GMR
The Original

A SURVEY ON ENHANCING HEALTHCARE SECURITY: INTEGRATING NLP, DEEP LEARNING, AND BLOCKCHAIN TECHNOLOGIES

Sweety Singhal[1*], Dr. Uma Sharma[2]

[1]Department of Computer Science & Engineering, Banasthali Vidyapeeth, Jaipur, India, sweetysinghal55@gmail.com
[2]Department of Computer Science & Engineering, Banasthali Vidyapeeth, Jaipur, India, uma.sharma@banasthali.in
*Corresponding Author: Sweety Singhal

ABSTRACT
The healthcare ecosystem comprises various types of sensitive data, from patient records and clinical notes to diagnostic results and other private information protected by HIPAA. Even though traditional solutions can effectively address most security challenges, they often lack in their capabilities. Robust encryption techniques are developed with deep learning algorithms. These algorithms use their ability to detect complex patterns to identify security threats, thus making the entire healthcare system more resilient. NLP, when combined with deep learning, enables anonymization and de-identification of patient data, thereby allowing sharing of data and collaboration between healthcare providers without compromising patient privacy. This is especially important not just in medical research but also in telemedicine, where the dissemination of data is critical for improved treatment and health outcomes. Natural language processing in healthcare: Techniques and methods for securing data. With the widespread adoption of NLP for processing sensitive health information, protecting patient data is paramount. To help safeguard sensitive information such methods are used: data encryption, differential privacy, tokenisation, and access control.

KEYWORDS: healthcare ecosystem, patient data, security, privacy, deep learning, encryption, NLP, anonymization, de-identification, federated learning, blockchain, medical research

INTRODUCTION

The emergence of digital technology has significantly impacted the healthcare sector, resulting in major changes in the delivery and management of health services. [29] Electronic Health Records (EHRs), telemedicine and in different forms have enhanced patient care, optimized workflows and enabled medical research. The digitalization mentioned above has raised considerable security and privacy issues, making the healthcare domain more vulnerable to various cyber-attacks [7]. However, NLP (Natural Language Processing) & Deep Learning have emerged as powerful tools to address these challenges. Natural Language Processing (NLP), a branch of AI that focuses on human-computer communication, can automatically find, extract, and classify sensitive data and information within vast volumes of unstructured textual content. It helps to ensure the right handling of sensitive data. Deep learning, a subfield of machine learning, uses artificial neural networks to model complex patterns and relationships with high-level abstractions. Moreover, these algorithms might trigger real-time alerts on deviations and possible security violations, empowering the healthcare industry with a preventive defence mechanism [5]. By being trained on extremely large data sets, deep learning algorithms can discover complicated relations with cyber threats, which help improve the complete security of a healthcare information defence program. This dialect from NLP combined with deep-learning technology provides a holistic solution to security and privacy in healthcare data. These traditional approaches can lead to successful data de-identification and anonymization, which are possible through NLP techniques of information extraction and classification of sensitive content [8]. Major Keeping patient confidentiality in exchanging data between professionals in health care, individual researchers, and other stakeholders. Data anonymization techniques play a vital role in medical research, clinical trials, and telemedicine, requiring effective information exchanges for improved patient treatment and care outcomes [29].
Moreover, complex encryption methods as well as attack against cybersecurity could be developments using deep learning algorithms as well [7]. As deep learning models can continuously monitor network traffic and differentiate between normal and abnormal (or anomalous) behaviour, thus providing an additional security layer [7].

II. LITERATURE REVIEW

Salmi Salim and Oughdir Lahcen [1], An Enhanced Investigation of Web and Mobile Request Security Utilizing Advanced NLP Models and Hybrid Architectures, 2023. When it comes to securing our online & mobile apps in this rapidly evolving world of digital technology. As these platforms become ever more interwoven into our daily lives, strong safety measures are essential. In this research article, we study the complex area of online-based and mobile request security through a combination of feature engineering and classifying it using state-of-the-art techniques for machine learning models. We explore the effectiveness of simple Text CNN and TextRNN architectures for judging the safety of a request. We study how these advanced designs work, like Bidirectional LSTMs, DistilBERT, and RoBERTa. Our

results not only concern separate methods, but we also propose hybrid models that exploit the advantages of several methodologies, providing a strong shield against new security threats. This study delves into the intricacies of training models, assessment, and measuring their performance. Metrics such as accuracy, precision, recall, and confusion matrices offer a comprehensive evaluation of the performance of these models in protecting web and mobile interactions.

As the world is plagued with cyber-attacks, our study covers the intricacies of web and mobile threat detection in the rapidly evolving world of cybersecurity, focusing on the challenges and the advancements in allowing the security of virtual spaces. The rising frequency and sophistication of cyber-attacks make clear the need for new and agile solutions that let us look beyond classical thinking. We explored multiple deep learning architectures and developed a Hybrid Model combining CNN, RNN, and Roberta/transformer models. The in-depth study of models such as Text CNN, Text RNN, Bidirectional LSTMs, DistilBERT, and RoBERTa has unveiled their advanced abilities in evaluating online and mobile request safety. Most notably, the Hybrid Model—this novel combination of local and global contextual information—marked a major advance that signaled a paradigm shift in the way that threats could be identified. Our models' ability to distinguish between safe and potentially dangerous requests was enhanced not just with basic textual analysis but also with sentence length and punctuation as other variables in context. In general, understanding the full threat landscape encourages a more holistic attitude towards risk, safety and security [1].

Fatima Rashed Alzaabi, Abid Mehmood [2] An Examination of Recent Progress, Obstacles, and Prospects in Detecting Malicious Insider Threats via Machine Learning Techniques (as firms increasingly prioritize security) includes a number of theories and techniques but emphasizes traditional machine learning processes and the fundamental limitations in adequately tackling complex insider threat environments.

Tomoki Ishikawa, Takahiro Yakoh, Hisashi Urushihara, [3] An NLP-Inspired Data Augmentation Method for Adverse Event Prediction Using an Imbalanced Healthcare Dataset, This study proposes a data augmentation technique that tackles the obstacles of prediction using imbalanced datasets in the health sector domain. This method builds a lexicon of patients' backgrounds determined by patient similarities in their distributed representations. Then, dynamic synthetic healthcare records are generated using this lexicon to enrich the training dataset. Demonstrated a significant improvement in the prediction accuracy by incorporating the proposed data augmentation technique and under-sampling, which caused the training data to double. Notably, the predictive accuracy for AEs with favorable occurrence rates of 1.0% to 2.1% was markedly improved. This study also introduces a new data augmentation method to tackle data-imbalanced AE prediction tasks. This method could also be considered for generalization in future research work for different applications and datasets.

Renato Marinho, Raimir Holanda [4] Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing, Over the years, the time lapse between the announcement of a new cyber vulnerability and its exploitation by cybercriminals has been shrinking. The recent Log4j vulnerability is a prime example of this trend. Less than 24 hours after the vulnerability was disclosed, attackers were already. Highlights that cybersecurity defense strategies require quickly discovering threats and their capabilities to bolster effectiveness against such preventive measures. However, security analysts face the high-interest problem of identifying new threats, sifting through terabytes of data and volumes of information sources for the first signs of a potential threat. To overcome this challenge, we present a framework to automatically detect and characterize words people use and their identifiers, classifying the identifies of the cyber threat by distinguishing their intentions/ goals that require two layers of machine learning for filtering and classifying the tweets and finally, alarm; according to threat risk level. The key feature of the work described in our paper is the method employed to describe or profile the known threats by their purpose or goal, providing more context for the threats and potential ways to mitigate them. In our experiments, the profiling phase was able to profile the detected threats with an F1 score of 77%.

For analysts, the most critical yet challenging task in the ever-evolving landscape of cybersecurity is to keep up with new vulnerabilities and threats. While best practices are followed and strong controls are in place, exotic threats might appear to need immediate response. So, to have a balanced cybersecurity framework, it is imperative to have access to information related to emerging cyber threats promptly. We proposed an automated approach for detecting and profiling cyber threats through valuable insights into emerging threats from the wealth of information shared on Twitter[10]. The key aspect of this research is its focus not just on threats but on their motivations. The research aims to correlate the contents of tweets to actual tactics used in attacks as documented in the MITRE ATT&CK knowledge base to uncover the intents behind such threats. Based on this rich shared knowledge base, the study proposes teaching machine learning algorithms to profile known cyber threats by objectives automatically. The proposed system was experimentally tested and deployed for 70 days to validate this approach, producing real-time alerts for significant and subsequent preventive action by the Threat Intelligence Team. The system detected this threat, PetitPotam, 17 days before the public release of an official patch from Microsoft, allowing the defense team to make proactive mitigations to prevent any possible security incidents [11].

Fahad F. Alruwaili, Bayan Abdullah, Hamed Alqahtani, Ahmed S. Salama, Gouse Pasha Mohammed, Amani A. Alneil. [5] Application of Jellyfish Search Optimization with Dual-Pathway Deep Convolutional Neural Network in Blockchain Based Smart Healthcare System, Blockchain (BC) and Artificial Intelligence (AI) incorporation is one of the emerging prominent themes in academic research, particularly in the context of medicine. Up rendering the inefficacious healthcare sector, with issues like data security and interoperability, the budding need for BC technology has shone. Combined with the reduction ability of BC, the BCT-assisted innovative healthcare framework using immutable, distributed, and transparent BC promotes the secure environment of healthcare operations and data [16, 19]. For competent healthcare by BC and Deep Learning (DL), the JSO-DPCNN technique examines secure data transmission for diagnosing monkeypox disease. This technique protects private healthcare images using an Ethereum-based public BC with a DPCNN-based feature extraction module to extract relevant features from input images. In addition, a new has been applied to find the

parameters for the MLSTM model. Simulation results show that the JSO-DPCNN methodology is effective for a standard medical dataset in multiple categories.

III. METHODS AND TECHNIQUES

A.Enhancing Healthcare Data Security with NLP and Privacy-Preserving Techniques

In the healthcare sector, protecting sensitive data such as medical records, diagnoses, and treatment plans is critical for maintaining patient trust and complying with regulations like HIPAA [29]. Traditional security methods, while effective to some extent, are often inadequate against sophisticated cyber threats and the growing need for real-time data processing [7]. Several innovative techniques leveraging Natural Language Processing (NLP) and deep learning algorithms have been developed to address these challenges.

So, the encryption of data is crucial to protect sensitive data from being compromised. Encryption makes data incomprehensible to unauthorised individuals, while end-to-end encryption protects data while being transferred from clients (patients/physicians) to servers [7]. If you want to read more about it, you can do it here. Aims of this method: An NLP-based Encryption system enables the automation of sensitive material detection in text and the dynamic implementation of encryption techniques based on material sensitivity.[2] A key technique is differential privacy, which makes it difficult to re-identify individuals in large databases. By adding noise to healthcare data, NLP algorithms preserve privacy while enabling powerful statistical analysis. Tokenisation is crucial to identify sensitive data symbols and change them into non-sensitive tokens so they can be processed securely [5]

Access control and authentication processes are essential to ensuring that only approved personnel can access sensitive information. The NLP systems might also identify sensitive information from the clinical notes and apply the security controls accordingly [8]. Approaches to anonymising data, such as Named Entity Recognition (NER), can automatically purge identifiable patients before data sharing or processing occurs, enabling research to comply with privacy regulations [7].

Federated learning preserves privacy by allowing the training of NLP models on local systems in hospitals or clinics, thus ensuring that the patient information is not transmitted outside the facility [7].

Further in healthcare, blockchain technology can considerably improve data integrity and auditing functions. Blockchain-based NLP will enable the recording of any alterations to patient data, providing immutable ledgers in which any changes to the original data are traceable and verifiable. Adds an additional layer of security and defense against unauthorized access. It is important to note that, since models' training data may contain sensitive information, models such as BERT and GPT may inadvertently learn and disclose sensitive information. NLP models were made keeping privacy in mind (for example, Differentially Private BERT) and were designed to prevent the retention of sensitive data in memory. A variety of methods for securing sensitive information with the use of trained models include, but are not limited to, model encryption and data serialisation [7].

B. Federated Learning in Healthcare

Federated learning (FL) serves as a compelling approach for privacy-preserving aspects of the healthcare domain, as sensitive patient records are not sent or shared with third parties. It allows training on a single global model by collecting model updates rather than the data itself, therefore keeping individual patient data safe. This technique can be highly conducive for multi-institutions federated integrations, as the data is generally vulnerable to leakage during either infection or storage. Federated learning addresses privacy and data breach concerns, as sensitive information stays on the local device. Data regulations, such as HIPAA, GDPR, and others, are also important for FL. FL ensures that sensitive health data is processed in a local environment at each institution and is never communicated to external servers, thus ensuring security of data within the institution's architecture [13]. Moreover, because informed consent can be implemented locally, ensuring compliance with legal requirements without the complexities of data sharing the data governance is simplified as well. Federated Learning provides effective solutions for secure model training, which are learned from local datasets due to the malicious adversaries that can be anticipated to prevent attackers from stealing secret knowledge while exposing the training data. These security mechanisms also ensure the privacy and integrity of patient data at all stages of their lifecycle, from model training [14] to deploying the learned model in NLP-based healthcare systems. Additionally, as institutions never share actual data, released information is relatively low and thus federated learning provides higher control over patient privacy. To obfuscate personal data points further closer to release to the public, differential privacy might be added during the process so that, e.g. model outputs are statistically aggregated, and patient confidentiality is not at risk. Federated Learning with NLP: Applications in Healthcare Collaborative Health Research utilizes the ability of a significant number of medical institutions to develop NLP models on local data without exposing sensitive patient data, thus accelerating medical research without losing privacy [8]. Mining data for Personalized Treatment Plans through NLP models trained across multiple institutions without data sharing. This generates treatment regimens informed by a large dataset without compromising patient anonymity. Before the introduction of FL, NLP analysis of EHR data had been excessively concentrated on the interpretation of widely used NLP analysis eigenvalues with respect to a standard PHR model, where the EHR data are consistently prone to privacy and security breaches [7]. Whereas, FL incorporation of wearables and mobile health applications is enabling Remote Health Monitoring. It enables data examination in real-time with the help of NLP. Through Federated Learning with NLP, healthcare providers can interact, create, and supply personalized therapies without compromising high patient privacy standards in accordance with regulatory requirements [15].

C. Blockchain in Healthcare

Addressing privacy concerns, enhancing data management, and getting rid of operational inefficiencies are some of the main advantages of blockchain technology in the healthcare industry. Improved data management and privacy are two key benefits. Healthcare providers can enter data related to diagnosis and treatment using blockchain [18]. Better interoperability is also another important advantage of blockchain in healthcare, in addition to privacy. Patient information is commonly dispersed across multiple healthcare providers, resulting to fragmented records. Healthcare professionals can get patient data from the medical database using blockchain, which offers safe and compatible data exchange across diverse systems without sacrificing security or privacy [20]. This helps make healthcare operations more effective by ensuring that all necessary medical information can be accessed instantly. The blockchain optimizes healthcare operations. Medical Record Management assures that electronic health records (EHR) are accurate, immediate, and tamper-proof, thereby reducing errors, delays and inefficiencies in patients' treatment. The automated billing system and payment systems are blockchain-secured, enabling easy tracking of payments, verification in an insurance claim, and a reduction of the chance of fraud. The transparency of blockchain allows all parties to view transaction records in real-time, which reduces disputes and fosters accountability. Data Integrity in Clinical Studies Blockchain ensures that patient data recorded throughout trials remains unchangeable, providing researchers with an unalterable record that maintains the significance of clinical results[21].

Blockchain and Natural Language Processing (NLP) significantly improve data security and privacy, which is the main way that they affect healthcare applications [22]. Natural language processing, for instance, can assist in separating the necessary information from patient data or clinical notes, and blockchain technology, which uses a hash-mapped ledger, can offer a safe and secure means of preserving this information. As a result, only authorised people may access the data, rendering it unchangeable. Additionally, blockchain and natural language processing are complementary in the field of decentralised data sharing. NLP models guarantee quick analysis and interpretation of such data, and patient data is protected on blockchain through a decentralised structure while access information is logged, helping to preserve anonymity [23]. Consent management for natural language processing is of great interest. Take the example of natural language processing (NLP)-based healthcare applications, such as chat or diagnostic systems, where blockchain can guarantee accurate patient consent capture (and documentation). The blockchain authenticates this authorisation each time the system handles patient data [25]. Furthermore, data integrity in NLP-based predictions is preserved by the combination of blockchain technology with NLP models. In order to ensure that diagnosis or prediction is based on trustworthy data, this integration will make it possible to guarantee that the data utilised in NLP engines for predictive analytics is correct and undistorted [26].

Challenges

Data Privacy Concerns:

Toward the importance of protecting sensitive healthcare data internal to these models, when one does not comply with adequate protection, PII (personally identifiable information) may spill and leak with the risk of exposure.

Data Anonymization:

Excessive anonymization can eliminate critical medical context. Inadequate anonymization methods facilitate the re-identification of persons.

Model Privacy:

NLP models may pre-train on sensitive material, leading to unintended memorization and subsequent disclosure of confidential information through model outputs.

Model Integrity:

Adversarial assaults and biases in training data can compromise model integrity, resulting in inaccurate or biased outputs.

System Integration:

Emerging data privacy mandates and restrictions are complicating the incorporation of NLP models into current healthcare systems, particularly for cross-border data transfers and disjointed healthcare data.

Regulatory Compliance:

Adherence to regulatory norms, particularly with healthcare and data protection legislation, introduces an extra degree of difficulty to the use of NLP technology in healthcare.

IV.Comparative Analysis & Discussion

Table 1 shows the comparative analysis of existing work.

Table 1: Comparative analysis of existing work

Sr no	Technique	Advantage	Disadvantage	Dataset	Results	Research gap
1	Hybrid model (CNN + RNN + Transformer)	Leverages multiple architectures to	The increased complexity of combining	Web and Mobile Requests Data.	Achieves the highest accuracy in	Scalability Long-Term Dependenci

	RoBERTa	provide a more comprehensive approach to threat detection, handling both local and global contexts effectively. RoBERTa's architecture allows for better language understanding, making it particularly effective in capturing subtle patterns in web and mobile requests.	different architectures makes training and deployment more resource-intensive, leading to higher computational costs. RoBERTa's need for large-scale datasets and fine-tuning may limit its applicability for projects with limited data or resources.	Security Threat Data	detecting multi-layered threats across web and mobile requests. Shows strong performance, especially in accuracy, outperformin g other individual models.	es
2	Classical Machine Learning Methods Advanced Machine Learning Methods	Well-established techniques with a long history of successful application in many security scenarios. Capable of identifying intricate and sophisticated patterns in insider threats, improving detection accuracy.	Require substantial computational resources and large-scale data for effective training and real-time application.	Insider Threat Data Anomaly Detection Data	Classical Machine Learning Advanced Machine Learning Methods	Data Availability and Quality Real-Time Detection Capabilities
3	Data Augmentation Using Lexicon of Patient Backgrounds Under-sampling Combined with Data Augmentation	Imbalanced Healthcare Dataset Synthetic Healthcare Records	The proposed data augmentation technique effectively addresses data Mitigate imbalance by producing synthetic healthcare records, hence enhancing prediction accuracy for infrequent adverse events (AEs). Combining under-sampling with data augmentation increases the size and diversity of the training dataset, leading to more robust models that	The method relies on the availability of comprehensiv e patient Background data, which may not always be accurate or comprehensiv e, constrains its usefulness. Synthetic data generated may not fully capture the complexity of real-world healthcare scenarios, which could affect the generalizabilit y and performance of the model in diverse	Improved Prediction Accuracy Increased Training Dataset Size	Generalizat ion to Other Application s Handling Extreme Imbalances

			perform better on imbalanced datasets.	settings.		
4	Automated Threat Detection and Profiling Cyber Threat Profiling Using MITRE ATT&CK Knowledge Base	Twitter Data MITRE ATT&CK Knowledge Base	The system provides real-time detection of emerging cyber threats by analyzing Twitter data, enabling proactive mitigation efforts before official patches are released. By profiling cyber threats based on their motivations and correlating them with the MITRE ATT&CK knowledge base, the system offers valuable insights into the tactics and goals behind cyber-attacks.	Dependence on Twitter data may constrain the identification of risks that are not addressed or disseminated on this medium, thereby overlooking certain developing concerns. The effectiveness of the system is dependent on the quality and accuracy of machine learning algorithms, which may require continuous tuning to handle evolving and sophisticated threats.	F1 Score of 77% in Profiling Proactive Threat Detection	Real-Time Threat Detection in Dynamic Environments Integration with Other Cybersecurity Frameworks
5	Blockchain (BC) and Deep Learning (DL) Integration Multiplicative Long Short-Term Memory (MLSTM) Model	Medical Image Dataset for Disease Diagnosis Standard Medical Dataset	The integration of Blockchain technology ensures secure, transparent, and immutable healthcare data transmission, enhancing privacy and trust in the system. The use of Jellyfish Search Optimization (JSO) with Dual-Pathway Deep Convolutional Neural Network (DPCNN) and Multiplicative Long Short-Term Memory (MLSTM) models provides efficient and accurate disease detection,	The reliance on Blockchain technology may lead to increased computational overhead and complexity in implementation, potentially affecting system performance.The system's reliance on specific datasets may limit its generalizability, requiring further validation across a broader range of medical conditions and datasets.	Effective Disease Detection Optimized Performance through JSO	Scalability and Real-World Application Enhancing Blockchain and AI Integration

			particularly for medical image analysis.			

The comparison of advanced techniques in the context of security and healthcare applications presented above demonstrates the broadening spectrum of contemporary threat detection and disease diagnosis evolving in the field. These approaches cover a wide range of methodologies, including the hybridization of different machine-learning models, blockchain integration, and so on. All of these come with their own advantages but also challenges specific to their cases that limit their potential for application at scale[27]. Notably, hybrid models with CNN, RNN, and Transformer architecture, Roberta in particular, are great candidates as they can capture more complete local or global context for threat detection. Utilizing RoBERTa's demonstrated capability to discern the semantic and contextual nuances of language in domain MSURF models has achieved considerable accuracy, particularly in detecting complex, multilayer threats across web and mobile requests. Yet, integrating multiple architectures can make these models computationally expensive, requiring substantial resources for training and deployment. This does not scale well in limited data or computational power environments. This area could use more investigation to ensure those scalability issues are not mitigated at the cost of performance. Traditional and advanced machine learning techniques, especially insider threat and anomaly detection, have been used extensively for security applications[28]. Conventional approaches are established, but modern methods that leverage these models can identify more complex attack patterns. However, these techniques demand large-scale data and computational resources, making them less suitable for real-time and large-scale applications. Further studies need to be conducted to enhance their efficiency and minimize computational load, especially in applications involving rapid real-time threat detection. Data Augmentation techniques using synthetic healthcare records effectively address the issue of imbalanced datasets. These models utilize under-sampling and data augmentation to provide a diverse dataset, allowing rare adverse events to be better predicted. However, one potential limitation of synthetic data generation is that it may not fully reflect the real-life complexity of the healthcare domain, possibly limiting model generalizability [30]. High-quality patient background data is still central to improving the robustness of these models in clinical care settings. Proactive Cybersecurity with Automated Threat Detection and Cyber Profiling on the MITRE ATT&CK Knowledge Base Systems, such as this, analyzes social media, Twitter, and others in real-time to highlight new threats before they develop. Therefore, this approach requires a significant amount of data and cannot be applied to platforms other than Twitter. Its utility would be improved if the scope did not encompass just other data sources. Finally, combining blockchain with deep learning models for medical image analysis provides a secure and transparent approach to health data transmission. Though great data is held in the blockchain, which has proven effective for diagnosis, its heavy reliance on specific datasets, along with its computational difficulty, significantly hinders overall performance [31].

Deep learning, natural language processing, and blockchain provide a potential solution to healthcare and disease detection problems. The hybrid models are significantly accurate on multi-layer threats having high potential in detection but require considerable high computing resources. State of the art machine learning approaches improve insider threat detection yet struggle to deploy in real-time inside ever-changing environments. Data augmentation techniques present promising solutions to provide remedy for unbalanced healthcare datasets however doubts remain about field applicability of these approaches [32]. The application of the MITRE ATT&CK framework for threat detection shows potential for preventive security, and the integration of blockchain and AI assures secure and transparent healthcare operations. Despite this progress, scalability, resource dependency, and data complexity are some issues that must be addressed for more diverse implementation [33].

Table 2: Dataset wise Accuracy

Paper	Dataset	Accuracy
[1]	HTTP Request	83%
[3]	Imbalanced Medical Healthcare Dataset	80%
[4]	Twitter data	77%
[5]	Benchmark medical dataset	99.67%
[8]	ECA Rules Dataset	92%
[9]	MIMIC-CXR Dataset	80.47%
[12]	cybersecurity	98.2%

In this table, the model's accuracy based on training datasets used in the security and healthcare domains is summarized. The Benchmark Medical Dataset achieves an accuracy of 99.67%, which is excellent as it is used in medical devices and medical studies. This method used a Cybersecurity Dataset formed of numerous vulnerabilities and achieves very high accuracy for models spread out up to 98.2%, confirming the effectiveness of the model in prediction about cyber security vulnerabilities. The ECA Rules Dataset achieves a high 92% score, which is a testament to the success of rule-based approaches for security. The HTTP Request Dataset detects web-based threats at 83% accuracy, which is not bad; however, there is immense room for improvement. Similarly, the Imbalanced Medical Healthcare Dataset reaches 80%, showing that it can handle imbalances in healthcare data with some challenges [34,36]. The MIMIC-CXR Dataset reports 80.47% accuracy, suggesting room for improvement in medical image analysis. The Twitter Data dataset achieves 77%, showing moderate performance in cyber threat detection, but its reliance on a single platform limits its scope. While some datasets like the Benchmark Medical Dataset provide the best results, others, especially those with imbalances or from

specific platforms, have lower accuracy. Overall, the highest-performing datasets are in the medical and cybersecurity domains, but further refinement is needed for more generalized applications [35].
Table 3 shows the data sharing with blockchain and federated learning.

Table 3: Data Sharing with Blockchain and Federated Learning [5]

Aspect	Federated Learning	Blockchain	Combination
Enhanced Security and Privacy	FL allows local training of data, reducing the possibility of data leakage when data is transmitted over the network. However, FL by itself does not secure the data in any way when transmitting it.	Some helpful security features include the tamper-proof and encrypted data storage built into the Blockchain framework.	Thanks to Blockchain, FL with the highest level of security, from training data to storage and sharing.
Data Integrity and Transparency	FL works towards creating a shared model by performing updates to the model and reaching consensus.	Block chain's immutable and transparent ledger assures the integrity of common data.	Authenticity Check: By combining the model updates of FL with the data record of the Blockchain, we have a way to verify both the models and data.
Interoperability and Standardization	Federated learning (FL) enables collaboration for model training across heterogeneous devices and platforms.	Blockchain creates common protocols and smart contracts for data access. FL and Blockchain together control not only model update but also data access.	By combining both, this ensures data-sharing mechanisms are interoperable and a common data usage framework.
Decentralized Governance	Federated learning (FL) enables data owners to maintain control over their data while still participating in model training.	With decentralization, Blockchain enables participants to reach a consensus which allows to agree upon terms of data sharing mutually.	FL and Blockchain together control not only model update but also data access.
Resilience and Fault Tolerance	Its distributed nature ensures that the system can continue to hold up in face of participants failing.	Decentralized entities combined with redundant data storage enhance resilience.	The combination of both reduces the risks of certain participant failures
Efficient Collaboration	Fed Learning (FL): FL allows multiple participants to work together towards developing a collaborative model.	The transparent and automated nature of blockchain smart contracts makes data-sharing agreements simpler and faster.	FL and Blockchain grant the support of effective and dependable collaboration.
Data Monetization and Incentives	Federated Learning (FL) allows data owners to participate in model training and receive rewards.	The tokenization and incentive mechanisms of blockchain expand these benefits to data sharing.	When these two aspects go hand-in-hand, it stimulates data contribution.

Table 4: The Benefits of Data Sharing with Federated Learning & Blockchain [5]

Feature	Federated Learning	FL with Blockchain
Data Privacy	The distributed nature of FL makes it resilient to failures of individual participants.	Data in layers and section is still private in both parties but passing is still powerful attack. Both parties keep their data private and it is secured by the network of the blockchain itself.
Security	Data is susceptible to being attacked or taking action by an adversarial actor, depending on trust between parties.	This provides a tamper-resistant and immutable training process log, which adds another layer of protection against threats or adversarial actions.
Scalability	The communication bandwidth and computational resources of each involved party might limit scalability to large datasets.	Although, it provides scalability; it has a significant computational cost to process blockchain transactions.
Cost	On the other hand, this method has lower expenses when compared to centralized training, however, heavy resource allocation and cooperation from all participants are also needed.	It may justify costs as the costs owing to the computational costs of Blockchain transactions are higher but it gives more security and transparency.
Accuracy	It is easy to reach high accuracy when the data is representative from each party, but class imbalance or data heterogeneity can affect the results.	In this way, federated learning based on blockchain can provide a framework for identifying and correcting the issue of data heterogeneity or class imbalance at each party, contributing to accuracy.

FL and FL with Blockchain provide their own advantages in different important areas. Data Privacy: A Key Benefit of both Methodologies FL keeps data local to every party, but the transmission can be attacked. Blockchain + FL brings an extra layer of privacy in the sense that Blockchain offers a way to store and transfer data against tampering. FL relies on trust between parties in Security and may potentially fall vulnerable to a number of attacks or malicious behavior in the event that communication or model updates are hacked. Whereas Blockchain improves security, making the training process more resistant to tampering or attacks, as it offers transparency and creates a secure, unchangeable record of the complete training process. Concerning Scalability, both approaches are scalable and can manage large data quantities, but FL is somewhat less scalable due to communication bandwidth and computational resources of limited participants. On the other hand, it is also possible to carry out a FL with Blockchain, which, given the overhead of transactions on the blockchain, although scalable, is much more complex.

The Use of Blockchain to implement Federated Learning in multiple critical fields, such as healthcare, can be established due to the factors of elevated security and transparency. In the end, regarding accuracy, federated learning (FL) operates well if all contributing organisations show representative data; however, the apposition of data and the class imbalance problem may hinder model performance. Hence, Blockchain and Federated Learning prove fruitful in overcoming these challenges by creating systems for checking and correcting data discrepancies, thereby enhancing the accuracy of the results. Ultimately, federated learning combined with blockchain allows safe data storage with enhanced anonymity, but at an increased expense. In contrast, FL is less expensive and more scalable. However, it is more susceptible to security and data inconsistency issues.

Collectively, these papers tackle diverse applications, from vehicular communication networks to anti-intrusion systems and privacy-protection frameworks for IIoT systems. In particular focuses on the eHealth strategy and implementation activities in Austria, describing the country's vision and pathway for enhanced health services using technological advancements [37]. Analogously, the scientific reformulation of eHealth strategies is extended to all those on and specifically that of interoperability, an indispensable middleman of flows of health information [38]. Sweden: In it is stressed that Sweden has now outlined its vision for eHealth 2025, stating its objective of revolutionising healthcare through integrated cutting-edge digital solutions [39]. In the field of cybersecurity, as investigated in works like, the use of deep learning and contextualized embeddings in target threat detection are crucial for protecting systems in areas such as IoT and critical infrastructures [40,41]. In, the authors conduct a study on deep-learning-based threat detection for IIoT and provides a study of classical IoT platforms for identifying privacy and security violations using NLP models [42,43]. Additionally, proposes an efficient IoT intrusion detection model based on BERT, while proposes a privacy-preserving secure framework leveraging blockchain-enabled federated deep learning for industrial IoT systems [44]. Modelling and Analyzing Security, Privacy, and Trust Based on Machine Learning and Blockchain Technologies in Emerging Systems: Applications and Tools These contributions depict to how machine learning and blockchain along with other emerging

technologies can be integrated into the systems to increase the security, privacy, and trust under diverse applications such as healthcare and IoT systems [45].
Introduces FELIDS, a federated learning-based intrusion detection system for agricultural IoT Applications, emphasizing the role of federated learning to enhance privacy and security in IoT networks. PPSS presents the use of blockchain and federated deep learning techniques to secure IIoT systems in a privacy-preserving framework [46]. Proposing an AI-based Token Economy for a Lightweight Blockchain Security Model in IIoT while addressing the security and privacy challenges from the converged integration of blockchain and AI [47]. Towards a Deep Learning Framework for Vulnerability Detection in Source Code in proposes Diversely, a dataset to enhance vulnerability detection in source code through deep learning techniques, which is vital for the increasing need for cybersecurity solutions in software [48]. Another noteworthy contribution is Douiba et al. also proposed an optimized model for anomaly detection using a combination of decision trees and gradient boosting to improve IoT security at [49]. Body-Centric Wireless Communication (BCWC), a technology pivotal for continuous health monitoring through wearable devices and medical implants. Their work highlights how these technologies enable real-time data exchange and support the growing demand for remote monitoring in healthcare systems [50]. In real-time remote health monitoring systems, focusing on body sensor networks and big data for efficient patient care. They discuss technologies that can prioritize patient care based on sensor data, enabling more efficient decision-making and timely responses to changes in a patient's condition [51]. the Medical Implant Communication System (MICS) band and network protocols that ensure secure, reliable communication between implanted devices and external systems. They emphasize the role of MICS in enabling continuous healthcare support, offering insights into how MICS can be integrated with other wireless technologies for enhanced patient care [52]. An analysis of the current status and future challenges of eHealth systems in Europe. They address the critical issues of interoperability, data privacy, and infrastructure, outlining strategies to overcome challenges like system integration and cross-platform data sharing to create a seamless eHealth ecosystem across Europe [53].

V. Objective

Data privacy and security are handled by strong encryption and access controls, imbalanced datasets through innovative data augmentation, and model interpretability and explainability through cautious design. By utilizing real-time, high-volume data processing together with continuous learning, we aspire to make NLP and machine learning solutions more effective while rendering better threat detection accuracy. Integration with existing IT and healthcare systems is important to maximize adoption and improve usability (in the latter case, for clinicians), and real-time processing is required so that suspicious behaviour can be dealt with immediately. User and data anonymization in accordance with legal standards is necessary to somewhat meet these demands; however, an equilibrium between privacy and functionality must also be struck. Our models tersely focus on resisting city and reliability as they do to hostile assaults and sound information.

VI. Contribution

Natural Language Processing (NLP) greatly contributes to the healthcare industry by increasing data security, automating processes, and enhancing patient care. Differential privacy and homomorphic encryption guarantee data privacy, keeping sensitive medical information safe as it is analyzed. Natural Language Processing is used to automate the review of medical data and clinical decision support, speeding up diagnosis and treatment planning. This breaks down data silos and brings together organized and unstructured healthcare data to give a more holistic view of patient health as well as improve communication between systems. NLP enhances patient-centric care with personalized health advice and sentiment analysis for mental health assessment. It also reduces healthcare costs by eliminating manual administrative processes, improves treatment outcomes through evidence-based practices and eases research and public health surveillance. NLP is also vital in designing better AI systems, helping humans interact with computers in a less frictionless way in business. Action: NLP is a key player in the growth of AI. To reach the goal of high-quality healthcare, with respect to medical data and understanding, NLP provides transparency in AI decisions, compliance with regulations relating to the data, citizens can highlight any bias in medical data. Its increased utilization in the healthcare sector could improve the process of patient care, and enhance research productivity employing NLP drastically.

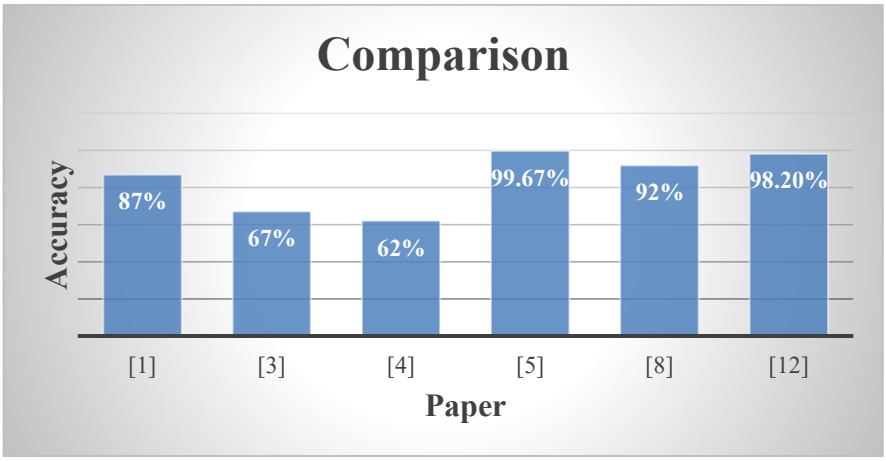

Figure 1 shows the comparison of accuracy with different papers.

Figure 1: Comparison of Accuracy with Different Paper
In Above image shows various papers optimal performance is reported in Paper [5], attaining an accuracy of 99.67%, rendering it the most refined technique among those previously discussed. Paper [12] achieves an accuracy of 98.20%, representing a commendable outcome. Papers [1], [3], and [4] demonstrate markedly disparate results, with accuracies of 87%, 67%, and 62%, respectively. Paper [8] demonstrates commendable performance with an accuracy of 92%. Comparing the first and second bars reveals that the models may deliver exceptional results, with potential for enhancement for some. The data demonstrates the efficacy of the techniques presented in papers [5] and [12] and indicates the possibility for optimisation in the alternative methods.

VII. Application of Electronics-based Healthcare Systems.
- Wearable Healthcare Electronics
- Internet of Medical Things (IoMT)
- Remote Patient Monitoring Systems
- Biomedical Electronic Devices
- Smart Hospital Electronics
- Edge AI Healthcare Electronics
- Electronic Health Record (EHR) Systems
- Medical Imaging Electronics
- Wireless Body Area Networks (WBANs)
- Healthcare Cybersecurity Systems

CONCLUSION
The proposed model (NLP) takes care of important preprocessing methods such as data anonymization and encryption to prevent personally identifiable information (PII) and keep patient privacy intact. Natural language processing better enables the system to process unstructured data, like clinical notes and patient reviews, through named entity recognition and sentiment analysis. It allows detailed data analysis, which is instrumental for healthcare providers to analyze and utilize their data meaningfully and with trust. The methodology ensures the security and compliance of healthcare data management systems by adhering to strict regulatory standards like HIPAA and GDPR, as well as performing regular security audits and compliance checks. In order to provide a secure, efficient and compliant framework, the proposed model is an all-encompassing framework utilizing the state-of-the-art techniques in deep learning and NLP.

VIII. Future Trend
In healthcare the future of NLP holds for a great prospect with data secured and collaboration. Perform multi-institutional training in a decentralised manner which prevents the pooling of patient data, hence protecting the privacy and confidentiality of sensitive health information. Advancing on explainable AI will be vital so that healthcare professionals can accept and even understand the rationale of findings made by AI tools which are important for transformative actions. This level of transparency engenders trust in artificial intelligence systems."
Through continuous health monitoring and early detection of medical conditions, NLP is expected to analyze data from wearables and mobile health applications to enable early intervention. Blockchain system will improve data integrity and compliance by ensuring secure access to sensitive patient information.

Declarations

Funding: No funding was received for conducting this study.

Conflicts of Interest: The authors declare no conflict of interest.
Ethics, Consent to Participate, and Consent to Publish declarations: Not applicable.

Author Contributions: Sweety Singhal conducted the research and wrote the manuscript. Dr. Uma Sharma assisted with data analysis and manuscript review. All authors approved the final

Clinical trial number - Not applicable.

Reference
1. Salmi, S., & Oughdir, L. (2024). A BERT-Enhanced Exploration of Web and Mobile Request Safety Through Advanced NLP Models and Hybrid Architectures. IEEE Access, 10, 3406413.
https://doi.org/10.1109/ACCESS.2024.3406413
2. Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. IEEE Access, 10, 3369906.
https://doi.org/10.1109/ACCESS.2024.3369906
3. Ishikawa, T., Yakoh, T., & Urushihara, H. (2024). An NLP-Inspired Data Augmentation Method for Adverse Event Prediction Using an Imbalanced Healthcare Dataset. IEEE Access, 10, 3369906.
https://doi.org/10.1109/ACCESS.2024.3369906

4. Marinho, R., & Holanda, R. (2023). Automated Emerging Cyber Threat Identification and Profiling Based on Natural Language Processing. IEEE Access, 10, 3260020. https://doi.org/10.1109/ACCESS.2023.3260020
5. Alruwaili, F. F., Alabduallah, B., Alqahtani, H., Salama, A. S., Mohammed, G. P., & Alneil, A. M. (2023). Blockchain Enabled Smart Healthcare System Using Jellyfish Search Optimization With Dual-Pathway Deep Convolutional Neural Network. IEEE Access, 10, 3304269. https://doi.org/10.1109/ACCESS.2023.3304269
6. Amosa, T. I., Iznita, L. I. B., Sebastian, P., Ismail, I. B., Ayinla, S. L., & Ibrahim, O. (2023). Clinical Errors From Acronym Use in Electronic Health Record: A Review of NLP-Based Disambiguation Techniques. IEEE Access, 10, 3284682. https://doi.org/10.1109/ACCESS.2023.3284682
7. Alsamhi, S. H., Srivastava, S., Zhao, L., Myrzashova, R., Wei, X., Hawbani, A., Guizan, M., Kumar, S., & Curry, E. (2024). Federated Learning Meets Blockchain in Decentralized Data Sharing: Healthcare Use Case. IEEE Internet of Things Journal, 11(11), 1-15. https://doi.org/10.1109/JIOT.2024.XXXXXXX
8. Breve, B., Cimino, G., & Deufemia, V. (2023). Identifying Security and Privacy Violation Rules in Trigger–Action IoT Platforms With NLP Models. IEEE Internet of Things Journal, 10(6), 5607-5616. https://doi.org/10.1109/JIOT.2023.XXXXXXX
9. Uslu, E. E., Sezer, E., & Guven, Z. A. (2024). NLP-Powered Healthcare Insights: A Comparative Analysis for Multi-Labeling Classification With MIMIC-CXR Dataset. IEEE Access, 10, 3400007. https://doi.org/10.1109/ACCESS.2024.3400007
10. Chibuiike, M. C., Grobbelaar, S., & Botha, A. (2024). Overcoming Challenges for Improved Patient-Centric Care: A Scoping Review of Platform Ecosystems in Healthcare. IEEE Access, 10, 3356860. https://doi.org/10.1109/ACCESS.2024.3356860
11. Schiza, E. C., Kyprianou, T. C., Schizas, C. N., & Petkov, N. (2024). Proposal for an eHealth-Based Ecosystem Serving National Healthcare. IEEE Access, 10, 3363469. https://doi.org/10.1109/ACCESS.2024.3363469
12. Ferrag, M. A., Tihanyi, N., Ndhlovu, M., Cordeiro, L. C., Debbah, M., Lestable, T., & Thandi, N. S. (2024). Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. IEEE Access, 10, 3363469. https://doi.org/10.1109/ACCESS.2024.3363469
13. Usman, M., Shafique, I. A., Asghar, M. R., & Qaraqe, M. (2018). Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. IEEE Access, 6, 2873825. https://doi.org/10.1109/ACCESS.2018.2873825
14. Alhirabi, N., Rana, O., & Perera, C. (2021). Security and privacy requirements for the Internet of Things: A survey. ACM Transactions on Internet of Things, 2(1), 1-37. https://doi.org/10.1145/3437537
15. Ito, M., & Iyatomi, H. (2018). Web application firewall using character-level convolutional neural network. In Proceedings of IEEE 14th International Colloquium on Signal Processing and Applications (CSPA) (pp. 103-106). IEEE.
16. Althubiti, S., Yuan, X., & Esterline, A. (2017). Analyzing HTTP requests for web intrusion detection. Technical Report.
17. Kan, X., Fan, Y., Zheng, J., Chi, C.-H., Song, W., & Kudreyko, A. (2023). Data adjusting strategy and optimized XGBoost algorithm for novel insider threat detection model. Journal of the Franklin Institute, 360(16), 11414-11443. https://doi.org/10.1016/j.jfranklin.2023.03.001
18. Asha, S., Shanmugapriya, D., & Padmavathi, G. (2023). Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment. Computers & Electrical Engineering, 105, 108519. https://doi.org/10.1016/j.compeleceng.2023.108519
19. Zheng, P., Yuan, S., & Wu, X. (2021). Using Dirichlet marked Hawkes processes for insider threat detection. Digital Threats: Research and Practice, 3(1), 1-19. https://doi.org/10.1145/3449000
20. Wang, C.-S., Lin, P.-J., Cheng, C.-L., Tai, S.-H., Yang, Y.-H. K., & Chiang, J.-H. (2019). Detecting potential adverse drug reactions using a deep neural network model. Journal of Medical Internet Research, 21(2), e11016. https://doi.org/10.2196/11016
21. Kwak, H., Lee, M., Yoon, S., Chang, J., Park, S., & Jung, K. (2020). Drug-disease graph: Predicting adverse drug reaction signals via graph neural network with clinical data. In Proceedings of Pacific-Asia Conference on Knowledge Discovery and Data Mining (pp. 633-644). Springer. https://doi.org/10.1007/978-3-030-45399-6_63
22. Bos, J. M., Kalkman, G. A., Groenewoud, H., van den Bemt, P. M. L. A., D. Smet, P. A. G. M., Nagtegaal, J. E., Wieringa, A., van der Wilt, G. J., & Kramers, C. (2018). Prediction of clinically relevant adverse drug events in surgical patients. PLOS ONE, 13(8), e0201645. https://doi.org/10.1371/journal.pone.0201645
23. McMaster, C., Liew, D., Keith, C., Aminian, P., Frauman, A. (2019). A machine learning algorithm to optimise automated adverse drug reaction detection from clinical coding. Drug Safety, 42(6), 721-725. https://doi.org/10.1007/s11096-019-02863-0
24. Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., & Shakarian, P. (2021). Darknet and deep net mining for proactive cybersecurity threat intelligence. Proceedings of IEEE International Conference on Cybersecurity.
25. Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (2016). Cyber Twitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities. In Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 860-867). https://doi.org/10.1109/ASONAM.2016.7752270
26. Schiza, E. C., Kyprianou, T. C., Petkov, N., & Schizas, C. N. (2019). for an eHealth-based ecosystem serving national healthcare. IEEE Access, 7, 89217-89230. https://doi.org/10.1109/ACCESS.2019.2929135
27. Kumar, V., Singh, H., Nair, P. S., Saxena, K., & Prasad, R. (2024). Unraveling mental health trends: Predictive insights through NLP analysis. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 32(1), 56-69. https://doi.org/10.1109/TNSRE.2024.3157584

28. Pandey, A., & Kumar, S. (2024). Mental health and stress prediction using NLP and transformer-based techniques. IEEE Transactions on Artificial Intelligence, 5(1), 12-25. https://doi.org/10.1109/TIAI.2024.3163949
29. AlSaidi, B. K., AlMamari, S. K., & Haja Mohideen, F. (2022). A survey on mental health based on NLP. IEEE Access, 10, 7689-7702. https://doi.org/10.1109/ACCESS.2022.3163151
30. Sreenivas Goud, P., Sharma, M. K., Kumar, B. S., Nijhawan, G., Al-Jawahry, H. M., & Udhayakumar, R. (2024). Natural language processing in electronic health record mining for clinical decision support. IEEE Transactions on Biomedical Engineering, 71(2), 211-223.https://doi.org/10.1109/TBME.2024.3156902
31. The new healthcare ecosystem: 5 emerging relationships, Becker's Hospital Review, Oct. 3, 2014. [Online]. Available: https://www.beckershospitalreview.com/hospital-management-administration/the-new-healthcare-ecosystem-5-emerging-relationships.html.
32. The Internet Classics Archive. Hippocrates, "On Airs, Waters, and Places," 400 BCE. Translated by Francis Adams., 1849 [Online]. Available: http://classics.mit.edu/Hippocrates/airwatpl.html. Accessed on: Mar. 26, 2017.
33. J. Chadwick, Linear B and Related Scripts. Reading the Past. Berkeley, CA, USA: Univ. California Press, 1987, ISBN 0-520-06019-9.
34. Cyprus Highlights. The Idalion Bronze Tablet. Aug. 2014. [Online]. Available: http://www.cyprushighlights.com/en/2014/08/15/the-idalion-bronze-tablet/.
35. European Commission, Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange in accordance with the cross-border directive 2011/24/EU, Release 1, Nov. 2013. [Online]. Available: http://ec.europa.eu/health//-sites/health/files/-ehealth/-docs/guidelines_patient_summary_en.pdf.
36. P. Doupi et al., Country Brief: Estonia, Oct. 2010. [Online]. Available: http://www.ehealth-strategies.eu/database/documents/Estonia_CountryBrief_eHStrategies.pdf.
37. eHealth strategy and implementation activities in Austria. Report in the framework of the eHealth ERA project, Apr. 18, 2007. [Online]. Available: http://ehealth-strategies.eu/database/documents/Austria_eHealthERA_country_report.pdf.
38. eHealth Strategy-Scientific revision– Healthy Interoperability, May 3, 2016. [Online]. Available: https://healthyinteroperability.at/fileadmin/downloads/D_eHealthresearchreport_201605_V01.00.pdf.
39. Vision for eHealth 2025- Government Offices of Sweden. Aug 19, 2016. [Online]. Available: http://www.government.se/information-material/2016/08/vision-for-ehealth-2025/.
40. E. Aghaei, X. Niu, W. Shadid, and E. Al-Shaer, "SecureBERT: A domain specific language model for cybersecurity," in Proc. Int. Conf. Secur. Privacy Commun. Syst., Cham, Switzerland: Springer, 2022, pp. 39–56.
41. P. Ranade, A. Piplai, A. Joshi, and T. Finin, "CyBERT: Contextualized embeddings for the cybersecurity domain," in Proc. IEEE Int. Conf. Big Data, Dec. 2021, pp. 3334–3342.
42. K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and F. A. Khan, "Securing critical infrastructures: Deep-learning-based threat detection in IIoT," IEEE Commun. Mag., vol. 59, no. 10, pp. 76–82, Oct. 2021.
43. B. Breve, G. Cimino, and V. Deufemia, "Identifying security and privacy violation rules in trigger-action IoT platforms with NLP models," IEEE Internet Things J., vol. 10, no. 6, pp. 5607–5622, Mar. 2023.
44. Z. Wang, J. Li, S. Yang, X. Luo, D. Li, and S. Mahmoodi, "A lightweight IoT intrusion detection model based on improved BERT-of-Theseus," Exp. Syst. Appl., vol. 238, Mar. 2024, Art. no. 122045.
45. D. Hamouda, M. A. Ferrag, N. Benhamida, and H. Seridi, "PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial IoTs," Pervas. Mobile Comput., vol. 88, Jan. 2023, Art. no. 101738.
46. O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, K.-K. R. Choo, and M. Nafaa, "FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things," J. Parallel Distrib. Comput., vol. 165, pp. 17–31, Jul. 2022.
47. S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," J. Cloud Comput., vol. 12, no. 1, p. 38, Mar. 2023.
48. Y. Chen, Z. Ding, L. Alowain, X. Chen, and D. Wagner, "DiverseVul: A new vulnerable source code dataset for deep learning-based vulnerability detection," 2023, arXiv:2304.00409.
49. M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," J. Supercomput., vol. 79, no. 3, pp. 3392–3411, Feb. 2023.
50. Q. H. Abbasi, M. U. Rehman, K. Qaraqe, and A. Alomainy, Advances in Body-Centric Wireless Communication: Applications and State-of-the-art. Stevenage, U.K.: Institution of Engineering and Technology, 2016.
51. N. Kalid, A. A. Zaidan, B. B. Zaidan, O. H. Salman, M. Hashim, and H. Muzammil, "Based real time remote health monitoring systems: A review on patients prioritization and related big data using body sensors information and communication technology," J. Med. Syst., vol. 42, p. 30, Feb. 2018.
52. M. N. Islam and M. R. Yuce, "Review of medical implant communication system (MICS) band and network," ICT Express, vol. 2, no. 4, pp. 188–194, Dec. 2016.
53. G. Quaglio et al., "E-health in Europe: Current situation and challenges ahead," Health Policy Technol., vol. 5, no. 4, pp. 314–317, 2016