Journal of Theoretical and Applied Information Technology
10th November 2015. Vol.81. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AUTHENTICATION MECHANISM FOR CLOUD NETWORK AND ITS FITNESS WITH QUANTUM KEY DISTRIBUTION PROTOCOL: A SURVEY

[1]ROSZELINDA KHALID, [2]ZURIATI AHMAD ZUKARNAIN, [3]ZURINA MOHD HANAPI, [4]MOHAMAD AFENDEE MOHAMED

[1] Faculty of Computer Science and Information Technology, University Putra Malaysia, UPM, 43300, Selangor, Malaysia
[2] Faculty of Computer Science and Information Technology, University Putra Malaysia, UPM, 43300, Selangor, Malaysia
[3] Faculty of Computer Science and Information Technology, University Putra Malaysia, UPM, 43300, Selangor, Malaysia
[4] Faculty of Computer Science and Information Technology, University Putra Malaysia, UPM, 43300, Selangor, Malaysia
E-mail: [1]roszelinda@hotmail.com, [2]zuriati@upm.edu.my, [3]zurinamh@upm.edu.my, [4]afendee@upm.edu.my

ABSTRACT

Communication in a huge network such as in cloud infrastructure is vast in demand. Almost all classified information transferred via the communication channel. Most types of attack can cause the classified information be in the hand of unauthorized party. This situation will lead to information disclosure and the user feel unsecured for using the services like offered by cloud infrastructure. Besides, we look into authentication as a primary concern; we also pay attention to the secure communication channel. We believe, with a secure communication channel additional with a secure authentication we may reduce the possibility of attack that may lead to information disclosure. This paper summarizing the issue and challenge facing in cloud authentication mechanism. We also review existing technique of authentication mechanism for cloud network and discuss important issues in this field such threat and insecure scheme, whereby the root of these kinds of issue originates from the weak-ness of the authentication mechanism on the security channel being using. After all, we found the implementation of quantum key distribution scheme in an enormous network such as cloud infrastructure may resolve the issue interception of unauthorized party in the network. A study investigating how the use of quantum key distribution key, can guarantee that the message has not been modified or replaced by a dishonest party with control of the communication line.

Keywords: *Cloud Authentication, Multi-Party Quantum Key Distribution, Secure Communication*

1. INTRODUCTION

Cloud computing is defined as deploying network services and storage resources over the Internet. It has an abstraction for the complex infrastructure. It supports remote data storage and accessing the remote services. Cloud computing improves its role in computer network. A number of public network sites are introduced presently to share data among each other. In the cloud computing, each user is a single owner of whole data stored in the cloud. So it needs fewer infrastructures to access data from the cloud and no need to require more knowledge to maintain the infrastructure of cloud storage. The cloud services were managed and maintained by the third parties called Cloud Services Providers (CSP) at remote locations. If just network connection is available, the cloud can allow the users to access to information. So cloud computing architecture is an alternative technique to the traditional information technology [1]. Data is centralized or outsourced to the cloud. The fundamental aspects of the cloud's paradigm are shifting data or sharing data one with others. It can access remotely, and flexible depend on demand manner. Not only it easy to access with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

local independence, but also less expensive in hardware and software. As large storage of data and limited resources of the client, it is a very crucial thing to determine the integrity verifications. There are many security models to solve, integrity verification problems [2]–[4]. Many researchers are proposing a number of schemes [5]–[7] to enable public audit ability. Even though there are lots of advantages of moving into cloud infrastructure, we are also take care of the privacy and security of the transaction. In cloud's, multiple users are accessing simultaneously through the Internet. In [8], the authors has discuss comprehensively about the challenge and proposed methodology in cloud computing. The most important is on how to secure the sensitive data and remain confidential.

Since the data is sensitive and confidential, it may not be secure to share in the public storage. Even the public storage is recommended various encryption techniques of data provide privacy and security [9]. Several schemes were proposed [10]–[13] to provide security for data sharing on untrusted servers. In these schemes, the data owners store the encrypted files in untrusted storage and distribute the corresponding keys to only authorized users. So, unauthorized users and untrusted servers cannot know about the content of data files since they do not no know the decryption keys. The most important issue for data is their confidentiality.

The need for highly secure communication system is a must in the current scenario and to the whole nation. Massive information are transferred continuously, whether it be top secret information on banking information. With this growing information exchange, the possibilities for unauthorized reception are also increased. Quantum cryptography based on physical principles that cannot be defeated. This need for secure communication provided the driving force for interest in quantum cryptography or quantum key distribution, in particular.

2 PRELIMINARIES

2.1 Authentication Scheme

Authentication is a scheme that needs to prove of continuity in a relationship that usually the basis of trust and identification. In computerization mechanism, we need to verify someone's identity in order to decide or figure out either there are legitimate. Currently, most of the security transmission depends on the unproven computational security. On any communication process, the mechanism should comply with the three top items that are confidentiality, integrity, and availability. With the role-playing by the authentication, integrity item is a must. Any mechanism needs it to make sure that all the transmission data is not change due to any event.

There are many standards in cryptographic, and authentication is one of them. As mention earlier, authentication is an important task to guarantee the initial phase of communication is secure before it can establish the connection between the legitimate parties.

The mutual authentication mechanism has the potential to make sure that the user and the server can correctly identify each other. Mutual authentication and session key agreement enable the user to transfer their data or to access the server correctly and securely over the public network [14].

In addition, the leakage of the user's specific information, enables the adversary to track the user current location and login history [15]. Although user's anonymity ensures user's privacy by preventing an attacker from acquiring user's sensitive personal information. In addition, anonymity makes remote user authentication mechanism more robust, as an attacker could not track which user-server are interacting'. By conceal entities with their real identity during communication, it can preserve the anonymity [16].

For this reason, to achieve secure and anonymous communication, a cloud infrastructure should support efficient mutual authentication protocols in which user and server can anonymously authenticate each other so that a secure session can be establish. In the past few years, many identity-based mutual authentication protocols have been proposed for cloud infrastructure [14][9], [17]–[19]. During mutual authentication, user and server interact with each other and verify the legitimacy of each other, and then establish a shared session key using a shared secret.

In this regard, Yang and Chang [18] proposed an identity-based remote user authentication protocol for mobile users based on an elliptic curve cryptography (ECC). Their scheme inherits the merits of both identity-based cryptosystem and elliptic curve. In 2009, Chen et al. [17] identified two security flaws, namely, insider attack and impersonation attack in Yang-Chang's scheme. To remove these security flaws, they presented an advanced password-based authentication scheme using ECC. The authors claimed that their protocol

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is secured to provide mutual authentication and is appropriate for cloud computing environment. However, Wang et al. [20] showed that Chen et al. [17] protocol is not secure and is vulnerable to password guessing attack. Besides that it also prone to key compromise impersonation attack and also suffers from the clock synchronization problem. In 2010, Wang et al. [9] proposed a public auditing protocol where auditing protocols are used to ensure authenticity and integrity of the outsource data. However, in 2012, Xu et al. [21] analyzed serious security flaws and showed that Wang et al. [9] protocol is vulnerable to existential forgeries. Their protocol is using known message attacks from a malicious cloud server and an outside attacker. Kang and Zhang [22] also presented short key size identity-based authentication scheme, although it suffers forward the secrecy attack and does not maintain users' anonymity.

Presently, most of the mutual authentication protocol does not prevent key compromise impersonation attack. In addition, if the users' long-term private key is compromised, then it cannot change its private key by itself (without server or private key generator (PKG) support). To achieve, the user has to communicate with PKG [17], [18], [22]. As a result, the attacker gets success to perform impersonation attacks. If a user will be able to change its private and public keys periodically, then the leaked key (key compromise) situation can be handled in a better way. In addition, periodical change of private–public keys will enhance user anonymity scenario, as the attacker cannot identify the user with the public key of the user, which is used to establish a session.

Anonymity protects consumer privacy and makes remote user authentication more robust during communication. In addition, user anonymity restrains an attacker from acquiring sensitive personal information about an individual's preferences, lifestyles, shopping patterns and expenses by analyzing the content consumption and accessing communications [23]. In this paper [24], we will apply the pairing based certificateless authenticated key agreement protocol for cloud infrastructure that is introduced by Al-Riyami and Paterson [25]. This proposed approach removes key escrow problem as PKG generates only partial key of the user, and the entity secret key depends on the entity's generated shared key. In this scheme, server and user achieve their partial private keys from PKG and can generate secret value to achieve their public– private keys. Moreover, user and server can change their private–public keys whenever they required without the involvement of PKG. Further, both parties can mutually authenticate each other and establish a session key to communicating securely. In addition, user and server's real identity and public key are not revealed during communication, which makes the communication completely anonymous.

2.2 Cloud Services

Discussing on cloud services we may define it as a practice of using a network of remote servers hosted via Internet to store, manage, and process data, rather than a local server or personal computer. B.Furht in [26] acknowledge that cloud computing can define as a new technique of computing which dynamically scalable and usually virtualized resources are provided as a service over the internet. It also has become a significant technology trend, and many experts expect that cloud computing will reshape information technology (IT) processes and the IT marketplace [27]. By applying this technology, we can gain cost savings, high availability, and easy scalability.

Table 1. Deployment Models ([28])

No	Model	Description
1	Private Clouds	Operated by or for a single organization
2	Community Clouds	Operated for groups of organizations with similar service requirements
3	Public Clouds	One general SLA for all; data resides on shared resources
4	Hybrid Clouds	Connect public and private clouds sharing services and data among them

Table 1 is a summary of a deployment model in cloud services. Users tend to choose their personal model that suits with their requirement.

Journal of Theoretical and Applied Information Technology
10th November 2015. Vol.81. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

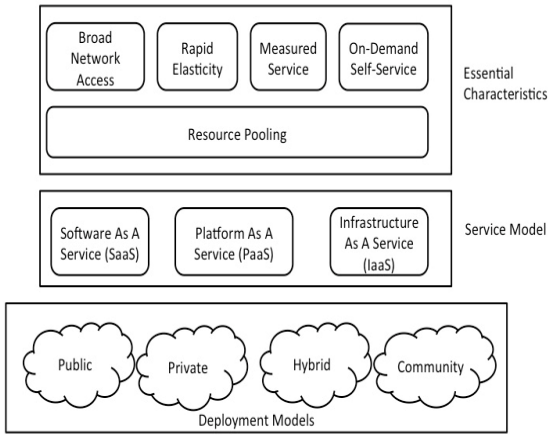

Fig.1. NIST Visual Model of Cloud Computing Definition adopts from[28]

Figure 1 depicts a definition of cloud computing. Begin with its essential characteristics that offer a better service such as broad network access, rapid elasticity, measured services and it is an on-demand self-service. All of these services if being pooled in one location named as resource pooling. Next, cloud computing is divided into three categories that are software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). This entire cloud service model is offering range of products with advanced capabilities like automated scalability, pay-per-use, and on-demand provisioning. In cloud computing, virtualization act as a core subject matter. For example, service providers or internal enterprise private cloud managers, they use virtualization technology with regards to its efficiencies and flexibility offered by cloud computing [29]. It covers the risks and considerations around cloud computing environment. Referring to [30] there are:

- How would we be harmed if the asset became widely public and widely distributed?
- How would we be harmed if an employee of our cloud provider accessed the asset?
- How would we be harmed if an outsider manipulated the process or function?
- How would we be harmed if the process or function failed to provide expected results?
- How would we be harmed if the information/data were unexpectedly changed?
- How would we be harmed if the asset were unavailable for a period of time?

From above questions, we could conclude the main constraint among the user of adopting cloud computing are confidentiality, integrity and availability.

Fig.2 shows the OpenCrowd Cloud Solution taxonomy. It is an initial points, to demonstrate the ranks of available solution for each cloud models. We believe from the shown taxonomy, the potential of migrating the classical approach to cloud computing is almost there. It just we need to find out the gap, and find out the solution for closing the gaps.

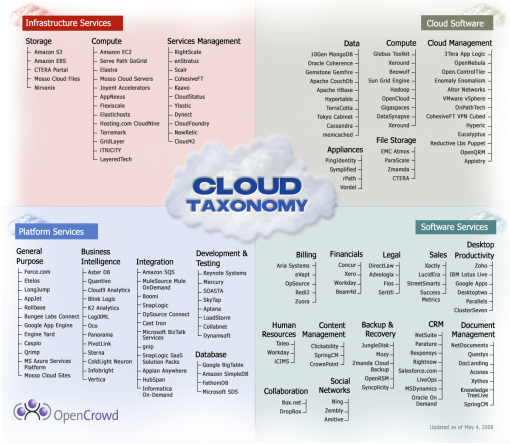

Fig.2. Cloud Taxonomy adopts from [30]

2.3 Cloud Computing Gap

We can see that is enormous potential in cloud computing. However, they are many users still have doubt to place their corporates data in the cloud. This can bring a gap between the user and cloud provider. The huge gap is getting trust from the user. According to National Institute of Standards and Technology the major barriers of adopting cloud computing are in terms of security, interoperability and portability. In [31] a comprehensive discussion on security issues in cloud. The issue highlight the obstacles in cloud computing. These are availability of service, data lock-in, data confidentiality and auditability, data transfer bottlenecks, performance unpredictability,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

scalable storage, bugs in large distributed system, scaling quickly, reputation fate sharing and software licensing.

Table 2. Security Barriers in Cloud Computing

Paper	Barriers
S.Sundareswara[32]	Data security strategy, authenticity
S.Zargari, A.Smith[33]	Privacy challenge
S.Haider[34]	Security, authenticity, auditing, security standard
A.Baldwin, D.Pym, S.Simon [35]	Risk Assesment, Quality Assuarance
C.Jinyin, Y.Dongyong, [36]	Data security strategy
Frank [37]	Cloud Security Audit
M.Taylor[38]	Forensic investigation of cloud computing systems

From the table above, most of the paper are more consent on the security aspects of adopting cloud in their infrastructure. However, security itself has many components. In this paper, we manage to extract the most important element in security classification. We named it as process validation. From all the security classification such data validation, storage security, auditing and forensic, we strongly believe process validation is the most crucial. From the classification, we manage to find out the gaps.

Table 3. Security Gaps in Process Validation of Cloud Computing.

Paper	Security Classification	Method	Gap
[39]	Process Validation	Identity Based Mutual Authentication in Cloud Storage Sharing using elliptic curve cryptography	The session key and shared key can be duplicate
[40]	Process Validation	Framework that provides identity management, mutual authentication. Using two network channel for interchange the shared key	Not using a randomization in generating the key, open the space for attacker to guess the key.
[41]	Process Validation	Introducing the multi-level authentication technique which authenticates the passwords in multiple levels to access the cloud services.	Using almost all authentication technique. It may incurs cost and time processing
[42]	Process Validation	Introducing efficient certificate less tripartite key agreement protocols. This authentication mechanism with encryption technique is dedicated for enterprise private cloud file system.	Increase cost and did not complete the identity authentication of the clouds.

In refining a gap as in Table 3, we found the authentication is important element in securing cloud. It is become the prior point to convince the users in adopting cloud computing technology.

2.4 Securing Cloud

Data loss or unauthorized leakage to a third party is one of the biggest threats in the cloud computing bussiness. As we have already mentioned in the previous section, cloud computing is a combination

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of various computing entities, globally separated, but electronically connected. As the geography of computation is moving towards corporate server rooms, it brings more issues including security, such as virtualization security, distributed computing, application security, identity management, access control, and authentication. However, strong user authentication is critical for cloud computing to ensure that only valid user have access to the server.

Study on some existing authentication schemes has been carried in order for highlighting the gap. Most of it is based on client-server architecture. The first remote user authentication schemes have been proposed by Lamport [38] in 1981, in which, the server stores the hashed value of a user's password. In Lamport's scheme, password table was used to verify the legitimacy of users. However, if this password table is compromised, stolen, or modified by an adversary, then the system could be partially or completely undermined [39],[5].

Some more recent smart card based password authentication schemes have been proposed in [40],[41]. Many of the schemes have been broken as shown by [42],[43],[5]. Shoup-Rubin [44] proposed extension of Bellare- Rogaway model [45]which is based on three party key distribution protocol and smartcard is used to store the long term secret keys. In their scheme, smartcard is used to prevent the adversaries and it is assumed that smartcard is never compromised. The scheme falls in one factor category as two factor schemes can be broken by compromising both the factors only. Liao et al. [46] tried to consolidate a number of passwords and smartcard based properties and proposed two factor smartcard and password authentication scheme. Cloud computing is a variant of client server architecture, where, thousands of clients use the same infrastructure at a large scale. Consequently, it needs stronger authentication than conventional client server inter-networking system. Lee et al. [47] have proposed public key and mobile out of band based authentication for cloud computing. However, the scheme transmits data (e.g. ID, PW, and PKI) in a plaintext form that can be easily intercepted by the adversaries. In addition, their scheme does not care about data confidentiality; data integrity, user privacy and users are not allowed to change their password. As a result, their scheme does not fit for real time cloud computing.

Mishra, Kumar, and Mukhopadhyay proposed a pairing free identity based authentication framework for cloud computing [39], in which they try to enhanced identity based mutual authentication scheme for client server cloud architecture. However, these schemes did not address access control for cloud computing users. Referring to a previous research[48], they introduce a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operates in concert with Single Sign On (SSO) and Lightweight Directory Access Protocol (LDAP).

To ensure the authentication, integrity and confidentiality of involved data and communications. The solution presents a horizontal level of service, available to all implicated entities, which realizes a security mesh, within which essential trust is maintained.

Public Key Infrastructure (PKI) including exchange key using certificates and revocation list has the capabilities to authenticate users in the cloud infrastructure. Most of the users agree that confidentiality, integrity, and authentication are the key concerns in this cloud infrastructure. However, there is a certain issue pertaining to the PKI authentication where the public key cryptography only provides computational security because PKI is based on Asymmetric Key Cryptography. It is exposed to widespread security threats such as eavesdropping, man in the middle attack, masquerade etc. By means, the attacker could easily determine a person's private key. It may prone to information disclosure. The other problem is the loss of the private key may be irreparable.

At this moment all, the received messages cannot decrypt anymore if the private key is less. This phenomenon has triggers the needs of authentication technique involving multiple users that ensure the safety communication across the nation. As we can see from above literature, the existing authentication schemes still have a room for improvement. Thus, from there we found a gap to enhance the existing schemes.

In mutual authentication, mechanism user must prove its identity to the server and the server must prove its identity to the user. In the proposed scheme user and server both authenticate each other. To achieve it, user and server exchange message authentication codes, which includes entities' identities and secrete keys. Mutual authentication is a security feature in which a client process must prove its identity to a server. On the other hand, server must prove its identity to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

client before any application traffic is sent over the client-to-server connection.

It also called two-way authentication, is a process or technology in which both entities in a communications link authenticate each other. In a network scenario, the client authenticates the server and vice-versa. In this way, network users can be assured that they are doing business exclusively with legitimate entities and servers can be sure that all would-be users are attempting to gain access for legitimate purposes. Mutual authentication is gaining acceptance as a tool that can minimize the risk in cloud computing. Mutual authentication should not be confused with two-factor authentication, a security process in which the client provides two means of identification to the server, such as a physical token and a password.

The fundamental problem of authentication is how to check for a shared secret under the guarantee that it will stay known only to Alice and Bob. For mutual authentication, of course, it is inevitable that they share some initial secret. If this not the case, one classical method is to use a trusted third party who can verify that a particular key belongs to whomever it is supposed to-like in public key cryptography. User authentication based on quantum cryptography using any public channel has previously been studied.

Therefore, a real possible solution to address this issue by integrating the multi-party Quantum Key Distribution (MQKD) protocol with the PKI mechanism. This integration will involve the deployment of enhance tight finite key scheme to authenticate the cloud infrastructure involving multi user communication.

2.4 Quantum Cryptography (QC)

The most well-known and developed application of quantum cryptography is quantum key distribution (QKD). QKD describes the process of using quantum communication to establish a shared key between two parties (usually called Alice and Bob). The scenario is without a third party (Eve) studgy anything regarding that key, even if Eve can eavesdrop on all communication between Alice and Bob. The condition is achieved by Alice encodes the bits of the key as quantum data and sending them to Bob; if Eve tries to learn these bits, the messages will be disturbed, and Alice and Bob will notice. The key is then typically used for encrypted communication.

Modern cryptography, which is widely used in computer networks, relies on computational complexity. In other words, dawn of the quantum computer with the quantum algorithm culminates the end of modern cryptography. However, QC can provide unconditional security, especially by its property no-cloning theorem and Heisenberg's uncertainty principle. Quantum based security schemes can classify into two major divisions called single photon and entangled photon.

A quantum entangled state is a correlated state between two particles such that result of measurement on one particle affects the state of another particle that is physically separated from the measured particle. Quantum Cryptography utilizes the original characteristics of quantum mechanics such as superposition, entanglement and so on. Using these properties, some information can be secretly shared between users through a quantum channel. The information can be a key or a message.

Quantum cryptography involving Quantum Key Distribution (QKD) protocols is used to share a key and Quantum Direct Communication (QDC) protocols are employed to send a message [49]. Quantum Key Distribution (QKD) is an active research with various protocols, scheme, and application. The reason QKD becomes an on demand research because a threat such as impersonation or man-in-middle attack makes QKD vulnerable.

In a meanwhile, the authentication domain in quantum cryptography is the hardest part due to its level of complexity. Despite this, quantum cryptography is only used to solve the key distribution problem, not transmit any useful data. The strength of any cryptosystem depends on the difficulty than an eavesdropper faces in breaking in. However, with the arrival of Quantum Computing, it becomes easy to crack any cryptosystem. The security of QKD can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution. This is usually described as "unconditional security".

Unconditional security means, Alice and Bob are required to authenticate each other. Such as, Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack perhaps possible. Classical cryptography is no longer a secure communication method. Securing data and data communication are a top priority because the consequences of unsecure data can have grave effects on both the economy and national security. Quantum cryptography relies on the laws of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

quantum mechanics to provide a secure system while the traditional system relies on the computational difficulty of the encryption methods used to provide a secure system [50].

As for this research, we are proposing to implement Quantum Key Distribution (QKD) as an aid to the process in authenticates the communication in a cloud infrastructure. The ultimate goal of quantum key distribution protocols is to provide the reliable parties, Alice and Bob with random, correlated, and private classical data, the key. To get into this, they have a quantum channel at their disposal, which is, however, to be assumed completely under the control of the adversary, Eve. Meaning that whatever quantum state Alice or Bob send through the channel, the output can be completely arbitrary, the only restriction is consistent with quantum mechanics. In addition to the quantum channel, the reliable parties can make use of a public, classical channel, which is assumed to be authentic, by mean, it cannot be altered or forge messages.

Instead of considering the distribution key between two parties, we have to pay attention to what happened if it involving more than two legitimate parties. In clouds we can see that it may involve a number or users, here we will introduce using of Multiparty Quantum Key Distribution (MQKD). Multiparty QKD (MQKD) is a key distribution protocol in which the same key is distributed to different parties based on quantum mechanism [51]. MQKD can be referred as a key distribution protocol establishes a shared key among a number of users. To achieve the practical feasibility and simplicity in MQKD, a standard cryptographic like authentication is needed. Authentication is the important task to secure the communication between users. User identification and the origin of the data is required to be genuine, because, if a malicious user masquerades as a legitimate user, the key distribution schemes, and encryption schemes will be easily compromised.

As a prior relevant research, Matsumoto proposed a first protocol without the use of entanglement to achieve MQKD. His findings enables three parties agrees at once on a shared common random bit string in the presence of eavesdroppers [52]. The main difference between our proposed protocol and Matsumo's protocol is that our protocol allows numbers of parties to share a common secret key after the establishment of the secret key among the parties. Furthermore, our protocol utilizes one-way public communication (post processing) to share a final secret key. Here, Matsumoto's protocol requires three-way post processing efficiently. All the parties are required to participate in the calculation. Contrastly, our proposed protocol needs only the sender to transmit a public message to the parties. As long as, the public channel is authenticated and unedited by Eve, then our proposed protocol proves unconditional security.

Moreover, we use simple post-processing technique to share a common secret key among the parties. We prove that our proposed method in [53] has a significant towards the attack resilient. The 10% of improvement, in order to reduce the possibility of man in the middle attack, shows that the scheme is reliable to implement in a cloud-computing environment. The simulation runs on the cloud environment that we have set up earlier.

Quantum mechanics effects can be used to transfer information from Alice to Bob, and any attempted eavesdropping by Eve will always be detectable. Three distinct phases are present: raw key exchange, key sifting, and key distillation, with the option, to discard the secret key at any of the stages if it appears that not enough security could obtain from it.

2.5 Quantum Authentication

Obviously, it would be nice if quantum methods could provide self-enforcing protocols. However, even if this would call for some ''asymmetric quantum key'' cryptography that remains to be invented, we would unfortunately still need a trusted authority to authenticate the public quantum key. What we are concerned with here is to reflect upon whether quantum mechanics with its inherent property unitary and entanglement can yield any advantage over classical methods providing authentication via an arbitrator. For protocols designed with Trent, like those proposed in [54], [55], we believe we cannot offer Alice and Bob with a key that can be unconditionally kept secret from Trent. As it is actually he/she who directs the entire authentication process.

In other words, if Alice and Bob's mutual authentication is guaranteed only by their individual and non-necessarily correlated secret with Trent. Then, Trent will also have full control over their communication (regardless of what channels are used) and can always do a "man in the middle" attack if he so chooses. We conclude that, in principle, no restrictions can be imposed on Trent.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3 QUANTUM KEY DISTRIBUTION REVIEW

In the classical cryptography, a variety of encryption algorithms has been introduced, providing different levels of security. Apart from that, they all have in common that in principle they can be cracked. For example, the RSA cryptosystem, one of the widely used algorithm (e.g. in SSL, SSH), relies on the fact that it 's hard to find the factors of large integers. There are two threats to this method: The first is that more computational power will help to make time consuming attacks (like brute-force attacks) more convenient. Moreover, someone might even think of an efficient algorithm for factoring integers. The second problem is that quantum computers are in fact already capable of executing the factorization efficiently. On the other hand, there exists a classical, unconditionally secure cryptographic algorithm, but it has a significant problem. It requires a random key, which has to be as long as the message itself, and this has to be transported securely from one party to the other. It cannot be done classically.

Here, an amazing idea comes to play. Quantum mechanics has the property of hiding some information from us, as expressed in Heisenberg's uncertainty relation. Could this inherent ignorance be used as an advantage over a potential eavesdropper? It turns out, that this is indeed possible and after discussing the essential quantum mechanical properties, it will be introduced a method establishing a secret key between two parties, which is provably secure. This security is a direct consequence of the fundamental axioms of quantum mechanics.

Interesting about this method is that a usually unfavorable property of quantum mechanics is employed to achieve something that cannot be done outside the quantum world. The fact that two non-commuting observables can only be measured with limited precision allows unconditionally secure key distribution. This idea been called as quantum key distribution (QKD).

3.1 Basic Quantum Key Distribution

QKD employs two difference channels. One is used for transmission of quantum key material by very dim (single photon) light pulses. The other, the public channel carries all message traffic, including the cryptographic protocols, encrypted user traffic. QKD provides a means to distribute unconditionally secure key for one time pad, using photons over an optical network. Key exchange or key distribution is at the heart of cryptography. Secure key by QKD can be used for many applications including secure communications and message authentication over any standard communication channels.

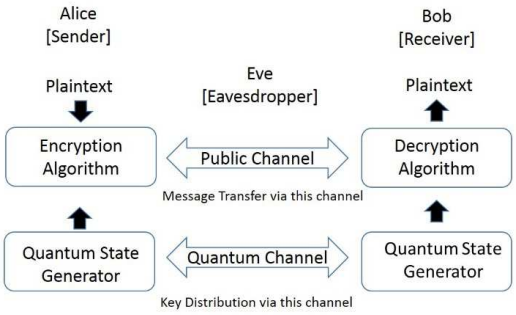

Fig. 3 The concept of quantum key distribution

A QKD protocol cannot work only by itself, and it needs to authenticate the classical messages that are exchanged between Alice and Bob. Typically, we use the Wegmen-Carter type authentication protocol, which is unconditionally secure at the expense of consuming a small portion of key. The use of the Wegman-Carter type authentication protocol requires the initial key for the very first run of a QKD protocol. Since this key is used only for authentication, it needs to be secure only until the end of authentication. For the next rounds of the QKD protocol, we can use the key generated in the previous rounds. Due to the consumption of the key, a QKD protocol is sometimes called a "key growing" or "key expansion protocol."

By the law of quantum physic, any eavesdropper (Eve) that snoops on the quantum channel will cause a measurable disturbance to the flow of single photons. Alice and Bob can detect this, take appropriate steps in response, and hence foil Eve's attempt at eavesdropping.

In QKD protocol, the use of the light wave makes it more reliable and fast. Light waves are electromagnetic waves that can show the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass.

Information about the photon's polarization can be determined by using a photon detector to determine whether it passed through a filter. In other words, photon is a quantum object. It can be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

considered to have a property only after measured it. The type of measurement impacts the property that find the purpose.

The algorithm for selecting base in quantum key distribution discussed in [56]. Selection of base is important to identify any attempt from eavesdropper. In quantum key distribution, any attempt of an eavesdropper to obtain the bits in a key not only fails, but gets detected as well. Specifically, each bit in a key corresponds to the state of a particular particle, such as the polarization of a photon, named quantum bit (qubit). The sender of a key has to prepare a sequence of polarized photons qubits, which are sent to the receiver through an optical fiber channel. In order to obtain the key represented by a given sequence of photons, the receiver must make a series of measurements using a set of polarization filters. A photon can be polarized rectilinear (0o, 90o), diagonal (45o, 135o) and circular (left - spinL, right - spinR).

The process of mapping a sequence of bits to a sequence of rectilinearly, diagonally or circularly polarized photons are referred to as conjugate coding while the rectilinear, diagonal and circular polarization is known as conjugate variables. Quantum theory suggests that it is impossible to measure the values of any pair of conjugate variables simultaneously due to Heisenberg's principle of uncertainty. The same impossibility applies to rectilinear, diagonal and circular polarization for photons. For example, if someone tries to measure a rectilinearly polarized photon with respect to the diagonal, all information about the previous "property" of the rectilinear polarization of the photon vanished.

BB84 Algorithm of QKD BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984. It allows two parties; as a standard convention that Alice as sender and Bob as receiver, to establish a secret shared key using polarized photons qubits. Eve is presented as eavesdropper. The steps of the algorithm are explained below:

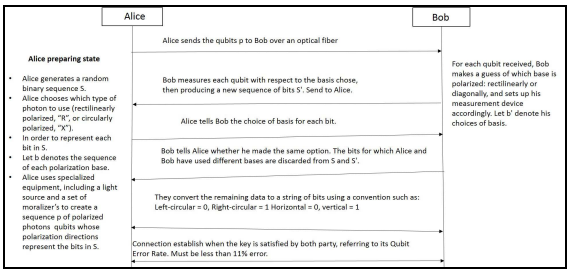

Fig.4 The BB84 protocol. Standard conversation between Alice and Bob.

3.2 Shannon Entropy, Von Neumann Entropy

Entropy itself has meant uncertainty in random variability. It is important in information theory. As for quantum information, the intelligence of quantum algorithms is achieved with the principle of minimum information distance between Shannon and von Neumann entropy. Typically it is measured in bits. In quantum information point of view, the Shor's algorithm could be used to compute the quantum states because of its dynamic condition.

Then, the Shannon entropy is interpreted as the degree of information accessed through measurement while the von Neumann entropy is employed to measure the quantum information of entanglement. Entanglement exists when it has a mutual exclusion between variable and quantum state. The intelligence of a state with respect to a subset of qubits is defined. The highest achievement of a state is at the maximum if the difference between the Shannon and the von Neumann entropy for the chosen result qubits is minimum.

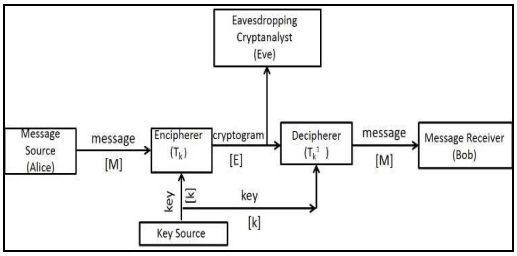

Fig. 5 Schematic diagram for cryptographic based on Shannon

The Shannon concept could be interpreted as in Fig.1. Quantum information can be measured by using an analogue of Shannon entropy called the von Neumann entropy. Shannon entropy is the average unpredictability in a random variable, which is equivalent to its information content.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Shannon entropy provides an absolute limit to the best possible lossless encoding or compression of any communication, assuming that the communication may be represented as a sequence of independent and identical distributed random variables.

Shannon's source coding theorem mentions that a lossless compression scheme cannot compress messages, on average, to have more than one bit of information per bit of the message [57]. The entropy of a message has to multiply by the length of that message, and then the measurement of how much information the message contains can be done.

Shannon's theorem also proves that no compression scheme can compress all messages. The Von Neumann theory also called as projective measurement. In this case, Shannon's entropy and Von Neumann entropy could be a compliment each other. The von Neumann entropy is being extensively used in different forms such as conditional entropies and relative entropies. It implies in the framework of quantum information theory[58]. Entanglement measures are based upon some quantity directly related to the von Neumann entropy [59].

However, there are several papers dealing with the possible inadequacy of the Shannon information measure, and consequently of the von Neumann entropy as an appropriate quantum generalization of Shannon entropy. Their primary concern is how the classical measurement in Shannon's theorem can measure the information with the ignorance about the properties in the system.

4. DISCUSSION

The current commercial systems are aimed mainly at governments and corporations with high security requirements. Key distribution by courier is typically used in such cases, where traditional key distribution schemes are not believed to offer enough guarantee. This scenario has the advantage of not being intrinsically distance limited, and despite long travel times the transfer rate can be high due to the availability of large capacity portable storage devices. The significant difference of quantum key distribution is the ability to detect any interception of the key because with courier the key security cannot be proven or tested. QKD (Quantum Key Distribution) systems also have the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network. QKD also is trusted to protect the information that been sent and received. This criteria is particular important in banking and defense.

Factors preventing full adoption of quantum key distribution outside high security areas include the cost of equipment and the lack of a demonstrated threat to existing key exchange protocols.

5. CONCLUSION

As a contribution in this paper, we present the in depth summary of security aspects in cloud computing. Then we narrow down and found that part of security that is very important is process validation that bring to authentication. There are many classical methods being used in cloud computing authentication. Besides that, there still a need for us to perform an extensive research study in order to find a new discoveries and innovation to overcome such issue in security aspects. The comparison with several schemes bring to the main issue that motivates us to find the best scheme to enhance the security level of authentication mechanism in cloud environment.

From the study, we found an interesting mechanism that relate with quantum theory that involve small particles. It is called quantum key distribution protocol. The main idea of presenting the quantum key distribution protocol in multi-party for a dedicated platform such as cloud is to provide a safe platform for establishing a communication between more than two parties. Therefore, in order to minimize damages or losses due to security threats, a reliable and robust key distribution protocol and communication channel is very much in demand. However, further work is requiring proposing a new framework.

6. FUTURE WORK

In near future, the focus mainly goes to the key size to minimize the damages due to security threat. Several scheme and protocol will get tested, and the result will be compared for us pick up the best protocol in our authentication framework. Our focus is in adopting quantum cryptography protocol.

ACKNOWLEDGEMENT(s)

We would like to thank everybody who involved in this research and for all the comments that greatly improved the manuscript. This research sponsored

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by Malaysian, Ministry Of Education under fundamental research grant.

REFRENCES:

[1] S. Pearson, "Privacy, Security and Trust in Cloud Computing," *Priv. Secur. Cloud Comput.*, pp. 3–42, 2013.

[2] S. Ziyad and A. Kannammal, "Computational Intelligence, Cyber Security and Computational Models," vol. 246, pp. 395–403, 2014.

[3] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[4] A. S. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model," *2011 5th Int. Conf. Netw. Syst. Secur.*, pp. 113–120, Sep. 2011.

[5] S. Roy, A. K. Das, and Y. Li, "Cryptanalysis and security enhancement of an advanced authentication scheme using smart cards, and a key agreement scheme for two-party communication," *30th IEEE Int. Perform. Comput. Commun. Conf.*, pp. 1–7, Nov. 2011.

[6] W. Xie, L. Xie, C. Zhang, Q. Zhang, and C. Tang, "Cloud-based RFID authentication," in *2013 IEEE International Conference on RFID (RFID)*, 2013, pp. 168–175.

[7] Z. Hao, S. Zhong, and N. Yu, "A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing," *Int. J. Comput. Commun. Control*, vol. 6, pp. 227–235, 2011.

[8] A. ALDEEN and Y. ABDUL, "STATE OF THE ART SURVEY ON SECURITY ISSUE IN CLOUD COMPUTING ARCHITECTURES, APPROACHES AND METHODS.," ... *Theor.* ..., vol. 75, no. 1, 2015.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–9.

[10] H. Tyagi and S. Watanabe, "A Bound For Multiparty Secret Key Agreement And Implications For A Problem Of Secure Computing," in *Advances in Cryptology--EUROCRYPT 2014*, 2014, pp. 369–386.

[11] R. Chow, M. Jakobsson, U. C. Davis, and E. Shi, "Authentication in the Clouds : A Framework and its Application To Mobile Users," *ACM*, pp. 1–6, 2010.

[12] N. M. Gonzalez, M. A. T. Rojas, M. V. M. da Silva, F. Redigolo, T. C. M. D. B. Carvalho, C. C. Miers, M. Naslund, and A. S. Ahmed, "A Framework for Authentication and Authorization Credentials in Cloud Computing," *2013 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun.*, pp. 509–516, Jul. 2013.

[13] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, no. 973, pp. 647–651, Mar. 2012.

[14] H. Chang and E. Choi, "User Authentication in Cloud Computing," in *Ubiquitous Computing and Multimedia Applications*, Springer, 2011, pp. 338–342.

[15] C. Tang and D. O. Wu, "Mobile privacy in wireless networks-revisited," *Wirel. Commun. IEEE Trans.*, vol. 7, no. 3, pp. 1035–1042, 2008.

[16] R. Petrlic and C. Sorge, "Privacy-preserving DRM for cloud computing," in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012, pp. 1286–1291.

[17] T.-H. Chen, H. Yeh, and W.-K. Shih, "An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing," in *Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on*, 2011, pp. 155–159.

[18] J.-H. Yang and C.-C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," *Comput. & Secur.*, vol. 28, no. 3, pp. 138–143, 2009.

[19] Z. Zhi-hua, L. Jian-jun, J. Wei, Z. Yong, and G. Bei, "An new anonymous authentication scheme for cloud computing," in *Computer Science & Education (ICCSE), 2012 7th International Conference on*, 2012, pp. 896–898.

[20] D. Wang, Y. Mei, C. Ma, and Z. Cui, "Comments on an advanced dynamic ID-based authentication scheme for cloud computing," in *Web Information Systems and Mining*, Springer, 2012, pp. 246–253.

[21] C. Xu, X. He, and D. Abraha-Weldemariam, "Cryptanalysis of Wang's

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

auditing protocol for data storage security in cloud computing," in *Information Computing and Applications*, Springer, 2012, pp. 422–428.

[22] L. Kang and X. Zhang, "Identity-based authentication in cloud storage sharing," in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 2010, pp. 851–855.

[23] F. Bao and R. Deng, "Privacy protection for transactions of digital goods," in *Information and communications security*, Springer, 2001, pp. 202–213.

[24] R. Mishra, "Anonymous Remote User Authentication and Key Agreement for Cloud Computing," in *Proceedings of the Third International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing 258*, 2014, vol. 258, pp. 899–913.

[25] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT 2003*, Springer, 2003, pp. 452–473.

[26] B. Furht, "Handbook of Cloud Computing," in *Handbook of Cloud Computing*, B. Furht and A. Escalante, Eds. Boston, MA: Springer US, 2010, pp. 3–19.

[27] M. Vuyyuru and P. Annapurna, "An overview of cloud computing technology," *Int. J. Soft Comput. Eng.*, vol. 2, no. 3, pp. 244–246, 2012.

[28] P. Mell and T. Grance, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standarts and Technology," *Natl. Inst. Stand. Technol. US ...*, 2011.

[29] K. Scarfone and P. Hoffman, "Guide to Security for Full Virtualization Technologies Recommendations of the National Institute of Standards and Technology," *NISt*, 2011.

[30] C. C. V, "Security Guidance Critical Areas of Focus for," no. December, pp. 1–76, 2009.

[31] D. a. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey," *Int. J. Inf. Secur.*, vol. 13, no. 2, pp. 113–170, Sep. 2013.

[32] S. Sundareswaran, "Ensuring distributed accountability for data sharing in the cloud," *Dependable Secur. ...*, vol. 9, no. 4, pp. 556–568, 2012.

[33] S. A. Zargari and A. Smith, "Policing as a service in the cloud," in *Proceedings - 4th International Conference on Emerging Intelligent Data and Web Technologies, EIDWT 2013*, 2013, pp. 589–596.

[34] S. Haider, "Security Threats in Cloud Computing," no. December, pp. 11–14, 2011.

[35] A. Baldwin, D. Pym, and S. Shiu, "Enterprise information risk management: Dealing with cloud computing," *Priv. Secur. Cloud Comput.*, 2013.

[36] C. Jinyin and Y. Dongyong, "Data Security Strategy Based on Artificial Immune Algorithm for Cloud Computing," *Appl. Math*, vol. 153, no. 1, pp. 149–153, 2013.

[37] F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl, and N. Clarke, "Validating Cloud Infrastructure Changes by Cloud Audits," *2012 IEEE Eighth World Congr. Serv.*, pp. 377–384, Jun. 2012.

[38] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," *Netw. Secur.*, vol. 2011, no. 3, pp. 4–10, Mar. 2011.

[39] D. Mishra, V. Kumar, and S. Mukhopadhyay, "A Pairing-Free Identity Based Authentication Framework for Cloud Computing," *Netw. Syst. Secur.*, pp. 721–727, 2013.

[40] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," *2011 IEEE Asia-Pacific Serv. Comput. Conf.*, pp. 110–115, Dec. 2011.

[41] H. Dinesha and V. Agrawal, "Multi-level authentication technique for accessing cloud services," in *Computing, Communication and Applications (ICCCA), 2012 International Conference on*, 2012, pp. 1–4.

[42] X. Li, W. Li, and D. Shi, "Enterprise private cloud file encryption system based on tripartite secret key protocol," no. Iiicec, pp. 166–169, 2015.

[43] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, 1981.

[44] J. Shen, C. Lin, and M. Hwang, "Using Smart Cards," *IEEE Trans. Consum. Electron.*, pp. 1–4, 2003.

[45] C. Yang, H. Yang, and R. Wang, "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards,"

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IEEE Trans. Consum. Electron., vol. 50, no. 2, pp. 578–579, May 2004.

[46] E. Yoon, E. Ryu, and K. Yoo, "Efficient remote user authentication scheme based on generalized elgamal signature scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 568–570, May 2004.

[47] M. Hwang, "Cryptanalysis of a remote login authentication scheme ૪," *Comput. Commun.*, vol. 22, pp. 742–744, 1999.

[48] M. Hwang, C. Lee, and Y. Tang, "An Improvement of SPLICE/AS in WIDE against Guessing Attack.," *Informatica, Lith. Acad. Sci.*, vol. 12, no. 2, pp. 297–302, 2001.

[49] V. Shoup and A. Rubin, "Session Key Distribution Using Smart Cards 1 Introduction," *Springer-Verlag*, pp. 1–11, 1996.

[50] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably secure authenticated group Diffie-Hellman key exchange," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 3, p. 10–es, Jul. 2007.

[51] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, Jun. 2006.

[52] S. Lee, T. Y. Kim, and H. Lee, "Future Information Communication Technology and Applications," vol. 235, pp. 149–157, 2013.

[53] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[54] H. Lo and N. Lütkenhaus, "Quantum cryptography: from theory to practice," *arXiv Prepr. quant-ph/0702202*, 2007.

[55] L. Decastro, "Fundamentals of natural computing: an overview," *Phys. Life Rev.*, vol. 4, no. 1, pp. 1–36, Mar. 2007.

[56] H. Yuan, J. Zhou, G. Zhang, H. Yang, and L. Xing, "Efficient Multiparty Quantum Secret Sharing of Secure Direct Communication Based on Bell States and Continuous Variable Operations," *Int. J. Theor. Phys.*, vol. 51, no. 11, pp. 3443–3451, Jun. 2012.

[57] R. Matsumoto, "Quantum multiparty key distribution protocol without use of entanglement," *arXiv Prepr. arXiv0708.0902*, pp. 1–8, 2007.

[58] R. Khalid and Z. A. Zukarnain, "Multi-Party System Authentication for Cloud Infrastructure by Implementing QKD," in *2 nd Asia-Pacific Conference on Computer Aided System Engineering--APCASE 2014*.

[59] D. Ljunggren, M. Bourennane, and A. Karlsson, "Authority-based user authentication in quantum key distribution," *Phys. Rev. A*, vol. 62, no. 2, p. 22305, 2000.

[60] G. Zeng and W. Zhang, "Identity verification in quantum key distribution," *Phys. Rev. A*, vol. 61, no. 2, p. 22303, 2000.

[61] C. Anghel, "Base Selection and Transmission Synchronization Algorithm in Quantum Cryptography," *arXiv Prepr. arXiv0909.1315*, pp. 5–8, 2009.

[62] R. Sharma and A. De, "A new secure model for quantum key distribution protocol," ... *Inf. Syst. (ICIIS), 2011 6th ...*, vol. 1984, pp. 462–466, 2011.

[63] L. Gyongyosi and S. Imre, "Information geometric security analysis of differential phaseâ€ shift quantum key distribution protocol," *Secur. Commun. Networks*, 2012.

[64] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A*, vol. 59, no. 1, pp. 162–168, Jan. 1999.