable according to this proposed method. But if anyone transfers an image to others via messenger or WhatsApp in where image pixels will change, then p and g will be changed. As a result, the proposed method will break down. On the other hand, having requirement same image to two users for the goal of a transaction is so boring and

absurd in some situations when you want a quick transaction. Hence, we think to have the same pictures requirement to begin and end-user should eliminate [1].

In the exploration of 3d graphical passwords, no algorithm is specified. It is an unexpected issue. This method is not implemented on a smartphone. But now most people use smartphone comparing with the computer. Thus, it is not convenient for a smartphone. Because another additional hardware called epic motion is required for object selection with the approach of passwords formation. So, it is expensive and hassles issue. In this paper, only sign up procedures are explained. But the login procedure is not mentioned. If a user wants to log in, then how objects will be generated that issue is not clear. On the other hand, if we want to apply this method on any website or app, then a website or app can be oppressed for the unity 3d software [2].

In this paper, they have suggested that the second stage 3d image will be changed when a new session will start. That's good. Because in this final stage an intruder will be puzzled to guess the user's image password by shoulder mapping. But the user has to retain his moveable objects for generating a password. If there is an easier way of avoiding remembering the picked moving objects, then this verification procedure will be more effective and easier, convenient for the user [4].

2.5 Challenges

2.5.1 Possibility of matching encrypted password

We have to design our methodology in such a way in which the chance of matching encrypted passwords of different users is reduced dramatically. We have to use a unique technique so that the encrypted password is generated uniquely. We have to think of making an innovative, new idea excepting other existing algorithms for overcoming the existing vulnerability to the aid of composing a powerful method.

2.5.2 Possibility of login if encrypted passwords are found out

Besides, we have to ensure if anyone can find out encrypted passwords against original passwords, he will not able to log in the user's profile.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

To recognize the encrypted final value exactly according to our method, the signup portion is the most important part. From the signup portion, the date of birth is the first priority for the calculation of our encryption. From the date of birth of the users we have to calculate the base value. Fig 3.1 reflects the sequence of the structure for this encryption methodology. In this article, number conversion system is used to convert the password of the users from string to binary. Then the rest of the procedures are extracted to the data flow diagram model. PHP, HTML, Bootstrap, JQuery, MySQL are used to visualize the encryption as output.

To determine the encryption a database system is required which will store the final outcome and fig 3.1 defines the ways of steps to do the operation and stores the final encrypted values.

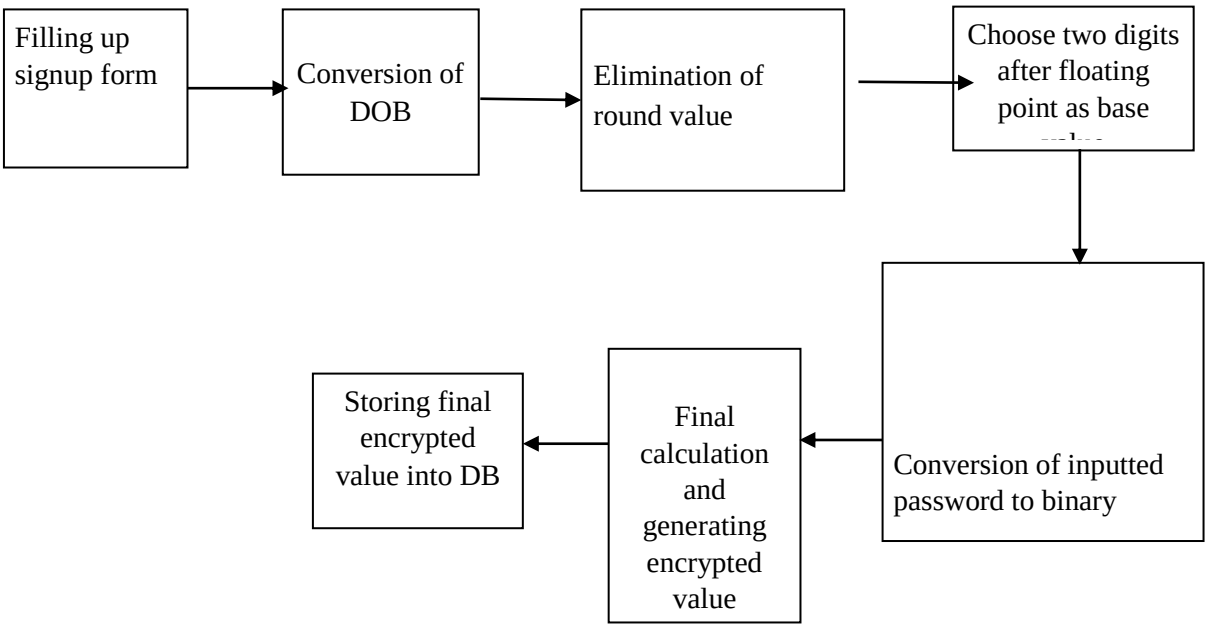


Figure 3.1.1: Proposed data flow diagram

3.2 Research Subject and Instrumentation

3.2.1 Filling up signup form

We are providing a simple sign up form including first name, last name email, password and date of birth to a user for storing user's information in the database to the aid of login.

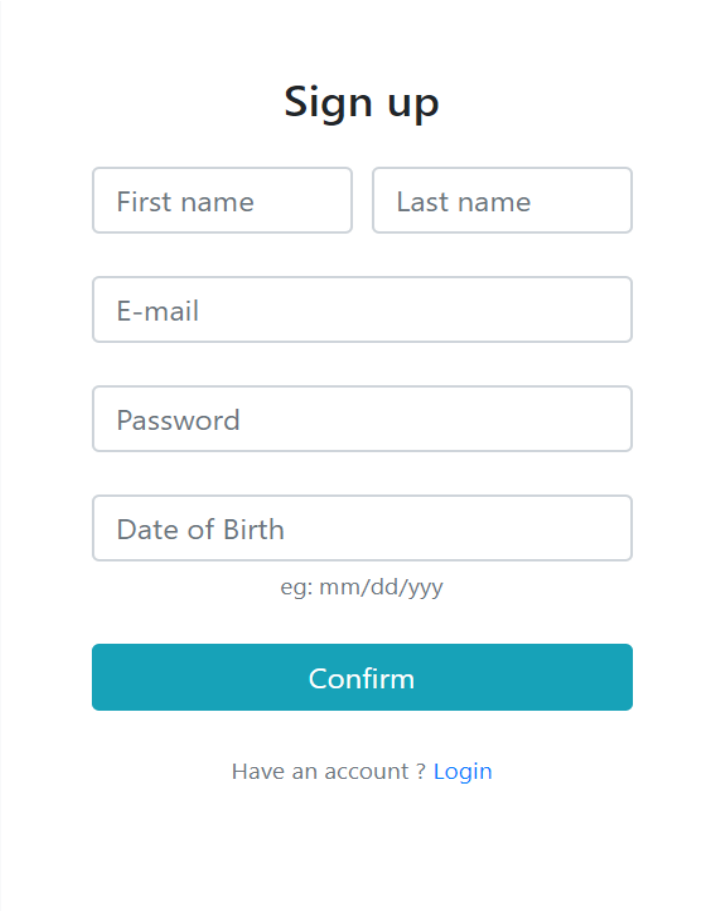


Figure 3.2.1:Signup form

3.2.2 Conversion of DOB

In this, section we or our recommended method will complete a calculation on the date of birth of a user's. The summation of 3 portions month, date and year is calculated here. We have used explode function to eliminate "/" symbol from date of birth. Then, again the square root of this summation is calculated. Suppose, here is an example of a user's date of birth and further calculation is given below.

Date of birth: 10/10/1991

Sum of portions of date of birth: 10+10+1991=2011

The square root of summation: $\sqrt{2011}$ =44.8441746

3.2.3 Elimination of round value

Then, we have to go to the next steps, elimination of round value. Here, our method will occur a performance to drop the round value of the square root value. By calling, explode function we have eliminated the round value in PHP.

Value of square root: 44.8441746

After the elimination of round value from the square root, we get from=8441746

3.2.4 Choose two digits after floating point as base value

In this step, we have to pick two digits as the base value after the elimination of round value for the further calculation of the main equation of our method. Assume, after the elimination of round value from the square root we get 8441746. So, the base value will be the first two digits and it is 84 against this value.

We can see that base values are different if the date of birth is different. There is no chance of being the same base value if the date of birth is different.

3.2.5 Conversion of inputted password to binary

In this step, we have converted the user's password in binary form. It is too much important to convert string in binary according to our method. We have used the PHP function strToBin3() for converting the string in binary form. Suppose, a user's password is aB45*c4.

So, the binary form against this password is 01100001 01000010 00110100 00110101 00101010 01100011 00110100.

3.2.6 Final calculation and generating encrypted value

Our main equation of our method is=binary form of user's password$*\sum_{m=0}^{n} b^n$

Here,

B=base value depending on date of birth.

n=index number of binary form array.

Suppose, the binary form of a password is 01100001 01000010 00110100 00110101 00101010 01100011 00110100 and the base value is 84.Hence, according the main equation the final desired encrypted password will be 7.6200006960217E+159.

Final encrypted password=01100001 01000010 00110100 00110101 00101010 01100011 00110100*(84^0 + 84^1+84^2+84^3+84^4+84^5+84^6+84^7+84^8+84^9+84^{10}+84^{11}+84^{12}+84^{13}+84^{14}+84^{15}+84^{16}+ 84^{17}+84^{18}+84^{19}+84^{20}+84^{21}+84^{22}+84^{23}+84^{24}+84^{25}+84^{26}+84^{27}+84^{28}+84^{29}+84^{30}+84^{31} +84^{32}+84^{33}+84^{34}+84^{35}+84^{36}+84^{37}+84^{38}+84^{39}+84^{40}+84^{41}+84^{42}+84^{43}+84^{44}+84^{45}+ 84^{46}+84^{47}+84^{48}+84^{49}+84^{50}+84^{51}+84^{52}+84^{53}+84^{54}+84^{55})= 7.6200006960217E+159

3.2.7 Storing final encrypted value into DB

In Here is a screenshot of the database, where 4 users' encrypted passwords have stored individually. The user's name, email, and date of birth also have stored in the database.

	id	fname	lname	email	pass	dob
Edit Copy Delete	12	test	user1	test1@gmail.com	7.6200006960217E+159	10/10/1991
Edit Copy Delete	13	test	user2	test2@gmail.com	2.7930067270043E+150	4/25/1960
Edit Copy Delete	14	test	user3	test3@gmail.com	2.4144589706416E+138	2/20/2001
Edit Copy Delete	15	test	user4	test4@gmail.com	4.2871345301351E+171	1/15/1971
Edit Copy Delete	16	test	user5	test5@gmail.com	6.7634676400115E+143	5/22/2005

Figure 3.2.7.1: Store into database

3.3 Data Collection Procedure

For the purpose of our research, we don't need any field work for data collection. Our main resource for data is users. In the time of signup process, the users input their basic information like first name, last name, email address, date of birth, password etc. Our main focus points are date of birth and inputted password of the users which we recognize by putting manual inputs of different date of birth and password in string includes special character. At time of signup, unique inputs of the users is the data set for our encryption methodology.

3.4 Statistical Analysis

As per the analysis of data, calculation of the accuracy of the proposed system is achieved 100%. In the case of the calculating base value from date of birth of two users are same then the base value of the two users will remain the same. But the final calculating values of encryption will be unique for the two users because the inputted password will be different and the length of the binary digit will be different. In the case of same date of birth and password then the final encrypted values will be same but it's hard to happen. Besides, we have compared our user's encrypted passwords according to our proposed method with MD5 hash, SHA1 hash generator algorithm.

Table 3.4.1: Same DOB and different password

Users	Date of birth	Base Value	Inputted Password	Final Encrypted value
Test1	10/10/1996	89	cse@diu	8312799159486E+161
Test2	10/10/1996	89	Love43bd	5607761371503E+184

Table 3.4.2**:** Comparison with MD5 hash

User	Original password	Our method	MD5 hash
User 1	aB45*c4	7.6200006960217E+159	1C122258F9C509243E16B64CF7ABEA4A
User 2	410Ac@d	2.7930067270043E+150	B3B9BA9FD9C9A4F7B13CEBC4085B7B4B
User 3	#xy$0B	2.4144589706416E+138	A95973979A3E7111E6033B8CFF426D9F
User 4	*06*#AsD	4.2871345301351E+171	858DED0BA509403AA036F35E32A50954

Table 3.4.3: Comparison with SHA1 hash

User	Original password	Our method	SHA1 hash
User1	aB45*c4	7.6200006960217E+159	C56BB2D36EF64780FD85D6DB46D5040C237D59C4
User2	410Ac@d	2.7930067270043E+150	EB840C7697D15AC42F324DF5AE05E6B255A48B4E
User3	#xy$0B	2.4144589706416E+138	633351DED7A545C9617EB260760E5ACB16688D32
User4	*06*#AsD	4.2871345301351E+171	1CA59B59D31697ACC620C3F1E8AF2F3FDCD43E13

Table 3.4.4: Comparison with SHA256 hash

User	Original password	Our method	SHA256 hash
User1	aB45*c4	7.6200006960217E+159	8C053DD814183E2B0A02231BE57F3895EA8FDF6452F5A0D31B993FDE70BEA1CB
User2	410Ac@d	2.7930067270043E+150	A8DDC65FB9C46EF69C093F6520F3E7BD57A9F736D5B5774E0AFC36ACF53B69D9
User3	#xy$0B	2.4144589706416E+138	8563E24732BF13CF7C91DDE5886F6EEDFA6B6EE2A265CB71E71B2E5C02358D76
User4	*06*#AsD	4.2871345301351E+171	78E9067AFE3BB6E910BF56EB68142A6A6F1AF49052D026C27EEEF4F194D3DDE3

3.5 Implementation Requirements

We have implement of our research methodology into a web application to get the output. For implementing the process XAMPP is installed must into the device. A web browser is also needed to test the graphical user interface. The focus point of this system is encryption. So both the database system and web browser is mandatory to visualize the input and output. Encryption is a very interesting area in computer science and also useful to protect personal, secret information.

On the other hand, when the method is implemented into an online server then the internet connection is a must besides the two other components. A fast internet and speedy servers provide the best service in this case because during the conversion of password a calculation will happen. At the time of login process, the calculation will happen and match the calculated value with the database value and the users can login.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

We have performed our experiments on 5 users to justify our methods so that we can see our methodology calculation for encrypting the user's password for ensuring data integrity from unexpected attacks. After several steps completing, finally our most desired password is generated. Steps are-

Filling up signup form, Conversion of DOB, Elimination of round value, Choose two digits after floating point as base value, Conversion of inputted password to binary, final calculation and generating encrypted value, Storing final encrypted value into DB.

4.2 Experimental Result

4.2.1 Conversion of DOB

We are providing 4 user's date of birth conversions as examples below.

User 1:

Date of birth: 10/10/1991

Sum of portions of date of birth: 10+10+1991=2011

Square root of summation: $\sqrt{2011}$=44.8441746

User 2:

Date of birth: 4/25/1960

Sum of portions of date of birth: 4+25+1960=1989

Square root of summation: $\sqrt{1989}$=44.5982062

User 3:

Date of birth: 2/20/2001

Sum of portions of date of birth: 2+20+2001=2023

Square root of summation: $\sqrt{2023}$=44.9777723

User 4:

Date of birth: 1/15/1971

Sum of portions of date of birth: 1+15+1971=1987

Square root of summation:$\sqrt{1987}$=44.5757782

User 5:

Date of birth: 5/22/2005

Sum of portions of date of birth: 5+22+2005=2032

Square root of summation:$\sqrt{2032}$=45.0777107

4.2.2 Elimination of round value

User 1:

Value of square root: 44.8441746

After the elimination of round value from the square root, we get from=8441746

User 2:

Value of square root: 44.5982062

After the elimination of round value from the square root, we get from=5982062

User 3:

Value of square root: 44.9777723

After the elimination of round value from the square root, we get from=9777723

User 4:

Value of square root: 44.5757782

After the elimination of round value from the square root, we get from=5757782

User 4:

Value of square root: 45.0777107

After the elimination of round value from the square root, we get from=0777107

4.2.3 Choose two digits after floating point as base value

We can see that base values are different if the date of birth is different. There is no chance of being the same base value if the date of birth is different.

Table 4.2.3.1: Base value table

User	Sqrt value	Picking base value
User1	44.8441746	84
User2	44.5982062	59
User3	44.9777723	97
User4	44.5757782	57
User5	45.0777107	07

4.2.4 Conversion of inputted password to binary

Table 4.2.4.1: Password to binary

User	Inputted password	Binary form
User1	aB45*c4	01100001 01000010 00110100 00110101 00101010 01100011 00110100
User2	410Ac@d	00110100 00110001 00110000 01000001 01100011 01000000 01100100
User3	#xy$0B	00100011 01111000 01111001 00100100 00110000 01000010

User4	*06*#AsD	00101010 00110000 00110110 00101010 00100011 01000001 01110011 01000100
User5	&$**500R#w	00100110 00100100 00101010 00101010 00110101 00110000 00110000 01010010 00100011 01110111

4.2.5 Final calculation and generating encrypted value

Our main equation of our method is=binary form of user's password$*\sum_{m=0}^{n} b^n$

Here,

B=base value depending on date of birth.

n=index number of binary form array.

Hence, we are giving a table of 4 users' encrypted keys against original passwords below:

Table 4.2.5.1: Binary to final encrypted value

User	Original password	Binary form	Final encrypted value
User1	aB45*c4	01100001 01000010 00110100 00110101 00101010 01100011 00110100	7.6200006960217E+159
User2	410Ac@d	00110100 00110001 00110000 01000001 01100011 01000000 01100100	2.7930067270043E+150
User3	#xy$0B	00100011 01111000 01111001 00100100 00110000 01000010	2.4144589706416E+138
User4	*06*#AsD	00101010 00110000 00110110 00101010 00100011 01000001 01110011 01000100	4.2871345301351E+171
User5	&$**500R#w	00100110 00100100 00101010 00101010 00110101 00110000 00110000 01010010 00100011 01110111	6.7634676400115E+143

4.2.6 Calculation and generating encrypted value with java

IEEE 754 in java: To generate the encrypted password in IEEE 754 format, we have used java.lang.Double.doubleToLongBits() method of java double class that is built-in function in

java. This function delivers a representation of the specified floating-point value according to the IEEE 754 floating-point "double format" bit layout.

Parameter: The method allows only one parameter which defines a double-precision floating-point number.

Table 4.2.6.1: Final encrypted value in IEEE 754 standard

User	Original password	Binary form	Final encrypted value
User1	aB45*c4	01100001 01000010 00110100 00110101 00101010 01100011 00110100	5501765265919460868
User2	410Ac@d	00110100 00110001 00110000 01000001 01100011 01000000 01100100	1083529704134127437
User3	#xy$0B	00100011 01111000 01111001 00100100 00110000 01000010	1257811888323256133
User4	*06*#AsD	00101010 00110000 00110110 00101010 00100011 01000001 01110011 01000100	-2109808448118426433
User5	&$**500R#w	00100110 00100100 00101010 00101010 00110101 00110000 00110000 01010010 00100011 01110111	4255901647865118720

4.2.7 Figures for user's encrypted password using java with IEEE representation

User1:

```
Enter your birthdate(dd-mm-yy):
11-11-1995
Enter Your Password:
aB45*c4
Enter Your Password Again:
aB45*c4
Converting Binary....
11000011000010110100110101101010110001111010 0
Square root value is:4491
After divide:91
Final Encrypted Value for Database: 5501765265919460868
```

Figure 4.2.7.1: IEE value of User1

User2:

```
Enter your birthdate(dd-mm-yy):
1-10-2000
Enter Your Password:
410Ac@d
Enter Your Password Again:
410Ac@d
Converting Binary....
11010011000111000010000011100011100000011001 00
Square root value is:4484
After divide:84
Final Encrypted Value for Database: 1083529704134127437
```

Figure 4.2.7.2: IEE value of User2

User3:

```
Enter your birthdate(dd-mm-yy):
11-1-2000
Enter Your Password:
       #xy$0B
Enter Your Password Again:
       #xy$0B
Converting Binary....
10000010000010000010000010000010000010000010001111110001111001100100110000100010
Square root value is:4486
After divide:86
Final Encrypted Value for Database: 1257811888323256133
```

Figure 4.2.7.3: IEE value of User3

User4:

```
Enter your birthdate(dd-mm-yy):
1-1-2008
Enter Your Password:
*06*#AsD
Enter Your Password Again:
*06*#AsD
Converting Binary....
10101011000011011010101010001110000011110011100010 0
Square root value is:4483
After divide:83
Final Encrypted Value for Database: -2109808448118426433
```

Figure 4.2.7.4: IEE value of User4

User5:

```
Enter your birthdate(dd-mm-yy):
23-7-1999
Enter Your Password:
&$**500R#w
Enter Your Password Again:
&$**500R#w
Converting Binary....
10011010010010101010101011010111000011000010100101000111110111
Square root value is:4504
After divide:4
Final Encrypted Value for Database: 4255901647865118720
```

Figure 4.2.7.5: IEE value of User5

4.3 Descriptive Analysis

We have wanted to develop a user-friendly, secure encryption system to provide effective security of the user's password from the intruder. We have tried our best behind our works to make a sustainable system as soon as possible. Many algorithms, papers, articles, books have played an important role to make this sustainable work. We have developed our method in such a way that if any attacker attacks the database and gets the actual password of users, then he cannot log in to the user's profile. Because the inputted password goes through an effective calculation successfully. The most fancied final encrypted value is not in a small size. It is perfect for a smartphone, laptop, tab, and all devices. An intruder has to get a big amount of annoyances, troubles, hassles, difficulties, jars, bothers to break down this method.

We are working on how these encrypted passwords can be decrypted. Mainly, we are looking for our lickings behind our suggested method. Every work has a weakness site we know. Maybe, our method has these unexpected defects sites. Hence, in this step, our work is to decrypt our meaningless encrypted password.

We could use the hash algorithm (like MD5 hash, SHA1 hash, SHA256 hash, SHA512 hash algorithms) to encrypt a string. But, there are available decrypt forms of encrypted strings online according to these hash algorithms. As a result, our main goal would gain failure. For this reason, we have developed a unique algorithm to avoid these disadvantages.

4.4 Summary

At last, we can recommend using this beneficial method to encrypt the user's password in case of security. It is perfect for a smartphone, laptop, tab, and all devices. It is an easy, cost-effective, longer time consuming, user's friendly, more convenient for any user. Otherwise, an intruder has to get a big amount of hassles to break down this method. In our experiments, our method has passed various lickings of other algorithms triumphantly and got a satisfying mark. No additional accessory is needed, no image is needed. Just a small amount of data pack is needed for executing this proposed procedure.

CHAPTER 5
SUMMARY OF THE STUDY, LIMITATIONS, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH

5.1 Summary of the Study

The world climate is changing with the wind flow of the technology. In the next years it will also increase more than today. New types of technologies are introduced every day to make people lazy. Nowadays it's a trend and easy way to complete official tasks, personal communication without visiting physically. No one minds about it today because it's the best medium today to the people. A huge amount of data are inputting daily and storing it into the online database. A lots of new farms are introduced their business or other staffs in the internet. They are using various types of web application to reach the targeted people. But many organisations have no policy to protect their users. There are many existing encryption methodologies but either the organisations have no clear idea about it neither they are not concern about their users. Some people in our society who are dishonest and they have a habit to collect the confidential information of others people. They take personal benefit by disclosing that information. In this century, various types of personal data has a great demand in the dark world. In this sectors there's a lot of people whose profession is snatched the data of the users. They can do it because of the limitations of that system. But encryption can protect to reveal the data to the third parties. If the third parties can access to the database, they will not get the raw information of the users of that system. They have to decrypt it and finally they can access but they may be success or not. Because the stability of the methodology will define that. Taking knowledge about the existing methods of encryption, we try to encrypt a specific personal information of a user which is password. By implementing the process, we get success and hopeful that our process can encrypt the password properly and keep the users safe.

5.2Limitations

Our methodology has some drawbacks. Like:

1) The encrypted password length is big. There is more space is required for encrypted password. So, space-consuming is one of the problems.

2)If anyone gives a password of 14 lengths (that may be only of character or only of number or only of special character or a mix of number, character, special character), then the encrypted password is infinity. So, we recommend the maximum 11 lengths of the password because the base value also effects of generating the encrypted password.

3) If, we want to decrypt this encrypted password the actual password is needed. Because for decrypting the encrypted password the binary form of actual password and summation form is needed. In both issues, the actual password is needed. So, this kind of decrypt is absurd. But, we are searching for another way to decrypt the final encrypted password where the actual password will not need.

5.3 Conclusions

In this report, we have presented an encryption methodology without merging the existing methods. By using the number conversion system and a defined mathematical calculation equation is the key to encrypt the password of the users. Password and date of birth are inputted by the users during the signup process. The encryption of the passwords has been stored into the database and manual calculation for the same cardinalities provides the same result. We have achieved an accuracy of 96%, which is good as well as promising. To complete and experiment a few obstacles occur. During the testing periods of the encryption value, we get infinity value against the encryption value. It happens because of using lots of special characters in the password string. All of us know that, the length of binary conversion of any special character is long. We have use PHP for implementing the method. For using too much special character the calculation is too long and it provides infinity against the encrypted value. From the analysis of the password, a large number of users do not use too many special character. Otherwise using any characters and numbers, our proposed method provides the best outcome. Encryption is using in every sectors to protect data and it has a wide range of future to work with it.

5.4 Recommendations

Encryption has a vast of areas to protect data from the thieves. It can also use to the defence to send their messages from one point to another point. Confidential records of any Government can be protected by using this method.

5.5 Implication for Further Study

Everyone wants to make their life more comfortable in a shortcut way. For the purpose of daily needs and make life easier, the use of technology is increasing in every sector. For this reason, the amount of data is also increasing in the web servers. By surfing the web technologies, it's getting easier to find out useful information within a time and it's easy to store the information than the analog method. Considering the billions data of the users, many of them are very confidential. Password is one of them. In many cases, the raw information or data are storing into the database by using encryption methodology. Day by day the use of encryption is increasing and it has a broad range to do research with it. In our proposed method we can encrypt password of the users but it has also some limitations. One of the limitations is getting infinity encrypted value because of special characters in the password. If the problem can be solved in any other way then the accuracy can be 100%. Another chance is about our final encrypted value because the final output is a decimal number. From this step, it can be a chance to convert it into another format like special character or others. Encryption will be the best solution to protect the information as well as the users.

Appendices

Appendix A: Research Reflection

This part is provided to tell about the research reflection. It's a great challenge for us to work with a team. Without hard working it's not possible to go ahead. In university we have completed various courses and do a lot of projects. But it's totally different from the others. This thing is the most interesting part and every members of our group are enjoying it and everyone feels proud to be a part of this team.

A proper planning and discussion are the key to success of our research. We have to go through a lot of documents about this domain. Among the documents we have taken ideas and find out a procedure to do the work. Everyone welcomes the ideas of other team members. From this part, we gather a lot of experience and it will be very helpful to do a lot of staffs.

Appendix B: Related Issues

We don't have to visit physically to collect data. But it is quiet tough to realize the mind setup of an individual user. The quantity of the special character used in the password is the main concern. Because it can drive the calculation into infinity. Otherwise it's good to do the encryption process smoothly.

REFERENCES

[1] P. Murali and R. Palraj, "True Random number generator method based on image for key exchange algorithm", International Symposium on Computing, Communication, and Control (ISCCC 2009) Proc .of CSIT vol.1 (2011) © (2011), Singapore, 2009.

[2] Ilesanmi Olade, Hai-ning Liang, Charles Fleming, "A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays", SmartWorld Ubiquitous Intelligence & Computing Advanced & Trusted Computing Scalable Computing &Communications Cloud & Big Data Computing Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2018 IEEE, pp. 1997-2004, 2018.

[3]A. Nath, S. Ghosh and M. Mallick, "Symmetric Key Cryptography Using Random Key Generator.", in Proceedings of the 2010 International Conference on Security & Management, Las Vegas, Nevada, USA, 2010, pp. 234-242.

[4] B. S. Yerne and F. I. Z. Qureshi, "Design 3D Password with session based technique for login security in Smartphone," *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, Coimbatore,2016,pp.1-4.doi: 10.1109/GET.2016.7916769

[5] Schnier B, Applied cryptography: protocols, algorithms and source code in C. New York: John Wiley and sons, 1996.

[6] Menezes AJ, Oorschot PCV, Vanstone SA, Handbook of applied cryptography. Boca Raton, Florida, USA: CRC Press; 1997.

[7] Johannes A.Buchmann, Introduction to Cryptography. Second Edition, Springer –Verlag NY, LLC, 2001.

[8] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi,2007.

[9] "Password Security Report: 83% of Users Surveyed Use the Same Password for Multiple Sites - Cyclonis", Cyclonis, 2019. [Online]. Available: https://www.cyclonis.com/report-83-percent-users-surveyed-use-same-password-multiple-sites/. [Accessed: 29- Oct- 2019].

[10] "List of data breaches", En.wikipedia.org, 2019. [Online]. Available: https://en.wikipedia.org/wiki/List_of_data_breaches. [Accessed: 29- Oct- 2019].

PLAGIARISM

ORIGINALITY REPORT

11%	7%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ipcsit.com Internet Source	3%
2	Submitted to Daffodil International University Student Paper	2%
3	Nath, Joyshree, and Asoke Nath. "Advanced Steganography Algorithm using Encrypted secret message", International Journal of Advanced Computer Science and Applications, 2011. Publication	1%
4	Submitted to University of South Florida Student Paper	1%
5	www.cyclonis.com Internet Source	1%
6	Submitted to Macquarie University Student Paper	<1%
7	Ambreen Bano. "Random key generator using human voice", IMPACT-2013, 2013 Publication	<1%