Sequential mathematical solution for authentication and authorization technique implementing encryption methodology creating secure transaction using various methods also at quantum level

To cite this article: Snigdha Gharami and M Dinakaran 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042013

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042013 doi:10.1088/1757-899X/263/4/042013

Sequential mathematical solution for authentication and authorization technique implementing encryption methodology creating secure transaction using various methods also at quantum level

Snigdha Gharami and Dinakaran M

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: dinkaran.m@vit.ac.in

Abstract. We see challenges in authenticating each aspect of electronic usage, starting from transaction to social interaction the authenticity and availability of correct information is guided in various ways. Authentication and authorization follow one another; a process of authentication is calculated on multiple layers of steps. In this paper we discuss various possibilities of modifying and using ways to deal with authentication and authorization mechanism. Idea is to work through authentication with mathematical calculations. We will go through various scenarios and find out the system of information that fits best at the moment of need. We will take account of new approaches of authentication and authorization while working on mathematical paradigm of information. The paper also takes an eye on quantum cryptography and discusses on how it could help one in the present scenario. This paper is divided into sections discussing on various paradigm of authentication and how one can achieve it in secure way, this paper is part of research work where analysis of various constraints are to be followed in the extended research work.

1. Introduction

The present scenario in electronics and communication with the trusted methods of transferring is being preferred if we could see the organizational paradigm of digitalization. We are submerging our needs into the signals and bytes of codes; we are just manipulating out the requirements and forming Tele-signalling. The more we try to complicate the code of transfer the more it finds ways to consider space and time. Security is not an issue most of the time; the issue is with the complexity of the security and the amount of trust we put into the electronic transfer or digital approach. Taking authentication and authorization of any physical entity which works on the other side of the screen is as conception as it appears to the understanding of the machine. The appearances of complex theories of algorithms are effective while working on the space and time paradigm. While working on the quantum level where things are as specific as they appear and to specify the physics in everything that science appears to hold. Authentication of digital implantation of any physical existence is specific and could be resolved using units of experimental challenges is quite emerging. If we take the existence of authentication mechanism those are currently available and in the range of associated

telecommunication, the results are as variant as they appear. Marking the extensile benefits of trying different aspects of authentication system could be a great deal of thought. The following article suggests few of the experimental techniques when commanded with the numerical, mathematical solution with the quantum approach to deal the calculation complexity while taking in the organizational prophecies. Taking the type modification into consideration and applying various trigonometric modifications and storing the values into matrix while calculating distance between the sender and secure server through either beacon signaling or using quantum physics through photon or anything relevant to it to get the value for calculating various values that corresponds to equations of circle, parabola, hyperbola or anything that takes them as calculation factors. Considering the efficiency and benefits of using such technology where such calculations are involved, it takes the authentication to some different direction making it visibly stronger and associative to the part of machine calculations and abbreviate the involvement of physics into the picture.

While there are all the better ways to understand why security is the concern now a days there is another way to explain why we are still at the level of not being secured all the time, not just the way we deal things as they appear but how everyone out there is keen to know what is being inside of which is being hidden. The concept of cryptosystem or high security paradigm has been into the version of present scenario but as the growing market for online organization and other transaction issues we just need to see each other's need to be honest enough while dealing the other sides of online honesty.

The trust based online system where we are not just keeping our things into another platform but we are also sharing our essential properties and resources. When we see everything around us they are already present at quantum form, every bit, word and matter, everything has its nominal form at quantum level that helps it to change states and form another state, they all go hand in hand and when we find that it is essential to generate the required prophecy of codes to secure the variety of mechanism that works while we subtle the hidden values in a network which is shared publically. There are varieties of reasons for taking an insight into quantum technology not just because it is emerging but also that it gives us variety of reasons to search for things in deeper level. Majority of our information is binary 0s and 1s and all these information's are stored into states where they are stable, sometimes in dynamic form sometimes in unstable or stable form, there are meanings to the storing values while we search for the original inspection for the reasons of their origins.

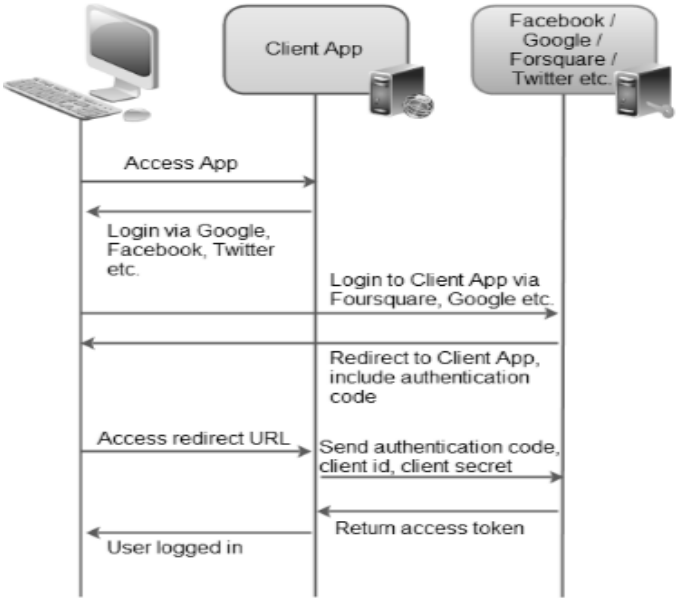

Fig. 1.1 - Overview on how authentication works

Presently we are dealing with kind of security which is strong enough to resist the attacks if we consider all the parameters of attack and how to resist them, unless there are more definition on attacking principles we cannot distribute the level of attacks, the list of attacks are based on the old-school and the techniques used are just as similar to the way we resist them. They are basic reason while restrictions made while making transactional values.

This paper deals with many such ways where we can actually see how we can reduce the complexity and other resisting factors taking into account various calculations or taking benefits of mathematical calculations where we can perform and consider various ideas on how we can make secure transaction and taking a bit of analysis for future extension of this work. This paper also discusses the factors which can be taken into measure while making security more strong and reliable at the same time reduces the complexity and other behavioral factors we deal with present scenario. On the brighter side we will take a note on how these things will make authentication and authorization more secure and understandable.

While this paper takes an insight on the authentication and authorization it is solemnly important to discuss about what authentication and authorization are, though sounds same but they both follow each other at some point, these procedures are used widely specially during online transaction where trust based information exchanges are made, it is important for one to take control of the security while we make relevant changes in it.Authentication is the process that verifies about the identity of the user who has asked for the access while authorization is the process that gives that user authority to access their resources.

2. Literature Survey

Protocol assigns aligned and understandable restore for any kind of physical or virtual network prospectus, while we take the decision to take steps on how any kind of design works for itself on a very high level of working principles. Protocols previously assigned in this field of authentication works on the similar way corresponding to the idea that it could be customized by various other users as per the requirement, when we talk of authentication and its steps to provide the other side user with the diligent and respective working principles it not only gives the insight on how one can approach the organization view but also that how it is set to the end points of arrangements.

The privacy mechanism that isolates the requirement prospectus with the arrangement ones is arranged into specification. Previously the use of certain steps in any kind of authentication process required the space and time consumption, our idea should be to reduce it to some extent keeping the profitable experience with the requirement specification.

2.1 Model based authentication

Authentication is normally multiple tier process. It takes relevant information into stages and converts them into the variety of sub modular to generate a proper authentication mechanism. Security is always seen in multiple tiers due to variety of reasons, some of them counts on may be the intruder could track the first one.

These modular based protocols generates the subatomic lever of information’s and combines the relevant information to provide the user right authority while authenticating the session.There are stages of models which works differently for different inputs and generates the relevant information on specified context are then taken as an approach for such conditional authentication.We will also take account of quantum mechanism to generate various information’s on how it could be helpful for present scenario of information security.

This paper also deals with approaches to secure the network information transfer generating algorithm using mathematical implications to produce generalized results.The main focus of this paper

is to study and provide information related to the topic with innovative ideas those could be used to calculate and avail better security.

3. Proposed Research Related Work

3.1 Authentication using Virtual Milestones with Timer:

Since that we are authenticating digital information our assumption will be that all the digital_equipements those are associated with the user and resource_provider are under their access and that they are not lost or stolen, we will try to present the scenario where the attack is middle-man-attack or information leakage.The normal information is generated on a platform of secure connection. Information is thus passed through the lane of connection thus provided. The visualization of the above is advice in the figure below:

Fig. 3.1 -

Considering that sender-A wants to send some secret-Data to receiver-B, while receiver-B (where receiver_B can be a normal receiver or service_provider who owns the resource) receives the information how he will understand that the information is coming from the right person, here comes the picture of authentication. There must be some unique feature about the sender-A which will make receiver-B understand that the information is coming from a right amateur. Authentication is an easy step, sender-A must make receiver-B believe that he is actually sender-A and not someone else. In physical world we recognize each other with different features, something like face identification, in case of similar faces some other feature identification like hair color, moles at different parts of the skin etc. digitally all these are done using methods where informations are hindered graphically into pixels of digitalized information such as finger_prints, iris_prints etc. In case of authentication over a live network the decisions are really necessary at quick event, granual level of authentications include steps of auntentications where one may be thought to have access to multiple resources at the same time so that the service_provider understands that the information is coming from the right_source.
In normal scenario the following is being seen between two parties:

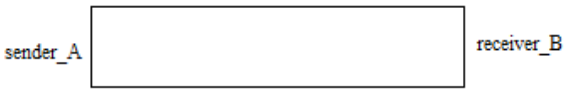

Fig 3.2

While the user wants to use the resources of receiver_B which in this case may be a normal receiver of the information or the owner of resources (like a Banking Website, online seller portal etc.).
Phase1:

In the first segment the sender_A sends a control signal to the receiver_B about the start of the segment (for example the sender_A will log into the website, after each login through the valid information like user Id and Password which must be pre-registered one token in shared with the user for secure connection establishment), it acts as a preamble.

By doing so we are making the resource_provider aware of our presence, this segment of token generation will now be considered for the second round of approval(generation of ticket/token will be taken for another unit in this paper at later on). Now the task is to authenticate if the information is from the right_User or not.

A random number of segment (virtual_milestone) with timer is calculated by the resource_provider, say 5 segment. Now the token which has been generated is based on the segments it has calculated, if the token was C_S1(control_signal_1)=1 the other side receives it as additive of 5 times of its original number or any other value based on the resource_provider's assumption, the following token is resend by the user on the same path with timer initiated with it, now when each virtual_milestone is trespassed the value is decreased with timer keeping the information on hand, if the user is valid then the resource_provider will get the same information of C_S it has thus generated.

Now if the information is altered by some other_party the value of C_S will change with the timer emphasized on it which when looked by the resource_provider will give the idea about the trespassing. The following segment is general prototype of virtual milestone authentication with timer emphasized on it. C_S and timer informations are shared in the form of packets or simple web timeline information.

Let us now see the contribution of middle attack on it.

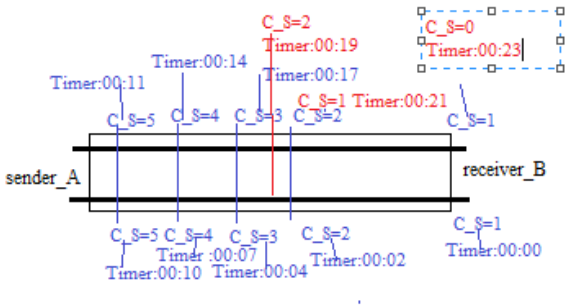

Fig. 3.3

The whole information is being altered in the scenario.

The following C_S path selection if successful will result in the secure path connection between sender_S and receiver_R for resource sharing. After which the authentication could be sensed multiple step choosing different channels to share the information's.

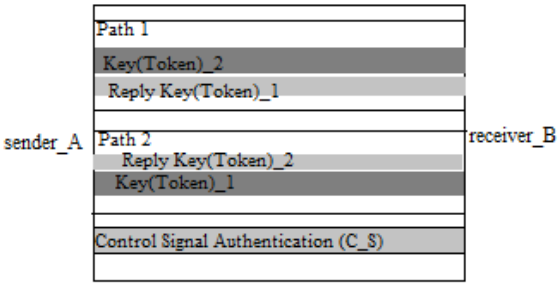

Fig. 3.4

Choosing different path for sending and receiving under same session could be another way of cross-sectioning the information authentication.

Key_1 (Token_1) and Key_2 (Token_2) between sender and receiver are send and received through two different paths, Token_1 is sent through path_1 & receiver through path_2 and Token_2 is sent through path_2 & receiver though path_1. This creates minimum chances of forgery while copying the information for false authentication.

Note: Token_1 and Token_2 can be values shared for authentication, it can be one_time_password, any secret information or random key sharing, etc.

This methodology could be seen as phases where C_S generation and validating face could be used in authorization as well.

3.2 Authentication Protocol Site-1

Considering the C_S generation protocol, this could be taken into account to generate C_S for the above mentioned specification.

This research topic takes the modular information to generate results, this is taken into consideration while the client has asked for the service and that the server needs to authenticate the user.

The protocol thus signs the requirement specification when these following modules are executed into one form.

Steps thus involve:

1. Representing the key values into Number System.
2. Transformation and Modulation.
3. Resultant Verified Number.

Transformation Phase consists of various states into what we can consider variety of results, we have considered few variables and equations, there can be many which still makes better than this but we have taken the minimal values to represent and provide inspection results.

1. Coordinate rotational digital computer (CRDC)
2. Parabola, Hyperbola, Trigonometric functions.
3. Point-to-Point Conversion.
4. BKM

There can be submissive formulation of Roots, modulus and logarithmic functions to generate further neutral variety of code. Idea is to utilize mathematical equations as much as possible.

Our main intention here is to create key generation and session authentication while keeping in mind that there is minimal amount of time provided during any transaction that could be considered for making changes. Our intention here is not just to save the authentication policy but also to create the transactional codes so strong that it couldn't be broken by anyone who could guess the values.

In recent authentication policy we try to divide the pattern of verification into stages, while one is not able to provide all the information's at various stages the request is denied, time consumption and calculation complexity increases with various stages, our intention is to reduce the stage complexity as possible as we can provided that the result should be generated in a valuable sense.

Idea is to provide a trapdoor function where it is hard to reverse the code, authentication principle works as if the receiver_B should know that it is from sender_A and not from some sender_A', in which case there should be a secret language that only receiver_B and sender_A knows among each other which will let receiver_B avail its resources to be used or it will be sure that it is from sender_A and has not be manipulated or faked on the way.

While we share information at digital platform there are many possibilities that the information could be leaked or transformed in that case receiver_B must know that the information thus created came along from the right source.We will try to deploy mathematical implication with functions on the

necessity to generate required verification.We will try to calculate among each other that the information/session_key/token coming from sender_A is exactly matching the information which verifies the sender_A.

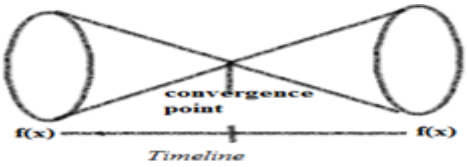

Fig. 3.5

Every function which making one way significant secure should not be termed back into the original value, this kind of resourceful submisive function would provide better and efficient security if that is within the trap_door function. A function which can not be reversed as per the significant requirenment. Given an normal scenario where equations are submerged itno properties of division we see that numbers and systems related to it plays a good time around. Mathematics and geometry has been part of all the learning that we have gathered into digital world, be it bits representation or any other significant resources that need encryption_mechanism in it. Numbers when transformed around creates result which when modified and saved becomes ausfule resource to gather a minified information.

This section will gather some of those implications of mathematics into science of authentication, taking equations of geometry to see and analyse that the information converges to a point dealing with various kind of geometrical shapes that corresponds to the equations that holds the values.

The first step in this includes the curve_tracing which distinguishes points in any graph which will have generated curve from any equation, tracing the point of equivalence to justify the result at coordination basis. Step where we will carry on discussion upon the image reflection policy to see if the same information could be used in the both sides of parties.

All the values thus generated will be stored into matrix data format which then will be multiplied with another set of matrix which resembles the property of its to some limit or could be totally anonymous, we will see whole data of equation and find the nth_derivative which will decide the last segment of the information. This may decide the point of convergence to some extent.

We will represent this action with various equations of geometry which logically gives appropriate result for the research document.

We carry around this theory using system of reversible number which inspects that the numbers when reversed and carried around with few implicit theories generates same result when worked around all together(keeping original number and reversed number). This principle in general behaves like

Any positive whole number a which is less than
100 with two digits x, y
$O=10x+y$
Its reverse is therefore
$R=10y+x$
Then sum of a and b is taken as

$$a+b= (10x+y) + (10y+x)$$
$$=11x+11y$$
$$=11(x+y)$$

Similarly,

$$a-b= (10x+y) - (10y+x)$$
$$=9x+9y$$
$$=9(x+y)$$

In general:

$$a+b=10^{n-1}(x_1+x_n) + 10^{n-2}(x_2+x_{n-1}) + 10^{n-3}(x_3+x_{n-2}) +\ldots+ (x_n+x_1)$$

$$a-b=10^{n-1}(x_1-x_n) + 10^{n-2}(x_2-x_{n-1}) + 10^{n-3}(x_3-x_{n-2}) +\ldots+ (x_n-x_1)$$

This system of implication could be helpful in later stages of relation.In this section we discuss on the server side authentication protocol which involves calculations andother mechanism based on the knowledge of user's presence.

Authentication is important and that it generates sequential behavior when presented into generalized pathways and timeline. Mathematical functions and equations when combined with such parameters generates and provides the legitimate functional behavior which when followed into steps and stages could be a way to provide secure connection while transaction and transmitting data.

Convergence theory would be taken into consideration in extended study of this work where we will analysis on various equations when they show this property which will be beneficial to study the level of security.We consider user (sender) and resource_provider (receiver) with secure connection and User login through interface and provides username and password that it is authorized with, a token is generated which in this case is not the password but any mathematical equation suppose a hyperbola.Now this equation is taken and curve is traced according to it, now the curve has various points, we take one tangent or line which touches the curve, this new point is its value for the equation, suppose the equation is for x and y values now the two new points are replaced with its old ones. We randomly decide timestamps and number of timestamps also, now this timestamp would be number of times the equation is modified. Idea is to not make it rigid but dynamic and random, some random mathematical functions and modifications are to be chosen and done, which is server side authentication protocol, and these modifications are normally irreversible. A part of this project is being explained here and rest of which is taken for further research study as extended work which includes analysis of various equations and functions including these steps and to see effectiveness of the security at much deeper level.

UserSide: Username+Password (ServerSide: Token-> Introspection of Series of Steps following it)

Each session generates a Token which needs session key and digital signature from which user has logged in, these parameters will help server to understand difference between live and valid information.There are many such functions that we have seen and tried to work on that makes a good

impulse to security solutions and trying out the information in random order few of those are being notified here.

We understand that every equation has calculation time and it depends upon the arrangement of logical and physical hardware into place, calculation varies with the arrangement, extended research work of this paper includes the analysis of all those arrangements possible and to determine the strength of various calculations.

Reciprocal equation
Multiplication of determinants
Image reflection
Nth Derivative
Curve Tracing
Matrix, Logarithm, Mode
Complex number Analysis
Geometric meaning of a differential equation
Homogenous Equation
Homogenous equation
Laplace transformation
Hyperbolic functions
Differential equations
Trigonometric equations
Method of least squares
Image reflection
Matrix calculations
Empirical laws & curve fitting
Method of group average
Lagrange's formula for unequal intervals etc.

3.3 Sequential Mathematical Solution

We will consider that the client and server is trying to communicate, server decided to provide authorization based on the principle that the client is authenticated, authentication includes providence of username-password while our task is to generate secure code of acceptance which will lead to secure connection between the two. Once the client generates username-password a sequence of mathematical calculation should follow, for a better security we encourage parallel calculations to be followed from client->server and vice-versa so that we could know which step of the sequence is being followed. To enhance the longitivity and security we encourage to choose random calculations of equations followed by one another making in progress that they are logically making sense to each other and are connected in some sense. We generate random milestones where calculations would be generated and in any case someone tries to eavesdrop the calculation should not understand the real meaning behind it. After few research on various methods and functions we have chosen one set of such information for representation.

Step 1. Number of Milestones: 4.

Step 2. @Milestone1. Equation: 9x*x-4y*y-18*x+32-91=0 (including trigonometric values makes it stronger, we have taken normal equation for the sake of simplicity and understanding).

Step 3. @Milestone2. Curve Tracing

The following Graph is generated for this equation.

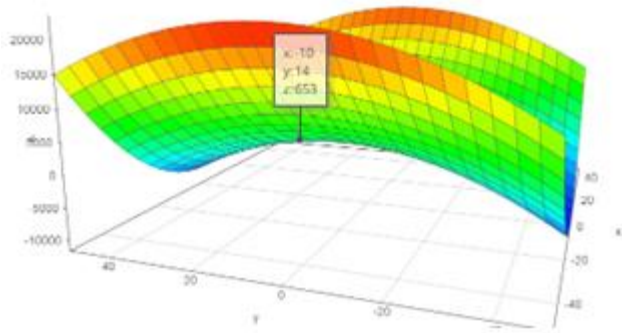

Fig. 3.6

Space for which could be choosen prior or through vector calculation

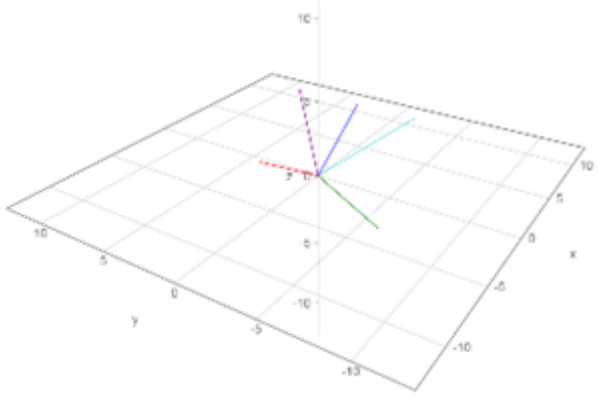

Fig. 3.7

Step 4. @Milestone3. Consider random coordinate values from the above graph: x=10,y=14,z=653 remember these coordinates are only possible with valid form of graph representation, assuming the right values only. It could also be calculated thought formulas or through intersection point of various other graphs inheriting the values from the previous ones. Like i/p for the second would be o/p from the random location of first and it continues.

Example:

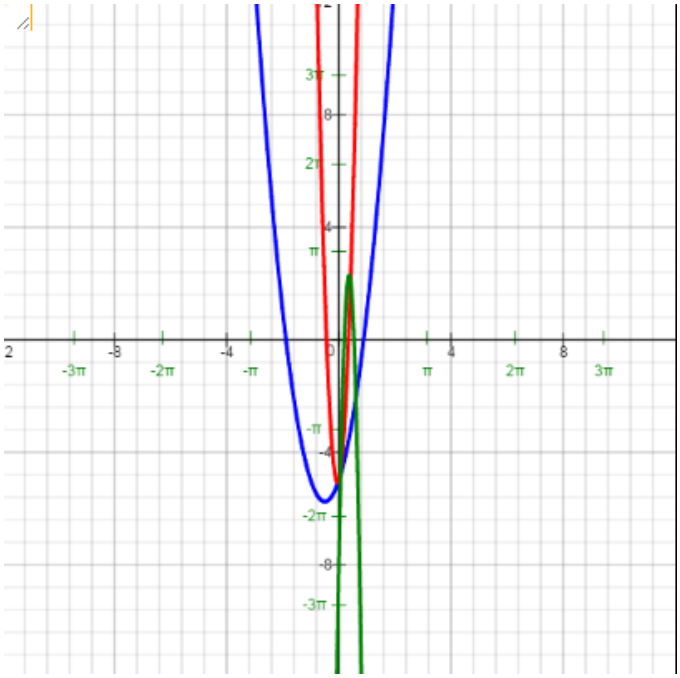

Fig. 3.8

Step 5. @Milestone4:Consider connecting calculation.

The next connecting calculation should include the values from the previous step.

Now let us consider 10, 14,653 as normal values which we will use through reversible number system re-arranging the letters and creating n times of it i.e. N x N matrix representation randomly distributing the values over the matrix.

[10,14,653], ternary:[101,112,220012],Octal:[12,16,1215].

Matrix A

№	A_1	A_2	A_3
1	10	16	220012
2	101	14	1215
3	112	653	12

Fig. 3.9

Consider a random numbers from this matrix, suppose 17408, 26910 now this will act as a input of multiplier_parameter and password converted into numebri parameter for dynamic use respectively, in the next calculation to verify the two sides which we will follow with SRP protocol.

Matrix A

№	A_1	A_2	A_3
1	10	16	220012
2	101	14	1215
3	112	653	12

№	C_1	C_2	C_3
1	143669116	2641900	5739752
2	804847	17408	22257662
3	26910	67665	25434931

N: Prime number calculated from N: 2q+1 where q is also a prime number.
k : Multiplier parameter(17408)
s : user-specified cryptographic random parameter for hashing.
I : Unique user identifier
p : Plain-text password(26910)
u : Masked value of protocol SRP

a,b : Secret random values
A,B : Ephemeral keys
x : Private key
v : Password-proof value
g : generator of prime module N

Fig. 3.10

User	Communication between the Two parties	Service Provider
Step 1: Computation of user public key, known identifier :I $A = g^a$	I,A -----→	Step 1: Computation of server public key, known identifier : s $B=k.v+g^b$
Step 2: Compute Masking value u=hash(A,B)		Step 2: Compute Masking value u=hash(A,B)
Step 3: Compute secret key x= hash(s,p)		
Step 4: computing Symettric key $S= (B-k.g^x)^{a+ux}$ Sessionkey: hash(S)		Step 4 : Computing secret key $S=(A.v^u)^b$, Sessionkey=hash(S)
Step 5 : check the identity of the key Client(computation) --→ Server M= hash(hash(N) XOR hash(g),hash(I),s,A,B,K	M -----→ ←-------- T	Step 5: Check Identity of Key, server(computation) -→ client T=hash(A,M,K)
Exit, if B=0modeN or u=0		Exit if A=0mod

Fig. 3.11

3.4 Quantum mechanism in digital security

Quantum mechanism as for now has been studied on photon particles with polarization, fulfilling the informational blank between the possibility and existence paradigm.

Quantum cryptography is designed to supervise the quantum mechanism to horizon the distribution of session_key and portal discussion to adhere attacks on passive summation including eaves-Drop, also to substantiate the accuracy of session_key. Protocol that works on implied level of quantum mechanism such as 3AQKDP [2] which is adhered to supply multiple (3) events of participation into authentication with generation of session_key at secure level.

This kind of system doesn't believe in mutual belief between one another as the communication link is achievable secure and reliable.

On the other hand overt or explicit unit of key distribution which is also known as 3AQKDPMA[2] developes pre understating based on common utility. Including these sharing mechanism is generating achievable reliability of secure connection over public network where the need for security is developed automatically.Considering the possibility of any third party attack of hindering session_key for their fake use, the resource provider couldn't guarantee that the information provided has been well authenticated in the form of session_key. There is thus need to customize and create higher security link to distribute keys at safer aspect.

The secure connection maintenance desires handshakes at various communication level, quantum physics however notes that information is polarized and get the quantum bit of 0 and 1.Next step is to generate the Q-bit which is considered to hold the distributed undisclosed key and randomly generated string-value which is the formulated into following steps:

- Hex-code Conversion
- Binary Conversion
- Calculate the lest significant bit of the generated value

Anything in quantum mechanism is either positive or negative if we don't include the nucleus of the vibrating object, thus any Q-bit is formulated using following significances.

i.If the value is 0 and 0, then $1/\sqrt{2}(p[0] + p[1])$.
ii.If the value is 1 and 0, then $1/\sqrt{2}(p[0] - p[1])$.
iii. If the value is 0 and 1, then p[0].
iv.If the value is 1 and 1, then p[1].

Another kind of step formulation is where the master details are linked with the corresponding other key values using hash function, to make sure that the encryption of session_key is done using a main_key which keeps the values at MS.Next the secret_key is shared along with the Q-bit to the request-sender to generate encryption values and Q-bit to the resource_provider for the decryption of the receiving value.Now the receiver makes the changes to see the original message, which received the message encrypted using hashing function and Q-bit which validates the origination and originality of Q-bit using MS thus reversing the hash-function for the session_key received from the other side and thus comparing the receiver key with existing key with re resource_provider which gives strong authentication between two parties.

Decryption is made using the session key ad thus original message is retrieved.

Advantages:

Taking quantum mechanism at the digitization level is a better way of providing security while making sure that necessary steps are being taken to formularize the whole process.

Discussion:

The (energy-E), (frequency-f), and (wavelength-λ) for a photon particle is related as follows:

$$E=hf=hc/\lambda,$$

||Where c: speed of light and h: Planck's constant.

So, given any one, the other two can be easily calculated. The above is for the particle travelling in

$$v=c/n.$$

vacuum but for it to be traveling in any medium where n is index-of-refraction, then c is replaced with

We understand that the frequency of any photon particle varies.

Wavelength decides the probability of any photon passed to hit on the space or target. Though we can calculate the energy efficiency of singleton particle of photon through which we can conclude its wavelength. It is considered into functions of wave.

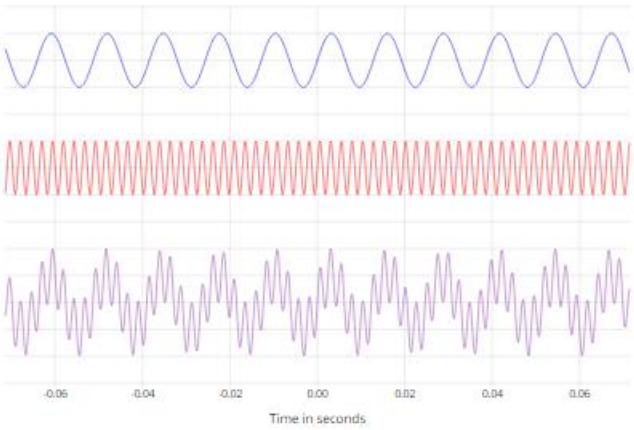

Fig. 3.12. Simulation of wave function

Given that each wavelength has a color and thus vice-versa is also true, this section is extended to another research work where we take colors and their property of frequency to encryptions and security purpose, we also encourage to work on how a string values could be turned into vibrations of code and thus generate wavelength which could be further considered as security measure.

Disadvantage:

Disadvantage with quantum mechanism is that it works on polarization which is basically charged with light particles, while these charged particles are made available to the network chances are if some other light source is shown to Q-bits they might change the value or polarization i.e. from0 to 1 or vice-versa making is difficult to distinguish between the real values.

Concluding the above section is that above mechanism is much reliable with efficiency for authentication and could be seen as promising approach securing attacks at passive-network also reducing hand-shake time consumption for the authentication. Benefit of using this approach is that the secret keys are recyclable; since each entity works independently a large section of groups could be controlled individually by their own sub-groups controlled and managed by itself.

3.5 Other Authentication Mechanism

While we talk of authentication there are numerous ways one can think of using physical entity as the information granter. We all share unique identity in our own bodies which are traced into digital environment gives unique results that's why physical presence are capable of generating right authentication, in the following scenario heartbeats could be calculated as an authentication tool which suggests that if the person while registering information is conducted with an emotional force the heartbeats reacts differently with different emotion even though the heart rates are fluctuating there could be diminishing value which suggests that one can be authenticated through this mechanism.

While we carry our devices which takes fingerprints while we type with the intensity also measures the information that came out of our prints, prints of various segments of body which distributes unique features are taken for request which when matched with the database are given verification results.

Our suggestion is that various facial expressions could be monitored to provide next level of security because every information comes from the pixel level which could be gradual level of submitting authentication [10].

Since the images are provided into format that a machine normally confuses with many information into one single data which needs to be converted into one_dimention since images are 2_dimention images and thus requires to provide with the information which unites the requirement specification.

Research Related Work on the Following Topic

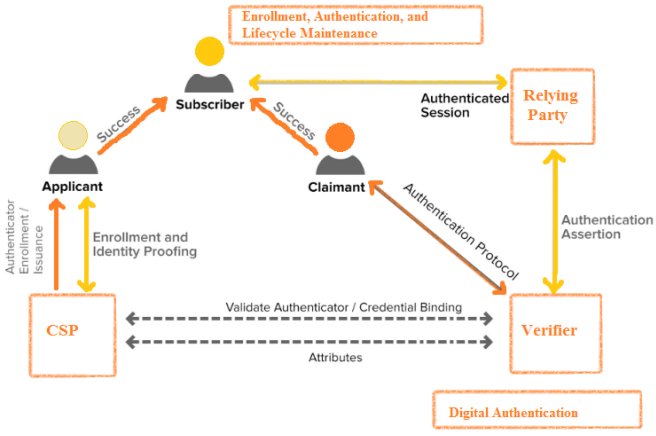

Fig. 3.13. NIST model for the authentication life cycle

Authentication is seen as a paradigm where we generate identification matrix based on the information available with the two parties, digitally these authentication process are cumulated with digital_signature, token or handshaking mechanism, and there are many other mechanism which are discussed in this section. We have tried to provide general information on the research work related to the topic.

A. Types of protocols

Generally we work on the authentication principles which are on the tropical level of association and shares common information between each other (different parties associated in the authentication grouping), taking them into stages of implications.

Authentication is generally point to point and thus creates the need to submerge and associate the required initialization between two points.

Authentication protocols developed for PPP Point-to-Point Protocol
•PAP - Password Authentication Protocol
•CHAP - Challenge-handshake authentication protocol
•EAP - Extensible Authentication Protocol

Wheras we see that there are other principles of working where the information's are put to efficient resource of allocation.

The Password Authentication Protocol (PAP)
The Shiva PAP (SPAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP (MS-CHAP)
The Extensible Authentication Protocol (EAP)

B. Challenges in making Authentication Secure

1. Validating the both side common subsidiary values.
2. Availability of the person while using the device which are arranged with the authentication and authorization.
3. Identity verification.
4. Cost for computation.
5. Phishing related issues with token verification.
6. Operational cost.
7. Privacy issues.
8. Forgery of physical biometric appearance etc.

4. Future Work

As a part of this paper includes analysis of various combinations of calculations based on the simple mathematical equations. We also put work on vibration based cryptography which could be visualized

Performance = (Ideal Cycle Time X Total Count) / Run Time

as colors, we also extend our work to calculate time efficiency and strength of any combination with the effects of choosing random equations for consideration.We also would forward our work in the convergence theory of any equation at given conditions.Our inclusion of extension also validates the efficiency and quality of equations which also includes:

5. Conclusion

This paper is divided into various sections discussing on the issues and substitutions of authentication paradigm, first part of the paper discusses upon various authentication mechanism to be followed in making a secure network, next of which includes the involvement of various calculations which could be considered in making a secure authentication code, a part of which included analysis of strength and quality of any calculation and its parameter which will be taken into future work consideration. This paper also generates the behaviour of quantum physics included into machine based security system, we have discussed on how we can efficiently use physical representation of photon Q-bits to enhance the security followed by discussion on the topic. A part of this paper presents various protocols on authentication and also the challenges in making them into consideration. This paper provides discussion for a secure authentication algorithm implementation using various mathematical calculations and modification providing few simulated results on them.

References

[1] Qi Jiang, Sherali Zeadally, Jianfeng Ma and Debiao He 2017 Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks *IEEE Access* **5** 3376 – 3392

[2] Jacobs S, Bean C P Rado G T and Suhl H 1963 Magnetism,Fine particles, thin films and exchange anisotropy *New York: Academic* 271-350

[3] Thangavel T S and Krishnan A 2010 Performance of integrated quantum and classical cryptographic model for password authentication Second *International conference on Computing, Communication and Networking Technologies* 2010 1 - 8

[4] Todd Booth and Karl Andersson 2017 Stronger authentication for password credential Internet Services *Third International Conference on Mobile and Secure Services* (MobiSecServ) 1-5.

[5] Minyoung Bae, Ju-Sung Kang and Yongjin Yeom 2017 A Study on the One-to-Many Authentication Scheme for Cryptosystem Based on Quantum Key Distribution *International Conference on Platform Technology and Service (PlatCon)* 1-4.

[6] Lan Zhang, Hong-yun Ning, Yun-yun Du, Yan-xia Cui and Yang Yang 2016 A new identity authentication scheme of single sign on for multi-database *7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*

[7] Balaka Ramesh Naidu, Prasad Babu M S 2016 Development of a biometric authentication system based on HAAR transformation and Score Level Fusion *7th IEEE International Conference on Software Engineering and Service Science (ICSESS)* 2090-1093

[8] Muhammad Muaaz and Rene Mayrhofer 2017 Smartphone-based Gait Recognition: From Authentication to Imitation *IEEE Transactions on Mobile Computing* **99** 1 –3.

[9] Matúš Uchnár and Ján Hurtuk 2017 Safe user authentication in a network environment *IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)* 451-454.

[10] Shadi Janbabaei, Hossein Gharaee and Naser Mohammadzadeh 2016 Lightweight, anonymous and mutual authentication in IoT infrastructure *8th International Symposium on Telecommunications (IST)* 162-166

[11] Murari mandal 2015 Comparison of human and machine based facial expression classification *Researchgate*