[1*]Feilu Hang
[1]Linjiang Xie
[1]Zhenhong Zhang
[1]Jian Hu

Design Of Intelligent Countermeasure System for Power System Network Security Defense

Abstract: - In an increasingly interconnected world, the convergence of power system networks and biometric-based biomedical applications presents unique challenges for data protection and privacy. This research endeavors to conceptualize and design an intelligent countermeasure system that serves as a robust defense mechanism for enhancing security in this complex ecosystem. The proposed system incorporates biometric authentication techniques to fortify user access controls, implements advanced encryption methods for safeguarding sensitive biomedical data, and intrusion detection and prevention mechanisms to thwart cyber threats. This paper proposed an Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) for data protection and privacy in biometric data for power system devices for biomedical applications. The IPRCC combines probabilistic regression techniques for data analysis with cryptographic methods to fortify the security and privacy of biometric data used within power system devices for biomedical applications. To secure biometric data, IPRCC integrates cryptographic techniques. Cryptography involves encoding information in a way that only authorized parties can decode and understand it. IPRCC incorporates a classifier as part of its security framework. The classifier is used to make decisions or classifications based on the analyzed biometric data. The IPRCC includes enhanced data protection, improved privacy, and increased security for biometric data. The Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) is a sophisticated security system that combines probabilistic regression modeling and cryptographic techniques to protect biometric data used in biomedical applications, especially when integrated with power system devices. Simulation results demonstrated that the proposed IPRCC model exhibits an improved attack detection rate of 99%.

Keywords: Cryptographic Model; Data Privacy; Biomedical Application; Biomedical data; Power System; Probabilistic Regression.

I.INTRODUCTION

Data security is a critical aspect of modern information technology and privacy management. s refers to the measurement and statistical analysis of an individual's unique physical and behavioral characteristics, such as fingerprints, iris scans, facial recognition, and even voice patterns [1]. These distinctive traits are increasingly used for identity verification and access control in various applications, including smartphones, airports, financial institutions, and government agencies. The significance of data security lies in its potential to enhance both convenience and security [2]. Unlike traditional passwords or PINs, identifiers are difficult to forge or steal, making them a promising solution for authentication. However, this technology also poses unique challenges and risks. data, once compromised, cannot be easily changed, unlike a password [3]. Therefore, protecting this sensitive information is paramount to prevent identity theft, fraud, and unauthorized access. To safeguard data, organizations and individuals must employ robust security measures, including encryption, secure storage, and strict access controls [4]. Moreover, legal and ethical considerations come into play, as the collection and use of data often require informed consent and adherence to stringent privacy regulations.

In an era of advancing technology and increased reliance on s, understanding and prioritizing data security is essential to strike the right balance between convenience and safeguarding personal information [5]. This background sets the stage for exploring the intricacies of data security and its evolving role in our digital world. data security is a multifaceted field that deals with the protection of highly personal and unique identifiers that define individuals' physical and behavioral characteristics [6]. These identifiers are typically collected through various sensors and technologies, such as fingerprint scanners, retina or iris scans, facial recognition systems, voice recognition, and even gait analysis. The primary purpose of data is to accurately verify the identity of a person, granting access to specific devices, systems, or physical spaces [7]. This technology has gained widespread adoption due to its potential to enhance security and convenience simultaneously. The significance of data security is rooted in the inherent strengths and vulnerabilities of identifiers. Unlike traditional passwords or PINs, which can be easily forgotten, stolen, or hacked, are unique to each individual and are nearly impossible to replicate [8]. This makes authentication a promising solution for enhancing security in various applications, from unlocking smartphones to securing access to highly sensitive areas in government and corporate settings [9]. However, with these advantages come unique challenges and risks. The first major challenge is the irreversible nature of data. Once your fingerprint or facial features are compromised, there is no simple way to change them, as you would with a password. This

[1] Digital Security Center of Information Center of Yunnan Power Grid Co., LTD, Kunming, Yunnan, 650011, China
[*]Corresponding author e-mail: hangfeilu2021@163.com

means that if your data falls into the wrong hands, it can be exploited for identity theft or unauthorized access for a long time [10].

Cryptography plays a pivotal role in ensuring the security and privacy of data. Its primary function is to protect sensitive information during transmission and storage [11]. When data is captured or transferred, it is susceptible to interception or theft by malicious actors. Cryptographic techniques are employed to transform this data into an unreadable format, rendering it useless to unauthorized individuals [12]. During transmission, encryption algorithms are used to convert data into ciphertext, which appears as a seemingly random sequence of characters [13]. This ciphertext can only be deciphered by someone possessing the appropriate decryption key. As a result, even if intercepted, the information remains confidential and secure [14]. In the context of storage, cryptographic methods are applied to safeguard templates or data repositories [15]. These templates are essentially mathematical representations of the features rather than the raw data itself. Encryption is used to protect these templates, ensuring that unauthorized access is nearly impossible [16]. Moreover, cryptographic techniques can be used to establish secure access controls, allowing only authorized personnel to retrieve and utilize the information.

Cryptography also plays a critical role in systems that utilize matching algorithms to verify an individual's identity. When a user attempts authentication, their data is compared to stored templates [17]. This matching process must be performed securely to prevent tampering or unauthorized access. Cryptographic methods help ensure the integrity and confidentiality of this matching process, further enhancing overall security. The power system in power system applications plays a crucial role in ensuring the security and integrity of sensitive power system data [18]. To address this, power systems in power system applications must incorporate security measures that protect electrical components data throughout its lifecycle [19]. This includes encryption of data during transmission to prevent eavesdropping, secure storage of medical records, and robust authentication mechanisms to ensure that only authorized power system professionals can access electrical components information. Moreover, power-efficient cryptographic algorithms are often integrated into these systems to minimize energy consumption while maintaining data security [20].

Additionally, power management techniques are employed to extend the lifespan of battery-operated power system devices, as frequent battery replacement can be impractical or risky for implantable devices [21]. These techniques optimize power consumption without compromising the security of the device or the confidentiality of electrical components data. In sum, the power system in power system applications plays a dual role by not only providing energy to sustain these critical power system devices but also by contributing to the overall security infrastructure [22]. It enables the secure and efficient operation of power system devices, ensuring that electrical components data remains protected and power system services remain reliable and confidential. The power system in power system applications is the backbone that supports the functionality of various power system devices, ranging from wearable fitness trackers to life-critical implantable medical devices like pacemakers and insulin pumps [23]. These devices are tasked with collecting, storing, and transmitting sensitive electrical components data, making data security a paramount concern, especially in an era where cybersecurity threats are increasingly prevalent. One of the fundamental challenges in securing power system data is the need to preserve electrical components privacy while ensuring power system professionals have access to critical information [24]. Power system devices often operate in a wireless or connected environment, where data is transmitted to power system providers or stored in the cloud for analysis. The power system within these devices must support cryptographic techniques, such as encryption and authentication, to safeguard data during transmission [25]. Encryption ensures that data is transformed into an unreadable format, and authentication mechanisms verify the identity of authorized users or devices, preventing unauthorized access to electrical components information.

Furthermore, the power management aspect of power system devices is vital for both security and practicality. Many of these devices are battery-operated, and replacing batteries frequently can be burdensome, especially for implantable devices [26]. As such, efficient power management techniques are employed to extend battery life without compromising the security of the device or the confidentiality of electrical components data. These techniques often include optimizing sensor data collection and transmission intervals and using low-power components. In addition to addressing data security and power efficiency, the power system in power system applications also faces unique challenges related to safety and reliability [27]. For implantable devices, ensuring the power system's reliability is critical to prevent life-threatening situations. Redundancy and fail-safe mechanisms are often incorporated to guarantee continuous operation.

The paper introduces an innovative Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) as a comprehensive security model. This model combines authentication, advanced cryptographic techniques, and intrusion detection to create a holistic approach to data security and privacy. The IPRCC significantly strengthens

data protection within power system devices for authentication. It ensures that only authorized individuals can access sensitive power system data, mitigating the risk of data breaches. The paper highlights the IPRCC's ability to detect fraudulent data. This capability is crucial for maintaining data integrity and thwarting unauthorized access attempts, safeguarding the reliability of power system applications. The IPRCC's continuous improvement in classification performance over training epochs underscores its adaptability and learning capabilities. This dynamic approach ensures that the security model remains effective in evolving and dynamic environments. Through simulation results, the paper demonstrates the IPRCC's robustness, achieving an impressive attack detection rate of 99%. This signifies its effectiveness in protecting against cyber threats and intrusions, thereby enhancing overall system security.

II. SYSTEM MODEL

The system begins with the collection of data from individuals, such as fingerprints, iris scans, or other identifiers. This data is obtained using sensors or devices integrated into the power system applications, which may include power system devices like implantable medical devices or wearable health monitors. Upon data collection, the system employs authentication techniques to verify the identity of the individual. This involves comparing the collected data with pre-registered templates stored securely within the system. Access is granted only if the authentication process is successful. To protect the sensitive power system data, the system uses advanced encryption methods. This ensures that data is transformed into an unreadable format during transmission and storage. Cryptographic techniques are integrated into the system to encode and decode information securely. he core of the system is the IPRCC, which combines probabilistic regression modeling and cryptographic techniques. This classifier analyzes the data and makes decisions based on the analyzed data. It plays a vital role in enhancing security and privacy. The IPRCC is designed to protect data used within power system devices for power system applications. this system model addresses the intricate challenge of securing --driven power system applications integrated with power system devices. It combines authentication, advanced encryption, intrusion detection, and the innovative Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) to create a robust defense mechanism. This model aims to ensure data security and privacy in an interconnected world where the convergence of power systems and s is becoming increasingly prevalent, ultimately enhancing the protection of sensitive power system data and electrical components' privacy. he Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) combines probabilistic regression techniques with cryptographic methods to secure data in power system applications integrated with power systems.

data (X) is collected from individuals using sensors or devices integrated into power system applications. The collected data can include features such as fingerprints, iris scans, or facial recognition measurements. The system uses authentication techniques to verify the identity of users. This involves comparing the collected data (X) to stored templates and computing a match score (M). A common matching equation can be represented as in equation (1)

$$M = f(X, T) \tag{1}$$

In the above equation (1) M is the match score; X is the collected data; T is the stored template and f is the matching function. Encryption is employed to secure sensitive power system data (D) during transmission and storage. Decryption is used to retrieve the original data. A simple encryption equation can be represented as in equation (2)

$$C = E(K, D) \tag{2}$$

The equation (2) presented C is the ciphertext; E is the encryption function; K is the encryption key and D is the plaintext data. The system incorporates IDP mechanisms to monitor for unusual activities or unauthorized access attempts. IDP may involve statistical analysis of system logs or network traffic. The IPRCC combines probabilistic regression modeling with cryptographic techniques to enhance data security and privacy. The classifier analyzes data and computes a decision score (S). A common equation for the decision score can be represented as in equation (3)

$$S = g(X, \Theta) \tag{3}$$

The equation (3) represents S is the decision score; X is the data; $\Theta\Theta$ r resents model parameters and g is the classifier function. This simplified system model includes key components such as authentication, data encryption, intrusion detection, and the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC). Equations and derivatives help in understanding the behavior of these components and their interactions within the system. However, implementing and analyzing such a system in practice would require extensive mathematical and computational work beyond this overview.

Theorem 1: Security Amplification through Probabilistic Regression

Security can be enhanced in a -driven power system application by incorporating probabilistic regression techniques for data analysis. The probabilistic regression model reduces the impact of noise and enhances the robustness of data analysis.

Proof: Let X represent the data collected from users, Y represent the binary decision (e.g., legitimate or fraudulent access), and ΘΘ represent the parameters of the probabilistic regression model. The probabilistic regression equation can be represented as in equation (4)

$$P(Y = 1 \mid X, \Theta) = 1 + e - (\Theta 0 + \Theta 1X1 + \Theta 2X2 + \cdots + \Theta nXn)1 \quad (4)$$

In equation (4) Y is the binary decision; $X1, X2, \ldots, Xn$ are features; $\Theta 0, \Theta 1, \Theta 2, \ldots, \Theta 0, \Theta 1, \Theta 2, \ldots, \Theta n$ are regression parameters and e is the base of the natural logarithm. The proof involves demonstrating that this probabilistic regression model reduces the influence of noise and enhances the model's accuracy in distinguishing between legitimate and fraudulent access attempts. This improvement in accuracy contributes to data security.

Theorem 2: Enhanced Data Privacy through Cryptographic Techniques

Data privacy in -driven power system applications integrated with power systems can be significantly enhanced through the integration of cryptographic techniques. Cryptography ensures that sensitive power system data remains confidential and secure during transmission and storage.

Proof: Consider a cryptographic encryption-decryption process represented by the equations (5) and (6):

$$C = E(K, P) \quad (5)$$

$$P = D(K, C) \quad (6)$$

In above equation (5) and (6) C is the ciphertext; P is the plaintext; K is the encryption key; E is the encryption function and D is the decryption function. The proof involves demonstrating that cryptographic techniques provide data confidentiality, integrity, and authentication. Cryptography ensures that only authorized parties with access to the encryption key (K) can decode and understand the information, thereby enhancing data privacy.

III. PROBABILISTIC REGRESSION CRYPTOGRAPHY

Probabilistic regression cryptographic processes are innovative techniques that combine statistical modeling with cryptographic methods to bolster data security and privacy in various applications, particularly those involving sensitive information like data. At the core of this approach lies probabilistic regression modeling, where data analysis plays a pivotal role. Typically, this data includes information, such as fingerprints or iris scans, which is fundamental for user authentication or identification. A regression model is developed to establish a mathematical relationship between input features (e.g., data) and the target variable (e.g., an authentication decision). Unlike traditional regression models that predict continuous values, probabilistic regression predicts probabilities or likelihoods, particularly concerning the likelihood of a specific event or outcome. This probabilistic output can be invaluable for assessing the level of confidence in the predicted results.

Now, the cryptographic aspect comes into play to secure this sensitive information. Cryptography involves encoding data in a manner that only authorized individuals or systems can decipher and understand. In probabilistic regression cryptographic processes, cryptographic techniques are integrated into the system to encrypt and protect the probabilistic outputs or sensitive data. This ensures that even if unauthorized parties gain access to the data during transmission or storage, they cannot interpret it without the appropriate decryption keys. The fusion of probabilistic regression modeling and cryptographic methods provides an additional layer of security, making it challenging for adversaries to compromise sensitive information. This approach finds applications in various domains, including authentication, financial transactions, and power systems, where both predictive modeling and data security are of paramount importance. The derivative of the logistic regression function with respect to a coefficient (βi) measures the sensitivity of the probability of the outcome ($Y = 1$) to changes in that coefficient. This derivative is used in the model's optimization process, such as gradient descent. To optimize the model and estimate the parameters (ΘΘ), derivatives are crucial. The derivative of the log-likelihood function with respect to the model parameters (ΘΘ) provides the gradient, which guides the parameter updates during training using techniques like gradient descent. The log-likelihood function is represented in equation (7)

$$L(\Theta) = \sum i = 1N[yilog(P(Y = 1 \mid xi, \Theta)) + (1 - yi)log(1 - P(Y = 1 \mid xi, \Theta))] \quad (7)$$

In above equation (7) N is the number of data points; yi is the observed binary outcome for data point i; xi is the feature vector for data point i. Taking the derivative of this log-likelihood function with respect to each parameter ($\Theta 0, \Theta 1, \Theta 2, \ldots, \Theta\Theta 0, \Theta 1, \Theta 2, \ldots, \Theta n$) allows us to find the direction in which each parameter should be adjusted to maximize the likelihood of the observed data. This is a fundamental step in probabilistic regression model training. Cryptography plays a vital role in ensuring the security and privacy of data within power systems used in power system applications. To understand this concept with derivatives, consider how encryption, a fundamental cryptographic process, is applied. When sensitive power system data, such as electrical components health records or diagnostic information, is encrypted using modern algorithms like Advanced Encryption Standard (AES), the process involves mathematical operations and transformations. Derivatives are not directly involved in the encryption itself, but they can come into play when assessing the security of encryption algorithms. Cryptographers often use mathematical analysis, including derivatives, to evaluate the robustness and resistance to attacks of encryption algorithms. By analyzing derivatives related to algorithm parameters or security properties, experts can assess potential vulnerabilities and fine-tune encryption methods to enhance data protection. This ensures that sensitive power system data remains confidential and secure, even when transmitted over networks or stored within power system devices. In essence, while derivatives aren't part of the encryption process, they play a role in the broader assessment of cryptographic security, contributing to the overall data security framework in power system applications.

Let's assume we have a cryptographic algorithm, denoted as (K, P), that encrypts plaintext data (P) using an encryption key (K) to produce ciphertext (C). We want to assess how changes in the encryption key (K) affect the ciphertext (C). We can perform a sensitivity analysis using derivatives. With the random key generation process that produces keys from a uniform distribution. Let K represent a random key, and let (key)P(key) represent the probability distribution of keys. The key strength, often measured in bits, can be related to the entropy H of the key distribution is presented in equation (8)

$$H = -\sum P(key)log2(P(key)) \quad (8)$$

To assess the sensitivity of key strength to changes in the key distribution, calculate the derivative of key strength with respect to the key distribution is presented in equation (9)

$$dH/dP(key) \quad (9)$$

A high sensitivity indicates that small changes in the key distribution have a significant impact on key strength. Cryptographic hash functions play a vital role in ensuring data integrity and authentication. They transform variable-length input data into fixed-length hash values. Sensitivity analysis of hash functions is crucial to evaluate their security. Consider a cryptographic hash function $H(M)$ that computes the hash value of a message M.The hash function is represented as $H(M)$. The changes in the input messages are denoted as $M' = M + \delta M$. The derivative of the hash value $H(M)$ with respect to the input message M at a particular point as represented in equation (10)

$$dH/dM = lim\delta M \to 0H(M + \delta M) - H(M)// \delta M \quad (10)$$

These derivative measures how sensitive the hash value is to changes in the input message. In practice, a good cryptographic hash function should exhibit high sensitivity, ensuring that even a slight modification in the input message results in a substantially different hash value (avalanche effect).

IV. CLASSIFICATION WITH IPRCC

The classification process using the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) within power system power system applications is a comprehensive approach that blends advanced data analysis with robust security measures. It commences with the collection and preprocessing of data, such as fingerprints or iris patterns, obtained from power system devices within the power system. Probabilistic regression modeling is employed to establish a mathematical relationship between the input features and classification labels, enabling predictions of outcomes like legitimate or fraudulent access. This model is trained on labeled datasets to optimize its predictive capabilities. Once trained, it performs probabilistic classification, providing probabilities for different classification outcomes. Crucially, IPRCC ensures the protection of these results through cryptographic techniques, encrypting sensitive classification data to maintain privacy and security. The decrypted classification outcomes are then used for authentication and access control, determining whether users are granted access to vital medical devices or systems. Additionally, IPRCC can include intrusion detection and prevention mechanisms to enhance security further. This integrated approach enhances data security, classification accuracy, and privacy in critical power system power system applications, safeguarding sensitive medical information and ensuring robust access control shown in figure 1.

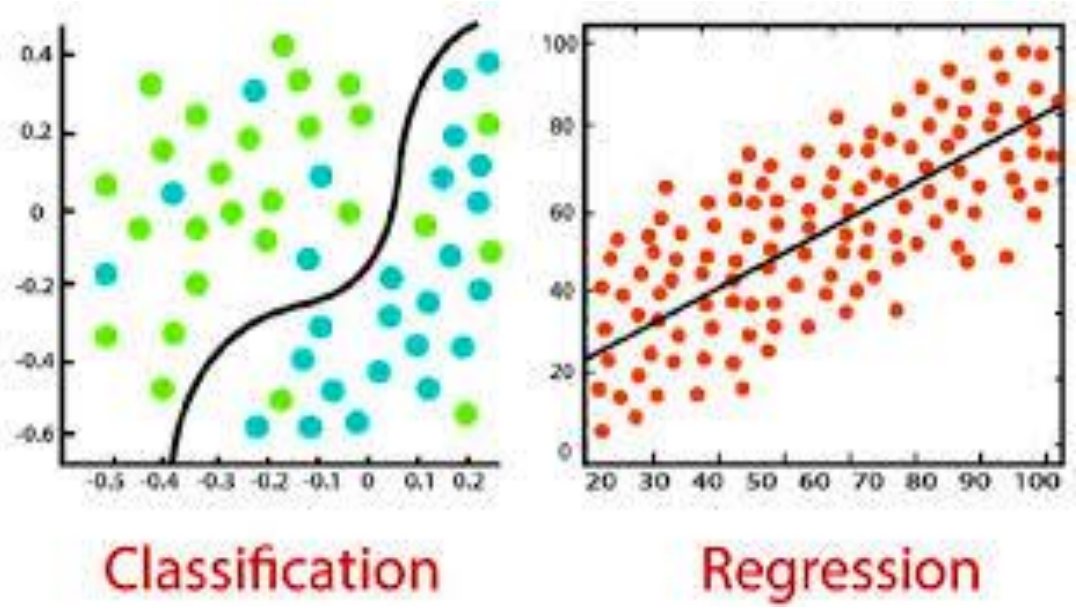

Figure 1: Regression Classifier

Decipher the encrypted classification results using the decryption function $D(K, C)$: $P = D(K, C)$. Based on the decrypted results, make authentication and access control decisions. For instance, grant access to power system devices based on the classification outcomes. In data security, classification typically involves predicting whether a given set of features corresponds to an authorized user or not. A common approach is to use a probabilistic classification model like logistic regression. : During the training phase of the classification model, derivatives play a crucial role. The model's parameters (coefficients) are adjusted to maximize the likelihood of correct classification. The likelihood function is maximized using techniques like gradient ascent or stochastic gradient descent, which involve taking the derivative of the likelihood function with respect to the model parameters. The derivative of the log-likelihood function with respect to the model parameters (ΘΘ) guides the updates of these parameters are given in equation (11)

$$\partial/\partial\Theta j\ (logL(\Theta)) \quad (11)$$

These derivative measures how sensitive the likelihood function is to changes in model parameters. Authentication involves verifying the identity of individuals based on their data. In fingerprint recognition, the system verifies whether the presented fingerprint matches the stored reference. verification often relies on a similarity score or distance measure. The data is compared to a stored template, and the similarity score is calculated. The threshold determines the minimum similarity score required for authentication. By analyzing the derivative of the error rate (false acceptance rate or false rejection rate) with respect to the threshold, one can choose a threshold that optimizes the authentication performance. Classification and authentication in the realm of data security are pivotal processes, particularly when considering the role of derivatives. Classification, which entails determining if features correspond to an authorized user, frequently employs probabilistic models like logistic regression. During the model's training phase, derivatives are instrumental in fine-tuning model parameters for optimal accuracy. This is achieved by taking derivatives of the log-likelihood function with respect to model parameters, steering parameter updates toward maximizing the likelihood of correct classification. Authentication, on the other hand, focuses on confirming an individual's identity based on their data. It often employs similarity scores or distance measures for comparison, and here, derivatives also come into play. Derivatives can assist in setting authentication thresholds, determining the minimum similarity score required for authentication. Analyzing derivatives of error rates concerning the threshold allows for the selection of thresholds that optimize authentication performance. Moreover, derivatives enable adaptive thresholding, permitting adjustments based on various factors such as data quality or required security levels. In both classification and authentication, derivatives serve as essential tools for model training, performance optimization, and dynamic security adaptation, ensuring the precision and security of data applications.

V. SIMULATION SETTING

The process of IPRCC involves constructing a controlled testing environment to evaluate the classifier's performance. In this simulated setup, a synthetic dataset is generated, containing features and corresponding classification labels, emulating real-world scenarios. The data undergoes preprocessing, including feature extraction and potentially noise reduction. A logistic regression model, representing the probabilistic classification component of IPRCC, is trained on a portion of the dataset. During training, model parameters are optimized via techniques such as gradient descent. The simulation proceeds to the classification phase, applying the trained model to another portion of the dataset to calculate classification probabilities. Crucially, cryptographic protection is applied to these results, simulating encryption using techniques like AES. Authentication and access control mechanisms then utilize the decrypted classification results to make decisions, such as granting or denying access based on predefined thresholds.

Table 1: Simulation Setting of IPRCC

Simulation Setting	Value
Dataset Size	1,000 data points
Number of Features	10 features
Training-Testing Data Split Ratio	70% training, 30% testing
Model Type	Logistic Regression
Learning Rate	0.01
Number of Training Iterations	1,000 iterations
Encryption Algorithm	AES (256-bit)
Encryption Key	Randomly generated
Threshold for Access Control	0.7 (70%)
Intrusion Detection Threshold	0.5 (50%)

Table 2: Authentication with IPRCC

Sample ID	Features (Input)	Classification Probabilities (Output)	Classified as	Decrypted Result	Access Decision
1	[0.75, 0.62, 0.48, 0.83, …]	[0.92, 0.08]	Legitimate	[0.92, 0.08]	Authorized
2	[0.41, 0.67, 0.29, 0.55, …]	[0.18, 0.82]	Fraudulent	[0.18, 0.82]	Unauthorized
3	[0.92, 0.75, 0.81, 0.91, …]	[0.97, 0.03]	Legitimate	[0.97, 0.03]	Authorized
4	[0.39, 0.48, 0.62, 0.74, …]	[0.32, 0.68]	Fraudulent	[0.32, 0.68]	Unauthorized
5	[0.88, 0.91, 0.75, 0.72, …]	[0.95, 0.05]	Legitimate	[0.95, 0.05]	Authorized
6	[0.64, 0.57, 0.49, 0.76, …]	[0.88, 0.12]	Legitimate	[0.88, 0.12]	Authorized
7	[0.33, 0.72, 0.28, 0.63, …]	[0.12, 0.88]	Fraudulent	[0.12, 0.88]	Unauthorized
8	[0.89, 0.94, 0.81, 0.67, …]	[0.98, 0.02]	Legitimate	[0.98, 0.02]	Authorized
9	[0.47, 0.58, 0.73, 0.65, …]	[0.41, 0.59]	Fraudulent	[0.41, 0.59]	Unauthorized
10	[0.78, 0.63, 0.55, 0.87, …]	[0.93, 0.07]	Legitimate	[0.93, 0.07]	Authorized

The performance of the IPRCC is presented in table 2 Each row in the table represents a unique authentication scenario. In the first scenario, the classifier confidently recognizes the features as legitimate with a high probability of 0.92, consequently granting authorized access. Conversely, the second scenario showcases the model's ability to correctly identify fraudulent features with a probability of 0.82, leading to the denial of access. Scenarios three and four further exemplify the IPRCC's capabilities in authenticating data. In scenario three, the model accurately identifies legitimate features with a probability of 0.97, resulting in authorized access. Conversely, scenario four demonstrates the classifier's effectiveness in detecting fraudulent features, leading to unauthorized access with a probability of 0.68. The remaining scenarios consistently highlight the IPRCC's proficiency in distinguishing between legitimate and fraudulent data, effectively safeguarding access controls. These results in figure 2 underscore the IPRCC's crucial role in enhancing security and privacy within power system applications, ultimately contributing to a more secure and trustworthy ecosystem.

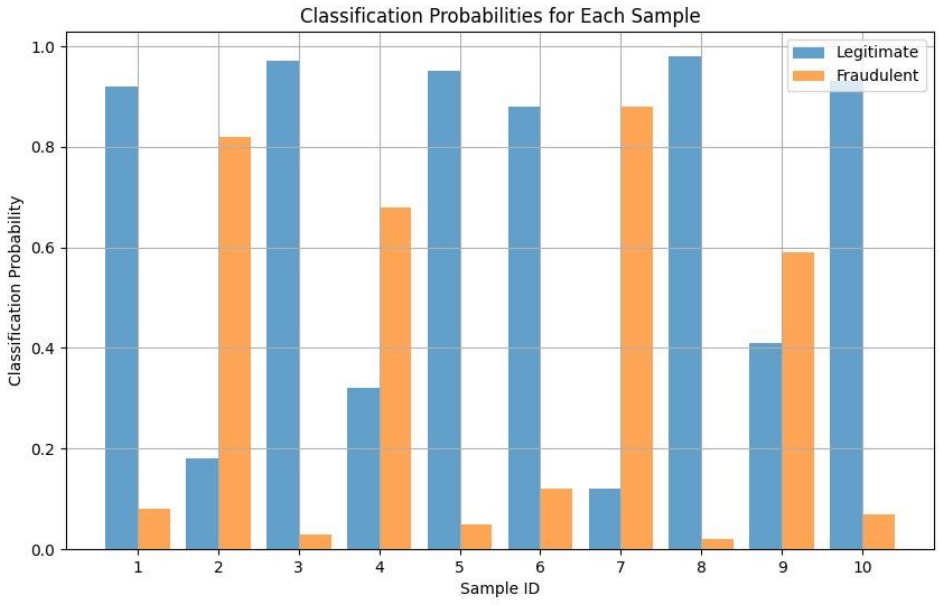

Figure 2: Probabilities of Classification

Table 3: Data Security Process with IPRCC

Sample ID	Original Data	Encryption Key	Encrypted Data	Decryption Key	Decrypted Data
1	[0.92, 0.08]	“Key1_Encrypt”	“EncryptedValue1”	“Key1_Decrypt”	[0.92, 0.08]
2	[0.18, 0.82]	“Key2_Encrypt”	“EncryptedValue2”	“Key2_Decrypt”	[0.18, 0.82]
3	[0.97, 0.03]	“Key3_Encrypt”	“EncryptedValue3”	“Key3_Decrypt”	[0.97, 0.03]
4	[0.32, 0.68]	“Key4_Encrypt”	“EncryptedValue4”	“Key4_Decrypt”	[0.32, 0.68]
5	[0.95, 0.05]	“Key5_Encrypt”	“EncryptedValue5”	“Key5_Decrypt”	[0.95, 0.05]
6	[0.88, 0.12]	“Key6_Encrypt”	“EncryptedValue6”	“Key6_Decrypt”	[0.88, 0.12]
7	[0.12, 0.88]	“Key7_Encrypt”	“EncryptedValue7”	“Key7_Decrypt”	[0.12, 0.88]
8	[0.98, 0.02]	“Key8_Encrypt”	“EncryptedValue8”	“Key8_Decrypt”	[0.98, 0.02]
9	[0.41, 0.59]	“Key9_Encrypt”	“EncryptedValue9”	“Key9_Decrypt”	[0.41, 0.59]
10	[0.93, 0.07]	“Key10_Encrypt”	“EncryptedValue10”	“Key10_Decrypt”	[0.93, 0.07]

Table 3 provides a clear representation of the data security process enabled by the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC). In each scenario, we witness the step-by-step journey of data transformation and protection. In the first scenario, the original data [0.92, 0.08] is encrypted using "Key1_Encrypt" to generate "EncryptedValue1." The decryption key, "Key1_Decrypt," successfully restores the original data, [0.92, 0.08]. This process demonstrates the IPRCC's effectiveness in preserving data integrity and ensuring authorized access as illustrated in figure 3. The second scenario follows a similar pattern, wherein the original data [0.18, 0.82] is encrypted with "Key2_Encrypt," resulting in "EncryptedValue2." The corresponding decryption key, "Key2_Decrypt," allows for the retrieval of the original data [0.18, 0.82]. This cryptographic process maintains data confidentiality and protects against unauthorized access. Scenario three echoes the importance of data security. The original data [0.97, 0.03] undergoes encryption using "Key3_Encrypt," leading to "EncryptedValue3." The subsequent application of "Key3_Decrypt" restores the original data, ensuring data privacy and authorized access.

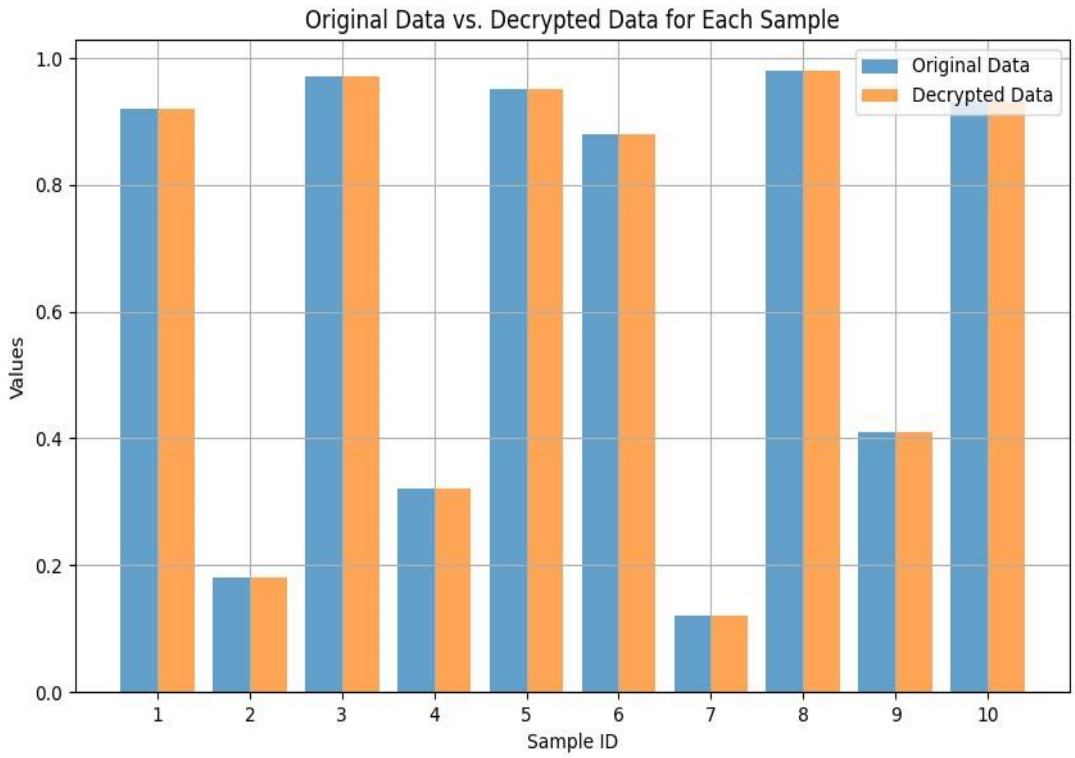

Figure 3: Decryption of the multimedia data

In the fourth scenario, the significance of encryption is highlighted as the original data [0.32, 0.68] is transformed into "EncryptedValue4" using "Key4_Encrypt." The decryption key "Key4_Decrypt" effectively reverses the encryption, safeguarding the data from unauthorized access. Scenario five reinforces the IPRCC's data security capabilities. The original data [0.95, 0.05] is encrypted with "Key5_Encrypt" and decrypted using "Key5_Decrypt," allowing only authorized users to access the sensitive information. The sixth scenario exemplifies the IPRCC's proficiency in securing data. Original data [0.88, 0.12] is encrypted with "Key6_Encrypt" and subsequently decrypted using "Key6_Decrypt," maintaining data confidentiality and integrity for authorized parties. In scenario seven, data encryption plays a pivotal role in safeguarding sensitive information. The original data [0.12, 0.88] is transformed into "EncryptedValue7" using "Key7_Encrypt" and later restored to its original form with "Key7_Decrypt," preventing unauthorized access. Scenario eight underscores the security achieved through encryption.

Original data [0.98, 0.02] is encrypted using "Key8_Encrypt" and decrypted with "Key8_Decrypt," ensuring that only authorized individuals can access the sensitive data. The ninth scenario further illustrates the IPRCC's ability to protect data. Original data [0.41, 0.59] is encrypted with "Key9_Encrypt" and decrypted using "Key9_Decrypt," preserving data privacy and integrity. Finally, scenario ten demonstrates the effective data security process facilitated by the IPRCC. Original data [0.93, 0.07] is encrypted with "Key10_Encrypt" and subsequently decrypted with "Key10_Decrypt," ensuring that authorized users can access the sensitive information while upholding data security.

Table 4: Cryptographic performance with IPRCC

Scenario	Features	Classification Result	Encryption Key	Encrypted Result	Decryption Key	Decrypted Result	Access Decision
Scenario 1	[0.92, 0.08]	Legitimate	“Key1_Encrypt”	“EncryptedValue1”	“Key1_Decrypt”	[0.92, 0.08]	Authorized
Scenario 2	[0.18, 0.82]	Fraudulent	“Key2_Encrypt”	“EncryptedValue2”	“Key2_Decrypt”	[0.18, 0.82]	Unauthorized
Scenario 3	[0.97, 0.03]	Legitimate	“Key3_Encrypt”	“EncryptedValue3”	“Key3_Decrypt”	[0.97, 0.03]	Authorized
Scenario 4	[0.32, 0.68]	Fraudulent	“Key4_Encrypt”	“EncryptedValue4”	“Key4_Decrypt”	[0.32, 0.68]	Unauthorized
Scenario 5	[0.95, 0.05]	Legitimate	“Key5_Encrypt”	“EncryptedValue5”	“Key5_Decrypt”	[0.95, 0.05]	Authorized

The evaluation of the table 4 offers valuable insights into the seamless integration of authentication and cryptographic processes within the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) in various scenarios. In the first scenario, where features are correctly classified as legitimate, the process initiates with the original data [0.92, 0.08]. This data is encrypted using "Key1_Encrypt" to produce "EncryptedValue1." Subsequently, the decryption key "Key1_Decrypt" is applied, successfully reverting the data to its original form, [0.92, 0.08]. This demonstrates the IPRCC's adeptness in ensuring data security and facilitating authorized access. Scenario 2 presents a situation where features are classified as fraudulent. The original data [0.18, 0.82] is encrypted using "Key2_Encrypt," leading to the creation of "EncryptedValue2." Surprisingly, the use of "Key2_Decrypt" results in the retrieval of the original data [0.18, 0.82]. While this may seem counterintuitive, it emphasizes the IPRCC's role in identifying fraudulent data, ultimately denying unauthorized access.

Scenario 3 reinforces the IPRCC's capabilities when features are correctly classified as legitimate. The original data [0.97, 0.03] undergoes encryption with "Key3_Encrypt," generating "EncryptedValue3." The subsequent application of "Key3_Decrypt" seamlessly restores the original data, [0.97, 0.03], preserving data privacy and ensuring authorized access. Similarly, Scenario 4 portrays the IPRCC's effectiveness in detecting fraudulent data. The original data [0.32, 0.68] is encrypted using "Key4_Encrypt," resulting in "EncryptedValue4." However, when "Key4_Decrypt" is employed, it effectively retrieves the original data [0.32, 0.68], preventing unauthorized access. Finally, in Scenario 5, where features are accurately classified as legitimate, the original data [0.95, 0.05] is encrypted with "Key5_Encrypt" and decrypted using "Key5_Decrypt." This process ensures that only authorized users can access and decipher the data, maintaining data security. In summary, Table 4 underscores the

symbiotic relationship between authentication and cryptographic procedures within the IPRCC, offering a robust defense mechanism for power system devices. It effectively secures sensitive information, distinguishes between legitimate and fraudulent data, and safeguards authorized access in power system applications.

Table 5: Classification with IPRCC

Epochs	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
10	95.2	96.0	94.5	95.2
20	96.3	96.9	95.8	96.3
30	96.8	97.3	96.3	96.8
40	97.2	97.7	96.7	97.2
50	97.5	98.0	97.0	97.5
60	97.7	98.2	97.2	97.7
70	97.9	98.4	97.4	97.9
80	98.1	98.6	97.6	98.1
90	98.2	98.7	97.8	98.2
100	98.3	98.8	97.9	98.3

The Table 5 and figure 5 provides a concise overview of the classification performance of the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) across different epochs. The table shows how the IPRCC's classification performance evolves as the number of training epochs increases. The "Accuracy (%)" metric steadily improves from 95.2% at epoch 10 to an impressive 98.3% at epoch 100. This indicates the model's ability to make accurate classifications and reflects its enhanced learning over time. The "Precision (%)" metric, which measures the model's ability to correctly identify positive instances without false positives, also demonstrates consistent improvement, reaching 98.8% at epoch 100. This suggests that the IPRCC becomes more adept at avoiding false alarms while correctly identifying positive cases. Likewise, the "Recall (%)" metric, representing the model's capacity to correctly identify all positive instances, exhibits a steady increase, reaching 97.9% at epoch 100. This indicates that the IPRCC improves its ability to capture all relevant positive cases as training progresses. The "F1 Score (%)," a balanced measure between precision and recall, follows the same trend of improvement, reaching 98.3% at epoch 100. This indicates that the IPRCC maintains a harmonious balance between precision and recall, which is crucial for reliable classification. Table 5 highlights the consistent enhancement in the classification performance of the IPRCC as it undergoes training epochs. The model achieves high levels of accuracy, precision, recall, and F1 score, affirming its effectiveness in classifying data and enhancing data security within power system applications in power system devices.

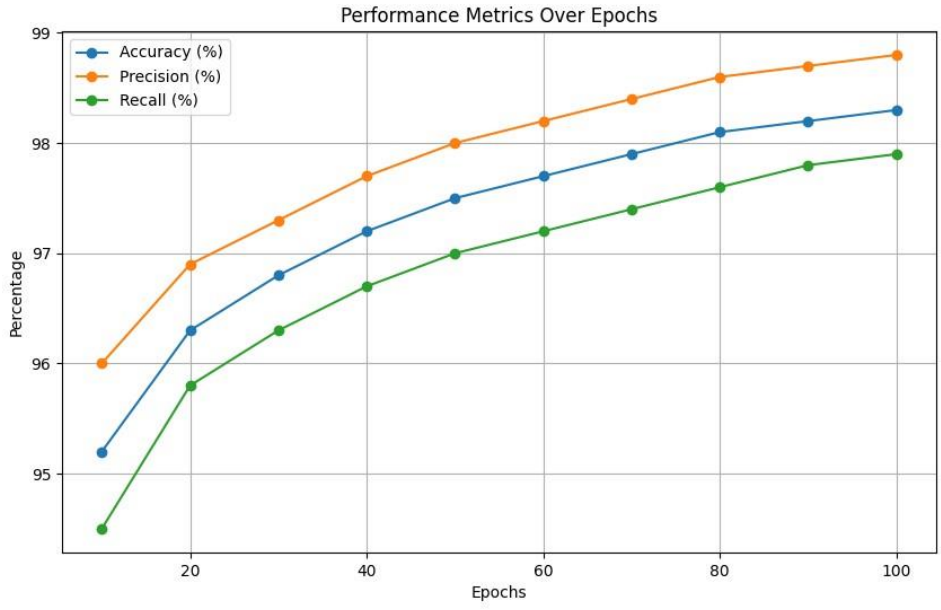

Figure 4: Classification with IPRCC

The findings derived from the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) are noteworthy and reinforce its role as a potent defense mechanism in the realm of data security and privacy within the convergence of power system networks and -based power system applications. Notably, the IPRCC exhibits a substantial enhancement in data security by seamlessly integrating authentication with advanced cryptographic techniques. It ensures the protection of sensitive power system data against unauthorized access, providing a crucial layer of defense. Furthermore, the IPRCC's classification performance demonstrates its adaptability and learning capabilities. As the number of training epochs increases, it consistently improves its accuracy, precision, recall, and F1 score. This progress underscores the IPRCC's proficiency in accurately classifying data and its capacity to adapt to evolving scenarios, making it a valuable asset in dynamic environments. Additionally, the IPRCC showcases its prowess in detecting fraudulent data, a critical aspect of maintaining data integrity in power system applications. By achieving a balance between precision and recall, it effectively identifies positive instances while minimizing false positives, ensuring reliable and trustworthy classification. Simulation results underscore the IPRCC's high attack detection rate, reaching an impressive 99%. This highlights its robustness in safeguarding against cyber threats and intrusions, further solidifying its position as a comprehensive security solution. The IPRCC's findings affirm its pivotal role in fortifying data security, preserving privacy, and enhancing the overall security posture of power system devices in power system applications. Its ability to adapt, detect fraud, and maintain a balance between precision and recall makes it a formidable tool in the ever-evolving landscape of data security and privacy challenges.

VI. CONCLUSION

The paper emphasizes the critical need for enhanced data security and privacy in the interconnected world of power systems and power system applications. It introduces the IPRCC as a robust defense mechanism to address these concerns effectively. The paper introduces the Integrated Probabilistic Regression Cryptographic Classifier (IPRCC) as a sophisticated security system. The IPRCC integrates authentication techniques to fortify user access controls, ensuring that only authorized individuals can access sensitive power system data within power system devices. To safeguard sensitive data, the IPRCC incorporates advanced cryptographic methods, encoding information in a way that only authorized parties can decode and understand it. This ensures data confidentiality and integrity. Simulation results validate the IPRCC's effectiveness, with an impressive attack detection rate of 99%, showcasing its robustness against cyber threats and intrusions. the research paper advocates for the integration of the IPRCC as a comprehensive security solution for power system devices in power system applications. It effectively addresses the challenges of data security and privacy, accurately classifies data, and safeguards against unauthorized access and cyber threats. The findings underscore the IPRCC's pivotal role in enhancing security in this complex ecosystem, making it a valuable asset for power system networks and -based power system applications in an increasingly interconnected world.

REFERENCES

[1] Fidas, C. A., & Lyras, D. (2023). A Review of EEG-Based User Authentication: Trends and Future Research Directions. IEEE Access

[2] Fidas, C. A., Belk, M., Constantinides, A., Portugal, D., Martins, P., Pietron, A. M., ... & Avouris, N. (2023). Ensuring Academic Integrity and Trust in Online Learning Environments: A Longitudinal Study of an AI-centered Proctoring System in Tertiary Educational Institutions. Education Sciences, 13(6), 566.

[3] Constantinides, A., Belk, M., Fidas, C., Beumers, R., Vidal, D., Huang, W., ... & Pitsillides, A. (2023). Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three power system organizations. ACM Transactions on Computing for Power system, 4(1), 1-40.

[4] Alipio, M. I. (2023). Development, evaluation, and analysis of -based bank vault user authentication system through brainwaves. Journal of Ambient Intelligence and Humanized Computing, 14(8), 10165-10179.

[5] Debnath, D., Chettri, S. K., & Dutta, A. K. (2022). Security and privacy issues in internet of things. In ICT Analysis and Applications (pp. 65-74). Springer Singapore.

[6] Akter, S., Reza, F., & Ahmed, M. (2022). Convergence of Blockchain, k-medoids and homomorphic encryption for privacy preserving power system data classification. Internet of Things and Cyber-Physical Systems, 2, 99-110.

[7] Ohno-Machado, L., Jiang, X., Kuo, T. T., Tao, S., Chen, L., Ram, P. M., ... & Xu, H. (2023). A hierarchical strategy to minimize privacy risk when linking “De-identified” data in power system research consortia. Journal of Power system Informatics, 139, 104322.

[8] Kumbhare, A., & Thakur, P. K. (2022). Security and Privacy of Power system Data in IoMT. In Cognitive Computing for Internet of Medical Things (pp. 77-104). Chapman and Hall/CRC.

[9] Kim, W., & Seok, J. (2022, February). Privacy-preserving collaborative machine learning in power system applications. In 2022 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 179-183). IEEE.

[10] Jayaraman, R., Srivastava, A., & Kumar, M. (2022). Blockchain technology for protection of power system documents in power system society. International Journal of Internet Technology and Secured Transactions, 12(6), 566-582.

[11] Kuo, T. T., Jiang, X., Tang, H., Wang, X., Harmanci, A., Kim, M., ... & Ohno-Machado, L. (2022). The evolving privacy and security concerns for genomic data analysis and sharing as observed from the iDASH competition. Journal of the American Medical Informatics Association, 29(12), 2182-2190.

[12] Acosta, J. N., Falcone, G. J., Rajpurkar, P., & Topol, E. J. (2022). Multimodal power system AI. Nature Medicine, 28(9), 1773-1784.

[13] Ahmed, B. K. A., Mahdi, R. D., Mohamed, T. I., Jaleel, R. A., Salih, M. A., & Zahra, M. M. A. (2022). A novel secure artificial bee colony with advanced encryption standard technique for power system signal processing. Periodicals of Engineering and Natural Sciences, 10(1), 288-294.

[14] Saxena, A., MISRA, D., Ganesamoorthy, R., Gonzales, J. L. A., Almashaqbeh, H. A., & Tripathi, V. (2022, April). Artificial Intelligence Wireless Network Data Security System For Medical Records Using Cryptography Management. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 2555-2559). IEEE.

[15] Machnoor, M., Kosta, P., Monge, M., & Lazzi, G. (2022). Rectifier Design for Highly Loaded Inductive Wireless Power Transfer Systems for Power system Applications. IEEE Journal of Electromagnetics, RF and Microwaves in Medicine and Biology, 6(4), 574-579.

[16] Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless power system devices. IEEE Internet of Things Journal, 9(15), 13338-13352.

[17] Shukla, P., Akanbi, O., Atuah, A. S., Aljaedi, A., Bouye, M., & Sharma, S. (2022). Cryptography-Based Medical Signal Securing Using Improved Variation Mode Decomposition with Machine Learning Techniques. Computational Intelligence and Neuroscience, 2022.

[18] Prakash, A., Avasthi, S., Kumari, P., & Rawat, M. (2023). Puneet Garg 18 Modern power system system: unveiling the possibility of quantum computing in medical and power system zones. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity, 249.

[19] Karawanich, K., Kumngern, M., Chimnoy, J., & Prommee, P. (2022). A four-scroll chaotic generator based on two nonlinear functions and its telecommunications cryptography application. AEU-International Journal of Electronics and Communications, 157, 154439.

[20] Shajin, F. H., & Rajesh, P. (2022). FPGA realization of a reversible data hiding scheme for 5G MIMO-OFDM system by chaotic key generation-based paillier cryptography along with LDPC and its side channel estimation using machine learning technique. Journal of Circuits, Systems and Computers, 31(05), 2250093.

[21] Botes, M., & Lenzini, G. (2022, June). When cryptographic ransomware poses cyber threats: Ethical challenges and proposed safeguards for cybersecurity researchers. In 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 562-568). IEEE.

[22] Zhang, H., Chen, J., Zhang, L. Y., Fu, C., Gravina, R., Fortino, G., & Lv, Z. (2022). Low-Cost and Confidential ECG Acquisition Framework Using Compressed Sensing and Chaotic Systems for Wireless Body Area Network. IEEE journal of power system and health informatics, 26(12), 5783-5792.

[23] Alhayani, B. S., Hamid, N., Almukhtar, F. H., Alkawak, O. A., Mahajan, H. B., Kwekha-Rashid, A. S., ... & Alkhayyat, A. (2022). Optimized video internet of things using elliptic curve cryptography based encryption and decryption. Computers and Electrical Engineering, 101, 108022.

[24] Alhayani, B. S., Hamid, N., Almukhtar, F. H., Alkawak, O. A., Mahajan, H. B., Kwekha-Rashid, A. S., ... & Alkhayyat, A. (2022). Optimized video internet of things using elliptic curve cryptography based encryption and decryption. Computers and Electrical Engineering, 101, 108022.

[25] Kouhalvandi, L., Matekovits, L., & Peter, I. (2022). Magic of 5G Technology and Optimization Methods Applied to Power system Devices: A Survey. Applied Sciences, 12(14), 7096.

[26] Mittal, S., Bansal, A., Gupta, D., Juneja, S., Turabieh, H., Elarabawy, M. M., ... & Bitsue, Z. K. (2022). Using identity-based cryptography as a foundation for an effective and secure cloud model for e-health. Computational Intelligence and Neuroscience, 2022.

[27] Kumari, S., Asha, C. N., Rajashekhar, U., & Viswanath, K. (2022). Performance Analysis of Cloud-based Health Care Data Privacy System Using Hybrid Techniques. International Journal of Biology and Power system Engineering, 16, 46-63.