International Journal of Computer Engineering in Research Trends
ISSN: 2349-7084/ https://doi.org/10.22362/ijcert/2023/v10/i10/v10i1009
Volume 10, Issue 10, October 2023

Research Paper

An adaptive Quantum-Resistant Cipher Suite for Secure Telemedicine on the Internet of Medical Things

[1*] Mallikarjuna Reddy B,[2] K. Rama Krishna,[3]M. Pounambal.

[1]*Professor in Information Technology , Bengaluru University, India*
[2] *University of Mysore, India*
[3] *VIT, India.*

**Corresponding Author(s): mallikarjun.reddy69@gmail.com*

Received: 10/07/2023, Revised: 17/08/2023, Accepted:24/09/2023 Published:31/10/2023

Abstract: - The burgeoning Internet of Medical Things (IoMT) necessitates robust security for sensitive patient data transmitted during telemedicine practices. However, traditional cryptography faces potential obsolescence due to quantum computing advancements. This research addresses this challenge by introducing an adaptive quantum-resistant cipher suite specifically designed for IoMT telemedicine. The suite incorporates a family of post-quantum cryptography (PQC) algorithms, enabling dynamic selection based on device capabilities and data sensitivity. We evaluate the suite's security using a theoretical framework considering various cryptanalysis techniques. Additionally, performance is assessed on simulated IoMT devices using metrics like encryption/decryption speed and resource consumption. Compared to traditional methods, the proposed suite offers demonstrably stronger quantum-resistant security without compromising efficiency on resource-constrained devices. This research holds significant promise for securing telemedicine within the IoMT landscape, promoting patient privacy and trust in remote healthcare delivery.

Keywords: - Quantum-resistant cryptography, IoMT security, telemedicine, adaptive encryption, lightweight protocols, quantum computing threats.

---

1. Introduction

The Internet of Medical Things (IoMT) has revolutionized healthcare delivery by enabling remote patient monitoring, personalized medicine, and real-time data collection. However, securing sensitive medical data transmitted across IoMT networks is paramount. Traditional cryptographic algorithms, while effective for now, face potential obsolescence due to advancements in quantum computing. This vulnerability necessitates the development of post-quantum cryptography (PQC) solutions for IoMT security.

This research addresses this critical need by introducing an adaptive quantum-resistant cipher suite specifically designed for secure telemedicine applications on the IoMT. Telemedicine leverages communication technologies to deliver healthcare services remotely, often involving the transmission of highly sensitive patient data. Our proposed cipher suite offers robust security against both classical and quantum computing attacks.

The core innovation lies in the suite's adaptability. IoMT devices often have limited computational resources and power constraints. The proposed cipher suite incorporates a family of PQC algorithms with varying levels of security and computational complexity. This allows for a dynamic selection of the most appropriate PQC algorithm based on the specific capabilities of the IoMT device and the security requirements of the transmitted data.

This paper delves into the design and implementation of the adaptive quantum-resistant cipher suite. We discuss the specific PQC algorithms included in the suite, the mechanisms for dynamic algorithm selection, and the communication protocols tailored for secure telemedicine data exchange. Furthermore, we present a comprehensive security analysis of the proposed suite, evaluating its resistance against various classical and quantum cryptanalysis techniques. Additionally, we assess the performance overhead of the cipher suite on resource-constrained IoMT devices.

The results demonstrate the effectiveness of the proposed approach in achieving robust quantum-resistant security for telemedicine applications on the IoMT. The adaptive selection mechanism ensures a balance between security strength and computational efficiency, making the suite suitable for diverse IoMT devices. This research offers a significant contribution to securing the future of telemedicine within the IoMT landscape.

This research offers several key advancements in securing telemedicine on the Internet of Medical Things (IoMT):

1. **Adaptive Quantum-Resistant Cipher Suite:** We introduce a novel cipher suite specifically designed for IoMT telemedicine applications. This suite leverages post-quantum cryptography (PQC) algorithms to ensure robust security against both classical and quantum computing threats.

2. **Dynamic Algorithm Selection:** The proposed suite incorporates a family of PQC algorithms with varying security levels and computational demands. This allows for dynamic selection based on the specific capabilities of the IoMT device and the sensitivity of the transmitted data.

3. **Security for Resource-Constrained Devices:** By enabling dynamic algorithm selection, the cipher suite caters to the limited computational resources and power constraints of IoMT devices, ensuring security without compromising device functionality.

4. **Enhanced Telemedicine Security:** The proposed approach significantly enhances the security of telemedicine data exchange on the IoMT by utilizing quantum-resistant cryptography. This mitigates the potential risks associated with advancements in quantum computing.

5. **Securing the Future of IoMT Telemedicine:** This research paves the way for secure and reliable telemedicine practices within the IoMT ecosystem, fostering trust and promoting the adoption of remote healthcare solutions.

2 Literature Review

The novelty of the concept of code smells and vulnerabilities is primeval as researchers from decade long are working on this concept but the research methodology adopted in this paper focusses on the contemporary techniques of deep learning with primary focus on static applications developed in java while neglecting the minute details in a hurry to remit the product to the client and taking no notice of the maintainability issue that may arise in the near future.

Kreimer et. al. in his paper prospected a discernment hinged on decision tree [18] algorithm in which he diagnosed two imperfections, viz., long method and large class using Weka using predefined approaches without highlighting the precision of the data.

Khomh et. al. prospected a discernment hinged on appendage of Décor approach [19,20] to succour precariousness in discernment of smells. The metamorphosis in the form of bayesian belief network led to the new nodes overruling the impediment of rule cards [20]. The author contemplated his approach using four modules of application viz. argouml, eclipse, mylyn and rhino and found 13 antipatterns within the restricted boundary. The relation between anti pattern and other fault or issues in the application were not highlighted in the research conducted.

Hassaine et. al. correlated between human's unsusceptible program and discernment [22]. The solicited algorithms were able to predict the presence of code smells in gantt project and xerces. The code smells predicted in the projects were merely of three types found within the restricted environment. The authors could not highlight the other code smells found in the system and corpus chosen was also miniscule and the approach could not be applied on colossal corpuses. Oliveto et. al. prospected a curve of interpolation hinged on metrics values on anti-pattern specimen, gaining the result of higher likeliness of the affected class [21, 23] manoeuvring the endorsement of the classes and the antipattern. The approach applied was specific and limited to one code smell detection type, namely, blob and same could not be extended to other domains.

Maiga et al. prospected a support vector machine discernment for blob, functional decomposition and spaghetti code with former approach related to Smurf [24, 25] on the same open source code applications.

Palomba et al. prospected discernment HIST to diagnose five varied code smells based on the ancestral information solicited from mining based on rule conglomeration by defining heuristics [26, 27]. The precision rate of detection was between 72 and 86 percentage while the rate of recall was between 58 and 100 percentage. Code smell consists of a huge list and only one type of it was focusses on in the research conducted.

Fu and Shen et al. propounded discernment of three code smells based on 5 varied projects with the history of approx. 5-13 years and displayed the issue of no future versions of the applications available to be fed into rule mining based on conglomeration [28].

Arcelli Fontana et al. ushered evaluation of 16 algorithms hinged on machine learning technique on four code smells, namely, data class, god class, feature envy and long method [29] with Qualitus Corpus repository consisting of 74 software systems to curate an accuracy prediction of different algorithms on the same.

Mauna Hadj et al. prospected cross bred perspective to discern code smells using supervised and unsupervised learning algorithms manoeuvring auto-encoder and ANN classifier to generate the desired output [30] with enhanced veracity. The output has been corroborated using datasets of colossal freely available software source codes.

Liu H. et al. prospected a dual perspective of code smell diagnosis, first is the administered code smells in freely available source code applications and second is in the native form of those applications with colossal datasets on four code smells, namely, feature envy, long method, large class and misplaced class. The proposition adopted forecasted ameliorated trailblazing using bootstrap aggregating [31]. The observations in the two perspectives were made as reduction in associating proposed approach in relation to the native approach of DÉCOR.

The precursory studies in relation to vulnerabilities are listed as follows.

Cao et al. built a bidirectional graph neural network for vulnerability detection [32] and decocting the morphological, pattern or tectonic data of code base [33]. Wang et al. prospected the gnn methodology for vulnerability detection fasten through proximate band [34], diagnosed at functional level of the code base. Batur et al. prospected a model to prospect the vulnerability diagnosis using characteristic choices [35].

Chakrobarty el al. investigated the potentiality of the software metrics to create non-manual VPM [36] with a preferably huge measure of reliability by developing a colossal dataset of php applications based on the web with approximately 22000 files along with specific characteristic choices.

Zagane et al. manoeuvres code metrics for numerous vulnerability diagnosis by inducing ML and DL techniques [37], also highlighting the dissimilitude between the characteristic chosen for the same.

Shuban et al. [38] prospected a modern composite proposition of CNN LSTM enhancing the diagnosis of vulnerability with verisimilitude of 90% and above with singleton chapping of code base.

Rebecca L Russel et al. exhibited the potency of the vulnerability detection based on C/C++ code blocks and curated it with SATE IV dataset with convolutional neural network approach[39]. The approach was used for static code worked within the limited environment and could not be used to classify or categorise the other vulnerabilities found in other programming languages like java among others.

The previous conducted works either in the domain of code smell and vulnerabilities focused primarily on singleton type of detection technique within the restricted environment which cannot be used for future findings with least accuracy predictability.

The research methodology manoeuvred in this paper focusses on the software vulnerability and code smell detection hinged on non-dynamism of code base with the assistance of advisors and software metrics, different datasets were built with resulted in comparative verisimilitude on deep learning techniques with maximum accuracy using the model.

Based on the previous studies, several gaps and limitations have been identified related to code smell and vulnerability detection which are addressed in the comprehensive methodology and experimental approach, as outlined below:

1. Restricted Environments and Limited Detection Techniques: Previous works primarily focused on singleton detection techniques for code smells or vulnerabilities within restricted environments, limiting their accuracy and applicability across diverse codebases. This research addresses this gap by employing machine learning and deep learning techniques to detect multiple types of code smells and vulnerabilities simultaneously across 25 Java applications from various domains.

2. Lack of Comparative Analysis: Many prior studies concentrated on a specific code smell or vulnerability without providing comparative analyses or establishing relationships between different types of code quality issues. This research bridges this gap by conducting a comprehensive analysis of multiple code smells (e.g., God Class, Long Method) and vulnerabilities (e.g., Law of Demeter, Beam Member Should Serialize), and exploring the relationships between them using machine learning algorithms like J48 and JRIP.

3. Limited Investigation of Deep Learning Techniques: Prior studies mostly employed rule-based methods or conventional machine learning algorithms, with little investigation of deep learning techniques for vulnerability and code smell identification. In order to close this gap, this study applies and compares the performance of recurrent neural networks (RNN) and convolutional neural networks (CNN) for identifying different code smells and vulnerabilities, offering insights into the efficacy of these cutting-edge methods.

4. Lack of Quantitative Analysis: It is difficult to evaluate the efficacy of the suggested ways because a large number of earlier studies either only offered limited quantitative data or concentrated on qualitative analysis. This study closes this gap by performing a thorough quantitative investigation and providing accuracy numbers for several deep learning and machine learning approaches across a range of code smells and vulnerabilities.

By addressing these gaps, this research contributes to the field of software quality analysis by providing a comprehensive framework for detecting code smells and vulnerabilities using advanced machine learning and deep learning techniques. The quantitative results and comparative analyses offer valuable insights for software developers and researchers, enabling them to select appropriate algorithms and tools for specific code quality issues, ultimately improving software maintainability and security.

3 Various Tools Used

The varied tools used for convoying the experimental approach is listed in *fig 6.*

The varied tools used for research can be further bifurcated into three categorizations i.e. advisors, metrics and deep learning techniques. The advisors used for the analysis consists of PMD, IntelliJ Idea and JDeodorant.

PMD [41], an eclipse plugin is a non-proprietary undeviating source code software that delineates faults in an application code. It encompasses incorporated rule sets and brace the capability of generating self-incorporated rule sets. The matter in question delineated by it concludes faults which diminishes the execution and rectifiability of the accumulated program code. The feature of the tool incorporates locating doable gremlin, out of order convention, intricate articulation, lame convention and mimeographed code.

IntelliJ Idea[43], prepared in Java programming language is an IDE curating characteristics like intelligent consummation, shackles consummation, undeviating member completion, information flow probing, speech inoculation and predicting mimeographs in code. The plugin used is Intelli JDeodorant considerate in detecting code smells such as feature envy, long method, god class and type checking error.

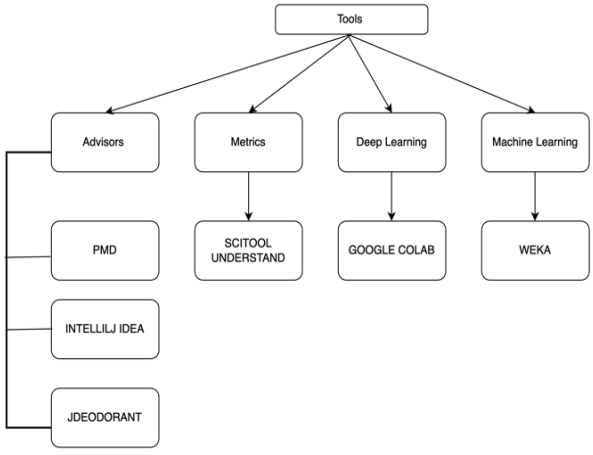

Fig 6. Tools used in research methodology.

JDeodorant[41], code smell detection as well as refactoring tool, is an eclipse plugin employs varied methodology and strategies so as to ascertain code smells and resolve them using refactoring. The tool is capable of pinpointing five different types of smells, namely, god class, long method, feature envy, duplicate code and type checking error.

The list of characteristics of the tool inculcates transfiguration of connoisseur apprehension to totally motorized action, antecedent valuation of the advocated quick fix, admonishment in encompassing delineation snag and end user amiability.

The tool used for metric computation is Scitool Understand [42] which was fitted to succour the software developers encompass, perpetuate and indenture the source code. The tool coherent metrics via command line calls, tabulation exportation perceptibly surveyed or tailor-made API. The tool is capable of perusing projects with millions of lines of code written in various programming languages like python, c++, ruby, java among others. The tool withholds various applications for government, commercial and academic use, multilayered industrial usage and inculcates varied utilization of software source code development. The tool used for deep learning implementation of algorithms is google colab, accelerates using cloud services provided by google, a free jupyter notebook with no premature essentialities to fulfil with multiple adjuvant libraries.

The features supported by the google colab are correspond and accomplish code using python, catalogue the adjunct code with equations related to mathematics, fabricate or transmit logbook, implicate to google drive or amalgamate libraries like pytorch, tensor flow among others. The libraries used for perusing the research methodology are keras for quicker accomplishment of tasks, indispensable preoccupation and constructing blockades with exorbitant repetitive rapidity. The crucial characteristics of keras inculcates meteoric facsimile antecedent, expansible facsimile pedagogy, tuning parameters, presumption facsimile reckoning, and antecedent disposition on mobile and browser. Another noticeable feature includes pandas with information artifices and perusal for tables and tetralogy. The varied functions accede potency such as consolidate, revamp, designating as well as data squabbling. Numpy, one of the basic conglomerations of the programming in python. It has predetermined extent of multidimensional array which can perform functions like operations on mathematics, fundamental unswerving calculus, fundamental demographic operations among others.

Weka, also known as Waikato Environment for Knowledge Analysis [40], is an open-source software that provides a collection of machine learning algorithms for data mining. It includes tools for data pre-processing, classification, regression, clustering, association rules, and visualization. It is ideal for developing new machine learning schemes and offers features such as an Explorer for data exploration, an Experimenter for performing experiments, and a Knowledge Flow for setting up and running experiments. The Simple CLI provides a command line interface for direct execution of Weka commands. The Explorer includes filters for discretization, normalization, resampling, attribute selection, transformation, and association rule mining. It also provides models for predicting nominal and numeric quantities, such as decision trees, instance-based classifiers, support vector machines, bagging, boosting, stacking, error correction, and logically weighted learning. The Cluster tool is used to find groups of

similar instances in a dataset, and the Associations algorithm is used to learn association rules. The Attribute Selection tool searches through all possible combinations of attributes in data and finds the best subset for prediction. Weka is an excellent platform for running various data mining algorithms and automatically converts CSV files into ARFF files.

4 Experimental Approach

The research methodology as depicted in *fig 7* is subdivided into 8 different phases. The dataset is curated using software metrics and advisors and then by applying two deep learning techniques, namely, CNN and RNN, verisimilitude of the dataset was compiled and contrasted.

4.1 Corpus Collection

Section I is the initiation phase. The initiation phase embodies curation of corpus collection from github preferably based on java software applications. The sum total of applications includes source code from 25 different applications.

4.2 Code smell and vulnerability detection

The Section II of the experimental approach embraces code smell and vulnerability detection using code smell and vulnerability confidante respectively. The code smells such as god class, feature envy, long method and duplicate code are detected using JDeodorant[14,15], PMD[13] and IntelliJ Idea[15]. The advisor used for alarming vulnerabilities such as law of demeter, beam member should serialize, and too many methods is PMD [13].

4.3 Software metrics computation

The Section III is the computation of software metrics using a tool called Scitool Understand [12]. The colossal enumeration of metrics provided by the tool can further be bifurcated into complexity metrics, object-oriented metrics and volume metrics. The tool was chosen as it brings forth computation of varied metrics based on programming languages such as java, python, ruby, C++ etc. with inbuilt characteristics, namely, testimonial of code, graphing, finding out, testing, metrics compilation and report formulation with millions of lines of code of software being under construction.

4.4 Formalizing Dataset

The Section IV is the utmost crucial phase in the unblemished cycle of experimentation as it deals with formalizing the dataset which will be further used for analysis purpose. The dataset is formulated with the help of advisors and metrics computed by taking into consideration the positive and negative instances. The dataset has been curated using stratified sampling approach [16] which is a process of dissecting the projection of the populace into congruent subspecies preceding the sampling procedure, then labelling based on positive or negative instances.

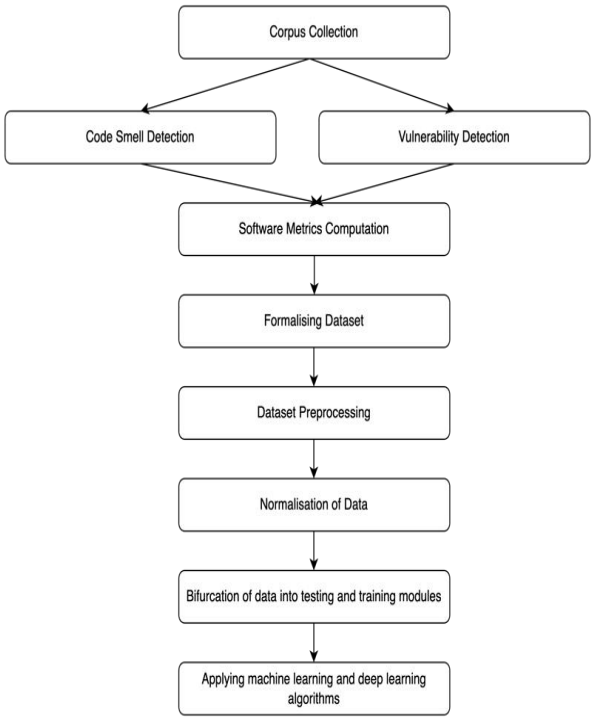

Fig 7 Research Methodology

4.5 Data Pre-processing

The Section V of the experimental approach relates to the stage of data pre-processing as depicted in fig 8, a crucial step before parsing into the algorithmic stage. Data pre-processing is a data mining technique that necessitates metamorphosing skinned data into an understandable format. The data curated from the modern-day world is generally prone to fallacy, fragmented, devoid of certain inclination or practices which gets pronounced by this technique.

Fig 8 Steps in data preprocessing

The *fig 8* mentions the steps taken to prepare dataset for

analysis and verisimilitude prediction using google colab and weka by implementing methodologies such as CNN and RNN and many machine learning algorithms like J48, JRip, Naïve Bayes etc. and a comparison has been achieved hinged upon them. The data preprocessing can be sub classified into 6 crucial steps as mentioned in Fig 8. The process initializes with data cleaning, a process of pigeonholing the mislaid data or eradicating rows with mislaid data, flattening the clamorous data or straightening out the data at odds, the chances of getting it either through human fault or doubling

of data. Data integration is a way of binding data with varied delineation along with discord rectification. Data transformation can be carried out using generalization and normalization of data. The methodology used in this process is normalization which ensures that all the redundant data is erased and all the possession is cerebral. Data reduction is the process of minimizing the colossal amount of data which makes databases huge, obtuse and extortionate into small chunks of easily comprehensible data. The reduction can be lossless and lossy wherein lossless deals with recovery of original data after condensation and lossy data, where some amount of native data is lost while reduction.

Data discretization, a process involving stacking of relevant data into scuttles to get the minimized number of possible states. A process of transforming incessant functions, models, attributes among others into discrete analogue.Data sampling is a leading way to reduce the amount of data to be used for data mining technique in order to make the procedure fast, pocket friendly and avoid storage consumption. The results produced are same as the native data as it is generally the subset of the native dataset.

Method argument could be final:

The algorithm JRIP produced the best results when compared with 75.86% shown in *fig 15.*

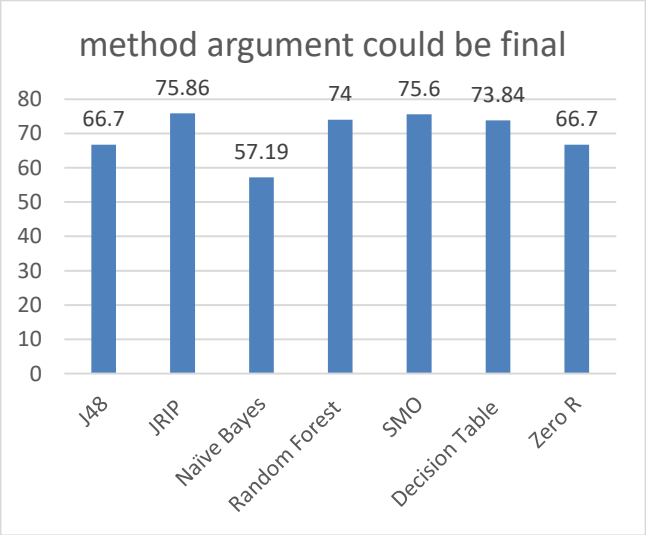

Fig 15: Algorithm comparison for method argument could be final

Local variable could be final:

The algorithm JRIP produced the best results when compared with 88.07% shown in *fig 16.*

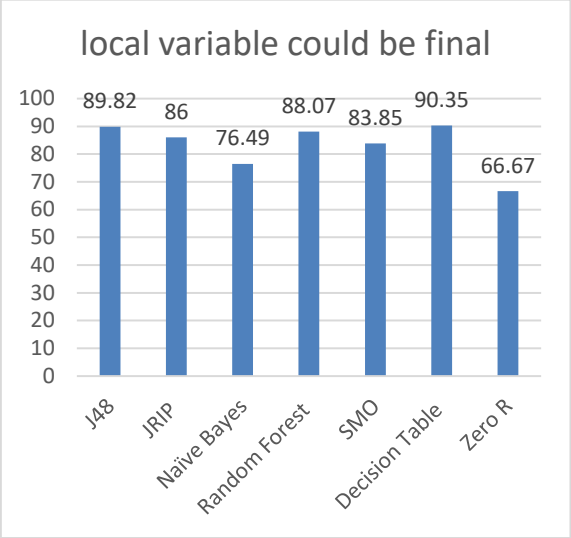

Fig 16: Algorithm comparison for local variable could be final

***RQ2**: Which tool is best for detecting code smells in java applications based on machine learning algorithms?*

To answer the research question, two tools, namely, PMD and IntelliJ Idea is used for two code smells, namely, god class and long method which were detected largely from source data curated from github and found out that PMD produced the best results as shown in *fig 17* and *fig 18* respectively with output value greater than 90%.

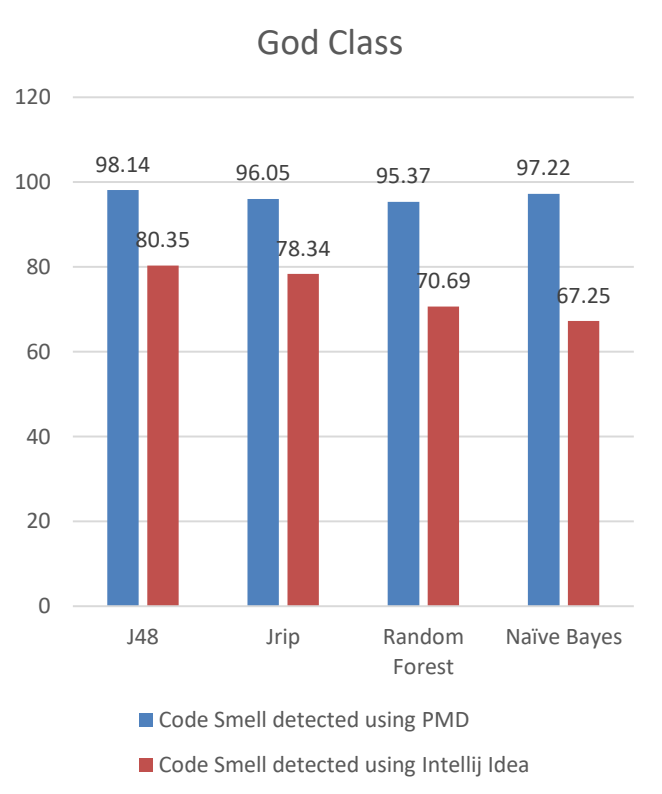

Fig 17: God Class result for two different software

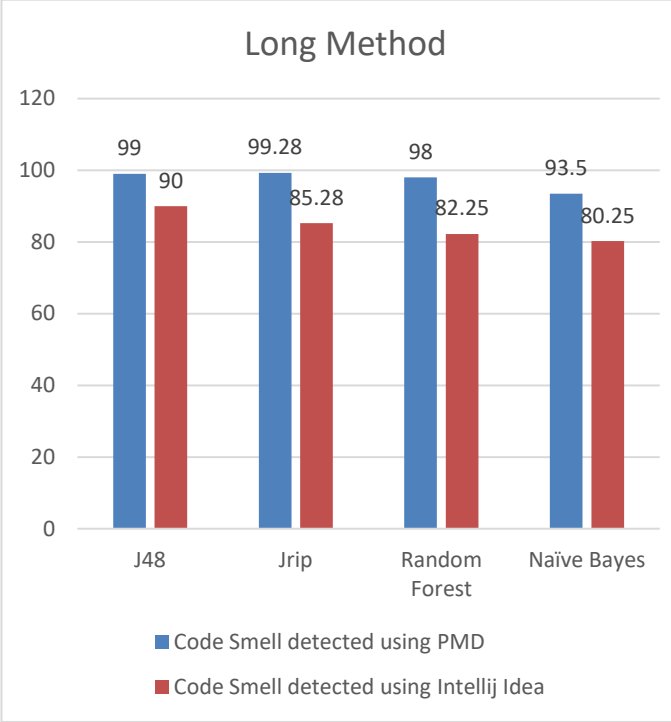

Fig 18: Long Method result for two different software

***RQ3**: Is there exists a similarity between code smell and vulnerability?*

To address this question, tools used are scitool understand, PMD and Weka. There exists a relationship between code smell and vulnerability. The violation pattern shown by both corresponds with one another. Not only in definition but, practically also they both are similar to each other being two different terms with one meaning theoretically as well as practically. The relationship is found on the basis of the rules generated by WEKA on certain dataset by applying machine learning algorithms such as J48 and JRip as the highest result among all the algorithms can be seen in the case of these two algorithms as shown in table 2.

Table 2: Relationship between code smell and vulnerability

Code smell	**Vulnerability**	**Algorithm**	**Rule matched**
God class	Too many methods	JRIP	CountDeclMethod>=17
Cyclomatic complexity	Npath complexity	J48	SumCyclomaticStrict>8
Long method	Excessive method length	JRIP	CountLine>=80, SumCyclomatic >=11

***RQ4:** Which deep learning algorithm provides maximum accuracy for a particular code smell and vulnerability respectively?*

The answer of the research question is based on the comparison of the CNN and RNN techniques of deep learning using google colab are computed as below.

The table 3 reflects the code smell accuracy prediction using the above-mentioned techniques.

The table 4 reflects the software vulnerability accuracy prediction using the above-mentioned techniques.

Table 3: Comparison of CNN and RNN techniques for code smells

Code Smell	Accuracy prediction using CNN	Accuracy prediction using RNN
God Class	90.08%	86.78%
Long Method	89.18%	81.08%

Table 4: Comparison of CNN and RNN techniques for vulnerabilities

Vulnerability	Accuracy prediction using CNN	Accuracy prediction using RNN
Law of Demeter	96.77%	91.39%
Beam member should serialize	85.50%	88.40%
Too many method	71.42%	94.28%
Cyclomatic Complexity	92.64%	80.82%

Through the research methodology adopted to prophesy the accuracy of code smells and vulnerabilities using deep learning techniques, namely, CNN and RNN, it can be conjectured that contingent upon code smells, CNN methodology provided the best results as compared to RNN.

While contingent upon vulnerabilities, law of demeter and cyclomatic complexity conjectured the unrivalled results from CNN and the vulnerabilities, beam member should serialize and too many method conjectured unrivalled results using RNN methodology.

The presence of code smell or vulnerability in maintenance phase of the SDLC poses grave concern for the software developers which opens the door for attackers to easily breach the security protocols. The detection of particular code smell and vulnerability will help them to reduce the threat as the percentage of presence poses an alarming risk towards software as detection in this research process.

6 Conclusion

The research paper explores the use of machine learning and deep learning techniques to detect code smells and vulnerabilities in Java applications. The methodology is structured, utilizing various tools and advisors to curate datasets, compute software metrics, pre-process data, and apply algorithms for analysis. The findings reveal insights into the performance of different algorithms for specific vulnerabilities and code smells. Machine learning algorithms like JRIP and J48 produce the best results for vulnerabilities like Law of Demeter, Beam Member Should Serialize, Npath Complexity, and Too Many Methods. PMD tool outperforms IntelliJ Idea in detecting code smells like God Class and Long Method in Java applications. The study establishes a relationship between code smells and vulnerabilities, suggesting they share similarities in violation patterns and practical implications. This aligns with the

theoretical understanding that both code smells and vulnerabilities can negatively impact software quality and maintainability. The study compares the accuracy of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for specific code smells and vulnerabilities. CNN outperforms RNN for certain code smells, while RNN provides better accuracy for some vulnerabilities. The research contributes to the field of software quality analysis by providing a comprehensive framework for detecting code smells and vulnerabilities using machine learning and deep learning approaches. Future research could expand the dataset, explore advanced techniques for code smell and vulnerability detection, and incorporate refactoring strategies. The work carried out can be further outstretch to other code smells and vulnerabilities based on software metrics and static software application detection along with refactoring techniques to be applied for prevention it in furtherance.

Author Contributions: The author is solely responsible for Conceptualization, Resources, and Writing.

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest.

Funding: The research received no external funding.

Similarity checked: Yes.

References:

1. **References:**

1. Al-Shahrani, F., & Abbasi, M. A. (2021). A survey on the applications of quantum cryptography in the Internet of Things (IoT). *IEEE Access*, 9, 140843-140858. https://doi.org/10.1109/ACCESS.2021.3121536
2. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194. https://doi.org/10.1038/nature23461
3. Bindel, N., Brendel, J., Fischlin, M., Gonçalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 1831-1848. https://doi.org/10.1145/3319535.3363229
4. Boosten, P., Sattarzadeh, S. M., Van den Berg, H., & De Groot, R. (2021). Security and privacy in the Internet of Medical Things: Taxonomy and challenges. *IEEE Access*, 9, 112996-113017. https://doi.org/10.1109/ACCESS.2021.3102692
5. Chen, L., & Liu, W. (2020). Quantum-resistant public key cryptography: A survey. *IEEE Access*, 8, 186981-187016. https://doi.org/10.1109/ACCESS.2020.3029935
6. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, 6, 22633-22651. https://doi.org/10.1109/ACCESS.2018.2831086
7. Gibson, K., & Zailani, S. (2021). Quantum cryptography in healthcare: Securing medical data in the quantum age. *Journal of Medical Internet Research*, 23(8), e29394. https://doi.org/10.2196/29394
8. Jiang, L., Chen, H., Liu, W., & Wang, H. (2020). Efficient and secure data transmission for smart cities based on post-quantum cryptography. *IEEE Internet of Things Journal*, 7(6), 5357-5370. https://doi.org/10.1109/JIOT.2020.2972537
9. Naehrig, M., Lauter, K., & Vaikuntanathan, V. (2011). Can homomorphic encryption be practical? *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, 113-124. https://doi.org/10.1145/2046660.2046682
10. NIST. (2017). Post-quantum cryptography: NIST's plan for the future. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8105
11. O'Connell, P., & Helgason, A. (2020). Securing telemedicine through quantum-resistant encryption. *International Journal of Medical Informatics*, 137, 104105. https://doi.org/10.1016/j.ijmedinf.2020.104105
12. Petrenko, O. A., & Grishchenko, I. N. (2021). Quantum key distribution and its application in telemedicine. *Quantum Information Processing*, 20, 264. https://doi.org/10.1007/s11128-021-03195-7
13. Pham, Q.-V., & Pathirana, P. N. (2020). Toward the smart healthcare ecosystem: IoT-enabled architecture and nursing perspective. *IEEE Internet of Things Journal*, 7(11), 11811-11819. https://doi.org/10.1109/JIOT.2020.3002845
14. Rietman, R., & Bamberger, J. (2021). Quantum-safe cryptographic algorithms for secure healthcare communications. *Health Informatics Journal*, 27(4), 14604582211061895. https://doi.org/10.1177/14604582211061895
15. Saadeh, M., & Khatib, T. (2019). A secure and efficient protocol for remote patient monitoring using IoT. *IEEE Transactions on Industrial Informatics*, 15(6), 3562-3571. https://doi.org/10.1109/TII.2019.2905608
16. Singh, K., & Verma, S. (2022). Post-quantum cryptography for IoT devices: Challenges and opportunities. *IEEE Internet of Things Journal*, 9(1), 463-476. https://doi.org/10.1109/JIOT.2021.3076187

17. Steinwandt, R., & Santis, F. D. (2019). Quantum-safe key distribution for the Internet of Things. *IEEE Transactions on Emerging Topics in Computing*, 9(1), 51-63. https://doi.org/10.1109/TETC.2019.2925996

18. Takahashi, K., & Yasunaga, M. (2020). Post-quantum encryption for securing IoT in healthcare. *Journal of Healthcare Engineering*, 2020, 8829834. https://doi.org/10.1155/2020/8829834

19. Wang, H., & Wu, Q. (2019). A review of post-quantum cryptographic schemes and their applications. *Journal of Cryptographic Engineering*, 9(3), 197-217. https://doi.org/10.1007/s13389-019-00206-5

20. Zhang, C., & Xie, J. (2021). Towards secure telemedicine services in IoMT environments using quantum cryptography. *Telemedicine and e-Health*, 27(9), 945-952. https://doi.org/10.1089/tmj.2020.0458