Analysis of Secure Hash Algorithm (SHA-512) For Encryption Process on College Web Based Application

SUJITHA KAMEPALLI[1], A SUDHARSAN REDDY[2]

[1, 2] *Department of Computer Applications, Vasireddy Venkatadri Institute of Technology, Guntur, India*

Abstract- Student Information Management System offers a easy interface for preservation of student information. It can be used through instructional institutes or schools to preserve the archives of college students easily. The creation and management of accurate, Student data gadget offers with all kind of pupil details, academic associated reports, college details, direction details, curriculum, batch details, placement important points and other useful resource related important points too. Password-Based Encryption is used in the software due to the fact commonly the attacker again and again tries to bet undetected key phrases and is beyond the authentic sender / recipient control, if the keyword is used to log in to the server, it can detect many possibilities that are now not proper done and in the worst case is to shut down the server to prevent greater effort, if a tapper take encrypted documents that we use. Password Based Encryption with SHA512 is a cryptographic method the usage of algorithms that mix both hashing and trendy encryption methods

Indexed Terms- Student Information System, Database, SQL, Cryptography, Encryption, Decryption, SHA512

I. INTRODUCTION

Previously, the college relied heavily on paper documents for this initiative. While paper archives are a typical way of managing pupil information there are a number of drawbacks to this method. First, to bring facts to the students it need to be displayed on the observe board and the student has to visit the observe board to check that information. It takes a very long time to bring the data to the student. Paper records are hard to manage and track. The physical exertion required to retrieve, alter, and re-file the paper data are all non-value added things to do .This device offers a easy interface for the upkeep of pupil information. It can be used with the aid of academic institutes or faculties to preserve the records of students easily. Achieving this objective is challenging the use of a guide device as the information is scattered, can be redundant and amassing applicable data can also be very time consuming. All these troubles are solved the use of on line pupil records administration system.

The paper focuses on offering information in an easy and intelligible manner which provides full of security by using the usage of the SHA-512(Secure Hash Algorithm).The plan and implementation of a comprehensive student facts system and person interface is to change the cutting-edge paper records. College Staff are capable to directly get admission to all elements of a student's educational development via a secure, on line interface embedded in the college's website. The gadget utilizes person authentication, exhibiting solely statistics critical for an individual's duties. Additionally, each sub-system has authentication allowing approved users to create or replace records in that subsystem. All information is stored securely on SQL servers managed via the college administrator and ensures easiest feasible stage of security.

A. Purpose

The reason is to graph a university internet site which includes up to date statistics of the college. That should improve effectiveness of college document management with full of security by using usingSHA-512(Secure Hash Algorithm).

B. Objectives

- Providing the on-line interface for faculty etc.
- Increasing the efficiency of college record management.
- Decrease time required to get entry to and deliver pupil records.
- To make the machine more tightly closed with the aid of using SHA-512(Secure Hash Algorithm).

- Decrease time spent on non-value brought tasks.

C. Organization Of The Paper

The paper is geared up as follows: Section II provide an explanation for system design. Section III presents technologies used. Section IV covers the small print of the testing consequences and Section V the conclusion.

II. SYSTEM DESIGN

The reason is to graph a university internet site which includes up to date statistics of the college. That should improve effectivity of college document management with full of security by using usingSHA-512(Secure Hash Algorithm).

A. Terms Used In Cryptography

Plain text: - The original message that the individual favor to send is known as undeniable text. For an instance Sudha is a character desires to send “how are you” message to Suji. The message “how are you” is a undeniable text.

Cipher text: - The message that can't be understood by using every person is known as cipher text. The cipher text is produced from undeniable text. The “%adgh = $dgfh” is a cipher textual content of message “how are you”.

Encryption: - when undeniable textual content is converted into cipher text then the cipher text is called encryption.

Decryption: - When cipher text is converted into plain textual content then it is referred as decryption. It additionally want two matters decryption algorithm and key. Key:-When numeric or alpha numeric textual content or distinct symbol is combined then it is referred as key. Key performs a very necessary role in cryptography.

Cryptography: - Cryptography is a information protection technique to make certain information confidentiality, in addition to cryptographic appreciation is the learn about of mathematical techniques associated to statistics security such as records confidentiality, statistics validity, data integrity, records authentication.

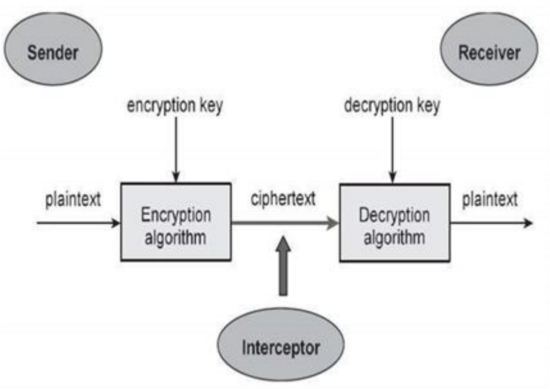


Figure 1.Encryption and Decryption Process

Encryption and Decryption: - Encryption is a method done to convert an undamaged message (plaintext) into an unreadable shape (chipertext), decryption is a system achieved to convert an unreadable message into a readable and understandable form. The encryption and decryption manner is governed by one or extra cryptographic keys. Cryptosystem is a facility to convert plaintext to chipertext and vice versa. Based on the keys used for encryption and decryption. Encryption and decryption technique can be considered in the Figure 1.

Cryptographic system or cryptosystem is a facility to convert plaintext to ciphertext and vice versa. In this system, the parameters that decide a precise involuntary transformation are called a set of keys. The encryption and decryption procedure is governed by way of one or extra cryptographic keys. In general, the keys used for the manner of encryption and description is now not always identical, depending on the device used. In general, the process of encryption and decryption operation can be explained mathematically as follows:

EK (M) = C (Encryption Process) DK (C) = M (Decryption Process)

In the message M we declare be message C by means of the use of the key K, whilst in the decryption procedure we use the key K and do the message C that has been in the encryption and generate the preliminary message that is M.

A. The Secure Hash Algorithm-Sha-512

The Secure Hash Algorithm (SHA) was once developed by means of the National Security Agency (NSA) and published in 1993 with the aid of the National Institute of Standard and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS PUB 180). SHA is based on and shares the identical building blocks as the MD4 algorithm. The sketch of SHA brought a new process which expands the 16-word message block input to the compression function to an 80-word block among other things. In 1994, NIST announced that a technical flaw in SHA used to be found. And, this flaw makes the algorithm much less impenetrable than initially believed. No similarly small print were given to the public, solely that a small change was made to the algorithm which used to be now acknowledged as SHA-1 and published in FIBS PUB 180-1.

The SHA-2 family of hash algorithm consists of 5 cryptographic hash features denoted through SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512[7-9]. The closing 4 versions are from time to time together referred to as SHA-2. In fact, NIST up to date its hash characteristic fashionable to FIPS PUB 180-2 in 2002.This replace designated three new hash functions, next to SHA-1, regarded as SHA-256, SHA-384, and SHA-512. SHA-1 is designed to produce a 160-bit message digest. The different hash functions have the size of their message digest indicated with the aid of the wide variety following prefix “SHA-"; hence SHA-256 produces a 256-bit message digest, whereas SHA-384 produces a 384-bit hash fee and so on. SHA-224 which produces a message digest of 224-bit was once introduced to the trendy in 2004[5]. Description of the SHA-1 algorithm The SHA-1 algorithm accepts as input a message with a most size of 264-1 and produces a 160- bit message digest as output. The message is processed by the compression function in 512-bit block. Each block is divided in addition into sixteen 32-bit words denoted with the aid of Mt for t = 0, 1, ... , 15. The compression function consists of 4 rounds; every round is made up of a sequence of twenty steps. A entire SHA-1 round consists of eighty steps where a block size of 512 bits is used collectively with a 160-bit chaining variable to sooner or later produce a 160-bit hash value.

The processing of SHA-1 works as follows:

Step 1: Append padding bits

The original message is padded so that its length is congruent to 448 modulo 512. Padding is constantly added even though the message already has the preferred length. Padding consists of a single 1 observed via the integral range of 0 bits.

Step 2: Append length

A 64-bit block dealt with as an unsigned 64-bit integer (most sizable byte first), and representing the length of the unique message (before padding in step 1), is appended to the message. The entire message's length is now a multiple of 512.

Step 3: Initialize the buffer

The buffer consists of five (5) registers of 32 bits every denoted by A, B, C, D, and E. This 160-bit buffer is used to maintain brief and last results of the compression function. These 5 registers are initialized to the following 32-bit integers (in hexadecimal notation).

A = sixty seven forty five 23 01
B = efcdab 89
C = ninety eight ba dc fe
D = 10 32 5476
E = c3 d2 e1f0

The registers A, B, C, and D are exactly the same as the four registers used in MD5 algorithm. But in SHA-1, these values are stored in big-endian format, which capability that the most huge byte of the phrase is positioned in the low-address byte position. Hence the initialization values (in hexadecimal notation) show up as follows:

word A = 67 45 2301
word B = ef cd ab 89
word C = ninety eight ba dc fe
phrase D = 10 32 5476
word E = c3 d2 e1f0

Step 4: Process message in 512-bit blocks

The compression function is divided into twenty sequential steps composed of 4 rounds of processing where every spherical is made up of twenty steps. The four rounds are structurally comparable to one another with the solely difference that every spherical uses a exclusive Boolean function, which we refer to as f1, f2, f3, f4 and one of 4 extraordinary additive constants Kt ($0 \leq t \leq 79$) which relies upon on the step under consideration. The values of the 4 distinct additives consistent are given in table 3below.

Step 5: Output
After processing the last 512-bit message block t (assuming that the message is divided into t 512-bit blocks), we gain a 160-bit message digest.

Table 1: Analysis of a number of factors

S. NO	Factor Analyzed	Sha-1	Sha-256	Sha-512
1	Message digest size	160	256	512
2	Block Size	512	512	1024
3	Rounds	80	80	64
4	Collision found	Yes	No	No
5	Word size	32	32	64

B. Data Flow Diagram
A Data Flow Diagram (DFD) is a graphical illustration of the “flow” of Student Information System. A statistics flow layout can also be used for the visualization of Data Processing. DFD shows the interplay between the machine and outside entities. This context-level DFD is then “exploded” to show greater element of the machine being modeled. A DFD represents float of facts through a device .Data float diagrams are typically used at some stage in problem analysis. It views a device as characteristic that transforms the given enter into required output. Movement of records thru the exclusive transformations or approaches in the machine are shown in Data Flow Diagram of Fig. 2

Table 2: Secure Hash Algorithm Properties

S. No	Algorithm	Collision status	Speed	security	Successful Attacks Reported
1	SHA -1	Yes	Slower ,80 iteration	More secure	YES
2	SHA - 254	Yes	Slower	More secure	YES
3	SHA - 256	Yes	Slower	More secure	YES
4	SHA - 384	Yes	Slower	More secure	YES
5	SHA - 512	Yes	Slower	More secure	NO
6	SHA - 512/224	Yes	Slower	More secure	NO
7	SHA - 512/556	Theory	Slower	More secure	-

This paper in general focuses on the managing the data of the students, faculty, placement phone information, examination section, related facts of the university which is maintained through the university administration through more than a few levels of controlling. The function of the man or woman entities will be explained in detail in the drift graph.

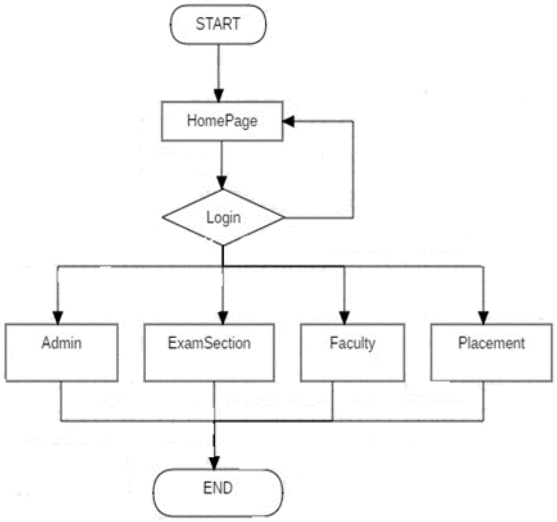


Fig. 2 Data Flow Diagram

Table 3: calculation of Hash values for message

Message: welcome hash coding			
S. No	Algorithm	Hash Value	Message Digest

			Size (bits)
1	SHA -1	ac5a02a45bb4af337236a052be798f694f8b7100	160
2	SHA -224	2df461c9c64dbdbc44b8c76a6901737d6a7bf15f197df072c204b471	160
3	SHA -256	e986d508289222244d3a1a4b8a4b9c000d777e19ae989afdc5b0aef4ab99d5cc	224
4	SHA -384	5848b9b8cc830b6db1d630fcb4fe73e1f6b4293c4c3ba570e8e33ee9ab656c6dfa289dbf6d43657daf7da2cbdf4b363f	256
5	SHA -512	da06fdbd388edac722a8f601e3313b2971f0c58d34dbe06ecf383969615db673e0df7e42242c22a4423b82caca1dfd968a861f4949cdc36be7c6a2859e63b405	384
6	SHA –512/224	fbc5b8100d70fea2a68399b2eca93d1c8d9421ac286843cb5aa91e88	512
7	SHA –512/256	b00601bca5a5654399fcb11f8ad3f00b0f1335f78890b258b3b8e0df4f5c45ff	224

C. Detailed Flow Graph

The certain go with the flow graph is proven in Fig. two .The format of the scholar records administration device includes the layout of the domestic page which gives the way for all the students, staff and different person to get right of entry to the SIMS. Every user of the SIMS has a special username and password provided by using the net grasp of the college. The home page in general consists of a login structure via which a new consumer can register, or an current consumer can login to the device via entering the username and password supplied via the net master.

STUDENT: The student is of middle focal point , because in each college student plays the very essential function . Student can access the facts of the college, direction details, problem details, college details, training and placement phone data and examination area records .The path important points include records concerning branch he is studying, the Academic curriculum of the college, 12 months clever situation supplied by way of the branch, the problem details consist of the syllabus of the subjects, data regarding the body of workers dealing with the subjects, the subjects he currently registered for the semester he is nowadays studying, attendance and internal marks of the subjects, he can additionally ask any queries to the team of workers related to the subjects. The placement important points encompass the statistics about the companies, the eligibility standards for attending recruitment of the companies, the method of recruitment, the date and time of the recruitment. The placement cell updates the college students facts who got selected for a company. The examination part small print include the internals and exterior time tables, the room allocation for the exams, it also incorporates the semester stop results.

FACULTY: The team of workers can replace the records concerning the college students attendance, interior marks of the college students and any facts concerning the subjects they handle. They can additionally view the student details for higher perception the student performance and enhancing the effectivity of the student. The team of workers additionally gets the updates from the university involving any occasions happening in the college. They can also get the notifications from the placement mobile and examination section.

EXAM SECTION: The examination section is responsible for updating internal and external examination time table. They are also responsible for the updating the supervision listing for the faculty and class room allocation for the college students in the examination. And they are accountable for the checking and approving the inside marks important points up to date with the aid of the staff.

PLACEMENT CELL: The placement officer is responsible for updating the placement related facts like eligible criteria for a particular company, arriving date for the business enterprise which is coming for recruitment, the listing of students who are eligible for attending the recruitment process. The list of pupil who received placed in a employer and the placement officer can access the pupil facts from the student database for selecting the eligible candidates list for placements. He additionally can send notifications to college students concerning any information.

ADMINISTRATOR: The administrator is accountable for getting into the new student, merchandising the student from one class to another, from one semester to every other and from one year to another. Managing the student debts like any modifications related to the name, tackle etc. The administrator also manages the erroneous bills like entering a new faculty, assigning the college to the subjects. The administrator also updates the college related data like calendar of events, data involving any other activities that take place in the college. The administrator will take a look at the all the updates i.e. scholar updates, college updates, examination updates etc. The administrator has the perfect level of strength in the student statistics system.

III. TECHNOLOGIES USED

This section explain about the applied sciences like React used for the frontend development ,CSS used for the styled to the web pages and SQL used for the information storage and protection they defined bellow in detail.

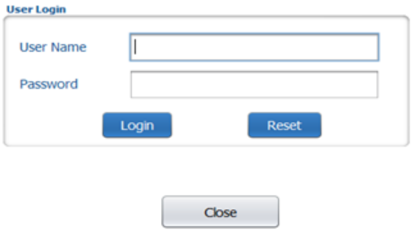
React is a front-end JavaScript library developed via Facebook in 2011. It follows the issue based method which helps in constructing reusable UI components. It is used for creating complex and interactive web and cell UI. Even although it was open-sourced solely in 2015, it has one of the biggest communities assisting it. Some of the principal advantages of React are It will increase the application's performance .Because of JSX, code's readability increases .React is handy to combine with different frameworks like Meteor, Angular, and many others Using React, writing UI test cases come to be extraordinarily easy

CSS Stands for "Cascading Style Sheet." Cascading style sheets are used to format the layout of Web pages. They can be used to outline textual content styles, table sizes, and other elements of Web pages that beforehand should only be defined in a page's HTML. CSS gives a degree of control over quite a number presentation traits of the document. It also helps in decreasing the complexity and helps in saving universal presentation time. CSS gives the option of deciding on a range of style schemes and guidelines in accordance to the necessities and it additionally approves the equal HTML report to be presented in more than one varying style.

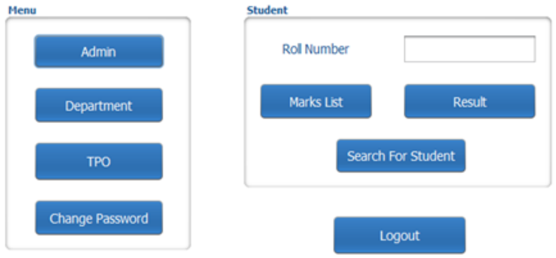
SQL stands for Structured Query Language. SQL lets us access and manipulate databases. SQL is an ANSI (American National Standards Institute) standard. SQL can execute queries in opposition to a database ,retrieve information from a database, insert data in a database, update data in a database, delete data from a database, create new databases , create new tables in a database , create saved approaches in a database, create views in a database, set permissions on tables, procedures, and views.

IV. RESULTS

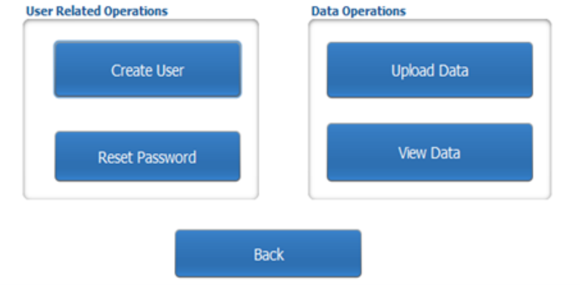
Login Form:
The gadget starts with login page where the registered person can enter user name and password to be in a position to get right of entry to the system.



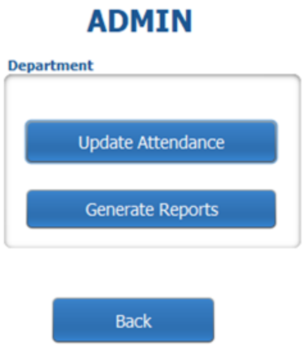
Menu Page:
The Menu Page incorporates two parts first phase includes the Admin, Department, TPO and Change Password. Second part about the students.



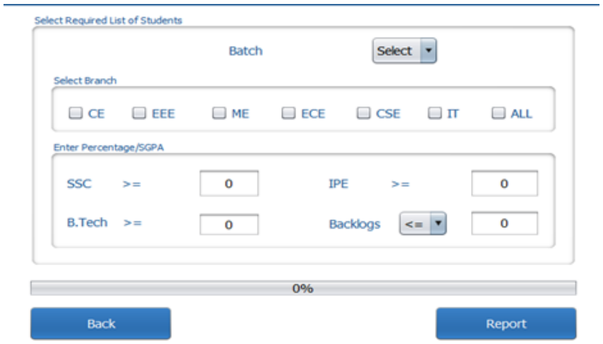
Admin Page:
The Admin Page includes two parts first part carries the User Related operations like create user and reset password. Second part about the Data operations updated data, view data.



Department Page:
The Department Page carries update attendance and generate reports.



Placement Page:
The Placement Page consists of important points of the student.


Select Required List of Students
Select Branch
□ CE □ EEE □ ME □ ECE □ CSE □ IT □ ALL
Enter Percentage/SGPA
0%
Back
Report

Batch: Select

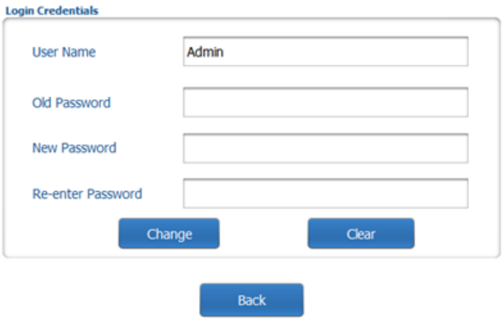
SSC >= 0

IPE >= 0

B.Tech >= 0

Backlogs <= 0

Password Change Page:
The Password Change Page used to change the user password.



User Name: Admin

CONCLUSION

This paper studied about one-of-a-kind hashing algorithms and conclude that, as the size of the hash enlarge the safety of hash increase. It is discovered that MD5 algorithm is computationally faster than the SHA 512 algorithm. But the impervious hash algorithm affords higher security than Message Digest algorithm. It is now not impenetrable to use only textual content only password because they can without problems cracked. MD5 algorithm is basically impenetrable but adding salting to it makes it greater and secure. SHA 512 is regarded extra secure.

This paper assists in automating the current manual system. This is a paperless work. It can be monitored and controlled remotely. It reduces the man electricity required. It gives accurate records always. Malpractice can be reduced. All years together gathered records can be saved and can be accessed at any time. The facts which is saved in the repository helps in taking shrewd selections with the aid of the management. So it is higher to have a Web Based Information Management system. All the stakeholders, faculty and administration can get the required data besides delay. This gadget is vital in the colleges/hostels and universities.

REFERENCES

[1] Liu Jian – dong, Tian Ye, Wang Shu-hong, Yang Kai, “A fast New one way cryptographic hash function”, IEEE 2010.

[2] Joseph Sterling Grah “Hash functions in cryptography”

[3] G. Bertoni, J. Daemen, M. Peeters, & G. V. Assche (2012), Keccak An update. Retrieved March 22-23,

2012, from Third SHA-3 candidate conference, Washington DC.

[4] DaniloGligoroski, Svein Johan Knapskog, J0rn Amundsen, Rune Erlend Jensen “Internationally Standardized Efficient Cryptographic Hash Function”.

[5] Abdulaziz Ali Alkandari, ImadFakhri Al-shaikhli, Mohammad A. Alahmad“Cryptographic Hash functions: A High Level View”International conference on informatics and creative multimedia.

[6] I. Damgård. A design principle for hash functions. In G. Brassard, editor, Advances in Cryptology - CRYPTO ’89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 416–427. Springer, 1990.

[7] FIPS 180, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, Washington D. C., 1993.

[8] FIPS 180-1, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, Washington D. C.,1995.

[9] FIPS 180-2, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, Washington D. C.,2002.