Abstract—Nuclear monitoring must be considered as high precedence against national security. Now, with the increasing nuclear threats it is crucial to ensure that malicious entities never procure nuclear warheads. Which comprises the prevention of illegal or terrorist access to nuclear weapons. The disastrous damage that could be the consequence of unauthorized, unapproved utilization of nuclear weapon and from the expansion of nuclear technologies to unacceptable states, has driven the nuclear forces to spend epic measures of securing nuclear warheads as well as the supporting materials, infrastructure, and industries. The procedure of ratifying user’s credentials is known as authentication. Cognitive based authentication is a type of authentication that is actually the amalgamation of neurobiological and psychological techniques. This research is intended to provide human inspired Cognitive Multi-level Authentication (CMLA) utilizing the extensive quantum processing capabilities. Simulation is being done on online QUVIS quantum simulator using quantum cryptography BB84 algorithm where the intended person is successfully authenticated while considering different scenarios. So, the proposed scheme will come up with self learning intelligence based secure, speedy and reliable authentication systems against nuclear command and control.

Keywords— Cognitive Computing, Natural computing, Quantum computing, Multi-level authentication

1. INTRODUCTION

It is hard to build up a demonstration of warfare from comparable and covering wording. Numerous people and groups cause harm by utilizing accounts illegally. Terrorists have a past filled with illegal utilization of nuclear warheads to contend with their adversaries. Terrorism fit inside this usual way of doing things. As nuclear states turn out to be increasingly more dependent on interconnected new advancements of technology, they turn into an inexorably suitable target. Illegal access based account’s misuse offers different lopsided advantages. Now, it has become moderately easy to access and hack accounts for terrorism. A wide variety of pre-composed, computerized, hacking devices are promptly accessible on the web and expect little to learn [1] [2].

As nuclear command and control is highly vulnerable against the terrorism. It requires more extensive secrecy than conventional terror based oppression, as the back tracking by intermediary hackers/intruders (i.e. proxies), IP addresses spoofing, botnets, and lawful impediments are now quite easy. As far as stealth, digital spying takes into consideration the quiet recovery of data from a system, or the remote utilization of another individuals’ account to lead illegal operations [3]. The word “security “has grown in not long past years. Security can be regarded as “affirmation of being safe or protected from attacks” or security against opponents, from the entities who can intentionally or un-intentionally damage or misuse. Following sections will explain the security background.

1.1 Principles of security:

The term security comprises six basic principles as described below:

1.1.1 Confidentiality:

This principle allows the accession of content only to the intended sender and recipient. [4]. It is generally identical to secrecy. Measures attempted to guarantee privacy is intended to keep delicate data from contacting the wrong individuals, while ensuring that the authorized individuals can, in reality, get it: Access must be confined to those approved to see the required information.

1.1.2 Integrity:

It refers to illegal access based manipulation. It includes keeping up the trustworthiness, consistency, and precision of
information throughout the whole life span. The confidential information must not be variate in transmission, and proceedings must guarantee that it can't be manipulated by unapproved individuals.

1.1.3 Authentication:
This phenomenon assists to setup proof of recognition. For authentication, three systematic parameters are utilized as: “Something you know” (Knowledge-based), “Something you have” (possession-based), “Something you are” (Biometric based).

1.1.4 Non-repudiation:
This phenomenon provides the guarantee and genuineness of authentication and assurance of integrity.

1.1.5 Access control:
This mechanism states the control strategy i.e. what can be accessed by whom?

1.1.6 Availability:
Ensures the data accessibility to the intended users at the time [4]. Both information systems and confidential information should be available and accessible to clients on time. Availability loss is the interruption of access to or utilization of information systems or confidential information.

1.2 Attacks:
Attacks usually categorizes as follows.

1.2.1 Active Attacks:
It is the manipulation of data contents by some means.

1.2.2 Passive Attacks:
Passive attack is a type of attack which comprises no data manipulation. An appropriate secure system should have the following layers of security [5].

1.3 Layers of security:
1.3.1 Physical security:
For the protection of physical objects from abuse or illegal access.

1.3.2 Personnel security:
For the protection of authorized personnel or group of personnel.

1.3.3 Operational security:
For the protection of specifications of operations, actions and corresponding activities. Monitoring of the security of confidential procedures and tasks.

1.3.4 Network Security:
For the protection of network related contents, constituents and their interrelationships.

1.3.5 Information security:
For the protection of “Confidentiality”, “Integrity” and “Availability” of sensitive information either in processing, storing or in sending. These measures can be attained by means of teaching, training or with the help of distinct plans and strategies and technologies [6].

1.3.6 Access control phases:
Access control is a verified mean to get into the organizational confidential places and sites. There are four major phases against ensuring verified access. That are Identification, Authentication, Authorization, and Accountability.

1.3.6.1 Identification:
After entering the user ID, matching of that ID with the help of database is known as the process of identification. For the protection against hackers and attackers, few systems are based upon arbitrary and unsystematic ID generation.

1.3.6.2 Authentication:
Authentication is the phenomenon of verifying the intended user.

1.3.6.3 Authorization:
Authorization is the process of examining and comparing the authenticated user to grant access.

1.3.6.4 Accessibility:
Accessibility refers to the availability or approachability to the authorized persons.

1.3.6.4 Accountability:
For retaining system’s records, a process is known as accountability. It retains the record of all signups and sign-ins that were “successful” or “unsuccessful” [7].

1.4 Quantum Computing:
Quantum computing is a sub-discipline of “Quantum Information Science”. It has two major applications quantum communication and quantum cryptography. It is a type of computing based upon a quantum mechanics to perform operations on data. It possesses various properties like entanglement, superposition, decoherence. It has revolutionized the way of computing by performing operations at atomic/subatomic level with exponential increase of parallel processing [8].

1.4.1 Utilization of Quantum Computational power:
The proposed system will utilize quantum computing power to manage extensive processing of Cognitive configuration module. As the advances in processing power and computation capabilities are starting to saturate, with
significant ramifications. Forty years prior after the invent of the silicon 'chip', Gordon E. Moore, the prime supporter of Intel, made an intense and original perception: "the intensity of PCs and their hardware multiplies every 18th months, and would proceed to twofold". This expectation depended on quickly propelling upgrades in transistors. Transistors are the computing workhorses, with a huge number of these minor systems packed into present day computing chips. These have kept on getting to be smaller and quicker, prompting exponentially-execution processing over all computing systems. The exponential development of computational power that we are noticing for a long time is beginning to soak. As processors are becoming smaller, with more prominent quantities of transistors packed into chips, their speed, ability wind up constrained by the measure of atom sizes themselves! So as to come back to further increase the computing power, a progressive change in the foundation of a computing system is required. Now we need to maintain strategies by utilizing such transistors, which contain billions of atomic particles to perform computations. 'Quantum computing', an energizing innovation, will boost up this saturation point of computation power. Quantum computing and its hidden strategies depend on the quantum mechanics, where computations are performed on atomic and sub-atomic level. In our plainly visible world, we can have either 0 or 1: as cats can be either in alive state or dead state! In the quantum world, cats are permitted to be both alive AND dead, a superposed state until we measure them. It is this interesting characteristic, that atoms and quantum objects are permitted to be in a mix of numerous states, that makes this a ground-breaking resource. Quantum computing guarantees new abilities for preparing data and carrying out computationally arduous tasks [9].

1.4.2 QuantumKey Distribution (QKD) Algorithm:
A mean for secure communication is Quantum cryptography scheme based upon the principles of quantum mechanics is regarded as Quantum Key Distribution [10]. Two parties are allowed to share arbitrary secret key between them against message encryption and decryption. QKD is used for the production and distribution of key, not for the transmission of cipher text. One of the quantum key distribution protocol is BB84 algorithm (i.e. pioneer of quantum cryptography protocol) [11].

Rest of the paper is organized as discussed below. Section.2 presents the motivation behind this research. Section.3 is all about the research gap and research directions. Section.4 reviews the literature for some of the commonly used authentication systems. Section.5 elucidates the entire proposed work. Section.6 explains the significance of proposed scheme. In the section.7 we described the simulation and their results. Finally section.8 concludes the paper.

2. Motivation:
As nuclear command and control is highly vulnerable against the terrorism. The extensive increase of illegal account hacking is leading to high terrorism rate. This rate is increasing day by day. Now, it requires a substantial level of security and controlled access. For attaining suitable level of protection demands a multi-aspect / multi-level security system. This research is deliberated to present cognitive computing based multi-level authentication with the amalgamation of quantum computing in order to intensify the authentication towards nuclear command and control. It will ensure user authentication approval, with multi-level intelligence augmenting (human inspired) measures.

3. Problem Statement:
One of the crucial challenges in the design and deployment of a secure authentication system is the requirement to have a balance between employing a procedure that guarantees nuclear weapons are ever accessed after legitimate authorization, and guaranteeing they are never accessed (or exploded) without appropriate approval. For example, the accession of ‘grimy bomb’ — a gadget that would scatter radioactive material over a city coverage — is likewise a genuine risk. It probably will not kill anybody however it could prompt threat, and in a financial focus it could cause incredible monetary harm.

There is a need of guaranteed authenticated access, whatever the location of the nuclear warheads and vias for accession. It require users’ efficient authentication and management across all kind of nuclear resources and devices. The increasing national nuclear demands makes nuclear security even more complex: how would we assemble new nuclear power stations without significantly expanding the hazards that awful individuals get access of weapons or fissile materials? As single aspect validation systems against nuclear command and control is not secure enough. The rapid technological enhancements recommends having multifaceted/ multi-level verification, against nuclear warheads. Following research questions depicts the dimensions of this research:

- Can nuclear power and systems be compromised or ‘spoofed’?
- Can cognitive computing be employed towards authentication?
- How could quantum computing be utilized to intensify authentication procedure?
- How could quantum key distribution be employed to enhance the security of user credentials?

4. Literature Review:
In literature, numerous techniques have been introduced ranges from simplest password authentication to more advance authentications. In this section, we will have an overview of these techniques.
Blonder proposed the graphical password scheme. It describes, a picture would show up on the screen, and the client would tap on a couple of its picked regions. In the event that the right areas were clicked by the user, then he would be verified. Jensen et al. proposed a solution of passwords based upon graphics also regarded as "picture - password" planned particularly for cell phones, for example, PDAs. For password generation, it is required to choose a theme by the user (for example ocean and shore, feline and hound and so forth), it may comprises of thumbnail photographs. The client at that point chooses and enlists an arrangement of the chose thumbnail photograph for password creation. The client needs to perceive and recognize the prior observed photographs and enlist them in the right sequence utilizing a stylus so as to be verified [12].

Trusted Computing Group [13] specified a chip for security i.e. TPM Trusted Platform Module (TPM) [14]. According to Kakei S. et al. it has been implanted in mobile devices and PCs etc and it is generally utilized as a main secure authentication scheme. Since TPM has an element of verifying a private key comparing to an open key comprised by the user certificate, it is feasible to utilize TPM simply like USB token or IC card without requiring extra devices, for example, a USB device or card reader [15].

According to Škorić B., Quantum-Secure Authentication (QSA) based upon quantum physical properties and principles gives a solution relies on the key readout security. Quantum physical key's readout like quantum cryptography uses the no cloning theorem to hide difficulties from the intruders [16].

One of the most profitable mean for banking is online banking. It allows users to acquire distinct services and utilize their accounts at low cost, with more flexibility and convenience. These systems must facilitate verification phenomenon before permitting access to them. For ensuring extensive security these online systems must employed efficient authentication schemes. According to Sharma A. et al. Quantum cryptography is frequently depicted by its advocates as "unequivocally secure" to highlight its distinction with classical cryptographic conventions. In this paper, the author disected the prerequisites of user verification from QKD perspective. They attempted to demonstrate the issues which show that the QKD verification will be extremely a decent scheme as multifaceted verification[17].

Smart chip based verification is a possession-based (i.e. something a client has). For user authentication, it comprises implanted certificate. User can embed the card into a smart card reader for authentication. Smart card based authentication is a common authentication scheme with a pin providing multifaceted verification. User must have something (smart card) and know something (i.e. pin code) are the authentication factors in smart–card based authentication [18].

According to Spector H., Biometric strategies give the something you are a factor of verification. Biometrics validation is a strategy that distinguishes a client as well as confirms their personality depending on the estimation of their extraordinary physiological attributes or social qualities. It comprises thumb pattern, facial pattern, iris-pattern, retina scanning, hand geometry-based authentication [18].

According to Kumar G. et al. a digital signature is an encryption scheme like the Internet ID version. Public and private key based advanced authentications guarantee to the receiver that the message is originating from a particular individual [18] [20].

According to Farik M. et al. nowadays, for communication and information exchanging, internet has appeared as most suitable and commonly utilized media. In this paper author presents a password based authentication mechanism. Length of a password is a greater strength, on the other hand a difficulty to break, While you are preferring passwords, compact password utilization is relatively crucial. A compact password should be the amalgamation of special letters, characters, numbers, capital and small words. Nowadays it is recommended to utilize 12 character password by the security administrator. A password with “12 characters”, with the “cardinality of 94” and “entropy of 78-bits”, using super computers will consume 55 days for cracking, while a common PC will consume “3018 years”. We can check the password strength by using online sites like "PasswordStrengthCalculator.org" [19].

5. METHODOLOGY:

Cognitive based authentication is a type of authentication, based upon natural computing as inspired by human authentication phenomenon that is actually the amalgamation of neurobiological and psychological techniques. No verification-proofing framework can exist in a vacuum. To provide the adaptable, vigorous identification management demands, a multi-level authentication scheme must be actualized due to vulnerabilities in single level authentication system. This research aims to propose a cognitive multi-level authentication model. This section elaborates the Cognitive Multi-level Authentication (CMLA) scheme. The overall authentication mechanism is shown in fig.5.

Motivation behind the integration of quantum computing in authentication process is that, as the cognitive information processing demands critical level of computing power. Due to the quantum exponential increase of parallel processing, it necessitates the merge of quantum computational power with Cognitive Multilevel Authentication as well as for its secure storage using Quantum Key Distribution(QKD).
5.1 Client request:

When the user interacts with the system and demands for access, he/she will have to go through three levels of authentication as discussed below. Quantum Key Distribution (QKD) is used here for user authentication using BB84 algorithm. Therefore, user entered information against these three level of authentication will have back end QKD based encrypted storage. If the user entered data and basis matched with backend data and selected basis then user will be granted access otherwise denied. Fig.1 shows the overall authentication process.

![Cognitive Multi-level Authentication (CMLA)](image)

**Fig.1 Authentication Process**

5.2 Smart-chip based authentication:

Overall this phase lies in ‘something user has category’. This chip is the equi-size of “credit-card”, with implanted certificate for the intended user identification. The smart-chip reader validates the inserted card. In conventional smart cards, user is provided with a pin code to utilize smart cards. However, this smart-chip is proposed to embed user pin code as well as thumb pattern to completely unlock it. So, after inserting the smart chip, it will be completely locked and it will require further two sub-steps (i.e. pincode and thumb pattern). Firstly, user has to enter the pincode. But it will be partially locked and to completely unlock it requires the user to enter thumb impression as well. Fig.2 elucidates the Smart-Chip based authentication i.e. first level of authentication in CMLA.

The most powerful specialty of smart chip authentication is its diverse authentication multi aspect authentication. One aspect is the smart chip that comprise the ‘user have something’ factor i.e. ownership factor, the pin code that encompasses the factor of ‘user know something’ i.e. knowledge factor and finally the thumb pattern comprises ‘user is eligible’ i.e. biometric factor. So only, the single chip enclosed three-aspect authentication and second it usually have a microprocessor that makes it more powerful authentication mean. This microprocessor keeps private and public key track [18]. This is a big attempt for prevention against ensuring confidential access. After successfully passing this level control will be forwarded to second level.

![Smart-Chip Verification](image)

**Fig.2 (First Level) Smart-Chip**

5.3 Interrogative Acoustical Verification:

Second level of authentication is based upon question based session (i.e. here acting as a visual stimulus based upon user written responses) and auditory input verification. Interrogative session is a propelled identity approval strategy to validate a user by making inquiries chose from ethical, psychological, sociological, behavioral and personal data related only to the user. Few of the exemplary questions are shown in fig.3. Dynamic questioning authentication can be made progressively viable due to the profundity and broadness of inquiries, which reference both currently perceived and past experienced based collected information. These questions generally necessitate the client to effectively answer numerous inquiries and could incorporate a diversionary inquiry that is intended to trap the illegal entity. In this dynamic scheme, the questions asked by the system are distinctive each time. While this is commonly more secure than static scheme, it forces an extra computational power on the system. This extensive computation power can be managed with the assistance of quantum computing. This phase is not just a questioning based but for the verification of auditory inputs as well. The entire auditory computational sense comprises a type of signal processing and machine learning for separating useful data, it might have some algorithm’s implementation with microphones for:

- Representing your caught sound
- Organizing/Detachment
- Identifying/Characterizing/Recognizing
5.4 Ocular based authentication:

This level of authentication is based upon biometric factor. Biometrics alludes to a programmed acknowledgment of an individual dependent on physiological highlights. Facial verification, when utilized in blend with another biometric technique (i.e. iris scanning), can improve check outcomes significantly.

A facial identification and recognition is a system that captures a pattern or a structure of the face and maps it to in the knowledge-base saved pattern to authenticate the user. Moreover, space between the eyes, nose, mouth and jaw, upper shapes of the eye attachments, the sides of the mouth,
area of the nose and eyes, and the zone encompassing the check bones are likewise considered. For ocular sense generation it may possess "Hyperspectral imager", "Radar imaging Lidar scanner", "organized light 3D scanner "," Thermographic camera", "Side scan SONAR", "Manufactured gap SONAR". Secondly, iris is the fundamental critical piece of the human eye; it comprises of roundabout muscle and the other longitudinal control in the measure of light going the retina through the human eye. Iris Recognition is one of the critical biometric acknowledgment frameworks that distinguishes individuals dependent on their eyes and iris. Individual ID dependent on iris acknowledgment gives a standout amongst the most solid outcomes. Fig.4 depicts the (third level) ocular verification.

5.5 Cognitive Configuration Management:
Quantum computing acquire its leaps forward computational power from the speedy scheme embedded in quantum mechanics. The tremendous measure of quantum computational power necessitates for the proposed Cognitive Multi Level Authentication (CMLA) scheme.

After passing through the three levels of authentication, for the maintenance of extensive levels of security we employed here QKD based encrypted storage as well. This QKD will start immediately after the three levels of authentication, at the beginning of Cognitive Configuration Management module (i.e. stimulus) and pass out these credentials to other modules in encrypted form as to secure from data hacking and finally mapping and matching process will based upon the QKD mechanics. For this here data from three levels will be further processed in the form of photons.
5.5.1 Procuring Phase:

This phase is known as procuring phase as it comprises the sensory stimulus detection and selection processes. The following modules assist in procuring phase.

5.5.1.1 Sensory Stimulus:

Stimulus is a noticeable change in outer or inside condition. It evokes a particular reflex. It goes about as a fundamental for creating perception. "Stimulus Filtering “permits to sieve and react to noteworthy stimulus to abstain from reacting to insignificant stimulus. When we observe our surroundings, we recognize and select the stimulus from the environment. "Distal Stimulus “is the physical stimulus around us reach to our senses. "Proximal stimulus" that is being enrolled/entered through receptors for example voice, facial pattern, thumb impression, pin code and so forth. Exteroceptive stimulus that is derived from the environment surrounding. As this system is based upon human cognitive psyche, so all the exteroceptive inputs (i.e. pin code, thumb impression, auditory input, facial pattern, iris pattern) acts as stimulus (from human nature perspective). All the inputs will pass out to their respective sensory memory buffers. These two small buffers inside sensory memory processing is based upon fusion process. For example for facial pattern recognition, obviously there is no single sensor or device for capturing the facial pattern. So, to fuse all the inputs of all sensors and provide a concrete single output i.e. complete facial pattern, this type of processing will be performed by these small buffers of sensory memory.

5.5.1.2 Iconic memory/visual memory store:

Portrayal of visual stimulus rationally known as "icons". In this manner, iconic memory will go about as a sort of buffer for operating the visual stimulus for 2-3 seconds. It will handle the visual based inputs (as human can visualize) i.e. thumb impression, pin code, facial pattern, Iris pattern etc.

5.5.1.3 Echoic Memory:

A sort of store ("holding tank") for the portrayal of hearing stimulus goes about as a buffer for processing acoustic input for 3-4 seconds to appropriately operate it. It will handle the acoustic interrogative session inputs.

5.5.1.4 Neural sensory stimuli:

Iconic and echoic memory output will act as neural sensory stimuli module's input. Auditory, Visual stimuli are the sensory inputs (as in human perspective). These stimulus caught through receptors prompts "action potentials" regarded as "Transduction". Action potential are the signs or spikes. These successive spikes generate a "Spike train". It is primarily useful to initiate inter-neural processes.

5.5 Operating Phase and Out-turn Phase:

This phase is known as operating phase as it evokes the inter-neural processes, This phase and the out-turn phase operates collectively for performing meta-cognition processes. And their collective processing results in the authentication completion process, that will be either access denied or successful access granting.

5.6.1 Perceptual Associative Memory(PAM):

From here, sensory inputs are transmitted to PAM (simply like Thalamus, which is a part of forebrain particularly of limbic system). It categorizes and analyses (like a doctor) the sensory data. Through extractor, it will excerpt and classify the required data of the observed stimulus. For example auditory input categorization i.e. amplitude, pitch, frequency etc. From that point forward, data will send to other parts for further handling. On the off chance that this part (module) gets harm, it results in deficiency of sensory data analysis and prompts 'sensory confusion'.

5.6.2 Mediator:

It helps in sensory input storage from sensory modalities to long-term memory (inspired by the working of Hippocampus part of limbic system in human forebrain). It additionally helps in memory recall (retrieval of memory). Any impairment in this module may prompt loss of memory or new memory creation as it gets information from PAM and store them as a new memory to knowledge base (i.e. long-term memory). The more knowledge base will populate for specific intended individual, greater is the trust level of that individual (just like human sharing and accession is greatly lies on the trust level between the interacting entities).

5.6.3 Knowledge base:

A consolidated storage or repository for compressive knowledge is regarded as knowledge base (i.e. Long Term Memory/LTM). A "necessary part" and the board of organizing, managing, storing and optimizing the explicit knowledge. Knowledge base stores the definite data of perceived stimulus. Here we have to comprehend the contrast between data, information and knowledge. Echoic and iconic sensory memory simply fuse the data. While separated or filtered data is regarded as information. PAM stores the information extricated through extractors and that information moves toward becoming knowledge where it is put away as a LTM in knowledge base in an organized way for reusability in future.

5.6.4 Meta-knowledge:

Meta knowledge base will comprehend the data about knowledge base. It will monitor and control the knowledge base structure.

5.6.5 Working Memory:
It performs the functionality of working memory (like prefrontal-cortex). Extracted data through PAM produces low-level perception. This data will recover related information from Knowledge base, on the off chance that there exists any subjective past experience, at that point it will go out to buffer as a prior memory for example sensory modality module have data including face structure (in low level perception) and if there exists any past experience with respect to that face structure, the entire knowledge will call back and will be appeared in buffer as a recent meeting and the two inputs from the sensory modality module (as of now observed-currently perceived) and from buffer (past experience) will go out to meta-cognition module for matching and mapping process to perform validation. This is a self-thinking control (metaphor-stage) stage. In any case, if there exists no past experience, at that point just sensory modality information will proliferate for metaphor stage. So, individual identification, will be performed in either of the two ways

- Current experience + past experience (login).

  OR

- Just current experience (registration).

Here mapping of current and past experience will be done based upon quantum mechanics as the information was encrypted using QKD (based upon polarized photon measurement steps as mentioned in simulation section.7). Here system will authenticate the interacting individual to access or denied.

5.6 Algorithm:

**Algorithm:** CMLA (SC, PC, TP, QAs, IP, FP, VP, VF, VA)

**Declaration:**

- SC ➔ SMART-Chip  
- PC ➔ Pin-Code  
- TP ➔ Thumb Pattern  
- QAs ➔ Question-Answering  
- IP ➔ Iris Pattern  
- FP ➔ Facial Pattern  
- VP ➔ Voice Pitch  
- VF ➔ Voice Frequency  
- VA ➔ Voice Amplitude  
- EI ➔ Echoic Input  
- IL ➔ Iconic Input  
- II ➔ Iconic Input

**Execution:**

- \text{II=}Iconic\text{Memory}(FP,\text{ IP, PC, TP, QAs})  
- \text{El=}Echoic\text{Memory}(VP, VF, VA)  
- \text{Current-Parameters = Sensory Memory(II, EI)}  
- \text{Current-Parameters, Perceptual AssociativeMemory(NeuralSensory Stimuli)/Activation of perceptual Associative memory}

\begin{itemize}
    \item Current-Parameters = Extractor.Perceptual Associative Memory() \ // low level perception
    \item Prior-Parameters=Search.KnowledgeBase()
    \item Prior-Parameters.MetaCognition.Map(Current-Parameters)
    \item Validation=Prior-Parameters.MetaCognition. 
    Match(Current-Parameters)// Validation is a boolean variable indicates true or false after mapping, true indicates Access granted and false indicates access denied
    \item End
\end{itemize}

5.8 System Flow:

Fig.6 shows the system front end user Interface (UI) based system flow, which comprises three levels of authentication. After successfully passing through these three level of authentication user will be allowed to access the system. Back end cognitive configuration management flow is shown in fig.7.

6. SIGNIFICANCE OF PROPOSED SCHEME:

This authentication scheme is proposed for Post Quantum era. Due to the involvement of quantum computing the proposed scheme would be more secure than classical authentication schemes (i.e. as quantum computing comprises atomic/subatomic level computing). As quantum computing performs exponential parallel processing than classical systems which perform linear processing, so the proposed scheme would be more speedy than classical authentication schemes. Based upon extensive speed and security the proposed scheme would be more reliable than other classical authentication systems.

Table .1 Literature review based Comparative analysis [20]

|                | Public-Key Cryptosystem | Private-Key Cryptosystem | Biometric Authentication System | CMLA/Proposed |
|----------------|-------------------------|--------------------------|---------------------------------|---------------|
| Security       | High                    | High                     | Reasonable                       | High          |
| Speed          | Low                     | High                     | High                            | Very High     |
| Reliability    | Very good               | Good                     | Good                            | Very Good     |

7. SIMULATIONS AND RESULTS:

We proposed cognitive multi-level authentication scheme using Quantum Key Distribution technique. This simulation is being done on online QUVIS quantum simulator [21] using quantum cryptography BB84 algorithm. Quantum key distribution will help in intended user authentication. Alice here is acting as an intended user and bob is acting as the backend knowledge base controlling entity, based upon
Alice’s registered information she will be either allowed access or denied. It comprises few steps as listed below in 7.1.

**Fig. 6 Front End System Flow (Three Levels)**
7.1 Steps for Alice  QKD based authentication:

While using BB84 Algorithm, single photons polarized into one polarization state from four polarization state chose from two sets of conjugate basis. 0° and 90° polarizations are comprised by the rectilinear basis and 45° and 135° polarizations are comprised by the diagonal basis

- Transmitter (i.e. Alice) arbitrarily creates both basis that can be either diagonal or rectilinear and a bit that can be either 1 or 0, perform photon polarization in like manner.
- Alice transmits polarized photon (towards Bob).
- Random selection by bob from one of the two bases and analyzer orientation accordingly.
- Bob is informed whenever Alice transmits a photon.
- Measurement procedure.
- Both Alice and Bob check the bit value for every individual particle.
- Both of them will come to know that they have same values only if they have same bases.
- By keeping the same basis value, both have keys.
- Now Alice data will be transmitted to bob.

Here, QKD based credential verification will be done. By following, the above-mentioned steps Alice will be authenticated, as the intended person and she will allowed to access.

Scenario 1:
The above phenomenon shows the fixed base based authentication. When Alice interacts with system to login, Alice entered information (for level 1, level 2 and level 3) will be authenticated using Quantum Key Distribution by Bob (i.e. back end monitoring entity). Here Alice and Bob both have selected fixed basis (i.e. H/V). Above scenario fig.8 shows the Alice successful authentication.

**Scenario 2:**

![Fig. 9 BB84 algorithm](image1)

Fig.9 shows the random base selection based QKD authentication. Where due to data destroying by the eve, Alice transmitted information is not forwarded to Bob. So, Alice and Bob will repeat this process.

**Scenario 3:**

![Fig.10 BB84 algorithm](image2)

The above mentioned scenario fig.10 shows quantum key distribution using polarized photons with eve attempt to access the information. Due to wrong base and data selection eve is not succeeded to access the data. Alice information is successfully transmitted to bob and Alice is authenticated as the intended person.

**8. CONCLUSION:**

With the immense advancements in technology, there is an extraordinary risk of terrorism-based oppression with the concern of nuclear weapons. The key security ensuring procedure of an “information system” is the authentication process. We proposed cognitive authentication technique based on natural computing (as inspired by human authentication natural phenomenon); that comprises the neurobiological study of human authentication scheme. This system is actually an attempt towards post quantum era. Secondly, this system demands extensive computation power that is proposed to tackle with quantum computing power in order to intensify the system efficiency. We performed simulation using QUVIS online simulator and while considering different situations towards the intended person successful authentication.

**9. REFERENCES:**

[1] Ning S. Practices on Nuclear Security and International Cooperation. International Atomic Energy Agency (IAEA). China Institute of Atomic Energy (CIAE). Beijing, China. 2009; IAEA-CN-166/57: 83-4.

[2] Ganjie L. Nuclear Security–New Challenge to the Safety of Nuclear Power Plants. International Atomic Energy Agency (IAEA). 2008; IAEA-CN—168/1-11.

[3] Anderson RJ. Chapter 11. Nuclear Command and Control in Security Engineering: A Guide to Building Dependable Distributed Systems, 2001 March: 231-41.

[4] Newman RE. Introduction to Computer and Network in Computer and Network Security. 32611-6120.

[5] Aggarwal H. Information Security : An Introduction. JICST. 2012 July – Sept; 3(3):951-4.

[6] Whitman ME, Mattord HJ. Chapter 1: Introduction to Information security in Principles of Information Security. © 2016, 2012 Cengage Learning:1-42.

[7] Alenius F. Authentication and Authorization. Achieving Single Sign-on in an Erlang Environment. 2010 August:8-10.

[8] Jafarpour S. Introduction to the World of Quantum Computers. 5th IEEE Int. Conf. on Cognitive Informatics (ICCI’06). 2006:760-64.

[9] Barker A. Quantum Computing: The Return of Exponential Growth. ResearchGate. 2016 April 5.

[10] Zhou T, Shen J, Li X, Wang C. and Shen J. Quantum Cryptography for the Future Internet and the Security Analysis. Hindawi Security and Communication Networks. 2018; Vol:2018 :ID:8216619 :7.

[11] Singh H, Gupta DL, Singh AK. Quantum Key Distribution Protocols: A Review. IOSR Journal of Computer Engineering (IOSR-JCE), 2014 Mar-Apr; 16(2):1-9.

[12] Kushwaha BK. An Approach For User Authentication One Time Password (Numeric And Graphical) Scheme. Journal of Global Research in Computer Science. 2012 Nov; 3(11): 54-7

[13] TrustedComputingGroup. [Online]. Available: http://www.trustedcomputinggroup.org/. [Accessed 13 May 2019].

[14] Trusted Platform Module (TPM) Summary, Trusted Computing Group, [Online]. Available: https://trustedcomputinggroup.org/press-rooms/events/trusted_computing_in_action/. [Accessed 13 May 2019].

[15] Kakei S. Mohri M, Shiraiishi Y, Morii M. SSL Client Authentication with TPM. IEICE Trans. Inf. & Syst. 2016 Apr; E99–D(4):1052-61.

[16] Škoric B. Quantum Readout of Physical Unclonable Functions. Int. J. Quant. Inf. 2012; 10(1): 1-21.
[17] Sharma A, Lenka SK. Authentication in Online Banking Systems: Quantum Cryptography Perspective. International Journal of Scientific & Engineering Research. 2014 February;5(2):561-64.

[18] Raju AS, Udayashankara V. Biometric Person Authentication: A Review. International Conference on Contemporary Computing and Informatics (IC3I), 2014;575-80.

[19] Farik M, Ali AS. Algorithm To Ensure And Enforce Brutce-Force Attack-Resilient Password In Routers. International Journal of Technology Enhancements and Emerging Engineering Research. 2015 Oct; 4(10):184-8.

[20] Kumar G, Anjala, Sharma J, Authentication Techniques in Computer Networks. International Advanced Research Journal in Science, Engineering and Technology. 2014 October; 1(2):76-9.

[21] The Quantum Mechanics Visualisation Project. University of St Andrews. [Online]. Available: https://www.st-andrews.ac.uk/physics/quvis/. [Accessed 3 May 2019].