ENHANCING CLOUD SECURITY USING MACHINE LEARNING

Dr. Kaja Masthan
Associate Professor, Department of Computer Science and Engineering
Sphoorthy Engineering College

Dr. Mahammad Shabana
Associate Professor, Department of Computer Science & Engineering
Neil Gogte Institute of Technology, Hyderabad, India

Mohammed Rafi
Lecturer, Computer Science Department
Northern borders University, Arar, Kingdom of Saudi Arabia.

ABSTRACT

Cloud security is crucial for attracting customers who prioritize data security and privacy. Online attackers often disrupt the on-demand services offered by cloud providers, making security a top concern for cloud computing users. As a result, the financial growth of cloud-based organizations is steadily increasing. A major challenge in cloud security is identifying attack types and developing effective defences to protect cloud data. Various methodologies have been reviewed to determine robust security mechanisms against threats like DoS or DDoS attacks, malware, MITM attacks, and other vulnerabilities. However, these reviews reveal that machine learning alone is insufficient to fully protect cloud systems.

This research paper addresses these gaps by developing advanced security mechanisms that integrate machine learning with emerging technologies such as block chain and quantum computing. The integration of machine learning with advanced algorithms, including deep neural networks and quantum neural networks, aims to enhance prediction and protection accuracy. These proposed models not only aim to reduce attack levels significantly but also enhance user trust and support the financial growth of cloud service providers (CSPs).

The research paper contributions focus on resolving security issues and advocating for comprehensive end-to-end protection and privacy for data stored in cloud environments. By addressing data security and privacy concerns, this work demonstrates that cloud environments can become more secure and user-friendly.

Keywords*:* Cloud security, data privacy, data protection, online attackers, cloud computing, DoS attacks, DDoS attacks, block chain, quantum computing, deep neural networks, quantum neural networks, prediction accuracy.

I. INTRODUCTION

Cloud Computing has become a popular trend in the Information Technology (IT) business, serving as an advanced extension of traditional technologies [1]. It enables direct communication between users and service providers within a cloud environment, offering benefits such as centralized data access, automatic software updates, high availability, flexibility to scale services and infrastructure, cost savings, mobility, security measures for theft detection and prevention, and improved quality control [2]. Cloud services can be easily accessed from anywhere on-demand. A key emerging trend in IT management is "Distributed Computing," which enables dynamic changes in computing resources without concerns about account administration, location, or operating system. These resources are virtualized. The rise of pervasive technology has been driven by the integration of wired and wireless devices accessible anytime and anywhere. High-Performance Computing (HPC) is commonly represented by computer clusters, where a group of interconnected, homogeneous computers work together on a shared task, managed by an application [3]. These clusters function as a single system via fast local area networks, offering a cost-effective alternative to a single computing system [10].

A hybrid cloud combines private, community, and public cloud models, allowing businesses to save costs while enhancing agility. In this setup, public and private clouds collaborate seamlessly, ensuring smooth operation of data and applications [9]. For instance, a user may store sensitive data in a private cloud while utilizing a public cloud for data archiving [4]. This hybrid cloud model requires layer 2 network connectivity for Virtual Machine (VM) migration and supports multiple hypervisors and related infrastructure software [5]. Additionally, a Cloud Federation, or Federated Cloud, is a type of Inter cloud, where internal and external cloud providers willingly collaborate to share resources, driving significant business growth [11].

The rapid growth of the digital world relies on both structured and unstructured data for analytics [7]. In recent years, cloud computing services have increasingly focused on Artificial Intelligence (AI) and Machine Learning (ML), leveraging enhanced computing power and the development of more advanced learning algorithms [6]. Machine learning has made significant progress due to new learning theories, algorithms, the abundance of online data, and affordable processing

power. AI engineers have recognized that systems can be trained through examples to achieve desired input-output behavior, rather than programming them manually for various tasks [12]. Machine learning uses a variety of algorithms to learn patterns and adapt data training to specific needs. One effective approach is the Decision Tree algorithm, which splits data samples based on different conditions [8]. This non-parametric algorithm is commonly used in supervised learning and is particularly effective in solving classification and regression problems, making it a prediction-based model. Deep learning, a subset of AI, is considered the next revolution in machine learning. Its name stems from the multiple hidden layers within artificial neural networks [13]. Deep learning excels at transitioning from higher-level conceptual representations to more detailed ones, allowing for more refined data analysis [14].

Block chain is a widely recognized technology today for recording digital transactions using small blocks. While often associated with crypto currency, block chain's scope extends beyond that. It can be categorized into public, private, and consortium types. In a public block chain, anyone can initiate a transaction, add, or verify a block, and the data is accessible to everyone on the internet. In a private block chain, only authorized individuals can verify transactions or add blocks, making it popular among private organizations for specific purposes. In a consortium block chain, authorized individuals from different organizations can initiate, add, or verify transactions, with data visibility restricted to members within the consortium [15 to 18]. Quantum Neural Networks (QNN) merges concepts from Quantum Computing and Machine Learning. Quantum computers, known for their ability to perform tasks quickly, combined with Artificial Intelligence, are driving significant innovations today, addressing both every day and complex scientific problems [19]

II. Proposed Framework for Secured Cloud Computing

The security of cloud systems and services has been enhanced through various approaches utilizing machine learning, a subset of Artificial Intelligence. Additionally, contemporary technologies such as Block chain and Quantum Computing have been integrated into this research to provide an elevated level of security against diverse cyber-attacks, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, as well as malware and Man-in-the-Middle (MITM) attacks [19].

To achieve high-quality security outcomes, Deep Learning has emerged as a modern algorithm that emulates human decision-making by drawing on past experiences. An intelligent honeynet system has been developed to trap malicious attackers and identify DDoS attack patterns by employing a Deep Learning approach. Traditional honey net systems lack the intelligence to recognize cyber-attacks effectively [17]. In contrast, the intelligent honey net system deceives cyber-attackers into believing they are interacting with a genuine cloud system. If an attacker successfully breaches the proposed honey net system, it captures valuable information about the hacker and their methods. This information is then utilized by Deep Learning algorithms to alert the cloud system, enhancing its reliability and making it more user-friendly for cloud customers.

III. Proposed Algorithm

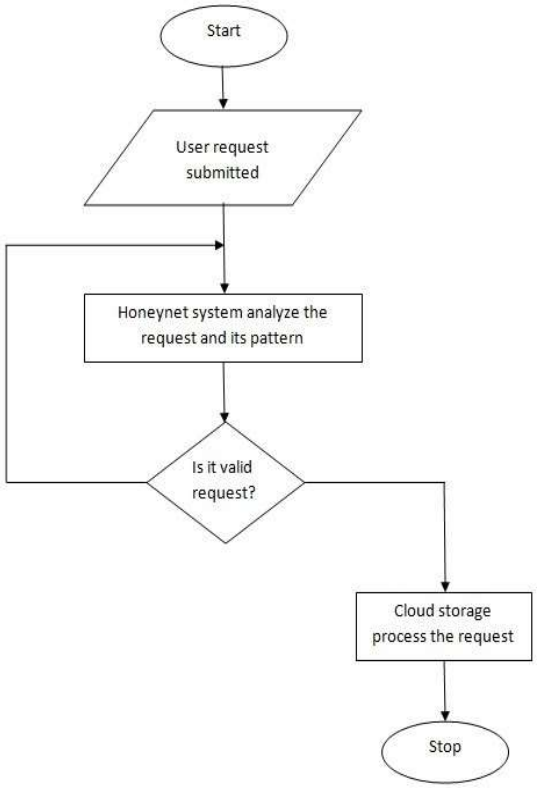


Fig. 1: Flowchart

The summary of the flowchart outlines the process of detecting and mitigating potential attacks in a cloud environment. When an attacker impersonates a legitimate cloud user with the intent to disrupt services for other users, they initiate a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack [15]. In response, the honey net system is triggered to monitor all requests from cloud users. These requests are directed to a decoy cloud system designed using the honey net trap concept. The secure honey net system evaluates whether the request is legitimate. If the request is deemed valid, trusted cloud users are allowed access to the on-demand services they have acquired. Conversely, if the request is suspicious, the attack patterns are logged by the Deep Neural Network for future analysis. The intelligent honey net system, leveraging Deep Learning techniques, can then take appropriate action against the attacker.

To facilitate this analysis, the intelligent system employs a Deep Neural Network, which gathers and analyzes various hacking patterns used by cyber-attackers. All identified patterns associated with DDoS attacks are recorded and preserved for future reference, as illustrated in Fig. 2

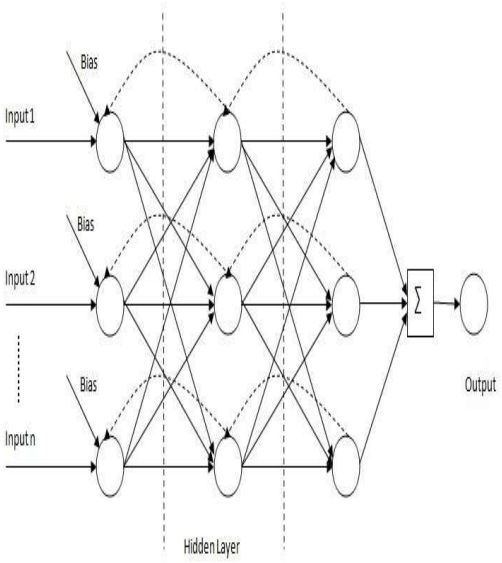
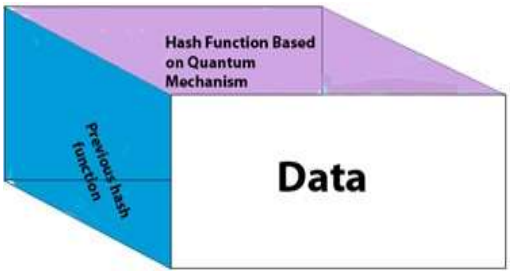


Fig. 2: Deep Neural Network for Intelligent Honey net system

IV. Cloud Security using Quantum-Block chain Technology

Cloud computing is a centralized technology, making it vulnerable to attacks as hackers can easily target the centralized system. With the rapid growth of cloud environments, the frequency of attacks is also increasing swiftly [11]. In contrast, block chain offers a distributed and decentralized ledger, which provides advanced security mechanisms to protect against data tampering, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, as well as Man-in-the-Middle (MITM) and malware attacks. Furthermore, quantum computing is recognized as an advanced computing paradigm that enhances security measures. By integrating these technologies- cloud computing, block chain, and quantum computing- a robust security framework can be established for cloud systems and services based on Quantum-Block chain technology [14]. This combination enhances the overall resilience of the cloud infrastructure. The Quantum superimposition principle will be employed to assess whether data has been tampered with, thereby ensuring data integrity and security.



(i) Proposed Approach

In this context, block chain consists of three key components: a block that represents data, a hash value that serves

as the digital signature, and the hash value of the preceding block. This advanced security mechanism relies on hash values based on the principles of quantum mechanics. Currently, data tampering poses a significant threat. To combat this issue, the superposition state of quantum mechanics is utilized to detect tampering within the blocks of the block chain. This technology presents a substantial advancement, serving as a superior alternative to traditional methods [13].

(ii) Proposed Framework

To enhance security at a higher level, existing block chain technology is integrated with quantum computing to safeguard outsourced data in cloud systems. Each block in the block chain is designed based on quantum mechanical principles and consists of data, a hash function, and the previous hash function, as illustrated in Fig. 3. This integration aims to provide a more robust security framework, leveraging the unique advantages of quantum mechanics to protect against data tampering and other cyber threats.

Fig. 3: A block of block chain based on quantum mechanism.

If an attacker attempts to tamper with the data, the superposition state of the hash function collapses, resulting in a representation of either black (denoted by 0) or white (denoted by 1). The next subsection of this research introduces an algorithm based on quantum mechanics principles. This algorithm processes large amounts of information utilizing the superposition behavior of quantum computing to enhance security effectively. Each point within the block is mapped to a corresponding superposition state, enabling the processing of vast datasets [16]. Furthermore, if data tampering occurs within the cloud environment, the superposition state will collapse, providing a clear indication of the breach.

V. Experimental Setup & Result

Various technologies, including Quantum Computing, Block chain, and Zero-Knowledge Proof techniques, have been integrated with Machine Learning to provide the highest quality of security for cloud server storage and services. The fundamental principles of machine learning, along with its subclasses such as Deep Learning and various neural networks like Deep Neural Networks and Quantum Neural Networks, have been utilized to bolster security measures against cyber-attacks, including Denial of Service (DoS),

Distributed Denial of Service (DDoS), malware attacks, and Man-in-the-Middle (MITM) attacks. This chapter explores the experimental setups of different approaches aimed at securing cloud systems and services to address existing research gaps. Additionally, the chapter presents the experimental results obtained from these investigations, highlighting their effectiveness in enhancing cloud security [12].

(i) Cloud System Security using Deep Learning

Deep Learning is a subclass of Machine Learning, which itself falls under the broader category of Artificial Intelligence technology [14]. Deep Learning enables computer systems to learn from previous experiences by leveraging stored knowledge to inform their actions. Pattern matching is a crucial aspect of Deep Learning, widely embraced by researchers and industry professionals across various domains, including text recognition, voice recognition, facial recognition, computer vision, and automated medical diagnosis. This list of applications continues to expand as researchers explore deeper concepts within Deep Learning, revealing new potential use cases and capabilities.

(ii) Experimental Setup

The security of the cloud system has been enhanced through the implementation of an intelligent honey net system. This honey net serves as a decoy, designed to attract hackers while the actual system remains secure elsewhere. For security analysis, the concept of a feed-forward Deep Neural Network (DNN) is illustrated in Fig. 28. The DNN operates through multiple hidden layers; the greater the number of hidden layers employed in the analysis, the more robust the security system becomes in defending against cyber-attacks. The hidden layers utilize activation functions such as Sigmoid and RELU (Rectified Linear Unit). To finalize the result processing, the Gradient Descent algorithm is employed within the machine learning framework. This algorithm continuously updates the parameters of the activation functions, ensuring the proposed model's effectiveness in providing security against potential threats.

(iii) Experimental Result

The experimental setup focuses on a Deep Neural Network (DNN) architecture that comprises multiple hidden layers. This proposed model is designed to defend against Distributed Denial of Service (DDoS) and Denial of Service (DoS) attacks, including malware and Man-in-the-Middle (MITM) threats, after undergoing comprehensive training phases. The dataset utilized for training adheres to the feed-forward DNN concept. As a result, the trained intelligent honey net system is capable of detecting and alerting against DDoS attacks when an attacker attempts to disrupt services within the cloud computing environment. Furthermore, the integrated Deep Learning framework captures detailed information about the attacker for future reference. To improve the system's response to cyber-attack scenarios within the cloud environment, the intelligent honey net system leverages the stored experiences and data collected by the DNN model to execute appropriate countermeasures. The experimental results of the intelligent honey net system in the cloud environment can be visualized in Fig. 4 below.

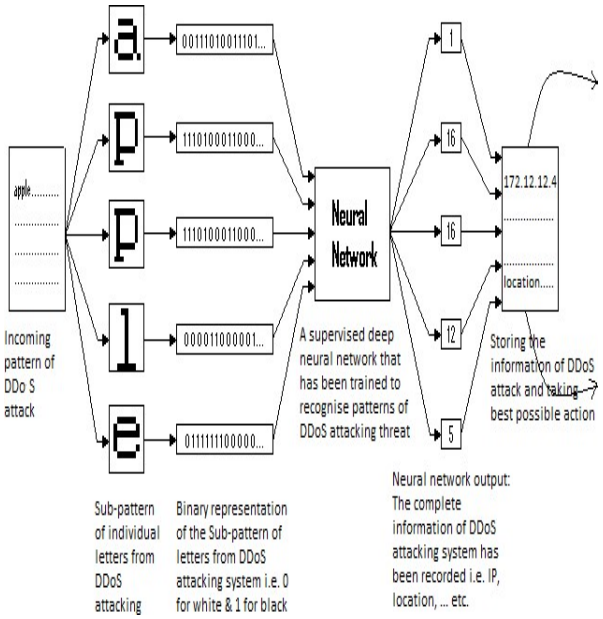


Fig. 4: Experimental result of the intelligent Honey net system

The ability to recognize and counteract the patterns of DDoS and DoS attacks has reached an impressive 99.99% effectiveness through the application of Deep Learning techniques. As a result of this achievement, the intelligent honeynet system is now fully equipped to defend against such attacks, ensuring enhanced security and resilience within the cloud computing environment.

(iv) Cloud Security using Quantum-Block chain Technology

Data security and privacy are paramount concerns in the cloud environment. This research focuses on enhancing the security of centralized cloud systems through the

integration of quantum computing and decentralized distributed block chain technologies. Block chain has emerged as a powerful technology for security, offering robust mechanisms to defend against cyber threats such as data tampering, DoS, and DDoS attacks. To address these challenges, a novel secure framework has been designed based on the polarization of photons at specific angles, leveraging distributed technology. The detection of attacks is facilitated by the quantum superposition principle, a key concept in quantum mechanics. Both the experimental setup and results are elaborated in the following sections.

(v) Experimental Setup

To initiate the experimental procedure, the quantum circuit has been used. A block contains hash value (|ψ>). To implement hash value over quantum circuit, superposition principle of quantum computing has been lay bare to result. The quantum circuit, for this purpose is shown in Fig. 5.

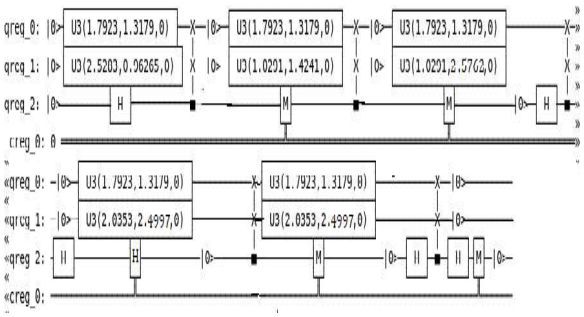


Fig. 5: Quantum Circuit of Proposed Algorithm

To secure cloud services using advanced technology, block chain is implemented as a key component. The proposed algorithm is designed using the Python programming language, with the Flask library imported to facilitate the display of the block chain in a web application. For data storage within the block chain, JavaScript Object Notation (JSON) is utilized. To attach digital fingerprints to the blocks through hash calculations, the Hashlib library is incorporated into the Python code. After implementing these countermeasures, the security of the cloud environment has been effectively enhanced, as demonstrated in the experimental results.

(vi) Experimental Result

Once the cloud user's data passes through this algorithm, Block chain technology ensures the data becomes immutable, preventing any future tampering. As a result, Quantum-Block chain technology fully secures the data. Additionally, manipulating the polarization of photons at specific angles is a highly complex task. This innovative security mechanism not only protects the cloud system from data tampering but also creates a chain of blocks. These connected blocks are stored in Block chain's distributed database, and if any block is tampered with, the entire chain is invalidated. Thus, after going through the

Quantum-Block chain process, the data becomes permanently immutable.

VII. Conclusion

Cloud computing, with its on-demand services and pay-as-you-go model, offers tremendous benefits to end-users and organizations by eliminating the need for internal infrastructure. However, the growing security challenges, particularly cyber-attacks, demand robust solutions to ensure data privacy and system protection. This research highlights the critical role of advanced technologies like Machine Learning, Deep Neural Networks, Block chain, and Quantum Computing in addressing these challenges. By integrating these technologies, we achieved significant improvements in defending against cyber-attacks, particularly DDoS, and ensuring the immutability of data through a Quantum-Block chain framework. As security vulnerabilities continue to evolve, this research provides a comprehensive approach to enhancing cloud security, focusing on both intrusion detection and data protection to safeguard the privacy of cloud users.

REFERENCES

[1] Mei-Ling. L. Liu, Distributed Computing: Principles and Applications, Addison Wesley. 2004, 05-06

[2] Jghef, Y. S., & Zeebaree, S., State of art survey for significant relations between cloud computing and distributed computing. International Journal of Science and Business, 2020, 4(12), pp. 53-61, DOI http://dx.doi.org/10.5281/zenodo.4237005

[3] Ibrahim, B. R., Zeebaree, S. R., & Hussan, B. K., Performance Measurement for Distributed Systems using 2TA and 3TA based on OPNET Principles. Science Journal of University of Zakho, 2019, 7(2), pp. 65–69, DOI http://dx.doi.org/10.25271/sjuoz.2019.7.2.603

[4] Jader, O. H., Zeebaree, S. R., & Zebari, R. R., A State Of Art Survey For Web Server Performance Measurement And Load Balancing Mechanisms. International Journal Of Scientific & Technology Research, 2019, 8(12), pp. 535–543.

[5] Papadimitriou, C. H., Computational Complexity. Addison-Wesley, 1994.

[6] Zeebaree, Subhi R M, M. Shukur, H., Haji, L., Zebari, R., Jacksi, K., and M. Abas, S., Characteristics and Analysis of Hadoop Distributed Systems. Technology Reports of Kansai University, 2020, 62(4), pp. 1555–1564.

[7] Thain, D., Tannenbaum, T., and Livny, M., Distributed computing in practice: The Condor experience. Concurrency and

Computation: Practice and Experience, 2005, 17(2–4), pp. 323–356, DOI https://doi.org/10.1002/cpe.938

[8] Borcea, C., Iyer, D., Kang, P., Saxena, A.and Iftode, L., Cooperative computing for distributed embedded systems. Proceedings 22nd International Conference on Distributed Computing Systems, 2002, pp. 227-236, doi: 10.1109/ICDCS.2002.1022260.

[9] Barbosa, J., Tavares, J., & Padilha, A., Parallel Image Processing System on a Cluster of Personal Computers. Vector and Parallel Processing, 2001, pp. 439-452.

[10] Neumann, D., Stößer, J., Weinhardt, C., Nimis, J., A framework for commercial grids – economic and technical challenges. Journal of Grid Computing, 2008, 6(3), pp. 325–347.

[11] Eric A. Fischer, Patricia Moloney Figliola, Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management. Congress research service, April 23, 2013.

[12] Badillo, S., Banfai, B., Birzele, Fabian., et. Al., An Introduction to Machine Learning. Clinical Pharmacology & Therapeutics, 2020, 107 (4), pp. 871-885 DOI:10.1002/cpt.1796.

[13] Lior Rokach and Oded Maimon, Top-Down Induction of Decision Trees Classifiers – A Survey. IEEE Transactions on Systems, Man, And Cybernetics – Part C: Applications and Reviews, November 2005, 35(4), pp. 476-487.

[14] Anzai Y., Pattern recognition and machine learning. Elsevier; 2012.

[15] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564, DOI: 10.1109/BigDataCongress.2017.85.

[16] Yaga, D., Mell, P., et. al., Blockchain Technology Overview. National Institute of Standards and Technology, U.S. Department of Commerce, 2018, https://doi.org/10.6028/NIST.IR.8202

[17] Dib, O., Brousmiche, Kei-Leo, et. al., Consortium Blockchains: Overview, Applications and Challenges. International Journal on Advances in Telecommunications, 2018, 11(1 & 2) pp. 51-64

[18] Foroglou, G., and Tsilidou, A. L., Further applications of the blockchain. 2015.

[19] Schuld, M., Sinayskiy, I., Petruccione, F., The quest for a Quantum Neural

Network. Quantum Inf Process, 2014, 13, pp. 2567–2586. https://doi.org/10.1007/s11128-014-0809-8.

[20] Kuyoro, S., Ibikunle, F., & Oludele, A., Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), 2011, 3, pp. 247- 255.

[21] Amin, Z., Singh, H., & Ahluwalia, N., Review on Fault Tolerance Techniques in Cloud Computing. International Journal of Computer Applications, 2015, 116, pp. 11-17.