Applying Communication Engineering ML Techniques to Security Enhancement in Cloud Computing

Benjamin* & Dylan**

*Associate Professor, Communication Technology, Singapore Institute of Technology, Singapore.
E-Mail: benjaminfrank@outlook.com
** Professor, Communication Technology, Singapore Institute of Technology, Singapore.
E-Mail: dylan_professor12@gmail.com

***Abstract*---** This paper has examined some of the ways in which machine learning (ML) can be used in cloud computing security. Indeed, the overall volume of data in the cloud has increased dramatically. This trend has also come with an increase in the amount of sensitive data that individuals and companies or organizations continue to keep in the cloud. As such, there has been a growing need for significant improvements in cloud computing security ─ to ensure that operations and data interactions in the cloud keep abreast with the dynamic nature of information technology. Motivated by the quest for cloud computing security, this paper has examined different approaches that most of the previous scholarly investigations (which focus on the adoption of machine learning in cloud computing security) have proposed ─ towards better threat detection. The paper has begun with a general algorithm responsible for establishing the summation of risk levels before proceeding to more advanced algorithms through which threats to cloud data could be determined. Imperative to note is that the advanced approaches have been found to embrace anomaly detection and signature detection, translating into a proposed hybrid model for threat detection in the cloud. Whereas a major weakness is that the proposed model is not compared to another competitive model, its strength lies in the capacity to give an insight into ways in which certain time frames and profile categories could be specified, leading to a better classification of cloud user profiles and the eventual detection of anomalies.

***Keywords*---** Machine Learning (ML), Cloud Computing Security, Operations and Data Interactions.

I. INTRODUCTION

THE increasing adoption of cloud computing has led to data explosion. However, the availability of this data comes with issues of security, energy efficiency, and resource management [1]. Some of the major companies that have embraced cloud computing include Microsoft, Google, and Amazon.

With an exponential increase in data amount, the resultant opportunities for utilization have culminated into partnerships between machine learning (ML) and cloud computing to benefit from each other's refinement and advancement [2].

This paper examines the concept of cloud computing relative to the adoption of machine learning as a path for enhancing the security of cloud computing applications. Indeed, the specific objective entails the examination of some of the security benefits that ML offers to the cloud computing practice.

The increase in overall cloud data has come with an increase in the cloud's amount of sensitive data [3]. This trend has motivated the quest for higher security. To improve cloud security in the form of enhanced threat detection, some of the previous scholarly investigations have proposed various approaches [4, 5].

Relative to the aspect of encryption, one of the approaches that have been documented to be straightforward in denying or enabling access to cloud data entails enforcing some trust level system [5]. Imperatively, the trust levels imply that any cloud system participant is dynamically allocated the trust level and the assignment of privileges to the parties depends on the trust level established and associated with the participant [6, 7, 9].

Therefore, the general algorithm (which is responsible for determining trust levels in the cloud) has been proposed. The algorithm is responsible for establishing risk level summations before determining the threat [3-5]. This algorithm works by enforcing some trust level system whereby cloud system participants are dynamically allocated trust levels, and the established trust level dictates the privileges of the participant [6]. Notably, the trust level established by the algorithm is established through the sum of all risk levels linked to the participant.

II. Methodology

Upon determining overall trust levels via risk level summation and the calculation of the overall risk level, the proposed general algorithm associates each cloud agent with a certain degree of trust. In turn, restrictions and privileges to certain cloud features are enabled for the agent [6-8].

Despite the promising nature of this algorithm in steering cloud computing security, it has been documented to be cumbersome [8] and also offered very little advice [9]; especially in complex cloud environments where features are unknown beforehand and, thus, not possible to assign them to reliable weights.

To address these limitations of the proposed general algorithm, two approaches have been proposed. These approaches include anomaly detection and signature detection [1].

In this case, the proposed hybrid method employs Random Forest (RF) and Naïve Bayes Tree (NBT). This algorithm has been proposed and works by using training sets to generate classification patterns [6]. The aim of this procedure is to use each connection's similarity features and the classification patterns to determine anomalies in the cloud environment [7].

To generate an accurate classification state, this hybrid algorithm demands extensive datasets [4]. To resolve this dilemma, most of the investigations have employed the KDD Cup '99 data set. Notably, the dataset employed has been divided into subclasses and the classification is dependent on the type of attack.

III. Results

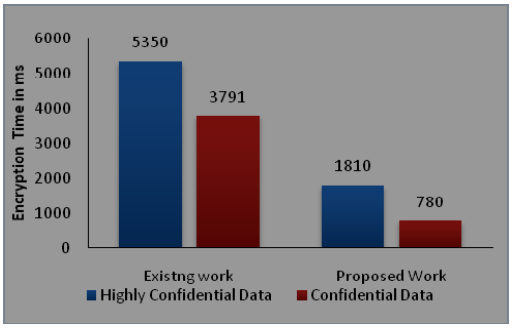

Figure 1 - An illustration of Encryption Time Performance between the Existing Framework and the Proposed Technique

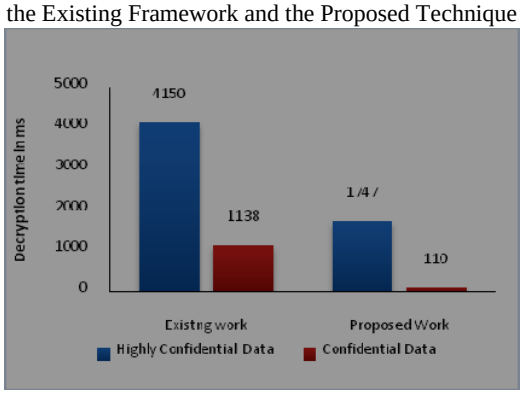

Figure 2 - Relative to the Decryption Time

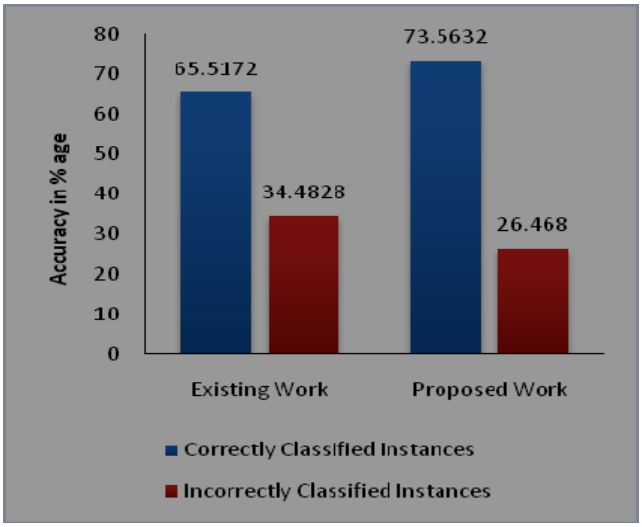

Figure 3 - In Relation to Model Accuracy

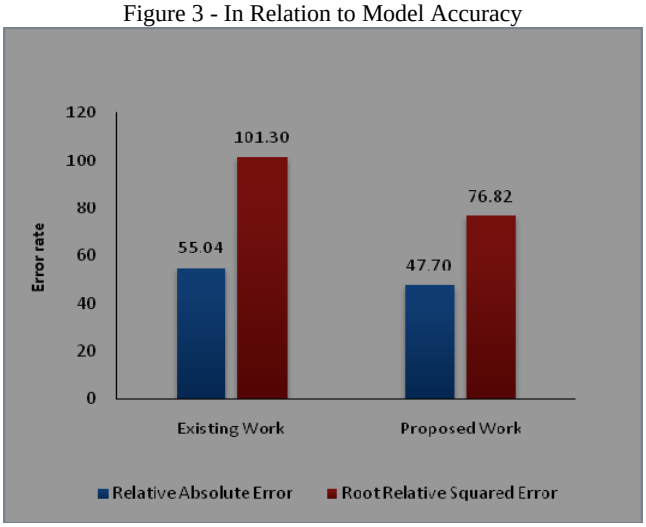

Figure 4 - Examining the Error Rate

From the results, most of the previous investigations that have examined the proposed hybrid algorithm as a machine learning technique for enhancing cloud computing security contend that the combination of RF + NBT poses better or superior results regarding the parameters of false positive rate (2.0 to 12.0) and accuracy (99.0 to 94.7) [8-10]. Imperative to highlight is that this hybrid technique (NBT + RF) outperforms the KNN + RF method but the results are not compared to wider varieties of ML techniques for enhancing cloud computing security. Despite this limitation, the importance of this ML algorithm's capacity to reduce the false positive rate is worth acknowledging and emphasizing because most of the anomaly detection techniques have failed to produce such promising results. Hence, this step is significant and could be embraced in anomaly detection within the cloud environment [9].

As mentioned earlier, the proposed hybrid method combining RF + NBT outperforms the hybrid method combing RF + KNN but fails to offer comparisons between the results and other competing methods of wider varieties [10]. Some of the reasons documented in relation to this limitation include the possible lack of relevance between the proposed hybrid method and other competing methods, and

possible lack of competing methods [8, 9]. To counter these limitations, an ML framework for detecting semantic gaps and anomalies in cloud computing has been proposed and is poised to counter the limitations of the hybrid technique above.

This proposed framework reflects the work of ML in enhancing cloud computing security by emphasizing the detection of threats in the cloud environment by identifying semantic gap and anomalies [1]. Overall, the hybrid framework is important because it highlights the manner in which most of the methods that are being implemented could have their models improved for purposes of identifying semantic gaps.

IV. Conclusion

In conclusion, cloud computing has led to vast amounts of data available in the environment, and this trend has come with security threats; especially those concerning possible leakages of sensitive data (or data loss). As such, there has been a need to embrace models that seek to enhance the security of the cloud computing environment. This pressure has led to the proposal of machine learning as a promising platform through which threat detection in the cloud environment might be realized. From the examination of the previous scholarly investigations, several algorithms have been proposed. These algorithms exhibit strengths and limitations and, these mixed outcomes have led to the propose from framework after framework, with each ML technique seeking to counter the demerits associated with a preceding approach to threat detection in the cloud environment. Some of the proposed algorithms that this paper has examined include the general algorithm, signature detection as an ML algorithm in cloud computing security, and anomaly detection as an ML algorithm for cloud computing security. Others include the Proposed Random Forest and **Naïve Bayes Tree As a hybrid algorithm for cloud computing security and the p**roposed ML framework for detecting semantic gaps and anomalies in cloud computing. According to the study, we find that machine learning can be extensively used in cloud computing security.

References

[1] Bhamare, D., Salman, T., Samaka, M., Erbad, A., & Jain, R. (2016, December). Feasibility of supervised machine learning for cloud security. In *2016 International Conference on Information Science and Security (ICISS)*, 1-5. IEEE.

[2] Pop, D. (2012). Machine Learning and Cloud Computing: Survey of Distributed and SaaS Solutions. *West University of Timisoara.*

[3] Kiran, C., & Sharma, S. (2017). Enhance Data Security in Cloud Computing Using Machine Learning and Hybrid Cryptography Techniques. *International Journal of Advanced Research in Computer Science*, 8(9), 393-397.

[4] Vijitha, K., & Greeshmananda, V. (2013). Machine Learning For Cloud Computing Intrusion Detection. *International Journal of Innovative Research & Development*, 2(5), 1250-1261.

[5] Moghaddam, F.F., Vala, M., Ahmadi, M., Khodadadi, T., & Madadipouya, K. (2015, August). A reliable data protection model based on re-encryption concepts in cloud environments. In *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)*, 11-16. IEEE.

[6] Zardari, M.A., Jung, L.T., & Zakaria, N. (2014, June). K-NN classifier for data confidentiality in cloud computing. In *2014 International Conference on Computer and Information Sciences (ICCOINS)*, 1-6. IEEE. *A Conf. World Eng. Sci. Technol. Congr. ESTCON 2014 - Proc.*

[7] Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering*, 1, 647-651. IEEE.

[8] Surv, N., Wanve, B., Kamble, R., Patil, S., & Katti, J. (2015, June). Framework for client side AES encryption technique in cloud computing. In *2015 IEEE International Advance Computing Conference (IACC). Souvenir 2015 IEEE*, 525-528.

[9] Yu, S., Wang, C., Ren, K., & Lou, W. (2010). "Achieving secure, scalable, and fine-grained data access control in cloud computing.pdf," *IEEE Infocom*, 1–9.

[10] Pant, V.K., Prakash, J., & Asthana, A. (2015). Three step data security model for cloud computing based on RSA and steganography. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 490-494). IEEE.