Modified Algorithm of Two Phase SHA Captcha for Secure Communication

Suresh Kumar Kadwa[1], Mrs. Shalini[2]
[1]M.Tech Research Scholar,[2] Assistant Professor
[1,2]Department of Computer Science Engineering, Jaipur Institute of Technology- Group of Institutions, Jaipur, Rajasthan, India

Abstract: Casting a ballot is the most significant vote based right of each resident of India. In any case, unlawful making of choice is likewise a significant issue, which looked during the decisions. So as to concentrate on these issues in our exploration we concentrated on the methodology, which can fathom these issues generally. So as to, further expand the security, we have given the picture as information and created the SHA Hash. Based on it and this hash code is further send in two stage on at the season of enlistment and another at the season of login and In the proposed methodology, made a cryptographic procedure of vote throwing by taking the idea of the photograph as secret key and two–stage secret word**.**

Index Terms **– Two Phase Password, Data Communication, SHA**

I. INTRODUCTION

In later years, security needs have heightened. Information correspondences and internet business are reshaping strategic policies and acquainting new dangers with corporate action. National barrier is likewise helpless as national framework frameworks, for instance transport and vitality dispersion, could be the objective of psychological oppressors or, in the midst of war, foe country states.

- On a less sensational note, reasons why associations need to devise viable system security procedures incorporate the accompanying:
- Security breaks can be extravagant as far as business disturbance and the money related misfortunes that may result.
- Expanding volumes of delicate data are moved over the web or intranets associated with it.
- Systems that utilize web connections are winding up more prevalent on the grounds that they are less expensive than devoted rented lines. This, in any case, includes various clients sharing web connects to move their information.
- Chiefs of business associations are progressively required to give successful data security.

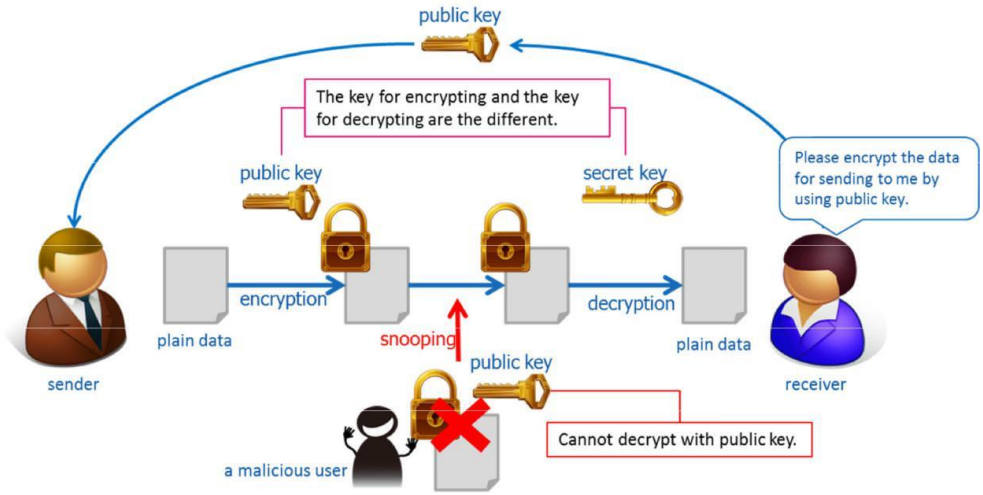

Fig 1. Secure Data Communication

For an association to accomplish the degree of security that is proper and at a cost that is satisfactory, it must do a point by point hazard evaluation to decide the nature and degree of existing and potential dangers. Countermeasures to the apparent dangers must adjust the level of security to be accomplished with their agreeableness to framework clients and the estimation of the information frameworks to be ensured. [1] Secure correspondence is once 2 substances are impartation and do not would like an outsider to tune up. For that they need to convey in a very manner not helpless to listening stealthily or interception.[1][2] Secure correspondence incorporates implies by that people will impart information to differing degrees of assurance that outsiders cannot block info disclosed. apart from spoken eye to eye correspondence with no conceivable nosey-parker, it's presumptively protected to state that no correspondence is ensured secure during this sense, albeit pragmatic impediments, for instance, enactment, assets, specialized problems (capture try and encryption), and therefore the sheer volume of correspondence serve to constrain observation. With varied interchanges occurring over long separation and intervened by innovation, and increasing consciousness of the importance of block

try problems, innovation and its trade off are at the core of this discussion. Consequently, this text centers around correspondences intervened or blocked by innovation.[2]

II. Related Work

S. Lee and K. Shin, [3] This paper depicts a structure of SHA processor actualizing three hash calculations of SHA-512, SHA-512/224 and SHA-512/256. The SHA processor creates condensations of three unique lengths with 512, 224, and 256 bits as per hash calculations. It was planned that the underlying hash estimations of SHA-512/224 and SHA-512/256 were produced utilizing SHA-512 and it depended on 32-bit datapath, bringing about a region effective execution. The SHA processor planned with HDL was checked by FPGA usage.

S. S. Omran and L. F. Jumma, [4] According to the wide improvements in the territory of interchanges, there is an interest for secure framework for information transmissions. In this paper, a Hash framework SHA-1 and SHA-2 Processor is planned utilizing Xilinx Spartan-3AN and interfaced with keyboard and Video Graphics Array (VGA) Display. The usage of the processor is finished by utilizing MIPS (Microprocessor without Interlocked Pipelines) single cycle by picking a specific number of directions that was important to conjure the SHA-1, SHA-224 and SHA-256 calculation.

K. A. Nugroho, et. Al [5] Providing inquiries with remarkable succession energizes members trustworthiness in an examination. In this investigation, Secure Hash Algorithm (SHA) 2 and 3 have been proposed and assessed in an inquiry rearranging issue for PC based test. Two techniques were tried to utilize the hash calculations. The primary used a couple of the most critical digits of the hash esteem and the second treated all digits of the hash an incentive as similarly significant.

III. Proposed Work

This section describes the algorithms which are involved in the proposed dissertation. The whole concept proposed involves the two main segments or sections. These are,

1. Registration
2. Login

3.1 Algorithm Registration Process

The algorithm of the registration process is described in the following steps:

Step 1: Input the photo/image which is to be used for the secure identification.

Step 2: Fill the details provided in the Registration Form.

Step 3: Validate the Email ID and aadhar card number in the database in order to cross validate whether the registration or the user already exists with the same email id or the aadhar card number.

Step 4: If the Details already exist then stop and provide the new details otherwise the photo provided as an input is validated from the aadhar database.

Step 5: If the photo details are verified successfully then the registration will proceed and the SHA algorithm will come into role and the HASH code will be generated corresponding the photo.

Step 6: The first half of the code generated is sent to the registered email id and also stored the details of first and second half of the code in the database.

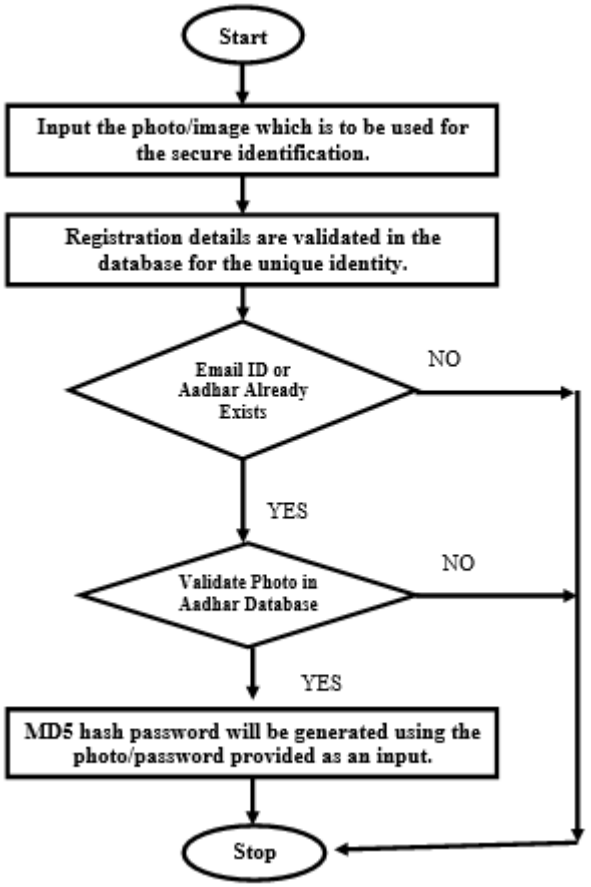

Fig 2. Registration Process

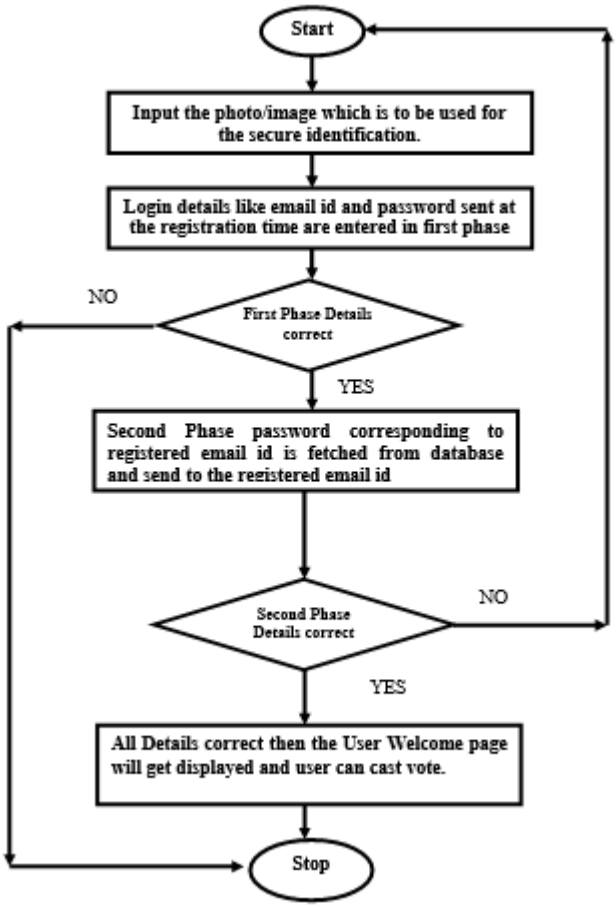

Fig 3. Login Process

IV. IMPLEMENTATION AND RESULT ANALYSIS

The implementation of the proposed work is done in the PHP and MYSQL and the implementation snapshot is shown in the fig 4.

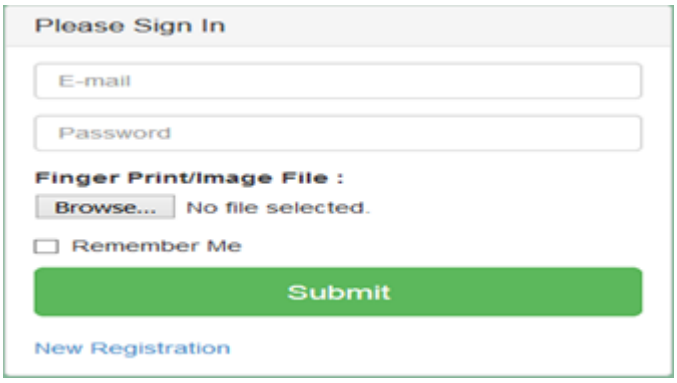

Fig 4. First Phase Sign-In

Fig 5. Second Phase Sign-In

The OTP pattern generated is examined using the various software's and tools and the fig 6 shows the comparison results.

Test Key	Website/Tool	Result
9d3e2423d210297c82fab05476c312ad71f84b10	Password Strength Calculator	Entropy :165.4 bits
9d3e2423d210297c82fab05476c312ad71f84b10	Rumkin Strength Test	Entropy: 166.8 bits
9d3e2423d210297c82fab05476c312ad71f84b10	Cygnius Password Strength Test	Entropy : 167.338 bits

Fig 6. Comparison Results

V. CONCLUSION

Secure casting a ballot is the progression towards the advanced and creates India. The thesis idea isn't just cutting edge yet additionally gives us the idea of how the 100% casting a ballot criteria can be accomplished. In the exposition the safe idea of utilizing the photograph MD5 hash two stage security improves the security as well as reduce the odds of the phony vote.

REFERENCES

[1] MdAsifMushtaque, Harsh Dhiman, ShahnawazHussain ,"A Hybrid Approach and Implementation of a New Encryption Algorithm for Data Security in Cloud Computing" ,International Journal of Electronic and Electrical Engineering,2014
[2] Pratap Chandra Mandal, "Dimensions Affecting Customer Satisfaction in Retail Banking: A Review", International Journal of Novel Research in Marketing Management and Economics, 2015.
[3] S. Lee and K. Shin, "An efficient implementation of SHA processor including three hash algorithms (SHA-512, SHA-512/224, SHA-512/256)," 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, 2018, pp. 1-4.
[4] S. S. Omran and L. F. Jumma, "Design of SHA-1 & SHA-2 MIPS processor using FPGA," 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, 2017, pp. 268-273.

[5] K. A. Nugroho, A. Hangga and I. M. Sudana, "SHA-2 and SHA-3 based sequence randomization algorithm," 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, 2016, pp. 150-154.
[6] S. S. Omran and L. F. Jumma, "Design of multithreading SHA-1 & SHA-2 MIPS processor using FPGA," 2017 8th International Conference on Information Technology (ICIT), Amman, 2017, pp. 632-637
[7] R. K. Ibrahim, R. A. J. Kadhim and A. S. H. Alkhalid, "Incorporating SHA-2 256 with OFB to realize a novel encryption method," 2015 World Symposium on Computer Networks and Information Security (WSCNIS), Hammamet, 2015, pp. 1-6.
[8] A.S. Eissa, M. A. Elmohr, M. A. Saleh, K. E. Ahmed and M. M. Farag, "SHA-3 Instruction Set Extension for A 32-bit RISC processor architecture," 2016 IEEE 27th International Conference on Application-specific Systems, Architectures and Processors (ASAP), London, 2016, pp. 233-234
[9] S.SridevisathyaPriya,P.Karthigai Kumar, N.M. SivaMangai, V.Rejula "FPGA Implementation of Efficient AES Encryption ",IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems p.12p
[10] JG pandey, S gurunarayan "Architectures and Algorithms for Image and Video Processing using FPGA-based Platform " ,2014
[11] VakkayilMeghaGopinath "MAES Base Data Encryption and Description Using VHDL",IJEDR | Volume 3, Issue 2 ,2015
[12] J. Cederlofet ,"Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, December 2013.