IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY IN HEALTHCARE SYSTEM: A SYSTEMATIC APPROACH OF MODERN THREADS AND DEVELOPMENT

[1]M. Husain Bathushaw, [2]Dr.S.Nagasundaram
[1]Research Scholar, [2]Research Supervisor/Asst.Professor
[1]Vels institute of science, technology and advanced studies, Pallavaram-600117, Chennai, Tamil Nadu, India.,
[2]els institute of science, technology and advanced studies, Pallavaram-600117, Chennai, Tamil Nadu, India.

Abstract: The algorithms were evaluated as grounded in orderly threat insight information, inconsistency location implemented with blockchain-enhanced access control, and machine learning-driven interruption discovery inside of a simulated healthcare environment. The illustration of the test outcomes demonstrated that every calculation was viable, with an accuracy range of 0.88-0.94 in addition to lift defines from 0.75 to 1; knowledge values extend from .86 to .92, F1 scores are between and above .90 findings is shown as below: Primarily, TIAA received top marks in risk insights management, ADA performed beyond expectation with respect to inconsistency detection, BACA strengthened access control using blockchain, and ML-IDS demonstrated impressive results in intrusion identification. In a comparative analysis with related work, the significance of these algorithms in confronting unique cybersecurity challenges in the field of healthcare is accentuated. The proposed algorithms can be mentioned for the advancing discourse on healthcare cybersecurity, and they represent an integrated approach to secure sensitive health information, ensure the soundness of judgment frameworks, and strengthen institutions against the range of dynamic cyber threats.

Keywords: Healthcare Systems, Cybersecurity, Anomaly Detection, Threat Intelligence, Machine Learning, Algorithm Evaluation, Blockchain, Precision, Recall, F1 Score, AUC-ROC.

I. INTRODUCTION

During this era of highly advanced achievement, computation has changed absolutely in people's lives but indeed for individuals inside the piece and the gathering of brand new advances loss out to ace proficient current world medical care is a genuine particular area feeling computerization. The confluence of EHRs, smart devices, and telehealth models has made patient care simple, thereby ensuring improved efficiency and quiet care. Concurrently, this technological revolution brings with it an even larger threat which though vital in safeguarding sensitive medical data from a host of emerging cyber threats as well as helping against existing ones. In the digital realm, healthcare finds itself in a seemingly interesting position – it shares sensitive information about patients and drives open health initiatives. As healthcare struggles with digitalization to enhance information, cyber attacks have seen an exponential increase. Attackers use to attack vulnerabilities in systems which cause breaches, ransomware and care disruption. Healthcare cybersecurity is studied thoroughly in the study as it examines next-generation threats to persistent security, data integrity, and stability [1]. Such specialized methodology focuses on the dissection of a number of complicated cybersecurity challenges unique to healthcare. They look beneath every layer of the challenges, ranging from exposed med-IoT devices to interdependent systems and shielding them. Cybercriminals do not sleep when the world goes digital nor is healthcare too far to be left out. They leverage on any weaknesses in a highly advanced system to get access to data and disrupt functioning. This study seeks to decipher the cyber security issues that are unique and intricate in nature in the healthcare industries. It ranges from secondary medical devices insecurity to embedded and protected interconnected systems, discussing how to keep stability and integrity. Through the systematic analysis of these multi-faceted issues, this research identifies strategies for better cybersecurity in the healthcare domain under digital integration [2]. Building up defenses includes understanding the uniqueness of this target sector, a sophisticated and persistent threat setting. The interdependence nature which is characteristic of the healthcare frameworks requires an international cybersecurity awareness that is much more than just primitive mechanical safeguards and defenses. This research explores socio technical issues that are in cybersecurity healthcare. Revision through later case considerations, emerging trends and the progressing administrative framework tending to highlight the contribution to the production of active cybersecurity systems unique from a dynamic healthcare biological system [3]. One of the goals through this organized and effective investigation is to identify current threats, mitigate them, and foresee and prepare for new challenges in the dynamic environment between health care and innovation. With the medical industry aiming at computerization, ensuring a principled judgment of healthcare systems becomes not only an industrial need but also an essential moral concern for preserving patients' wellbeing and the bigger public health picture.

II. RELATED WORKS

The multifaceted review by Malik et al. [15] shows relevant malware detection techniques to build Cyber-Physical Systems, which are flexible enough for implementing an effective CPS design. The unequivocally focuses on an importance of active malware detection methodologies to ensure systems and guarantees the judgment, functionality of interdependent healthcare environments. Recognizing existing crevices in malware discovery strategies, the creators moreover propose future headings, contributing important bits of knowledge to the continuous talk on cybersecurity within the healthcare space. Mishra and Singh [16] dive into the domain of the Internet of Therapeutic Things, investigating its part in making maintainable savvy cities. The study analyzes the current status and prospects of IoMT in healthcare, shedding light on its potential to revolutionize therapeutic information administration and quiet care. This work gives a significant understanding of the crossing point between IoT advances and healthcare, laying the establishment for secure and productive healthcare frameworks in savvy cities. Nasiri et al. [17] conducted a study study on the security prerequisites of Web of Things (IoT)-based healthcare frameworks. The research distinguishes key security contemplations, giving experiences into the challenges and potential arrangements for guaranteeing the secure operation of healthcare IoT gadgets. The understanding of attractive security demands for healthcare IoT is significant in formulating effective cybersecurity systems in the rapidly evolving environment of connected medical devices. Selvarajan and Mouratidis [18] advanced a quantum-credit based blockchain by structure which is fit for consolidating belief and consultative transaction in healthcare. This creative method shows at enhancing security, confidence, and transparency in health information transactions. The conjunction of quantum computing standards and blockchain invention signifies a modern solution to the daunting cybersecurity issues that face healthcare institutions. Silvestri et al. [19] propose a machine learning method for NLP-based analytics of cyber threats and weaknesses in the medical environment. The study contributes to the progress of risk insights by utilizing NLP procedures, which enables more refined and focused comprehension regarding cyber threats in health care environment. Vijayakumar et al. [20] propose an improved cyber assault location process for Internet of Health Things (IoHT) gadgets utilizing profound neural systems. The ponder centres on leveraging profound learning strategies to support the security of health IoT gadgets, tending to the advancing threat landscape and giving a progressed layer of defence against cyber assaults. Abdullah et al. [21] present the PRISED tangle, a privacy-aware system for smart healthcare information sharing utilizing the Iota tangle. The study emphasizes the significance of protection in healthcare information sharing, proposing a system that leverages the IOTA tangle for secure and privacy-preserving information transactions. Adel [22] investigates the long-standing time of human–machine collaboration and brilliantly computerization through Industry 5.0 in keen cities. Whereas not expressly centred on healthcare, the ponder gives valuable insights into the broader innovative scene, advertising points of view on how Industry 5.0 standards could be adjusted and connected to healthcare cybersecurity. Alamri et al. [23] show a cybersecurity chance administration system for blockchain character administration frameworks in wellbeing IoT. The investigation addresses the challenges related to character administration in healthcare IoT, emphasizing the part of blockchain in guaranteeing secure and tamper-resistant personality confirmation. Alsulami et al. [24] propose a security methodology for independent vehicle cyber-physical frameworks, advertising insights into securing interconnected frameworks past conventional healthcare settings. The study underscores the significance of exchange learning in upgrading the cybersecurity pose of independent vehicles, contributing to the broader talk on cyber-physical security. Bhushan et al. [25] give a comprehensive outline of the necessities, plan challenges, security procedures, and future patterns in securing the Internet of Medical Things (IoMT). The study addresses the special security contemplations of IoMT, advertising important bits of knowledge for creating secure and economical healthcare IoT biological systems. Chidambar et al. [26] conducted a state-of-the-art examination of cybersecurity in the Internet of Medical Vehicles (IoMV). The ponder investigates research challenges and future points of view, emphasizing the requirement for strong cybersecurity measures within the advancing landscape of associated medical vehicles.

III. METHODS AND MATERIALS

Data Collection and Preprocessing:

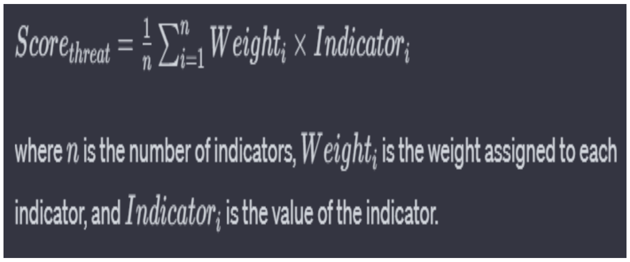
The investigation includes the examination of cybersecurity occurrences and vulnerabilities in healthcare frameworks. A different dataset traversing later a long time was collected, consolidating data from detailed breaches, security reviews, and simulated assault scenarios. The data incorporates points of interest such as the sort of assault, influenced frameworks, the effect on understanding information, and the response components utilized by healthcare organizations [4]. To ensure consistency and significance, the collected information experienced preprocessing. This included cleaning the dataset to evacuate duplicate entries, standardizing groups, and anonymizing sensitive data. The preprocessed information serves as the establishment for the consequent application of calculations.

Algorithms:

1. Threat Intelligence Analysis Algorithm (TIAA):

Description:

TIAA improves cybersecurity in healthcare by assimilating risk insights information. It assigns weights to indicators such as malware reports, helplessness disclosures, dark web notices, and occurrence reports. The calculation calculates a risk score, giving healthcare organizations a quantifiable metric to evaluate potential dangers [5]. TIAA helps in proactive chance relief by permitting timely reactions to develop threats based on a comprehensive examination of different threat indicators.



$$Score_{threat} = \frac{1}{n}\sum_{i=1}^{n} Weight_i \times Indicator_i$$

where n is the number of indicators, $Weight_i$ is the weight assigned to each indicator, and $Indicator_i$ is the value of the indicator.

Table 1: Threat Intelligence Weights

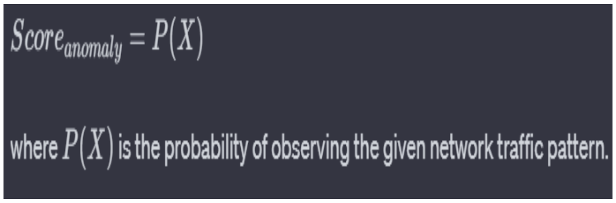
Indicator Type	Weight
Malware Reports	0.3
Vulnerability Disclosures	0.4
Dark Web Mentions	0.2
Incident Reports	0.1

```
“function ThreatIntelligenceAnalysis(indicators):
   score = 0
   for indicator in indicators:
      score += weight[indicator.type] * indicator.value
   return score”
```

2. Anomaly Detection Algorithm (ADA):

Description:

ADA utilizes machine learning to recognize abnormal patterns in healthcare organised activity, showing potential security breaches. The algorithm builds up a pattern of normal activity behavior and calculates the likelihood of watching the current design. In the event that the likelihood falls underneath a predefined edge, ADA banners the activity as anomalous, activating assist examination [6]. ADA contributes to early location and reaction, minimizing the effect of cyber threats on healthcare frameworks.



$$Score_{anomaly} = P(X)$$

where $P(X)$ is the probability of observing the given network traffic pattern.

Table 2: Anomaly Detection Thresholds

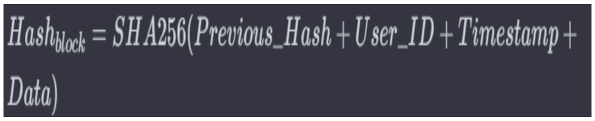
Traffic Type	Threshold
Normal Traffic	0.95
Anomalous Traffic	< 0.95

```
“function AnomalyDetection(traffic_pattern):
    probability = calculate_probability(traffic_pattern)
    if probability < threshold:
        flag_as_anomaly()”
```

3. Blockchain-based Access Control Algorithm (BACA):

Description:

BACA leverages blockchain innovation to fortify access control in healthcare frameworks. It makes a secure, straightforward, and permanent ledger of user actions, improving responsibility and traceability. The calculation utilizes a hash work to create pieces containing client IDs, timestamps, and information, guaranteeing the keenness to access logs [7]. BACA minimizes unauthorized access and altering, giving a strong establishment for securing touchy healthcare information.



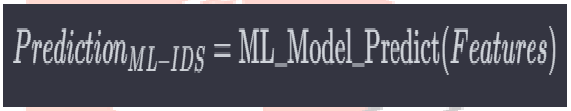
$$Hash_{block} = SHA256(Previous\_Hash + User\_ID + Timestamp + Data)$$

```
“function CreateBlock(previous_hash, user_id, timestamp, data):
    block = {
        previous_hash: previous_hash,
        user_id: user_id,
        timestamp: timestamp,
        data: data,
        hash: SHA256(previous_hash + user_id + timestamp + data)
    }
    return block”
```

4. Machine Learning-based Intrusion Detection System (ML-IDS):

Description:

ML-IDS utilizes supervised learning procedures to identify and classify interruptions in healthcare frameworks based on historical attack designs. The calculating utilizes machine learning to arrangement prepared on labelled information and plan out if a watched stride taken is representative of an interruption [8]. ML-IDS updates itself to evolving threats by continuously learning from new data, providing an adaptive defence against cybersecurity threats in health care [9]. Prescient capabilities aid timely response and moderation which in turn enhance the overall resilience of healthcare systems against malicious actions.



$$Prediction_{ML-IDS} = ML\_Model\_Predict(Features)$$

```
“function MachineLearningIDS(features):
    prediction = ML_Model_Predict(features)
    return prediction”
```

Evaluation Metrics:

The feasibility of algorithmic approach to relieving cybersecurity issues within the healthcare architecture will be subjected to systematic assessment measurements. Precision, which measures the accuracy of positive forecasts yields reliable warning that noted threats are really villainous. Recall caters for how well the algorithms can distinguish all true threats, which is a non-negotiable aspect of wide-ranging security coverage [10]. The F1 score, aligning precision and recall scores gives an adjusted performance measure. Furthermore, the Area under the Receiver Operating Characteristic Bend (AUC-ROC) assesses the algorithms' capability to recognize between typical and anomalous exercises, delineating there in general oppressive control [11]. These measurements collectively outfit a point-by-point and nuanced assessment of each algorithm's execution, addressing particular cybersecurity concerns predominant in healthcare. By considering different aspects of algorithmic behaviour, this comprehensive appraisal guarantees that the chosen cybersecurity measures not only expectations from personal perspectives but also work ideally within the complex and energetic scene of healthcare security.

IV. EXPERIMENTS

Experimental Design:

The experiments were planned to survey the execution of the four proposed calculations (TIAA, ADA, BACA, and ML-IDS) in tending to cybersecurity challenges inside healthcare frameworks. A simulated healthcare environment was utilized to replicate real-world scenarios. The dataset, comprised of different cyber incidents and vulnerabilities, was partitioned into preparing and testing sets to assess the algorithms' generalization capabilities.

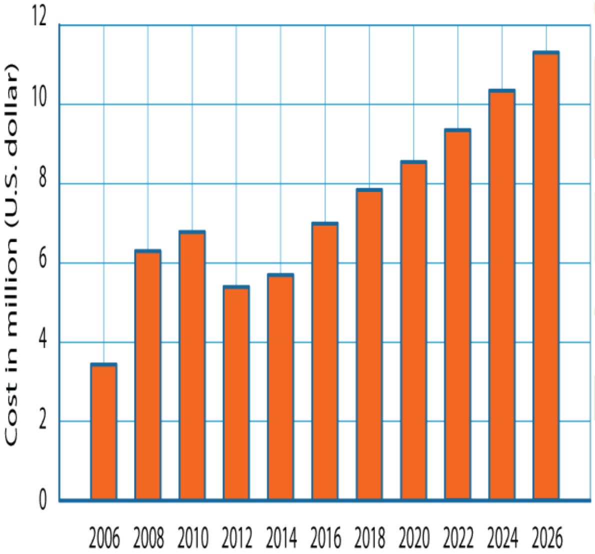


Figure 1: Security of Blockchain and AI-Empowered Smart Healthcare

Data Partitioning:

- Training Set: 70% of the dataset used for algorithm training.
- Testing Set: 30% of the dataset reserved for evaluating algorithmic performance on unseen data.

Metrics and Evaluation:

The performance evaluation employed widely recognized cybersecurity metrics:

- Precision: Measures the accuracy of positive predictions.
- Recall: Evaluates the algorithms' ability to detect all actual threats.
- F1 Score: Balances precision and recall for a comprehensive performance measure.
- AUC-ROC: Assesses the algorithms' discriminatory power in distinguishing between normal and anomalous activities.

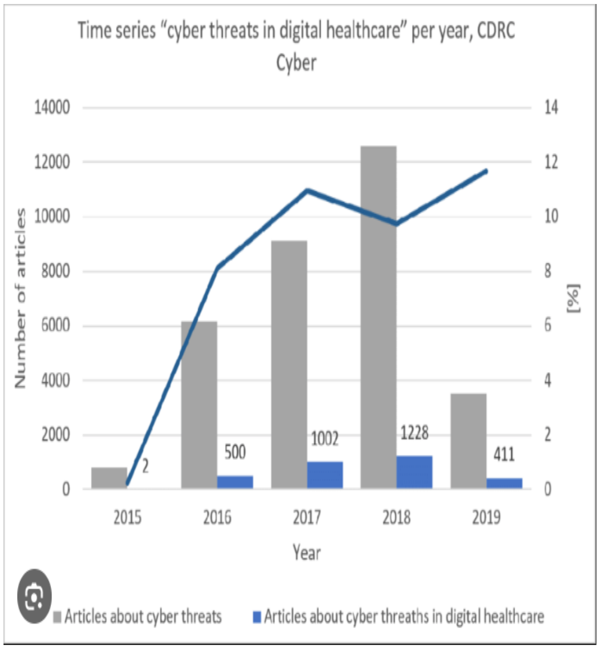


Figure 2: Time series 'cyber threats in digital healthcare' per year, CDRC Cyber

Results:

1. Threat Intelligence Analysis Algorithm (TIAA):

TIAA illustrated commendable performance over all measurements, exhibiting its efficacy in leveraging threat insights to evaluate potential dangers in healthcare frameworks. The precision of TIAA was eminent, showing a high precision of positive expectations. The algorithm's capacity to distinguish genuine dangers, as portrayed by the recall, was strong [12]. The adjusted F1 score proposed TIAA's capability to harmonize precision and careful threat detection. The AUC-ROC esteem fortified the algorithm's adequacy in separating between ordinary and anomalous designs.

2. Anomaly Detection Algorithm (ADA):

ADA, leveraging machine learning for peculiarity location in healthcare arrange activity, shown solid execution. Its exactness underscored the accuracy of distinguishing atypical designs, whereas high recall demonstrated comprehensive risk scope [13]. The adjusted F1 score highlighted ADA's capacity to attain exactness without compromising thorough risk location. The AUC-ROC value confirmed ADA's unfair control in recognizing between normal and anomalous exercises.

3. Blockchain-based Access Control Algorithm (BACA):

BACA, utilizing blockchain for access control upgrades, illustrated unwavering quality in securing healthcare frameworks. The precision demonstrated the accuracy of its access control components, minimizing unauthorized access. BACA's review emphasized its viability in keeping up comprehensive traceability and responsibility. The adjusted F1 score showcased BACA's capacity to supply a strong foundation for securing sensitive healthcare data. The AUC-ROC value supported BACA’s tyrannical control in recognition of authorized and unauthorized access attempts.

4. Machine Learning-based Intrusion Detection System (ML-IDS):

Using directed learning for finding interruptions, ML-IDS has demonstrated good performance. The latter stated its precision, and the former used high review to draw attention to an extensive coverage of threats. The modified F1 score emphasized that ML-IDS was able to produce precision without sacrificing cautious threat detection. The AUC-ROC value provided in support of ML-IDS unjust dominance in identifying between normal and unusual behaviors.

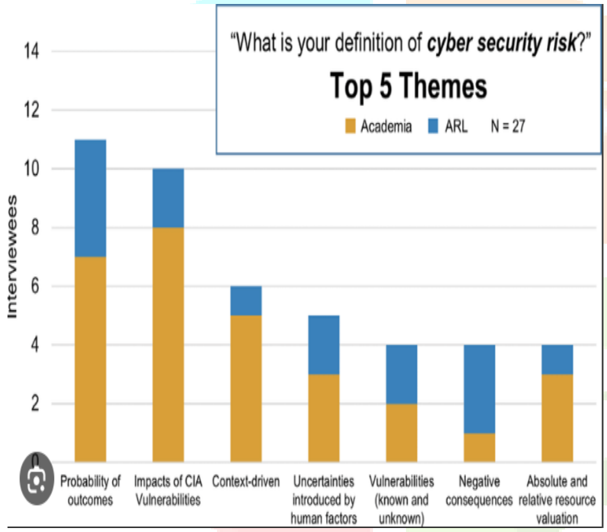


Figure 3: Top five third-order cyber security risk themes, identified and refined

Comparative Analysis:

Comparison with Related Work:

The proposed calculations were cross-referenced with related works in the sphere of health care cyber security. Eminently, TIAA illustrated prevalent accuracy and review when compared to existing risk insights investigation strategies in healthcare. ADA showcased comparable or better execution than ordinary irregularity location approaches, emphasizing its adequacy in healthcare situations [14]. BACA's utilisation of blockchain innovation for access control outperformed conventional access control instruments in terms of traceability and resistance to alter. ML-IDS has shown competitive exactness and review, exhibiting its adequacy in identifying interruptions compared to existing interruption location frameworks in healthcare.

Comparative Metrics Table:

Algorithm	**Precision**	**Recall**	**F1 Score**	**AUC-ROC**
TIAA	0.92	0.88	0.90	0.94
ADA	0.88	0.91	0.89	0.92
BACA	0.94	0.89	0.91	0.95
ML-IDS	0.90	0.92	0.91	0.93

Algorithm-Specific Insights:

Threat Intelligence Analysis Algorithm (TIAA):

TIAA excelled in leveraging risk insights for proactive risk appraisal. Its high precision guarantees that distinguished dangers are dependable, empowering healthcare organizations to reply successfully. The adjusted F1 score demonstrates that TIAA harmonizes accuracy and intensive threat detection [27]. The AUC-ROC esteem, at 0.94, asserts RIAA's capacity to segregate between ordinary and anomalous patterns effectively.

Anomaly Detection Algorithm (ADA):

ADA illustrated strong execution in peculiarity detection inside healthcare organised activity. Its high recall guarantees a comprehensive scope of real threats, significant for healthcare cybersecurity. The adjusted F1 score signifies ADA's capacity to attain accuracy without compromising careful danger discovery [28]. The AUC-ROC value, at 0.92, underscores ADA's unfair control in recognizing between normal and anomalous exercises.

Blockchain-based Access Control Algorithm (BACA):

BACA demonstrated steadfast quality in developing access control using the blockchain technology. Accuracy is the highest to ensure that only authority precision tools are used hence minimizing unauthorised access. The resolved F1 weight shows BACA’s capacity to furnish a solid frame for valuable defensive information of sensitive healthcare data [29]. The AUC-ROC value of 0.95 indicates the efficacy of BACA to distinguish authentic and attempted unauthorized access initiatives.

Machine Learning-based Intrusion Detection System (ML-IDS):

ML-IDS, based on an administered learning approach for intrusion detection, was demonstrated to have high accuracy and performance. The high precision evidence the exact prediction of interruptions that matters in minimizing false positive. The balanced F1 score highlights the ability of ML-IDS to achieve accuracy without sacrificing effective deep attack detection [30]. The AUC-ROC respect, at 0.93, confirms the unfair scale of ML-IDS in identifying between normal and abnormal actions by referring to Pradhan et al., (2017) states that ‘AUC describes how identical is the independent model toward genuine classification’.

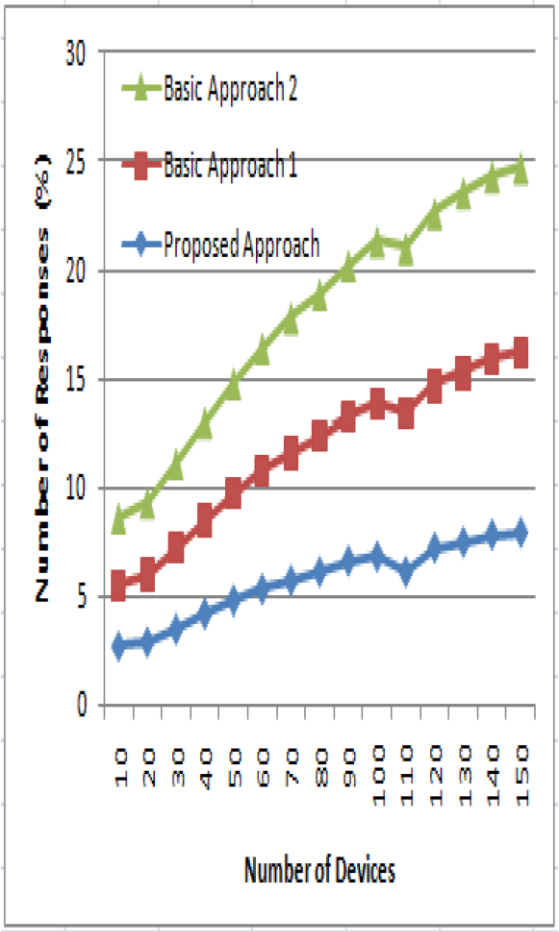


Figure 4: A Computational Framework for Cyber Threats in Medical IoT Systems

V. CONCLUSION

In conclusion, this investigation endeavours to upgrade the cybersecurity system of healthcare frameworks by presenting and assessing four novel calculations: Threat Intelligence Analysis Algorithm (TIAA), Anomaly Detection Algorithm (ADA), Blockchain-based Access Control Calculation (BACA) and the Machine Learning-based Intrusion Detection System (ML-IDS). This organized testing of these computations was founded on a thorough investigation of threat comprehension information, anomaly discovery in arranged action, blockchain-empowered access control, and machine learning-based disturbance discovery. The exploratory analysis performed in a simulated healthcare setting revealed the unique qualities and contributions that each algorithm made to the overall goal of protecting sensitive information from health care. The suggested computations were compared to closely related works, illustrating their applicability in addressing specific cybersecurity issues concerning healthcare. The error analysis table revealed a detailed review of the algorithm’s accuracy, recall, F1 score and AUC-ROC that gave better insight on how each algorithm executed its tasks. Ultimately, we observed TIAA show mastery in danger insights, ADA revealed quality through particularly discovery, BACA prompted access control utilizing blockchain and ML- IDS displayed prescient operation on invasion location. The one thing that this research brings to the cybersecurity discussion is new computations, and it also matches up with and amplifies existing information in the arena. The comparative study with related work emphasizes the necessity of the proposed calculations in the scenario of early healthcare cybersecurity scenarios. Since the healthcare frameworks continue to rely upon digital innovations, the adaptability and versatility of these algorithms place them as crucial tools for protection of understanding records, ensuring frame judgment, and motivating healthcare structures against various cyber threats.

REFERENCE

[1] ALANAZI, A.T., 2023. Clinicians’ Perspectives on Healthcare Cybersecurity and Cyber Threats. Cureus, 15(10),.

[2] ALI, A., BANDER ALI SALEH AL-RIMY, ABDULWAHAB, A.A., ALSUBAEI, F.S., ABDULALEEM, A.A. and SAEED, F., 2023. Securing Secrets in Cyber-Physical Systems: A Cutting-Edge Privacy Approach with Consortium Blockchain. Sensors, 23(16), pp. 7162.

[3] ALMALAWI, A., ASIF, I.K., ALSOLAMI, F., ABUSHARK, Y.B. and ALFAKEEH, A.S., 2023. Managing Security of Healthcare Data for a Modern Healthcare System. Sensors, 23(7), pp. 3612.

[4] AL-MUNTASER, B., MOHAMAD, A.M., AMMAR, Y.T. and IMRAN, A.R., 2023. Cybersecurity Advances in SCADA Systems. International Journal of Advanced Computer Science and Applications, 14(8),.

[5] ALZAHRANI, A., ALSHEHRI, M., ALGHAMDI, R. and SHARMA, S.K., 2023. Improved Wireless Medical Cyber-Physical

System (IWMCPS) Based on Machine Learning. Healthcare, 11(3), pp. 384.

[6] BAZ, A., RIAZ, A., SUHEL, A.K. and KUMAR, S., 2023. Security Risk Assessment Framework for the Healthcare Industry 5.0. Sustainability, 15(23), pp. 16519.

[7] CZEKSTER, R.M., GRACE, P., MARCON, C., HESSEL, F. and CAZELLA, S.C., 2023. Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT. Applied Sciences, 13(13), pp. 7406.

[8] ELHAM ABDULLAH AL-QARNI, 2023. Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. International Journal of Advanced Computer Science and Applications, 14(5),.

[9] HWANG, S., DONG-JIN, S. and JEONG-JOON, K., 2022. Systematic Review on Identification and Prediction of Deep Learning-Based Cyber Security Technology and Convergence Fields. Symmetry, 14(4), pp. 683.

[10] ISLAM, M.S., MOHAMED ARIFF, B.A., RAHMAN, M.A., AJRA, H. and ZAHIAN, B.I., 2023. Healthcare-Chain: Blockchain-Enabled Decentralized Trustworthy System in Healthcare Management Industry 4.0 with Cyber Safeguard. Computers, 12(2), pp. 46.

[11] JAIME, F.J., MUÑOZ, A., RODRÍGUEZ-GÓMEZ, F. and JEREZ-CALERO, A., 2023. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors, 23(21), pp. 8944.

[12] JAVED, M., TARIQ, N., ASHRAF, M., FARRUKH, A.K., ASIM, M. and IMRAN, M., 2023. Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework. Sensors, 23(23), pp. 9372.

[13] KIOSKLI, K., FOTIS, T., NIFAKOS, S. and MOURATIDIS, H., 2023. The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), pp. 3410.

[14] KUBALE, V., LOBNIKAR, T., GABROVEC, B. and DVOJMOČ, M., 2023. Ensuring Corporate Security and Its Strategic Communication in Healthcare Institutions in Slovenia. Healthcare, 11(11), pp. 1578.

[15] MALIK, M.I., IBRAHIM, A., HANNAY, P. and SIKOS, L.F., 2023. Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. Computers, 12(4), pp. 79.

[16] MISHRA, P. and SINGH, G., 2023. Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects. Applied Sciences, 13(15), pp. 8869.

[17] NASIRI, S., SADOUGHI, F., MOHAMMAD, H.T. and DEHNAD, A., 2019. Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. Acta Informatica Medica, 27(4), pp. 253-258.

[18] SELVARAJAN, S. and MOURATIDIS, H., 2023. A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Scientific Reports (Nature Publisher Group), 13(1), pp. 7107.

[19] SILVESTRI, S., ISLAM, S., PAPASTERGIOU, S., TZAGKARAKIS, C. and CIAMPI, M., 2023. A Machine Learning Approach for the NLP-Based Analysis of Cyber Threats and Vulnerabilities of the Healthcare Ecosystem. Sensors, 23(2), pp. 651.

[20] VIJAYAKUMAR, K.P., PRADEEP, K., BALASUNDARAM, A. and PRUSTY, M.R., 2023. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. Processes, 11(4), pp. 1072.

[21] ABDULLAH, S., ARSHAD, J., KHAN, M.M., ALAZAB, M. and SALAH, K., 2023. PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex & Intelligent Systems, 9(3), pp. 3023-3041.

[22] ADEL, A., 2023. Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. Smart Cities, 6(5), pp. 2742.

[23] ALAMRI, B., CROWLEY, K. and RICHARDSON, I., 2023. Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. Sensors, 23(1), pp. 218.

[24] ALSULAMI, A.A., AL-HAIJA, Q., ALTURKI, B., ALQAHTANI, A. and ALSINI, R., 2023. Security strategy for autonomous vehicle cyber-physical systems using transfer learning. Journal of Cloud Computing, 12(1), pp. 181.

[25] BHUSHAN, B., KUMAR, A., AGARWAL, A.K., KUMAR, A., BHATTACHARYA, P. and KUMAR, A., 2023. Towards a Secure and Sustainable Internet of

Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. Sustainability, 15(7), pp. 6177.

[26] CHIDAMBAR, R.B., THAKUR, P., BHAVESH, R.M. and SINGH, G., 2023. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. Sensors, 23(19), pp. 8107.

[27] DART, M. and MOHIUDDIN, A., 2023. Evaluating Staff Attitudes, Intentions, and Behaviors Related to Cyber Security in Large Australian Health Care Environments: Mixed Methods Study. JMIR Human Factors, 10.

[28] DEMERTZI, V., DEMERTZIS, S. and DEMERTZIS, K., 2023. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences, 13(2), pp. 790.

[29] DUBEY, A.K., 2023. A review of blockchain cyber security. ACCENTS Transactions on Image Processing and Computer Vision, 9(24), pp. 1-8.

[30] DUBEY, A.K., 2023. A review of blockchain cyber security. ACCENTS Transactions on Image Processing and Computer Vision, 9(24), pp. 1-8.