ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

A COMPARATIVE REVIEW OF QUANTUM CRYPTOGRAPHY AND NEURAL CRYPTOGRAPHY

Adith M
adithmeyana200@gmail.com

Aditya V S
adityavsreenivas10@gmial.com

Ankith Shetty
ankushetty7@gmail.com

Akshay M
akshaymendon51@gmail.com

Chandra naik
chandranaik@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY, MIJAR MOODBIRDE

ABSTRACT- It should go without saying that security risks rise in tandem with data volume. We've looked at the encryption strategies used to counter these new security risks. Moreover, it has been observed that neural and quantum cryptography are the primary fields in which encryption techniques are used. The benefits and drawbacks of these two state-of-the-art cryptography techniques are discussed. The goal of this work is to address big data security and privacy issues by utilizing Neural and Quantum Cryptography approaches, particularly when their applicability is called into doubt.

Keywords-*Big data security, neural cryptography, quantum cryptography, and cryptography*

I. INTRODUCTION

The exponential growth of big data in today's society has been made possible by significant technological advancements, which have also altered the view of big data authority. The concept of big data has gained even more significance with the increasing use of Internet of Things devices and the noticeable rise in Internet traffic. Large-scale data collection requires robust security measures for networks, infrastructure, and data privacy because cyber security threats and attacks are expanding quickly to keep up with the growth of big data. As seen in the documentary The Great Hack, which Karim Amer and Jehane Noujaim recorded, safeguarding data and using it to reach rational conclusions is one of the most crucial concerns of the current era. Among the most crucial requirements Currently, there are worries about how big data firms should monitor their compliance with security protocols and how They respect the privacy of personal information. According to Bhatia and Sood's Security of Big Data: A Review, big data poses a risk even in the absence of technological components due to the difficulties in managing it securely [1]. But as Mandek D. and colleagues point out in their study Security Analytics in the Big Data Era [2], many popular information security approaches, such as behavior analysis and "anomaly detection," depend on dubious detection techniques.

Even with massive data quantities, techniques for behavioral analysis and anomaly detection can nevertheless generate a status warning when applied to several systems that are under the jurisdiction of data security [3, 4]. A technique for ascertaining potential hazards is conducting behavioral research. However, it only allows for their examination and research, not their preservation [5]. The two potent progeny that arise from the gradual evolution of encryption techniques to offer security in Big Data are neural and quantum cryptography. Brain cryptography makes use of artificial neural networks and cryptography techniques, whereas quantum cryptography relies on Heisenberg's uncertainty theory and the photon polarization principle The main objective of this paper is to discuss the advantages and disadvantages of neural and quantum cryptography techniques. since some of the most important encryption solutions for large-

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

scale data security are now provided by these two techniques [6, 7], to do this, we separated the flow into three main pieces. A quick description of neural cryptography follows that. A brief introduction to quantum cryptography is given in the second section, and a comparison of the advantages and disadvantages of neural and quantum encryption is covered in the following section. This brings this document to an end.

II. NEURAL CRYPTOGRAPHY

In Virtualization and Big Data Security Measures, According to Bahulikar, cloud infrastructure contributes to the growing prevalence of big data stacks as internet traffic rises. they are growing in response to the increase in the number of one-on-one internet interactions. The biggest problem facing the cyber security sector right now is finding a haven for the massive volumes of data that need to be kept on file [3]. Thus, we begin this effort by introducing the Neural Cryptography security approach, which examines infrastructure, cloud, and virtualization security. An understanding of brain impulse conduction theory is necessary to comprehend brain cryptography. Artificial neural networks (ANNNs) are a form of machine learning system that classify outputs by constructing a mathematical connection between a variety of inputs and their corresponding outputs, much like brain cells do [8, 9, 10]. In "Security of Big Data: A Review," Bhatia and Sood talk about big data as a threat to data collection, curation & analysis, and visualization in several business scenarios, instead of just concentrating on technology. They also discuss the difficulties posed by big data, including the need for secure large-volume data management, access control, and real-time big data monitoring, among other things. The author believes that a workable substitute is provided by machine learning assessments and upgrades, which are now feasible due to recent developments. Big data is becoming more and more essential, which makes more targets vulnerable to hacker attacks. Machine learning, according to the authors, can be utilized to find hidden patterns and safe solutions [1]. Neural cryptography finally takes the stage. Neural cryptography is described as a multi-layered system in "Use of Neural Networks in Cryptography" by Hadke and Kale. Data from the first layer is synaptically sent to the second layer, which applies "weights" factors to alter the information being examined, and then to the third layer[11, 12]. The three steps of this cryptography technology are activation, learning, and connection. Furthermore, the authors [11, 13] state that a variety of intricate multi-input and multi-directional feedback loops are used in the construction of an autonomous neural cryptography system. The authors assert that neural cryptography is well-known for its robust network security because of its three-step encryption process and challenging-to-crack keys. Activation, learning, and connection are a few of these [4]. Correlation links are formed between neurons as they synapse. When managing the data for assessment during the learning process, the saved settings are changed. The output resulting from the modified inputs is provided during the activation process. As neurons synapse, correlation linkages are created between them. The saved settings are modified during the management of the data for assessment during the learning process. Throughout the activation process, the output that comes from the altered inputs is given. Thus, examining these phases yields integrative, inductive responses to the main assertion [14, 15, 16]. Numerous encryption methods are compatible with neural cryptography. They are very helpful for producing secret keys because it is almost impossible to crack them without the neuron-network map of the key. This figure[1] shows the encryption and decryption of the voice using neural cryptography.

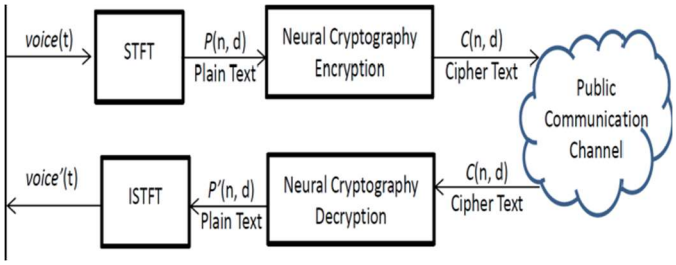

Fig [1] Neural cryptographic representation of Voice

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

III.IMPLEMENTATION OF QUANTUM CRYPTOGRAPHY

Neural networks were used by Sebastien Dourlens in 1995 for DES cryptanalysis. He was the one who taught the networks how to flip the DES S-tables. Adi Shamir's work on Differential Cryptanalysis sheds light on DES bias. The experiment suggests that more than half of the key's components may be discovered, which speeds up the search for the complete key. The ease of constructing multilayer neural networks in hardware has led to the proposal of numerous hardware applications for microcontrollers.

Safety and violations of this procedure

Attackers E are always assumed to be able to listen in on communications between parties A and B without having the ability to alter them.

Brute force

A brute force attack requires the attacker to try every key (all weight values that may be assigned to wij). In turn, this generates (2L+1)KN possibilities at the boundary of weights L, K×N input neurons, and K hidden neurons. For instance, when K = 3, L = 3, and N = 100 are coupled, 3*10253 key possibilities cannot be achieved given the capability of existing computers.

Using one's own tree parity machine for learning

One of the basic attacks can be launched by anyone sharing the same tree parity machine as parties A and B. Between these two people and his tree parity device, he wants everything to be in perfect harmony. For every stage, there are three possible outcomes:

1. Output (A) ≠ Output (B): The weights are not updated by any party.
2. The formula output(A) = output(B) = output(E) illustrates how the three parties update the weights in their tree parity machines.
3. Output(A) = Output(B) ≠ Output(E): The attacker cannot update the tree parity machines of Parties A and B. This circumstance causes him to learn more slowly than parties A and B are synchronizing.

It has been demonstrated that synchronizing two parties happens more quickly than an attacker discovering their whereabouts. It can be made better by raising the neural network's synaptic depth L. This provides adequate security for this protocol, making it unlikely that an attacker will discover the key.

Other attacks

We could improve the security of the protocol for conventional cryptography systems by raising the key. Increasing the neural network's synaptic depth L can improve neural cryptography. Changing this number causes the cost of a successful attack to climb exponentially, although user effort increases polynomially. For this reason, security flaws related to neural key exchange are categorized as belonging to complexity class NP.

Three key strategies—geometry, genetic algorithms, and probability analysis—are proposed by Adi Shamir, Anton Mityaguine, and Alexander Klimov to undermine the original brain synchronization technique. Despite the limitations of this particular implementation, the principles behind chaotic synchronization may eventually lead to a secure solution.[27]

IV. QUANTUM CRYPTOGRAPHY

The most well-known use of quantum cryptography is in research because it provides 100% security and is based on the ideas of entanglement and supervision. Several quantum key distribution protocols, including COW, BB84, and BB92, were reviewed and assessed in Singh et al.'s paper "Quantum Key Distribution Protocols: A Review" [5]. Heisenberg's Uncertainty Principle, photon polarization, and entanglement form the foundation of quantum cryptography. However, certain noteworthy distribution schemes in particular make use of these tangible concepts

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

[5,17]. For example, the BB84 protocol has four polarization states, whereas the BB92 protocol only has two, according to Heisenberg's Uncertainty Principle. They also go into the privacy and security issues with quantum cryptography. The authors claim that maintaining secrecy is mostly dependent on the QKD's capacity to generate new, random keys frequently. However, because the keys were changing often, only a small portion of the data could be decoded [5,18]. In 1984, the Quantum Key Distribution Protocol (QKD), also known as the BB84 protocol, was developed based on Heisenberg's Uncertainty Principle, photon polarization, and entanglement [19].In Amellal H., Meslouhi A., and El Allati A.'s study Secure Big Data Using QKD Protocols, they evaluate the usefulness of quantum information theory for large data by contrasting the outcomes with those of classical procedures [6]. The BB84 protocol stops the attacker from employing or replicating the non-cloning, entanglement, and superposition ideas. would result in a malfunctioning database [6]. As a result, they assert that transmitting qubits via a quantum channel and utilizing the Grover algorithm to investigate NoSQL databases in a quantum environment are two ways to

accomplish massive data security. German physicist Weiner Heisenberg claimed that since one particle's precision must decrease while another's increases, it is impossible to know certain physical properties simultaneously with absolute certainty. According to Singh and colleagues' article "Quantum Key Distribution: A Review" [5], the Uncertainty Principle also implies that it is challenging to observe a quantum state since the system can collapse.

Big Data Security Issues Based on Quantum Cryptography and Privacy with Authentication for Mobile Data Center [7] authors Thayananthan, V., and Albeshri, A. state that "Quantum cryptography derives from Grover's Algorithm is a necessity." Improving security and privacy in mobile data centers is their main objective. They argue that PairHood is still the best available protocol until light-based quantum cryptography solutions are found. For three key reasons, they are relevant to our circumstances [18, 19]. Above all, a mobile data center with specific security is required in every situation. The second is quantum cryptography's ability to generate strong keys. Thirdly, sensitive data can be handled more easily with the Pairhood protocol [7], which conceals information from prying eyes and even authorized personnel operating in the data center. A variety of filters can be used to alter the direction of the unpolarized light. In QKD, the electromagnetic wave's orientation is managed by the use of vertical and horizontal filters, commonly referred to as "bases" Using the BB84 protocol, messages can be delivered via photon transmission or traditional data transfer. The sender of a photon transmission uses a preconditioned sequence to ascertain the assertions of the photons. To ascertain the bases, the receiver concurrently prepares a second sequence of the same length. Figure [1] shows the representation of quantum cryptography

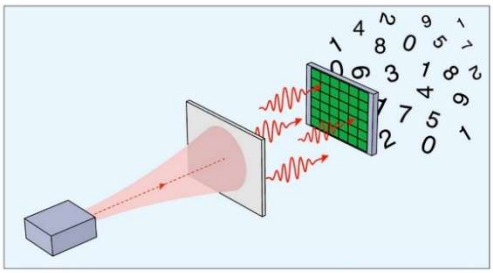

Figure [1] Representation of quantum cryptography

to quantify photons. The most crucial aspect of this transmission is the need to transmit two entangled signals. As an illustration, consider the two photons, A and B. The entangled principle prevents photons A and B from being characterized independently since they are qualitatively mixed (and vice versa). To keep communication from breaking down, two communications must be read at the same time as they arrive. If you are not traveling at the speed of light, it is also difficult to block the photon transmission message so that the message itself cannot be read. In this way, the data is safely encrypted during transmission and protected against several threats [18, 20]. These characteristics have made quantum cryptography a hot area for research right now, and it's expected that additional scientific advancements will be made possible by it in the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

future. It is a common misconception that today's technological breakthroughs can meet every requirement, even though there are still a lot of prospects for success and progress in this industry.

V.IMPLEMENTATION OF QUANTUM CRYPTOGRAPHY

Quantum cryptography has the potential to improve information security greatly. However, no cryptographic method can ever be 100% secure.[22] Because quantum cryptography relies on several important presumptions, it can only be considered conditionally safe.[23]

supposition of a single photon source

Single-photon source applications are based on the concept of quantum key distribution. Most real-world quantum cryptography systems use weak laser sources for information transport since they are hard to create. Photon-splitting assaults, which are eavesdropping attacks, are possible with these multi-photon systems. [23].Eve divides the multi-photon source in two, keeping one for herself so she can listen in on talks.[24] Subsequently, Bob is given the remaining photons without any measurement or evidence that Eve repeated the data.[24] Researchers think they can maintain security when employing a multi-photon source by making use of decoy states that indicate the presence of a spy.[24] Nonetheless, researchers created a nearly flawless single-photon source in 2016 and believe more might be

Same detector efficiency presumption

In actuality, quantum key distribution systems require two single-photon detectors: one for Alice and one for Bob. These photodetectors can identify an incoming photon in a matter of nanoseconds thanks to calibration. [23].[25] The matched detection windows of the two detectors will diverge to some extent due to manufacturing differences.[25] Using Alice's qubit measurement, Bob can ascertain the detector's inefficiency and persuade Eve, the eavesdropper, to offer a "fake state".[25] Eve makes a new photon to send to Bob after first capturing the one Alice sent.[25] Eve tinkers with the phase and timing of the "faked" photon to make Bob believe that nobody is listening in.[25] Eliminating this vulnerability requires removing differences in photodetector efficiency, which is difficult to do because of minute manufacturing tolerances that cause variations in wire lengths, optical path lengths, and other faults.[25]

Governmental institutions are continuing the distribution of quantum keys.

Many governmental organizations advise against using quantum key distribution in Favor of post-quantum cryptography, sometimes referred to as quantum-resistant encryption, due to practical difficulties. Post-quantum cryptography has been advocated by numerous agencies, including the National Cyber Security Centre of the United Kingdom (NCC), the German Federal Office for Information Security (BSI), the French Secretariat for Defense and Security (ANSSI), and the US National Security Agency.

For example, the US National Security Agency covers the following five topics: [26]

1. There are other approaches to solving the problem besides the distribution of quantum keys. QKD is used to create keying material for systems that use concealed encryption. As long as one obtains the cryptographic guarantee that the first QKD transmission originated from the acknowledged entity, these keying materials can also be used in symmetric key cryptography techniques to provide integrity and authentication (entity source authentication). The source of the QKD communication cannot be confirmed with QKD. Thus, pre-placed keys or asymmetric cryptography are needed for source authentication. Furthermore, QKD's secrecy services can be obtained using quantum-resistant cryptography, which is typically less costly and has a more defined risk profile.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

2. Hardware specific to quantum key distribution is required. Physical attributes are the basis of QKD, and distinct physical layer communications ensure its security. This implies that either user will need to physically run free-space transmitters or lease dedicated fiber connections. It is difficult to integrate into the network equipment that is currently in use, and it cannot be implemented in software or as a network service. QKD's hardware base limits its capacity to apply security updates and upgrades.

3. Insider threat concerns are heightened by quantum key distribution, which also drives up infrastructure costs. Reliable relays are typically needed for QKD networks, which drives up the cost of secure facilities and increases the risk of insider threats. As a result, many of the possible applications are eliminated.

4. Validating and safeguarding the quantum key distribution is one of the primary responsibilities. Rather than offering the theoretical ultimate security from the rules of physics (as modeled and sometimes provided), a QKD system provides a more restricted level of security that can be reached through hardware and technical solutions. Validation is particularly difficult, though, because cryptographic security has orders of magnitude less error tolerance than physical engineering scenarios. Several thoroughly investigated attacks against commercial QKD systems have been connected to vulnerabilities in the specific hardware used in QKD.
5. The risk of denial of service is increased by quantum key distribution. Denial of service attacks poses a serious danger to the corporation because QKD's security claims are vulnerable to interception.

VI. ADVANTAGE & DISADVANTAGES OF NEURAL & QUANTUM CRYPTOGRAPHY

According to Sergio and colleagues' study Security and Privacy of Big Data for Social Networking Services in Cloud, big data is playing an increasingly essential role in wireless communication because of social networks' fast growth and the sensitive content they contain[8]. Their results show a substantial correlation between the volume, velocity, and variety of big data and data concealment. Therefore, protecting the privacy of massive amounts of data becomes even more crucial at this stage. For increasingly complex encryption algorithms, the techniques of neural and quantum cryptography are examined and discussed in this table. This was selected after a careful evaluation of the advantages and disadvantages of neural & quantum cryptography solutions [11, 21].

Multi-location operation is currently one of the two most used encryption methods. The use of neural and quantum cryptography is growing in popularity. Compared to its competitors, quantum cryptography offers significantly superior security because it is based on quantum physics. The most widely used technique, "Quantum Key Distribution" (QKD), allows users to access sensitive data without encrypting it. Quantum cryptography uses encrypted Fiber networks to enable secure communication.

Photons in these networks, which are in are provided to distinguish between the binary and zero qubits until the key is generated and cracked. The major barrier to this technology's widespread application is the photon's more than 100-kilometer fiber optic cable transmission range. However since these systems need very secure connections, several major institutions, particularly in the UK, have already started using quantum cryptology for message transmission. Despite the great level of security offered by quantum cryptography, Niemiec points out that the paper "Error Correction in Quantum Cryptography Based on Artificial Neural Networks"[9] has a few small security issues. This is the motivation behind the development of cutting-edge quantum cryptography methods such as neural networks.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

Table 1: Basic Advantages and Disadvantages of Quantum and Neurological Cryptography Techniques [11]

	Neural Cryptography	Quantum Cryptography
Advantages	Any arbitrary secret code. The message that has to be communicated is less distorted thanks to the secret key, which is challenging to decipher.	any arbitrary secret code Elevated security: ensures that persona non-grants did not read or change the communication.
Disadvantages	If the problem isn't with the weight or network design, knowing the key by itself won't help with the encryption or decryption procedure.	There's no quantum channel present. High-bit mistakes only happen in tiny spaces and happen often.

VII. CONCLUSION

This article discusses the characteristics, applications, benefits, and drawbacks of neural and quantum cryptography approaches, which are used to counter growing data quantities and security flaws. It is commonly known that existing encryption methods, such as behavior analysis and anomaly detection, are not well suited for real-world situations involving substantial data security. It is necessary to create new security scenarios in the wide realm of data privacy. This is why the goal of the project is to introduce neural and quantum cryptography, two state-of-the-art techniques for big data security. Neural cryptography established a mathematical relationship between the inputs and outputs using weights

and a structure modeled like brain cells. Nevertheless, many scientists believe that quantum cryptography is now the finest encryption technique available. Heisenber's theory of uncertainty, photon polarization, and fiber optic technology enable continuous communication. While all cryptographic techniques are incredibly safe, there are two primary distinctions: in quantum cryptography, the workspace is constrained, while in neural cryptography, the secret key is encrypted and subsequently decoded. Variations in data security and quality have been explored about big data's huge volume, diversity, and replication speed. If quality control mechanisms are not put in place, big data will quickly become irrelevant, which will have a significant impact on policy and decision-making processes. To preserve data quality, we therefore investigate data security using neural and quantum cryptography. Although both methods are recognized for secure and reliable communication, it appears that implementing quantum cryptography will be challenging shortly using neural and quantum cryptography. Although both methods are recognized for secure and reliable communication, it appears that implementing quantum cryptography will be challenging shortly

REFERENCES

[1] R. Bhatia and M. Sood, “Security of Big Data: A Review”, IEEE, 2018, pp.182-186.

[2] D.Mondek, R.B. Blazek, T. Zahradnicky, “Security Analytics in Big Data Era”, IEEE, 2017,pp.605-606.

[3] S. Bahulikar, “Security Measures for Big Data, Virtualization and the threat mobile Infrastructure”, IEEE,2014.

[4] P. P. Hadke and S.G.Kale, “Use of Neural Networks in Cryptography: A Review”, 2016, World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16)

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

[5] H. Singh, D.L.Gupta, A.K.Singh, "Quantum Key Distribution Protocols: A Review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 01-09

[6] H.Amellal, A.Meslouhi, A. Allati, "Secure Big Data Using QKD Protocols", 2018, Second International Conference on Intelligence Computing in Data Science, Procedia Computer Science 148, 21-29.

[7] V.Thayananthan and A.Albeshiri, "Big data security issues based on quantum cryptography and privacy with authentication for mobile data center", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), pp.149-156.

[8] C.Stergiou, A.P.Plageras, K.E.Psannis, T.Xifilidis, B.B.Gupta, "Security of Privacy of Big Data for Social Networking Services in Cloud", IEEE, 2018,pp.438-442.

[9] M. Niemiec, "Error Correction in Quantum Cryptography Based on Artificial Neural Networks",IEEE,2018 pp. 174-192.

[10] M.Talha, A.A. El Kalam, N.Elmarzouqui, "Big Data: Trade- of between Data Quality and Data Security", The 9th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS) April 29 – May 2, 2019, Leuven, Belgium pp.916-922.

[11] D. Sharma and A. Sharma, "Big Data Protection via Neural and Quantum Cryptography", IEEE, 2018, pp.3701-3704.

[12] C. Dinçer, G. Akpolat, E. Zeydan, "Mobil Operatörler Tarafndan Servis Edilen Büyük Veri Uygulamalarnda Güvenlik Sorunlar ", IEEE, 2018.

[13] A.K.Bishwas, A.Mani and V.Palade, "Quantum Supervised Clustering Algorithm for Big Data", 2018, 3rd International Conference for Convergence in Technology (I2CT) The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Apr 06-08, 2018 pp.1-5.

[14] D.Lv, S.Zhu, H.Xu, R.Liu, "A Review of Big Data Security and Privacy Protection Technology", IEEE, 2018, pp.1082-1091.

[15]D.S.Terzi,R.Terzi and S.Sagiroglu, "A Survey of Security and Privacy in Big Data",IEEE, 2018, pp.202-207.

[16] T.Schmidt, H.Rahmana, A.Sadeghian, "A Review of Applications of Artificial Neural Networks in Cryptosystems", IEEE, 2008.

[17] N.Chaudhari, Dr.S.Srivastava, "Big Data Security Issues and Challenges",IEEE, 2016, pp.60-64.

[18] N.Moustafa," A Systemic IoT-Fog-Cloud Architecture for Data Analytics and Cyber Security Systems: A Review of Fog Computing",

[19] N.Srivastava and U.C.Jaiswal, "Big Data Analytics Technique in Cyber Security: A Review",IEEE,2019, pp.579 585.

[20]K-K R. Choo, M.Conti, A.Deghhantanha,"Special Issue on Big Data Application in Cyber Security and Threat Intelligence, Part-1",IEEE,2019, pp.279-281.

[21] M.M. Mijwel, "Artificial Neural Networks Advantages and Disadvantages",2018,https://www.linkedin.com/pulse/artificial_neural-networks-advantages-disadvantages-maad-m-mijwel/

[22] Scarani, Valerio; Bechmann-Pasquinucci, Helle; Cerf, Nicolas J.; Dušek, Miloslav; Lütkenhaus, Norbert; Peev, Momtchil (29 September 2009). "The security of practical quantum key distribution". Reviews of Modern Physics. **81** (3): 1301–1350. arXiv:0802.4155. Bibcode:2009RvMP...81.1301S. doi:10.1103/revmodphys.81.1301. ISSN 0034-6861. S2CID 15873250.

[23] Jump up to:[a] [b] [c] Zhao, Yi (2009). Quantum cryptography in real-life applications: assumptions and security (PDF) (Thesis). Bibcode:2009PhDT.....94Z. S2CID 118227839. Archived from the original (PDF) on 28 February 2020.

[24] Jump up to:[a] [b] [c] [d] Lo, Hoi-Kwong (22 October 2005). "Decoy State Quantum Key

Distribution". Quantum Information Science. WORLD SCIENTIFIC. **94** (23): 143. arXiv:quant-ph/0411004. Bibcode:2005qis..conf..143L. doi:10.1142/9789812701633_0013. ISBN 978-981-256-460-3. PMID 16090452.

[25] Makarov, Vadim; Anisimov, Andrey; Skaar, Johannes (31 July 2008). "Erratum: Effects of detector efficiency mismatch on security of quantum cryptosystems [Phys. Rev. A74, 022313 (2006)]". Physical Review A. **78** (1): 019905. Bibcode:2008PhRvA..78a9905M. doi:10.1103/physreva.78.019905. ISSN 1050-2947.

[26] "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)". National Security Agency. Retrieved 16 July 2022. This article incorporates text from this source, which is in the public domain.

[27]Klimov, Alexander; Mityagin, Anton; Shamir, Adi (2002). "Analysis of Neural Cryptography" (PDF). *Advances in Cryptology*. ASIACRYPT 2002. LNCS. Vol. 2501. pp. 288–298. doi:10.1007/3-540-36178-2_18. ISSN 0302-9743. Retrieved 2017-11-15.

.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 10, Issue 5, May 2024

.