NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 12, Dec.-2017

A NEW TECHNIQUE TO SECURE DATA USING COLORS AND WHOLE NUMBERS

PROF. N. J. GHATGE
Department of Computer Engineering, TKIET, Warananngar Kolhapur, India
ghatgen@gmail.com

PROF. U. A. PATIL
Department of Computer Engineering, DYP College of Engineering Kolhapur, India
uap.patil@gmail.co

ABSTRACT
Now day's data security is the major issue. Confidentiality, Integrity, Non-repudiation is the main components of data security. The widespread strategy for the security of transmitted data is cryptography. In this work, a prime approach for security and encryption of data has been examined. In this, colors are used as a passwords involving key and whole numbers are utilized for the encryption purpose. The secure data transmission is given by utilizing set of three key point with a crucial security component acted by the colors along these lines giving authentication.

KEYWORDS: Data security; Whole numbers; Cryptography.

I. INTRODUCTION
Cyber security is the group of technologies and procedure intended to ensure systems networks, resources, code and information from attack or unauthorized access. In a computing context, security incorporates both cyber security and physical security. Guaranteeing cyber security composed endeavors all through a data information system.

A standout amongst the most dangerous components cyber security is the rapidly and continually developing nature of security risks. The customary approach has been to think most assets on the most crucial system components and protect against the greatest known dangers, which required leaving some abandoning some less vital system components undefended and some less risky dangers. Such an approach is inadequate in the present condition. Adam Vincent, CTO-public sector at Layer 7 Technologies describes the problem "The threat is progressing speedier than we can stay aware of it. The danger changes quicker than our idea. it's never again conceivable to compose an expansive white paper about the risk to a specific system. You would be change the white paper always constantly.."

a shift toward continuous monitoring and real-time assessments. As per Forbes, the global cyber security market achieved 75 billion for 2015 and is expected to hit 170 billion in 2020.

II. SURVEY OF SIMILAR WORK

Sr. No.	Literature Overvie		
	Title	Author	Description
1.	Security using Colors and Armstrong Numbers	S. Pavithra Deepa,S. Kannimuthu, V. Keerthika. 17,18 February,2011	This work provides a technique in which Armstrong number is used for encryption of message.
2.	Armstrong Numbers	Gordon L. Miller and Mary T. Whalen October 1990	This work talk the importance of Armstrong numbers in today's world
3.	Data Security Using Armstrong Numbers	S.Belose, M.Malekar , G.Dharmawat April 2012	In this paper Encryption and decryption procedure uses Armstrong number which is used as a secret key. To do the Authentication between two expected clients with the security, server is utilized.
4.	A brief introduction to Armstrong Numbers	M.F.Armstrong	This paper describes the analytical approch to determine Armstrong number.

In the information protection the utilization of public-key cryptography is persistent and privacy areas. The real numbers are a vital piece of the public key systems hence the real numbers uses by private key cryptography algorithms comprehensively. This method guarantees that information transfer can be performed with protection utilizing two principle steps. In that initial step is the convert the information into ASCII code, at that point by including it with the Armstrong numbers digits.

On the off chance that all these key values along with this technique is known then only data can be recovered. Encoding and decoding the exits data involve by Simple decryption and encryption strategies. But in this proposed work to give greatest security for getting the initial data, the data itself is encoded. colors and Armstrong numbers are used as a part of this procedure. To whom the message must be sent to the required receiver.

III. EXISTING SYSTEM

In today's world, Information security while transferring information from one place to other is major issue. To protection of information from unwanted user Information security mainly refers. At receiver and senders side this technique uses decryption and encryption respectively. In this day's, Information security while exchanging information from one place to other is real issue.. Particularly while decrypting and encrypting the information this technique makes utilization of Armstrong number. For exchanging key between receiver and sender this method additionally utilize Diffie-Hellman key exchange algorithm. The suggested Algorithm is simple, adaptable and making both software and hardware execution simpler. To both information as well as its key, Decryption and Encryption process applies. Hence to the application two way securities is given. After successful authentication, by random Armstrong number information is encrypted and Armstrong number gets encrypted in the mean time.

Presently current system timestamp is appended, for both these encrypted data and key. So receiver can without much of a stretch perceive which key is for which data at whatever point he gets both the data. At that point by senders public key encrypted key is decrypted and to decrypt actual data, that resulted Armstrong number is utilized.

So to get the data it is troublesome and take it. Hacker must have key by which that information is encrypted with its timestamp once he steals the information. To recover both key and data, if hackers get both key and data then he should have knowledge of the encryption algorithm which is extremely troublesome.

A. Drawbacks of existing system

- Diffie-Hellman key exchange algorithm includes costly exponential activities. The proper way to break into this system is by Brute force attack, which additionally can take up to a few years.
- Execution speed is slow because the file size after encryption is significantly bigger than unique file.

IV. PROBLEM STATEMENT

Presently information security is the fundamental issue. What's more, the mechanisms which are utilized for encryption is "Security Using Colors and whole Numbers, however one of the fundamental hindrances is that the execution speed is moderate because the file size after encryption is considerably bigger than the original file. Along these lines, to counter this issue we are going to utilize a mechanism called" Security Using Whole Numbers and Colors" which uses much lighter and secure algorithms for Decrypting and Encrypting .

A. Objective

- To provide effective authentication using colors.
- To overcome the complexities and difficulties in the existing system called security using Armstrong numbers.
- To provide efficient and authorized way for data transfer between receiver and sender.

V. SYSTEM ARCHITECTURE

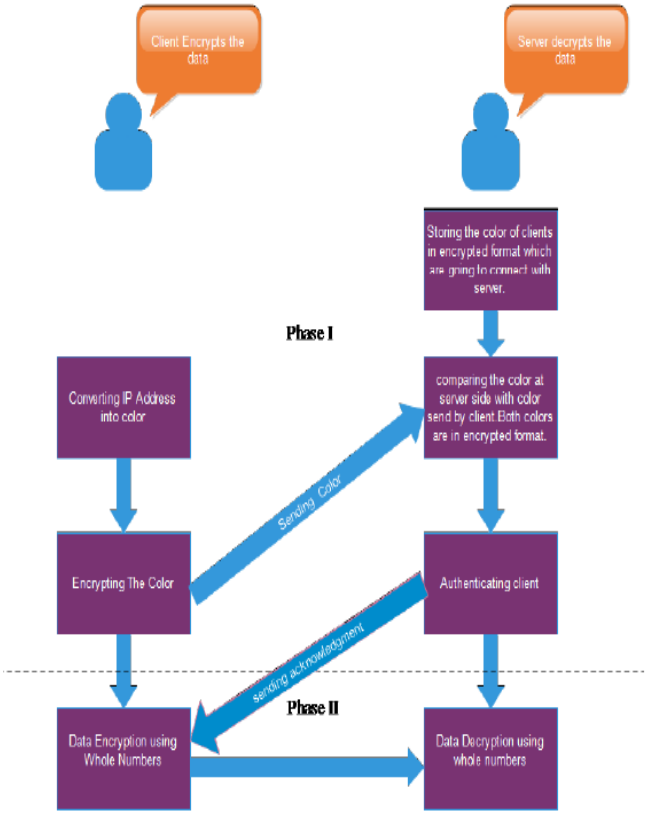

Fig. 1. System Architecture

A. Server Authentication

In Sender Side Authentication we first store all color values of client which are going to connect with sender in file. After storing these values when client sends it IP address which is converted into color at server side. At server side the color is matched with entries in file in which color is stored previously

In the server side, we must store the encrypted color in a file which was derived from the IP address of the client by running the conversion program on the server-side. This method provides at most security was no Client can prove that they belong to that network unless their encrypt color is present in the file. After the color is stored, the Start button is clicked which makes the Server ready to receive requests from client.

B. Client Authentication

In client side authentication we convert the IP address of the client in the color value. This color value is send to the server and then compared with the entries at the server side.

The client sends the server its encrypted color through the network and then when the encrypted color is matched with the encrypted color from the file, the client is verified. After the client is verified, the server send an acknowledgement to the Client informing that Server side is ready to receive the transmission. And it goes into continues running thread until Logout button is pressed.

Once the client is verified and at the client side receives acknowledgement from the server, client is ready to transmit information for the transmitting information.

C. Data Encryption

After establishing connection between Server and Client the actual part of data encryption is starts at client side. Client encrypts the data and sends the data over the channel which is received by the server side.

D. Data Decryption

Data which is get in encrypted format is decrypted in its intial form and displayed to end user in the color which belongs to the IP address of the client.

VI. SYSTEM DESIGN AND IMPLEMENTATION

The following screenshots shows server and client screen on the same machine

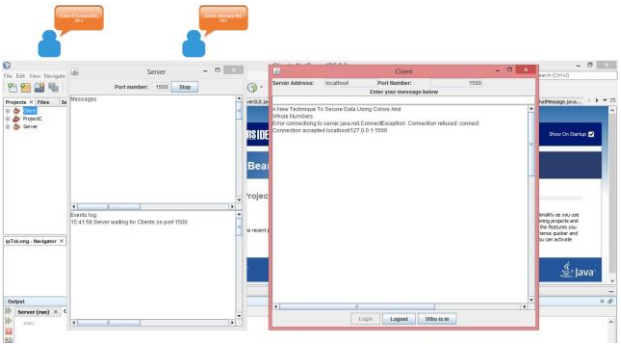

Fig. 2. Intial State

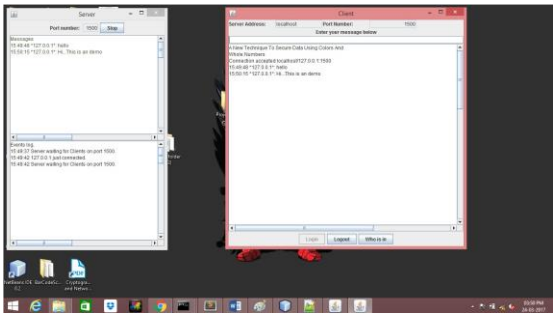

Fig. 3. Final State

VII. CONCLUSION AND FUTURE SCOPE

- In this framework, we are utilizing the color and whole number to secure data. Utilizing color, we will generate the secured key. This secured key sends to the receiver. Then receiver side key is checked with the sender database. On the off chance that both match, at that point the sender send the data to the receiver which is encrypted using the whole number. At receiver side, opposite process of encryption is performed to decrypt the data and original information.
  In military, the above combination of public key and secrete key cryptography can be applied because, more significance is for security of data. At the point when the length of the key of the whole numbers increase, at that point this strategy gives more security. Accordingly by the utilization whole numbers, additional set of key values and colors in this technique there is surety that the data is deliver securely and that only authorized peoples can get to it.

FUTURE SCOPE

- As our goal is to establish communication between client and server using color and whole number we achieve our goal. To further extend the idea we can add two way communication. Currently we are sending message from client to server in further enhancement this process can be done in both direction.

REFERENCES

I. Chavan Satish, Lokhande Yogesh, Shinde Pravin, Yewale Sandeep, Sardeshpande S. A, “Secure Email using Colors and Armstrong Numbers over web services,” International Journal Of Research In Computer Engineering And Information Technology VOLUME 1 No. 2.
II. M.Renuga Devi, S.Christobel Diana, Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers, International Conference on Computing and Control Engineering(ICCCE 2012), 12 13 April, 2012.
III. Atul Kahate, “Cryptography and Network Security “, Tata McGraw Hill Publications.
IV. http://aix1.uottawa.ca/~jkhoury/cryptography.htm
V. http://mathworld.wolfram.com/UnimodularMatrix.html.