IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 7, July 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

Enhanced Medical Record System Using Embedded Computing Model

Bedford-Fubara, Chioma Onyinyechukwu[1], Prof. Prince .O. Asagba[2]

Department of Computer Science, Ignatius Ajuru University of Education, Rumuolumeni, Port Harcourt, Rivers State, Nigeria[1]

Department of Computer Science, University of Port Harcourt, Choba, Port Harcourt, Rivers State,Nigeria [2]

ABSTRACT:Health information is vital and confidential therefore it should be shared in a secured manner. The problem of data leakage over the internet has infiltrated the management of medical records. As a result of this, people no longer have trust in how their health information is being stored, shared and managed. In this work, an embedded computing model using Support Vector Machine (SVM) Algorithm was developed to enhance the secure management of data in medical record system. The study adopted Object-Oriented System Development Methodology (OOSDM) at the analysis stage of developing the new system rather than at the design stage in order to improve the performance and quality of the new system. In addition to this, the datasets used were trained with Artificial Neural Network (ANN) and Python programming language. Implementation of the new improved medical record system was carried out with Hypertext Preprocessor (PHP) and MySQL. The results obtained from the study after testing the new system showed that it performed better than the existing Computer Aided Search for Epidemics (CASE) system in the following areas: the methodology adopted, the Artificial Intelligence (AI) Technology used, the volume of test-sets used in performance evaluation, the number of created databases, the number of implemented hardware devices, the number of tested records. Also, after comparing the proposed system (improved CASE system) to the existing system (CASE system), the improved CASE system proved to be better in fundamental Internet of Things (IoT) parameters such as trust, security, confidentiality and privacy. Hence, the study highly recommends the application of unique IoT biometric system like a finger-print scanner, embedded with Radio Frequency Identification (RFID) technology alongside support vector machine algorithm will ensure security in how patients' medical records are computed. Thus, this approach gives users sole access to their medical records that can be shared only with their permission.

KEYWORDS:Medical Record, Security, Embedded System, Internet of Things, Computing Model.

I. INTRODUCTION

An embedded system is the hybrid of computer hardware and software designed for a specific function or functions within a larger system. Complexities range from a single microcontroller to a suite of processors with connected peripherals and networks; from no user interface to complex graphical user interfaces. The complexity of an embedded system varies significantly depending on the task for which it is designed. They can be linked to databases using various technologies such as Radio Frequency Identification (RFID). Embedded systems are managed by microcontrollers or digital signal processors (DSP), application-specific integrated circuits (ASIC), field-programmable gate arrays (FPGA), GPU technology, and gate arrays. These processing systems are integrated with components dedicated to handling electric and/or mechanical interfacing [1].

The Internet of Things (IoT) is a new technology of the Internet accessing physical objects. Internet of Things enables objects recognize themselves and obtain intelligent behaviour that prompts them to make related decisions on account of the fact that they can communicate information with themselves. These objects can access information that has been aggregated by other things, or they can be added to other services. The Internet of Things (IoT) is the interconnection of physical objects such as vehicles, home appliances, and other items embedded with electronic software, sensors, and connectivity which enable these objects to connect and exchange data. Secondly, the general concept of the Internet of Things (IoT) is to effectively manage big data of physical objects on the internet. Internet of Things is a technology that functions using the Internet. But with small, powerful wireless solutions such as smart health devices; e.g smart BP monitors, smart pulse rate checker etc which can be connected through the IoT, it is now possible for monitoring to come to these patients. These solutions can be used to securely capture patient health data from a variety of sensors, apply complex algorithms to analyze the data and then share it through wireless connectivity with medical professionals who can make appropriate health recommendations.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

A close attention in the application of IoT in medical field is one that requires hospitalized patients whose physiological status need to be monitored continuously.

II. RELATED WORK

A hybrid security model for securing the diagnostic text data in medical images was researched by [2]. Their model was developed through integrating a steganography technique with a hybrid encryption scheme. The hybrid encryption scheme was built using a combination of Advanced Encryption Standard, and Rivest, Shamir, and Adleman algorithms. This model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image. However, analysis of the study showed that the authors failed to implement their design in a way that a patient can have access to his medical records for further clarification and understanding.

The principles of security for Embedded Systems were looked into by [3]. According to the study, trusted computing is a delicate and important factor considered in many automated domains. Those involved in current efforts to achieve trusted computing typically believe that, regardless of what is meant by trusted, their efforts will require a secure infrastructure and development of correct application codes that extend security to enable trusted applications. A trusted computing platform is a computing infrastructure that provides a variety of hardware-supported security functions. Although trust, trusted, and trustworthiness are never defined, it is hoped that trusted computing platforms and resulting improvements in the security in computing infrastructure and applications will enable trustworthy applications and systems.

Software Intelligence (SI): The Future was researched [4]. The authors summarized the state of practice and research of SI, and lays out future research directions for mining software engineering data to enable SI. The authors did a good job but failed to illustrate the drawbacks of software intelligence that could be capitalized by hackers.

[5]looked at Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends and Directions. The purpose of the study was to classify the literature, including publication year, authors, scientific sector, country, institution, and keywords. However, a major limitation of their study is that the reviewed issues were deficient in benchmarking and cost benefits analysis.

The development of computer-aided design software for the qualitative evaluation of aesthetic damage was proposed by [6]. The objective of the study was to develop computer-aided design software for aesthetic damage quantification/evaluation. However, a major limitation of their study is that the developed model was deficient in benchmarking and cost benefits analysis.

[3]researched on design science in decision support systems research. According to the authors, “design science has been an important strategy in decision support systems (DSS) research since the field’s inception in the early 1970s”. However, analysis of the study showed that the author failed to implement the discussed decision support system methods to a model for further clarification and understanding.

A secure framework for database in cloud computing was studied by [7]. In the study, the authors proposed the data on cloud computing is encrypted due to security concern or the factor of third party digging into it. However, a major limitation of their study is that the developed model was deficient in benchmarking and cost benefits analysis.

The developed framework in the study is described with an acronym called CASE, which stands for Computer Assisted Search for Epidemics. CASE uses data retrieved from SmiNet to perform outbreak detection. A case report is created in SmiNet when a clinical or a laboratory report is received, provided that this patient does not already exist in the database. When additional reports arrive, the original case report is automatically updated with the new information. Depending on the number of days that have elapsed since the last time a patient received a particular diagnosis, a new case report might be created for the same diagnosis and patient. The extraction component populates the local database with data from the case reports stored in SmiNet. Diagnosis, lab species, date, and reporting county are copied for every case, except those with infections that are reported to have originated abroad. No information that can reveal a patient's identity is used in the outbreak detection process. There are approximately twenty dates in SmiNet for each case report, ranging from dates that are automatically generated by the system to dates entered by the clinician or the laboratory. There is, however, only one date that is available on all case reports, namely statistics date. However, [8] failed to implement the discussed CASE with a secured embedded IoT device.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

III. ANALYSIS

A. Analysis of the Existing System

The existing embedded system is CASE (Computer Assisted Search for Epidemics): an Untrusted Embedded framework for Medical Information System used in supporting outbreak detection as shown in Fig. 1. The CASE was designed to automatically detect and trace unsuspected carriers of epidemic. This is because; studies of partly automated contact tracing generally reported more complete contact identification and follow-up compared with manual systems. Furthermore, the CASE contact tracing could potentially reduce transmission with sufficient population uptake. However, concerns regarding privacy and equity should be considered. Well-designed prospective studies are needed given gaps in evidence of effectiveness, and to investigate the integration and relative effects of manual and automated systems. Large-scale manual contact tracing is therefore still an important key in most contexts. Typically, the limitations of contact tracing by CASE include incomplete or incorrect recall of contact events by cases; the time taken to notify contacts manually, which can delay quarantine; and the fact that it is often resource intensive and time consuming.

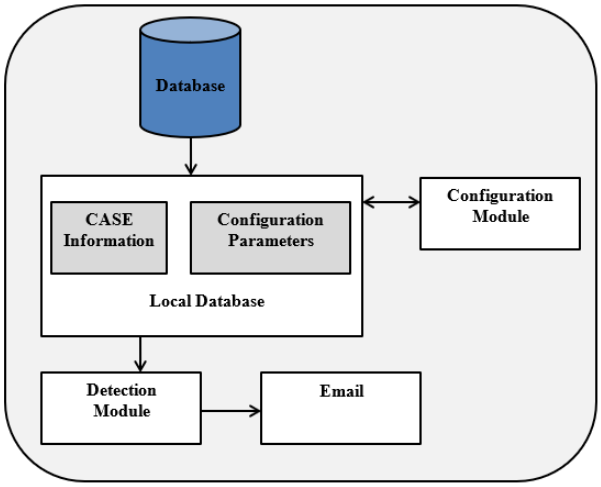


Fig. 1. Existing System Architecture of CASE: an Untrusted Embedded framework for Medical Information System used in supporting outbreak detection
(Source: [8])

1) Description of the Existing CASE Embedded System

The following components of the existing system are:

i) Database: This component illustrates an organized and centralized collection of health data of different individuals that resides in a country.

ii) Local Database: This component illustrates a storage section for two sub-component namely CASE information and configuration parameters. The CASE sub-component illustrates Computer Assisted Search for Epidemics. The system is currently in use at the Swedish Institute for Infectious Disease Control (SMI) and performs daily surveillance using data obtained from SmiNet, the national notifiable disease database in Sweden. Furthermore, the configuration parameter sub-component is used for a wide range of services, from basic to specific server operations, and for performance tuning.

iii) Configuration Module: The configuration component is a graphical user interface that allows the administrator to mark diseases for detection, choose the detection methods to be applied to each diagnosis/subtype and manage the list of epidemiologists that will receive alerts in case a warning is generated. The settings are stored in a local database that is also accessed by the other two components. The system can be administered by multiple users who access the same local database.

iv) Detection and Email Modules: The detection component is executed automatically after all required data have been extracted from the Database. It applies the detection methods with the given parameters to the case data for the selected diseases, and emails notifications if any alerts are generated. Detailed logs of these processes are generated automatically.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

2) Disadvantages of the Existing System (CASE Embedded System)

The following disadvantages of the CASE Embedded System are:

i) Security and latencies issues, due to the lack of an IoT embedded device to provide trust and confidentiality when processing the health data of different individuals.

ii) With most embedded devices getting connected to the Internet, the information risk due to its value, and the risk associated with information storage, transfer, and duplication is high. The critical aspect of this information in the embedded world is that the majority of this information has a direct impact on the physical world., and emails notifications if any alerts are generated. Detailed logs of these processes are generated automatically.

B. Proposed System (Improved CASE Embedded System)

We intend to enhance the CASE embedded system developed by Baki et al (2018) with a Secured Embedded System using an RFID (Radio Frequency Identification) IoT Technology and SVM algorithm for trusted computing of health Information Systems as shown in fig. 2. The Improved CASE Embedded System will integrate fingerprinting in the computing of patients' medical records after an ailment has been detected; and further secure trust in the process. This is because the Internet of Things (IoT) is already one of the dominating technologies presently due to the fact that it enables communication by making networking accessible anytime, anywhere. Security for IoT will be given more focus as the principle needs to unite different technologies and have to communicate with diverse kind of networks.

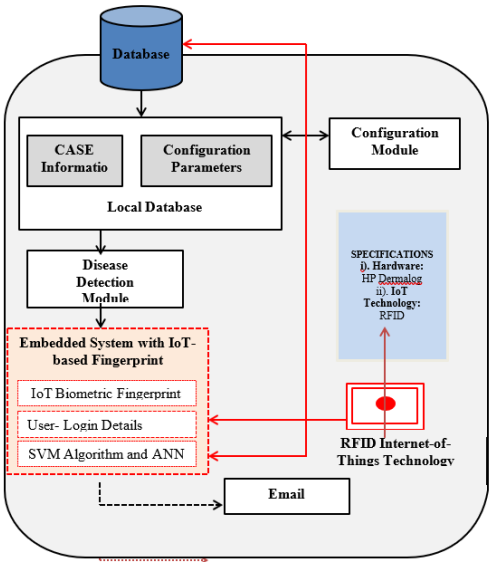


Fig. 2. Architecture of the Proposed System (Improved CASE Embedded System)

IV. METHODOLOGY

Many system methodologies are available to structure, plan and control the overall activities involved in the optimization of the existing system or development of the new system. These methodologies combine set of principles, practices and processes that allows the development of systems quickly and properly. This research work will be achieved following the Object-Oriented System Development Methodology (OOSDM). This is aimed at viewing, modeling and implementing the proposed system as a collection of interacting classes and objects. OOSDM is adopted because it is more effective, efficient, reliable, reusable and a faster way of developing systems.

V. EXPERIMENTAL RESULTS

Fig. 3, shows the welcome page of the Improved CASE Embedded System. The welcome page contains animated backgrounds and three navigation links namely home, register and test-set input for health status. The register link navigates a new user to the registration page (Fig. 4), while the test-set link navigates a registered user to the login and test-set input page respectively (Fig. 5 and Fig. 6). Fig. 7, shows the IoT biometric fingerprint page in which the user's data is captured and authenticated by the system. Fig. 8, shows the Disease Detection tracking result page by the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

system. In addition, the proposed system proves that recent advances in information and communication technologies have made the development and operation of complex disease surveillance systems technically feasible.

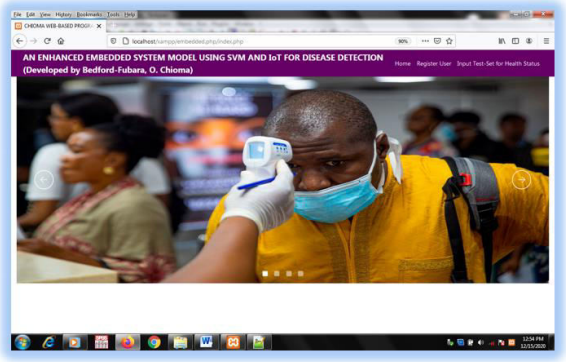


Fig. 3. Welcome Page of the Enhanced CASE Embedded System

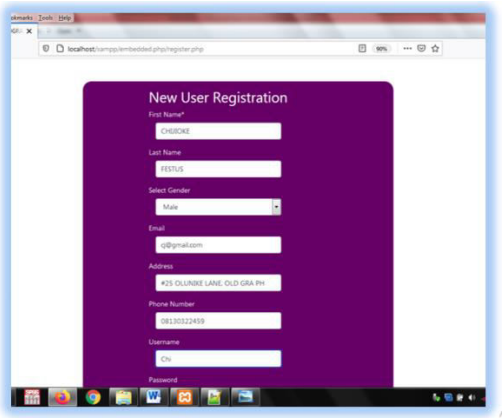


Fig. 4. New User Registration Page

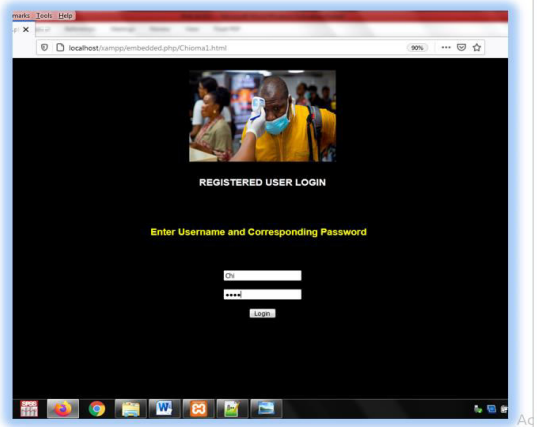


Fig. 5. Login Page for Registered Users

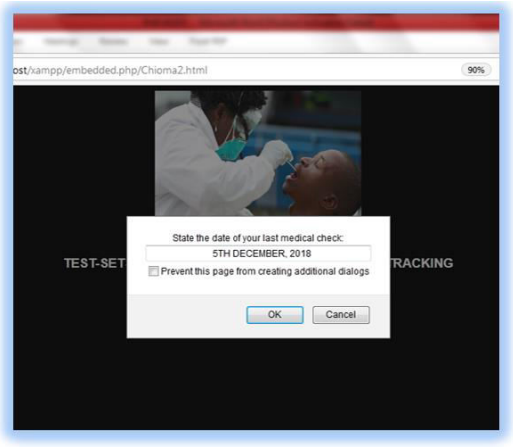
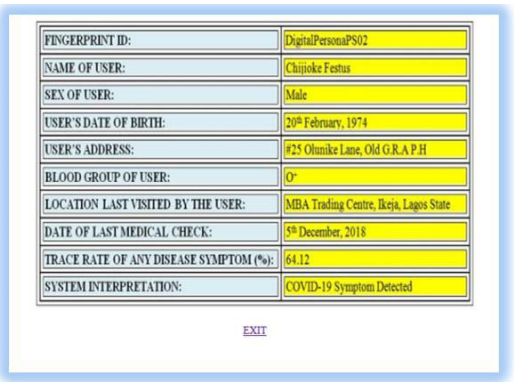


Fig. 6. Test-Set Input Page for Secured Health Tracking

Fig. 7. IoT Biometric Fingerprint Page



FINGERPRINT ID:	DigitalPersonaPS02
NAME OF USER:	Chijioke Festus
SEX OF USER:	Male
USER'S DATE OF BIRTH:	20th February, 1974
USER'S ADDRESS:	#25 Olunike Lane, Old G.R.A P.H
BLOOD GROUP OF USER:	O+
LOCATION LAST VISITED BY THE USER:	MBA Trading Centre, Ikeja, Lagos State
DATE OF LAST MEDICAL CHECK:	5th December, 2018
TRACE RATE OF ANY DISEASE SYMPTOM (%):	64.12
SYSTEM INTERPRETATION:	COVID-19 Symptom Detected

EXIT

Fig. 8. Result Page

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

Table 1.Detected Disease Possibility Calculation for the Proposed System

Positive	TP	FP
Negative	FN	TN

Where

TP = True Positive (the number of cases correctly identified to have COVID-19) = 72

FP = False Positive (the number of cases incorrectly identified to have COVID-19) = 10

FN = False Negative (the number of cases incorrectly identified to not have COVID-19) = 13

TN = True Negative(the number of cases correctly identified to not have COVID-19) = 5

Table 2.Confusion Matrix Table for the Proposed System

	No. of Possibilities for Detected Disease	No. of Possibilities for No Detected Disease	
Disease Occurring	72	5	77
Disease not Occurring	10	13	23
Total Sample	82	18	

To obtain overall accuracy of the Proposed System

$$\text{Accuracy} = \frac{\text{No. of correct possibilities}}{\text{Total number of possibilities made}} \quad (1)$$

$$= \frac{TP + TN}{TP + TN + FP + FN}$$

$$= 72 + 5/72 + 5 + 10 + 13$$

$$= 77/100 = 0.77 = 77\%$$

Misclassification rate (a.k.a. classification error) = (FP+FN) / (TP+TN+FP+FN) (2)

Or 1 – Accuracy of the System = 1 -77% = 0.23 = 23%

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

Table 3.Performance Evaluation Matrix table for the Existing and Proposed Systems

	Accuracy	Classification Error
Disease Occurring	67%	33%
Disease not Occurring		
Percentage of Trained Data	70%	
	Accuracy	Classification Error
Disease Occurring	87%	13%
Disease not Occurring		
Percentage of Trained Data	80%	

Table 1, Table 2, and Table 3, show the comparative analysis and performance evaluation of the CASE Embedded System and Improved CASE Embedded System respectively. Parameters of the result for both systems encompassed the number of adopted algorithms, the number of adopted methods, the number of adopted technologies, the number of created databases, the number of implemented hardware devices, and the number of tested records.

After performance evaluation and accuracy check for the proposed system was carried out, the accuracy of the proposed system was determined to be 77%.

In order to know the strength of the proposed system; a confusion matrix was obtained, for the accuracy and classification error to be computed. The confusion matrix gives a matrix output, and further describes the performance of the model. Accuracy is simply the ratio of number of correct predictions to the total number of input samples. Accuracy is usually called classification accuracy.

Accuracy of the matrix was gotten by obtaining average values which lie across the main diagonal. The True Positive rate is called Sensitivity. It is the portion of positive rate which corresponds to the portion of positive data points that are correctly considered as positive, with respect to all positive data points. True Negative rate is called the specificity. The false positive rate is simply the portion that corresponds to the proportion of negative data points which are correctly considered as negative, with respect to all negative data points. False positive rate is simply the portion that corresponds to the proportion of negative data points that are mistakenly considered as positive, with respects to all negative data points. False Negative rate is simply the number of predictions where the classifier incorrectly predicts the positive class as negative.

The Precision is simply the number of correct positive results divided by the number of positive results predicted by the classifier. Recall is simply the number of correct positive results divided by the number of all relevant samples (all samples that should have been identified as positive). The F1 Score is simply utilized to measure test accuracy; it is also the harmonic mean between precision and recall. The F1 score ranges from [0,1]. It determines how precise your classifier is. Like how many instances is classified correctly. It also tells how robust your classifier is. The F1 score does not miss a significant value of instances. The greater the F1 score the better the performance of the model. Classification Error is one minus the value of accuracy. In addition, comparative analysis of the existing and proposed systems was carried out. The parameters for the analysis encompassed accuracy, classification error, processing speed, and area under curve (AUC). The result values for the Existing System based on the mentioned parameters were 51.67, 38.10, 35.00 and 0.94 respectively, while that for the Proposed System was 77.00, 23.00, 5.33 and 0.97 respectively. In other words, the results clearly showed the proposed system performing better than the existing system. Furthermore, the accuracy of the performance evaluation of both systems was gotten by obtaining average values which lye across the main diagonal. The True Positive rate is called Sensitivity. It is the portion of positive rate which corresponds to the portion of positive data points that are correctly considered as positive, with respect to all positive data points. True Negative rate is called the specificity.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 7, July 2022||

| DOI:10.15680/IJIRSET.2022.1107006 |

The false positive rate is simply the portion that corresponds to the proportion of negative data points which are correctly considered as negative, with respect to all negative data points. False positive rate is simply the portion that corresponds to the proportion of negative data points that are mistakenly considered as positive, with respects to all negative data points. False Negative rate is simply the number of predictions where the classifier incorrectly predicts the positive class as negative. The Precision is simply the number of correct positive results divided by the number of positive results predicted by the classifier. Recall is simply the number of correct positive results divided by the number of all relevant samples (all samples that should have been identified as positive). Fig.9,shows the Existing and Proposed Systems Result, the performance evaluation of the proposed system, and the comparative analysis of both systems.

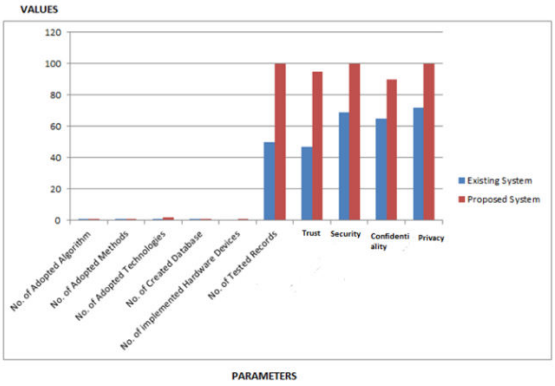


Fig. 9. Comparative Analysis Chart of the Existing and Proposed Systems

VI. CONCLUSION

In this study, we developed a secured embedded system model for health tracking of infectious disease carriers. The developed system intends to optimize trust in embedded system computing. This is because; a secured embedded system model is one that fulfills the expectations of its owners and users. Thus, our research in trusted embedded systems is focused on the design and implementation of embedded systems that can be trusted to fulfill the expectations of their owners and users. It seeks methods that clarify expectations under normal and adverse circumstances, provide dynamic evidence of success or failure, and implement appropriate runtime failure semantics. It recognizes the differences between trust and security and that secure infrastructure is critical to trusted systems whether or not the trusted systems have application-level security requirements.

REFERENCES

[1] F.Jinsong, O. Aling, and F. Chen, "Historical survey of modern embedded systems". ACM Journal of Computing, Vol. 7, No. 10, pp. 21-27, 2014.

[2] Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O., Shawkat, S., Arunkumar, N., and Farouk, A. "Secure medical data transmission model for IoT-based healthcare systems," IEEE Access, 6, 20596-20608. doi: 10.1109/access.2018.2817615, 2018

[3] David, F., and Graham, "Principles of trust for embedded systems". Software Engineering Institute.http://www.sci.cmu.edu, 2012

[4] Ahmed, H., & Tao, X." Software intelligence: The future of mining software engineering data". FoSER Conference 2010, Santa Fe, New Mexico, USA.

[5] C. Raffaele, T., Marta, P., Giuseppina, P., Antonella, and F., Fabio, "Artificial intelligenceand machine learning applications in smart production". Progress, Trends & Directions, Sustainability, Vol. 12, No. 492. doi 10.3390/su12020492, 2020

[6] Nelson, S. Mario, F., Luiz, E., Nigro, M., Juan, P., Ferna, B., &Rogerio, O. "Development of a computer-aided design software for the qualitative evaluation of aesthetic damage". PLos ONE, Vol.12. https://doi.org/10.1371/journal.pone.0226322, 2019.

[7] Abhinay, S., Ashwini, B., Snehal, B., Puja, K., and Shital, K,"Secure framework for database in cloud computing". International Journal of Computer Engineering & Applications, Vol. 13, No. 14, pp. 1-5, 2019

[8] Baki, C., Kenneth, H., Maria, G., Paul, S., and Anette, H. "CASE: A Framework for computer supported outbreak detection". International Journal of Computer Applications (IJCA), Vol. 8, No. 7, pp. 44-53. 2018

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details