International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4s, 2025
https://theaspd.com/index.php

Enhancing Security For Sensitive Medical Data In Iot-Based Healthcare Systems

Mukesh Kumar Bhardwaj[1*], Manish Saraswat[2]
[1,2]Faculty of Science & Technology, The ICFAI University, Himachal Pradesh
*mukeshbhardwaj85@gmail.com

Abstract

The internet of things (IoT) offers huge advantages to healthcare, allowing closer affected person monitoring and facts evaluation. Integrating scientific gadgets like glucose meters and blood strain cuffs into the IoT environment allows the collection of essential signs. but, securing healthcare data in IoT-cloud environments is a main task because of vulnerabilities and assaults. artificial intelligence (AI) era is increasingly more used to enhance information security in such settings, but it faces demanding situations like computational complexity and excessive sensor charges. To deal with these problems, this observe proposes Probabilistic incredible mastering-(PSL-) Arbitrary Hashing (RH), an AI-based totally method, aiming to enhance both safety and fee- effectiveness in IoT healthcare records management.

Keywords: *Probabilistic Super Learning; Arbitrary Hashing; Security; IoT Data; Healthcare; Artificial Intelligence.*

INTRODUCTION

The intersection of bodily items with embedded connectivity and intelligence, called the internet of things (IoT), has revolutionized various industries, consisting of healthcare. IoT devices geared up with software, sensors, and community connectivity can efficaciously acquire and trade data. This seamless integration into current laptop-based totally systems complement operational accuracy and efficiency, providing economic advantages [1]. In healthcare, IoT technologies are hired in digital physical structures, making use of sensors and actuators for programs like clever grids, smart houses, and far off monitoring of scientific device [2]. The growing occurrence of IoT in healthcare is evidenced through the prediction that through 2020, the IoT will encompass almost 50 billion interconnected devices, with a massive portion committed to scientific packages [2]. those devices variety from implantable scientific devices like pacemakers to wearable gadgets like health trackers, all contributing to the giant community of interconnected healthcare gadgets. The security of healthcare facts in IoT environments is paramount because of the sensitive nature of the facts worried. affected person statistics, which includes scientific statistics and treatment histories, is incredibly treasured to cybercriminals and have to be safeguarded to ensure affected person confidentiality and accept as true with [3]. Compliance with policies along with the medical health insurance Portability and accountability Act (HIPAA) and the general information protection regulation (GDPR) is essential, as violations can cause intense financial and reputational results for healthcare corporations [3]. furthermore, making sure records protection is crucial for maintaining affected person protection and care pleasant, as compromised statistics can at once effect treatment plans and affected person well-being [3]. The healthcare zone faces particular challenges in IoT protection. The wide kind of IoT devices utilized in healthcare environments makes standardizing security measures challenging, leading to an increased assault surface and control complexity [4]. actual-time data processing and get admission to are vital in healthcare, and any security measures that hinder this get right of entry to can pose dangers to affected person care [4]. Integrating legacy structures with present day IoT devices gives compatibility and safety challenges, as older systems may additionally lack important protection features

[4]. moreover, IoT gadgets in healthcare frequently have resource obstacles, together with low computational strength and memory, making it tough to put in force strong security features [4]. eventually, vulnerabilities in clinical gadgets pose huge risks, as they may be exploited to compromise affected person safety and care [4]. In end, while IoT offers mammoth potential for remodeling healthcare, addressing the associated security demanding situations is essential to ensure the integrity, confidentiality, and availability of healthcare information and offerings. The mixing of Artificial intelligence (AI) into security strategies for internet of things (IoT) frameworks is a vital region of research. this article examines conventional security techniques and evaluates their advantages and downsides in light of their useful components and characteristics. The IoT architecture [4] incorporated an AI gadget to at ease healthcare applications, aiming to guard patient statistics confidentiality and protection stored on-line through a Deep Neural network (DNN)-based totally malware detection technique, which decreased reaction time, accelerated packet shipping, and minimized latency even as proscribing unauthorized cloud information get entry to and enhancing key authentication with particular weight and bias values. The clever and at ease IoT framework [5] changed into designed to enhance protection inside the healthcare sector with the aid of integrating AI-related rules and rules, which include accountability, transparency, facts privacy, safety, interoperability, and sustainability, and whilst it targeted on identifying numerous assault sorts based on host attributes, data disturbances, and network characteristics, it lacked particular strategies for detecting network threats, for this reason affecting the overall system overall performance.The latest trends in IoT-AI framework design [6] were examined to develop intelligent healthcare systems, integrating Wireless Body Sensor Networks (WBSN), field sensor networks, and cloud services into a three-tier architecture for creating Web of Medical Things (IoMT) systems. A comprehensive study [7] was conducted on various AI techniques used in IoT (Healthcare IoT) systems, emphasizing the importance of adhering to guidelines such as interoperability, integrity, low latency, privacy, and security to establish effective and secure IoT networks, covering different similarity matching approaches, including dimensionality reduction methods, discriminant analysis, K-means, logistic regression, and linear regression, along with their practical principles.

Objective of Study

The growing deployment of IoT gadgets in healthcare applications has raised concerns about securely storing and retrieving facts from IoT-cloud frameworks. current records safety answers face challenges in figuring out and shielding in opposition to each ordinary and antagonistic records access, posing an enormous chance to affected person data and healthcare machine integrity. traditional encryption techniques have boundaries in key generation, encryption times, complexity, and computational charges. This studies goals to deal with those challenges with the aid of developing an artificial intelligence-based totally Probabilistic extraordinary getting to know (PSL) model for actual-time information safety. additionally, it proposes an Elliptic Curve Cryptography (ECC)-based Random Hashing (RH) approach to beautify facts encryption and decryption. The purpose is to make sure the relaxed storage and retrieval of healthcare data in IoT- cloud environments while efficaciously identifying and responding to protection threats.

Proposed Method

A complete description of the proposed method, including algorithm and flow drawings is set three on this section. The main contribution of this work is that we identify the characteristics/attributes features of data received from IoT devices and apply our proposed framework with AI based Probabilistic Super Learning (PSL) model to handle secure data transaction [8]. In contrast, the w adjustment). Different from the SECP256K1 model, in ECC (Elliptic Curve Cryptography) uses Random Hashing method for data encryption and decryption steps make sure that its security of stored and retrieved data [9]. We used two methods ECC

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4s, 2025
https://theaspd.com/index.php

Random Hash Technique for Data Security and Probabilistic Super Learning (PSL)Algorithm to achieve our objectives

1.1 ECC Random Hash Technique for Data Security- The ECC Random Hash Technique for Data Security encodes the source data prior to storage on IoT cloud by RH. It is a difficult and challenging task to ensure data security in many application systems with rich data feature arrangement [10]. Data security has always included the traditional aspects of storing securely in unencrypted form before encryption and accessing it based on appropriate authenticated manner after decrypting. Classical works detail different standards, such as AES and DES or RS4 for decryption. However, they are around a longer key generation and encryption time, complex to implement and have computational costs. Consequently, this paper combined the intelligent RH key generation method and encryption mechanism based on ECC.

Hashing plays an important role in ECC-based cryptosystems, particularly for:

- Generating unique and secure keys.
- Ensuring data integrity.
- Preventing replay attacks.

3.2 Probabilistic Super Learning- PSL Algorithm also uses feature learning method on a large scale to detect attacks and trains the model by using the features of system also. The features are extracted from the IoT device using PSL method mentioned in section 3. This modifies the training data model to incorporate normal and adversarial feature classes. The PSL is essentially feature learning model developed to conform the dataset characteristic features with respect to it and identify attacks in case certain alerts are triggered.The attributes of IoT devices are matched with this training model to determine if any compromising devices would attempt to access the cloud-stored data during the data storage and retrieval process. If the access was authorized, automatic actions such as data storage and retrieval were performed [11]. The firewall or routing device that initially restricts access can receive an automatic report if being a determined. The Figure 1 illustrates the proposed security framework's overall flow.

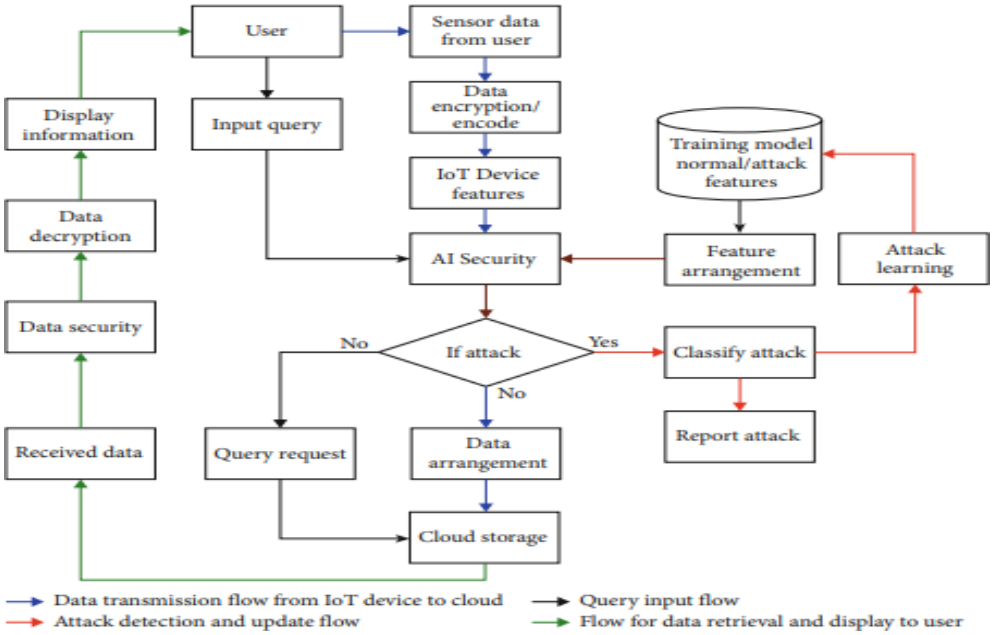


Fig 1**:** The proposed security framework's general stream.

To successfully implement the proposed methodology, several key steps must be taken. First, it's essential to implement the Probabilistic Super Learning (PSL) model to address data security and threat recognition. This involves selecting a suitable machine learning or artificial intelligence framework and training the model with labeled data to distinguish normal data access from potential threats. Real-time monitoring is crucial, with the PSL model playing a central role in identifying and responding to security threats as they arise. Regular updates and refinements to the model based on emerging threats and changing data patterns are also necessary. Next, the combination of Elliptic Curve Cryptography (ECC) with Random Hashing (RH) is essential for ensuring facts protection. ECC and RH have to be carried out into the records storage and retrieval systems, with records being encrypted the use of ECC and decrypted the usage of RH. proper management of keys and parameters is important for preserving the confidentiality and integrity of the encryption procedure.

RESEARCH METHODOLOGY

The section analyzes the effectiveness of present day and proposed safety techniques using metrics along with precision, take into account, F1-rating, Matthews Correlation Coefficient (MCC), throughput, packet transport fee, and computational time. The observe examines the performance of numerous encryption strategies, which include excessive-level Encryption trendy (AES), Ciphertext policy-attribute based totally Encryption (CP-ABE), modified CP-ABE (MCP-ABE), and the proposed ECC-RH approach, across distinctive key sizes. outcomes show that larger key sizes typically require better computational assets, with AES consistently demonstrating decrease computational fees and ECC-RH showing the very best computational demands however presenting advanced security.

Data Collection

Many real-world datasets can be adapted to simulate:

Medical datasets: Add attribute-based policies like Role: Doctor, Department: Cardiology.
Example: MIMIC-III dataset.
Financial datasets: Policies can be based on Access Level, Branch, etc.
IoT datasets: Many IoT use cases (e.g., smart homes, smart cities) rely on access control.
Example: IoT datasets from Kaggle.

Data Analysis

The discussion emphasizes the importance of balancing safety requirements and computational performance whilst deciding on cryptographic techniques for unique applications. moreover, the studies propose a twin-layered method combining characteristic-based totally Encryption (ABE) and position-based totally get entry to manipulate (RBAC) to beautify statistics security in IoT-Cloud frameworks, especially in healthcare programs. This technique pursuits to offer precise manage over information get admission to whilst making sure robust security measures are in place.

The machine learning process is commonly used in this stage to detect attacks by constructing a model based on the system's components. Features are extracted from IoT devices (Fig. 2) using the proposed PSL method. As the model incorporates normal and adversarial features, the data model is refined. The PSL is designed as a machine learning model to correlate device attributes with datasets to identify attacks. This model assesses the characteristics of IoT devices to determine if any malicious devices are attempting to access or alter cloud-stored data during the data storage and retrieval process. Upon approval, automated actions, such as data storage or recovery, are executed. Additionally, the firewall or controlling device that initially limits access can receive a modified report indicating the status of the system's security.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4s, 2025
https://theaspd.com/index.php

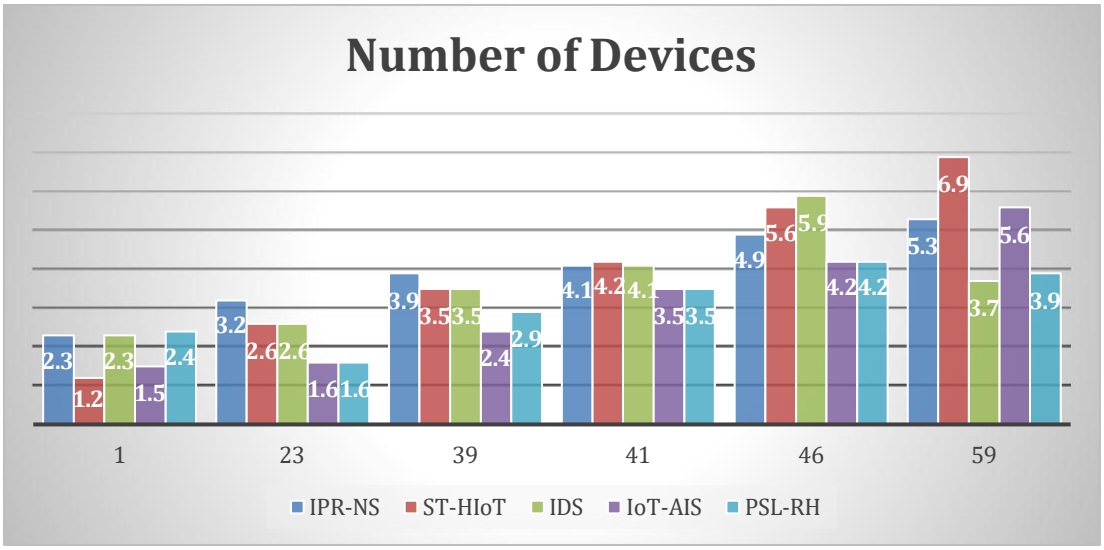
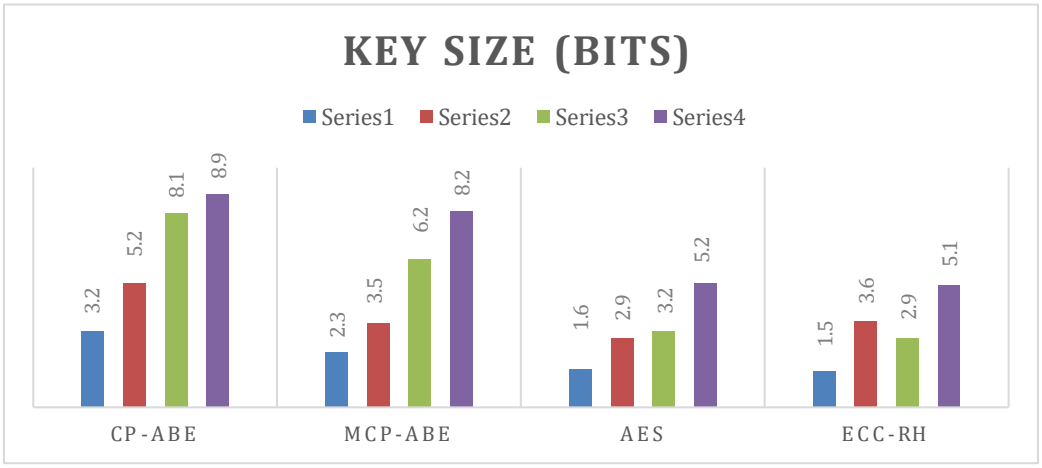


Figure 2: Investigation of current and recommended approaches' throughput

Concerning variable key size (bits), Fig. 3 compares the encryption and decryption instances of existing encryption strategies which include superior Encryption fashionable (AES), Ciphertext coverage-characteristic based Encryption (CP-ABE), modified CP-ABE (MPC-ABE), and the proposed ECC-RH technique.



.

Figure 3: Encryption times for current and impending information security techniques.

Encryption Times	Series1	Series2	Series3	Series4
CP-ABE	3.2	5.2	8.1	8.9
MCP-ABE	2.3	3.5	6.2	8.2
AES	1.6	2.9	3.2	5.2
ECC-RH	1.5	3.6	2.9	5.1

Table 1: Encryption times for current and impending information security techniques

The data presented in Fig.4 demonstrates the analysis of different cryptographic algorithms concerning their bit key sizes. A consistent pattern is observed across all four encryption techniques (CP-ABE, MCP-ABE, AES, and ECC-RH) as the key size increases. Specifically,

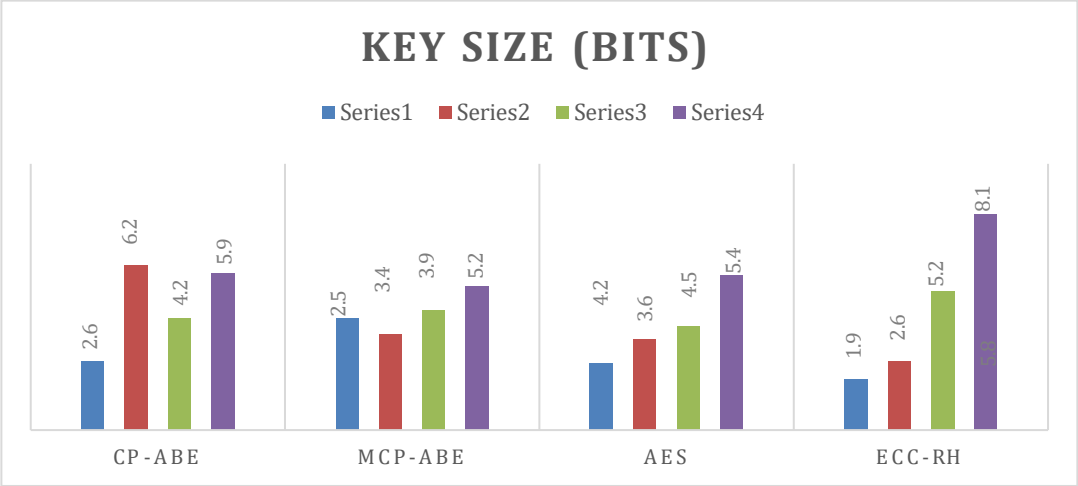


Figure 4: Unscrambling times for current and impending information security strategies.

Unscrambling times	Series1	Series2	Series3	Series4
CP-ABE	2.6	6.2	4.2	5.9
MCP-ABE	4.2	3.6	4.5	5.4
AES	2.5	3.4	3.9	5.8
ECC-RH	1.9	2.6	5.2	8.1

Table 2: Unscrambling times for current and impending information security techniques

larger key sizes correspond to higher computational overheads, indicating a greater need for processing resources. Interestingly, AES consistently exhibits the lowest computational requirements across all key sizes, while ECC-RH consistently utilizes the most resources. This trend highlights the importance of striking a balance between security requirements and computational efficiency when selecting a cryptographic algorithm for a specific security application. ECC-RH is suitable for applications requiring a high level of security but with a higher computational overhead, whereas AES is a more efficient choice for lower key sizes. [13].

The above data analyzes the performance of different cryptographic algorithms with keys of varying sizes. Several trends emerge from the results. For instance, CP-ABE demonstrates significantly lower computational requirements compared to other methods for smaller key sizes (132 and 186 bits). However, as the key size increases, the computational demands for CP-ABE also increase, eventually aligning with other methods, particularly AES and MCP-ABE. [14] Across all key sizes, the widely used symmetric encryption method AES consistently exhibits low computational costs. In contrast, ECC-RH, based on elliptic curve cryptography, shows relatively higher computational overheads even for smaller key sizes but provides enhanced security, as evidenced by its faster decryption time compared to AES and MCP-ABE for the largest key size (1039 bits). These results underscore the trade-offs between security and computational performance, emphasizing the importance of selecting the appropriate cryptographic method based on specific security requirements and key sizes in a given application.

CONCLUSION AND DISCUSSION

In nut-shell, this study gives a progressive synthetic intelligence-based totally safety answer geared toward safeguarding the privacy and confidentiality trendy healthcare programs inside an IoT- cloud environment. The primary objective ultra-modern this take a look at is to leverage artificial intelligence techniques to make certain at ease data storage and retrieval processes. The proposed Probabilistic fantastic brand new (PSL) technique, designed to count on assaults proactively, is intended to decorate the safety contemporary the healthcare application framework through schooling the version with a numerous set contemporary learned capability. moreover, to make certain the at ease garage and retrieval latest facts, the research has advanced and integrated a Random Hashing (RH)-based key generation method with the Elliptic Curve Cryptography (ECC) mechanism. This precise synthetic intelligence technique includes maintaining a trained facts version with a variety of everyday and attack attributes, allowing early detection latest capability threats. additionally, it carries an alert machine that notifies the firewall and updates the skilled model with the information ultra-modern any detected assaults. furthermore, the data safety device is reinforced by means of producing a random key based at the hash price and signature pattern present day the information grid. The research also highlights the challenges posed by the entry of devices into a healthcare provider's temporary workplace, such as the complexities of determining the device's operating system and life cycle management, especially in cases like Bring Your Own Device (BYOD). Devices that connect to the network through unconventional channels may present connectivity issues and exploit vulnerabilities due to their unorthodox entry into the network, requiring heightened awareness and security measures. Overall, this research contributes to the field of data security in IoT-cloud environments by proposing an advanced artificial intelligence-based security solution that addresses the specific challenges of healthcare applications. By integrating cutting- edge techniques and methodologies, the proposed solution aims to establish a robust and proactive security framework for protecting sensitive healthcare data.

REFERENCES

[1]. M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, "Sensors of smart devices in the internet of everything (IoE) era: Big opportunities and massive doubts," Journal of Sensors, vol (2019), 26 pages, https://doi.org/10.1155/2019/6514520.

[2]. Z. Ahmed, K. Mohamed, S. Zeeshan, and X. Dong, "Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine," Database. vol. (2020) DOI: 10.1093/database/baaa010

[3]. K. Saleem, I. S. Bajwa, N. Sarwar, W. Anwar, and A. Ashraf, "IoT healthcare: design of smart and cost-effective sleep quality monitoring system," Journal of Sensors, vol. (2020), 17 pages, https://doi.org/10.1155/2020/8882378

[4]. T. M. Ghazal, "Internet of things with artificial intelligence for health care security," Arabian Journal for Science and Engineering, vol.2, (2021), pp. 1–12. https://doi.org/10.1007/s13369-021-06083-8

[5]. M. R. Valanarasu, "Smart and secure IoT and AI integration framework for hospital environment," Journal of ISMAC, vol.1, (2019), pp. 172–179. DOI:10.36548/jismac.2019.3.004

[6]. L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: moving AI to the edge," Pattern Recognition Letters, vol. 135, (2020) pp. 346–353. DOI: 10.1016/j.patrec.2020.05.016

[7]. H. K. Bharadwaj, A. Agarwal, V. Chamola et al., "A review on the role of machine learning in enabling IoT based healthcare applications," IEEE Access, vol. 9, (2021) pp. 38859–38890, DOI:10.1109/ACCESS.2021.3059858

[8]. M. Anuradha, T. Jayasankar, N. Prakash et al., "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," Microprocessors and Microsystems, vol. 80, (2021) article 103301. DOI:10.1016/j.micpro.2020.103301

[9]. J.-X. Hu, C.-L. Chen, C.-L. Fan, K. H. Wang, and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," Journal of Sensors, vol. (2017), pages 11. https://doi.org/10.1155/2017/3734764

[10]. G. B. Mohammada, S. Shitharthb, and P. R. Kumarc, "Integrated machine learning model for an URL phishing detection," International Journal of Grid and Distributed Computing, vol. 14, (2020) no. 1, pp. 513–529. DOI: https://doi.org/10.4108/eai.20-4-2022.173950

[11]. S. S. Gill, S. Tuli, M. Xu et al., "Transformative effects of IoT, blockchain and artificial intelligence on cloud computing:

evolution, vision, trends and open challenges," Internet of Things, vol. 8, (2020),article 100118. https://doi.org/10.1016/j.iot.2019.100118

[12]. S.Shakya, "An efficient security framework for data migration in a cloud computing environment," Journal of Artificial Intelligence, vol. 1, (2019) no. 1, pp. 45–53. DOI 10.36548/jaicn.2019.1.006

[13]. M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," IEEE Transactions on Industrial Informatics,,vol. 16, (2019) no. 10, pp. 6532–6542, DOI:10.1109/TII.2019.2945367

[14]. T. Hidayat and R. Mahardiko, "A systematic literature review method on aes algorithm for data sharing encryption on cloud computing," International Journal of Artificial Intelligence Research, ,vol. 4,(2020) no. 1, pp. 49–57. DOI:10.29099/ijair.v4i1.154

[15]. S. Shitharth, N. Satheesh, B. P. Kumar, and K. Sangeetha, "IDS detection based on optimization based on WI-CS and GNN algorithm in SCADA network," in Architectural Wireless Networks Solutions and Security Issues, Springer, Singapore 2021. https://doi.org/10.1155/2022/8457116