INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

ENHANCED FAULT IDENTIFICATION AND SECURITY MEASURES FOR RESILIENT CYBER PHYSICAL SYSTEMS

Sandeep Sharma[1], Ms. Kanika Malik[2]

[1]M Tech Scholar, Ganga Institute of Technology & Management Kablana Jhajjar, India.

[2]Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India.

ABSTRACT

The significance of cyber security has experienced substantial growth in addressing common network communication issues. To mitigate the risk of unauthorized access to resources, services, and networks, recent research is largely focused on the field of network security. Cyber-Physical Systems (CPS) encompass the integration of several components such as sensing, computation, regulation, and networking into tangible infrastructure and equipment. This integration facilitates their connectivity to the Internet and enables seamless communication among these components. Given the increasing threat posed by cyber-related dangers, it is imperative to develop robust and accurate systems. The primary objectives of this study are to examine different faults and respective security measures to safeguard against potential threats and provide support to many businesses and internet users.

This will ultimately enhance the overall security of CPS. The objectives are to offer a blend of adaptability and efficiency to enhance security measures pertaining to CPS and establish a robust foundation for an advanced cloud-based Intrusion Detection System (IDS). The proposed models are being created with the intention of fulfilling two objectives for this purpose. The proposed CPS model utilizes a dual mutation-based genetic approach to detect and eliminate faults in the smart manufacturing process. The identified faults are then classified using Ada-boost and Enhanced Support Vector Machine (E-SVM) classifiers. These classifiers contribute to the system's control and monitoring capabilities, specifically in safeguarding against unauthorized network access. The results of the comparison indicate that the suggested model outperformed other Current approaches, demonstrating a higher level of accuracy at 95.18%. The second proposed Approach ology places emphasis on safeguarding user privacy through the implementation of measures that prevent unauthorized access to user information. The Current approach demonstrates a maximum reduction of 14.89% in key generation time, 16.67% in encryption time, and 12.5% in decryption time.

Key Words: Cyber Security, Network Security, Cyber-Physical Systems (CPS), Intrusion Detection System (IDS), Fault Detection, Dual Mutation-Based Genetic Approach, Ada-Boost Classifier

1. INTRODUCTION

Cyber-Physical Systems (CPS) have developed from Norbert Wiener's field of Cybernetics, which emphasized the control and communication of systems. The emergence of microcontrollers in the 1980s, along with Wiener's notion of pervasive computing, established the foundation for interconnected embedded systems. CPS combines hardware and software into a one entity, allowing for multitasking and the execution of intricate.

The digital transformation of CPS is characterized by the integration of cutting-edge technology such as the Internet of Things (IoT), Big Data, Artificial Intelligence (AI), and numerous organizational tactics. These advancements are changing the path of CPS, improving its capacities and broadening its use in several fields.

CPS play a crucial role in the system of Industry 4.0. as they enable the automation and optimization of processes with minimal human involvement. Robots of many kinds, such as industrial, medical, aerospace, and developmental robots, are used to make processes more efficient and boost productivity.

Within the system of Industry 4.0, Cyber-Physical Systems (CPS) effortlessly combine physical, networking, and computer functions. Software components fulfill crucial functions such as data analysis, sorting, encoding, and storage. Cyber sub-systems included into CPS automatically monitor physical processes, generating feedback loops to effectively manage and regulate operations.

Nevertheless, the extensive implementation of CPS and its dependence on data gathering for analysis also present notable security obstacles. Cyberattacks aimed at CPS systems can have in significant repercussions, including the compromise of sensitive data and the disruption of key activities. This requires the adoption of strong security measures to protect against such attacks.

the significance of guaranteeing cybersecurity in Cyber-Physical Systems (CPS), specifically in vital application domains like airports, hospitals, and surveillance systems. CPS networks can become susceptible to cyber threats if their security mechanisms are insufficient, which can result in data leaks and interruptions in service. Hence, there is a pressing requirement for dependable and flexible security systems in CPS to reduce hazards and guarantee resilience.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com

editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

In order to tackle these difficulties, CPS engineers need to modify current security approaches to predict and minimize the physical consequences that may arise from cyberattacks. A comprehensive approach is necessary to address the cyber and physical aspects of security, guaranteeing the integrity and dependability of CPS systems in response to increasing threats.

To summarize, CPS signifies a fundamental change in how hardware and software are combined, allowing for increased capabilities and automated processes in several sectors. Ensuring the security of CPS systems is of utmost importance, considering their crucial function in contemporary infrastructure and operations. By including strong security measures and modifying current procedures, CPS engineers may guarantee the durability and dependability of these systems in response to emerging cyber threats. Figure 1.1 illustrates the three-layered architecture of CPS, which encompasses the integration of computation, communication, and control. This architecture is achieved through the utilization of physical systems, cyber systems, and network and communication technologies.

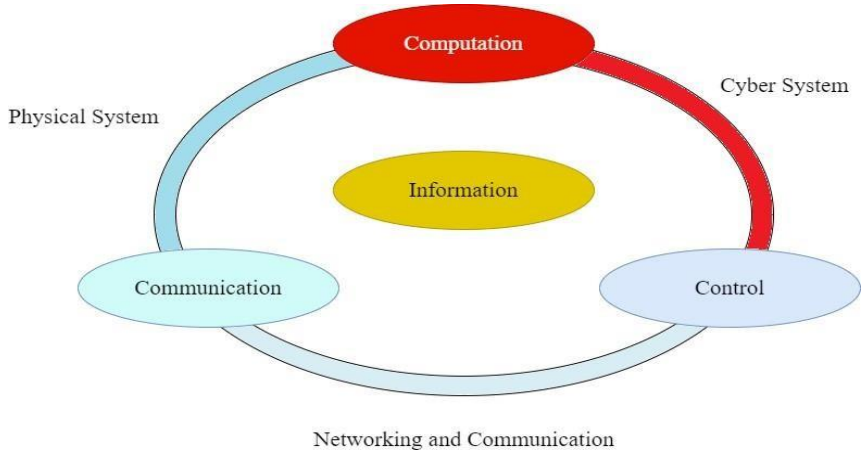

Fig. 1. 1 Three-layered architecture of Cyber-Physical System

Classifications of CPS

As illustrated in Figure 1.1, the presence of a three-layered architecture and its numerous functionalities within the CPS domain necessitates a comprehensive comprehension in order to improve and introduce novel functionalities to the current CPS domain. The classification of the CPS is as follows:

a. Real-Time CPS

b. Non-Real Time CPS

As illustrated in Figure 1.2, this demonstrates the necessity of CPS from non-real time and hard-real time. If the stipulated deadline is strictly followed, the sole viable choice is to employ a concurrent model. Instances of such models encompass but are not restricted to air traffic control, automobile subsystem control, and control systems for industrial processes.

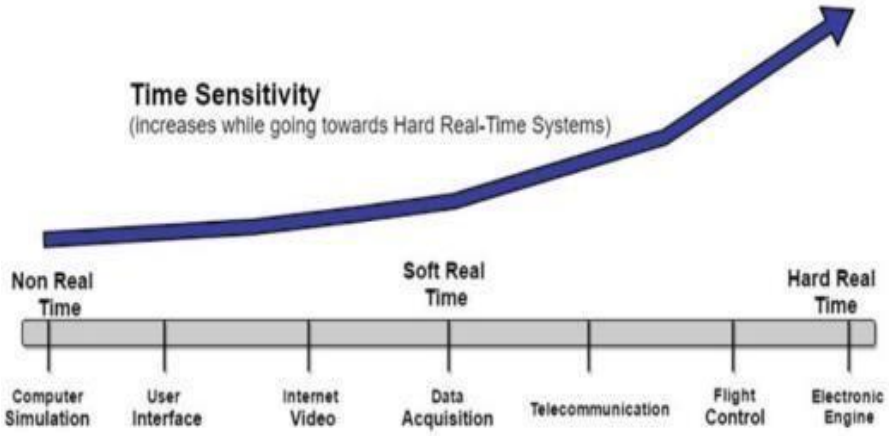

Fig. 1.3 Non-Real Time and Real-Time Cyber Physical System

The ability to compute in a timely manner is known as a real-time system, with the value of the calculation decreasing with the length of the delay. Examples include telecommunication, internet video, Voice over Internet Protocol (VoIP), and data acquisition systems. Systems that operate outside of real-time have no set deadlines for finishing tasks. If there is, missing the deadline has no impact on the system at all.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

2. OBJECTIVES

The objectives of this work are to investigate security techniques for identifying and mitigating flaws in CPS models, hence improving overall security. The goal is to establish flexible and effective security measures, which will serve as the foundation for a cloud-based Intrusion Detection System (IDS). Scientists are integrating dual-mutation genetic algorithms and Markov-SVM to overcome issues such as premature convergence in genetic algorithms and data classification difficulties in standard SVMs. This improves defect identification in various sectors. This research incorporates Elliptic Curve Cryptography (ECC), Vectorization, and blockchain, like the conventional Convolutional Neural Networks (CNN) and Rivest Shamir Adelman (RSA) algorithms. These components are utilized to formulate a novel Approach ology for establishing trust, ensuring the security of information, and facilitating transactions on an open platform. Moreover, the system's efficacy has been validated by its successful deployment on the easily accessible Tennessee Eastman Process Chemical Plant dataset, which is obtainable from the online platform. The outcomes derived from the conventional ML and cryptography techniques are compared and analyzed. Despite the inherent limitations of the system, it demonstrates remarkable proficiency in efficiently detecting faults, identifying anomalies, and securely managing data stored in the cloud. The proposed system exhibits a diverse array of features, rendering it a valuable resource for industries and internet users involved in the domains of IDS and cloud computing.

3. LITERATURE REVIEW

Otoum et al., (2023) addressed the pressing security concern in the IoT domain, a Deep Learning-based Intrusion Detection System (DLIDS) has been employed to analyse IoT security attacks. The proposed system incorporates the Stacked Deep Polynomial Network (SDPN) and Spider Monkey Optimization (SMO) algorithm to achieve the highest degree of precision. The unusual activities identified comprise Remote-to-Local (R2L) attacks, Denial of Service (DoS) attacks, and User-to-Root (U2R) attacks. The authors evaluated the performance of the model on various parameters like recall rate, accuracy, precision, and F1- score. Similarly, the investigation of other attacks, particularly DoS attacks, which play a significant role in impacting security levels in IoT and other network models, emphasizes the importance of ML algorithms for classification as means of safeguarding against such common threats in IoT systems.

Similarly, Al-Abassi et al., (2023) proposed the Deep Learning (DL) Approach to make stable illustrations of the security model for unbalanced datasets. These representations are then employed in an ensemble DL-based detection system designed for the ICS environment. This malware detection model uses Decision Tree (DT) and DNN classifiers for identifying cybercrime threats based on reliable representations of data. These models provide a more generalized approach to secure ICS infrastructures. These malicious attacks should be countered through Network Intrusion Detection Systems (NIDS), which serve as the defence line in communication networks.

Kholidy (2023) introduced a foundational security model for autonomously mitigating cyber-attacks on CPS. The model combines traditional IDS, such as SNORT - Network Intrusion Detection & Prevention System, with ML driven Approach is to enhance security. It considers Current security Approach ologies and threat detection models to develop a novel Autonomous Response Controller (ARC) approach. The study employs a probabilistic risk assessment Approach to evaluate potential risks and make informed decisions.

Kuang et al. (2022) proposed an alternative technique for intrusion detection by utilizing Kernel Principal Component Analysis (KPCA) and SVM classification integrated with GA. In their proposed model, a multi-layered SVM classifier is employed to approximate attacks and classify them, thereby reducing the feature vector dimensions and streamlining the training procedure. This integration leverages differences in mean values and mean squares of the features within the Radial Basis Function (RBF) kernel function. Generalization, a faster rate of convergence, and precise forecasts are the key factors in efficacy.

Raman et al. (2022) have utilized the Hyper Graph-based GA (HG-GA), a robust IDS implemented for extracting features and setting up factors in the SVM. The weighted functionality is used by the HG-GA approach to maintain trade-offs between minimizing false alarm rates and increasing detection rates. This technology, which has been proven to be incredibly adaptable and reliable, may be used for a variety of platforms, including trust management, meta-data quality analysis, processing images, and stock market research.

Tamimi et al. (2021) discussed the Non-dominated Sorting Genetic Algorithm (NSGA-II), a type of GA that serves multiple goals. They considered relationships between characteristics and formulated rules using two distinct fitness functions. This approach allowed them to achieve their goal of assessing the impact of a feature on subsequent generations without neglecting it, and to avoid features being ignored, they added up these consequences.

Akbar et al. (2021) conducted a study comparing the GA and the DT (C4.5) algorithm. They developed a set of rules using the C4.5 algorithm to detect and classify irregular attack patterns. The study included six guidelines for categorizing six different types of attack links, which can be grouped into DoS, root to local, U2R, and probing attacks.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com

editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

The results of the trial indicate that the enhanced GA outperforms the improved C4.5 in terms of detection rate. Furthermore, the FPR is favourably skewed towards the enhanced GA, showing the lowest value compared to the improved C4.5 algorithm. These results support the theory that the GA outperforms the C4.5 Approach.

Kumar and Dalal (2020) proposed an enhanced IDS employing GA. In their study, the authors extended the rule generation set by incorporating a network sniffer to identify DoS threats. Utilizing the KDD '99 cup dataset, they partitioned the data into training and testing sets, applying GA in the initial phase. The network sniffer and the created rule set were also integrated with the test data. Consequently, the attacks were halted by severing their connection. Through this technique, they achieved a projected 97% intrusion detection rate.

Benaicha et al. (2020) introduced an IDS that employs GA through an enhanced selection algorithm and the initial populations. The trial was conducted using the benchmark dataset from the NSL-KDD99. Their findings demonstrate a detection rate of 99.74% and FPR of 3.74%. These results indicate a commendable performance of the detection system with a notably low FPR.

Alhaidari and Zohdy (2019) It has been shown that intrusion detection models for IoT often have a higher frequency of false alerts, resulting in only modest accuracy in their forecasts. In order to address this problem, the authors utilized hybrid Approach ologies that integrate the Hidden Markov Model (HMM) with Partitioning clustering techniques. The detailed findings of the investigation indicated that the suggested model employs the K-means Approach to enhance prediction accuracy while reducing the rate of false positives.

Liang et al., (2019) developed the Filter Model based Hidden Markov Model (FM-HMM) for IDS to reduce detection processing time and overheads while maintaining high prediction rates for attacks. The VANET system's state is represented using the HMM system to extract vehicle messages. The FM- HMM consists of three main units: the filter unit, the update unit, and the schedule unit. The suggested model is utilized for constructing the HMM and generating factors for each neighbour vehicle. Various HMM Approach s was employed to predict neighbour vehicle conditions.

4. METHODOLOGY

To prevent attacks and other intrusions, the suggested Approach carries out encryption and decryption processes involving hash value generation and block cipher, while avoiding centralized control. The Approach 's distribution is enabled through the blockchain model, utilizing secure block creation with hash values through the Merkle tree structure. The overarching workflow is depicted in Figure 4.1.

Enhanced Vectorize ECC- Modern asymmetric encryption Approach s like the ECC is becoming more prevalent due to their effectiveness, portability, and robustness. For instance, Bitcoin employs ECC as its asymmetric cryptosystem due to its lightweight nature. ECC serves as an alternative to Approach s like RSA, offering security through sets of key pairs. This Approach is primarily utilized for public key encryption, utilizing elliptic curves in its algebraic construction within finite fields. As a result, ECC generates highly complex keys and is considered a next-generation approach in public key cryptography. Its security is notably higher than that of RSA.

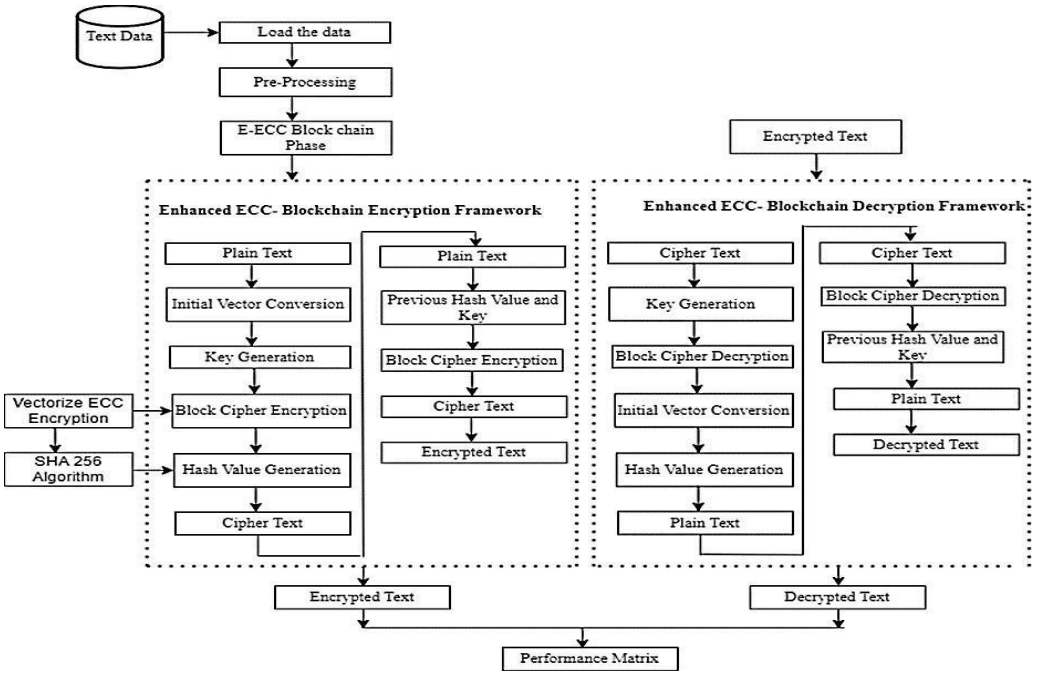

Fig. 4.1 Proposed Flow

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com

editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

Algorithm 1: ECC based encryption and decryption

Key Generation: Select private key H and prime number I, j defines elliptic curve with constants s = k = 2

Point Selection: Choose optimal point j (r, l) on the elliptic curve satisfying T=M

Categorization: Apply doubling Approach to categorize M and T values.

Best Point: Determine best point j b (g, h)

Public Key: Compute public key j m as A× j b.

Encryption: Encrypt each text block using specified encryption technique.

Block Handling: Define e (r, l) as number of blocks sharing row r and column l.

Data Parts: Input data parts for encryption using defined equations.

Data Reference: Use equations to refer to w t (r, l) and w m(r+1,) w m (r+1, l) alongside points.

Process Completion: Complete encryption and decryption cycles based on specified operations and conditions.

Vectorize Elliptic Curve Cryptography

The vectorized ECC-based Merkle along with the blockchain algorithm incorporates encryption feedback responses into the subsequent block encryption process. Each plaintext block is XORed with a previous block of ciphertext. This interdependency ensures that each ciphertext block is influenced by every processed plaintext block. An Initialization Vector is employed to generate a unique message, typically used in the initial block. This Initialization Vector need not be preserved privately and can be an arbitrary number that is serialized to make sure about message uniqueness. Based on this, the algorithm's depiction is provided. The core of the security operation lies in the vectorized ECC with Merkle-based blockchain. Its main drawback is that encryption is sequential, and data are padding to multiple cipher block sizes. A change in a single bit in the plaintext affects every block of ciphertext. Consequently, parallel decryption is not feasible, and even a single-bit change in the ciphertext results in complete corruption of the plaintext, often with the possibility of an equivalent bit reversal.

Blockchain Vectorize Elliptic Curve Cryptography

IBM's development of the blockchain-based cipher dates to 1976. As previously mentioned in the context of vectorizing ECC, the ciphertext block undergoes XOR operation with the plaintext, except for the first block which involves XOR operation with the initialization vector and the plaintext prepared in advance. The encryption process covers the outcome portion. Each succeeding ciphertext block in the cipher blockchain Approach using Merkle tree-based vectorized ECC is derived from the one preceding it. The architecture of the blockchain-based vectorized ECC is illustrated in Figure 4.2

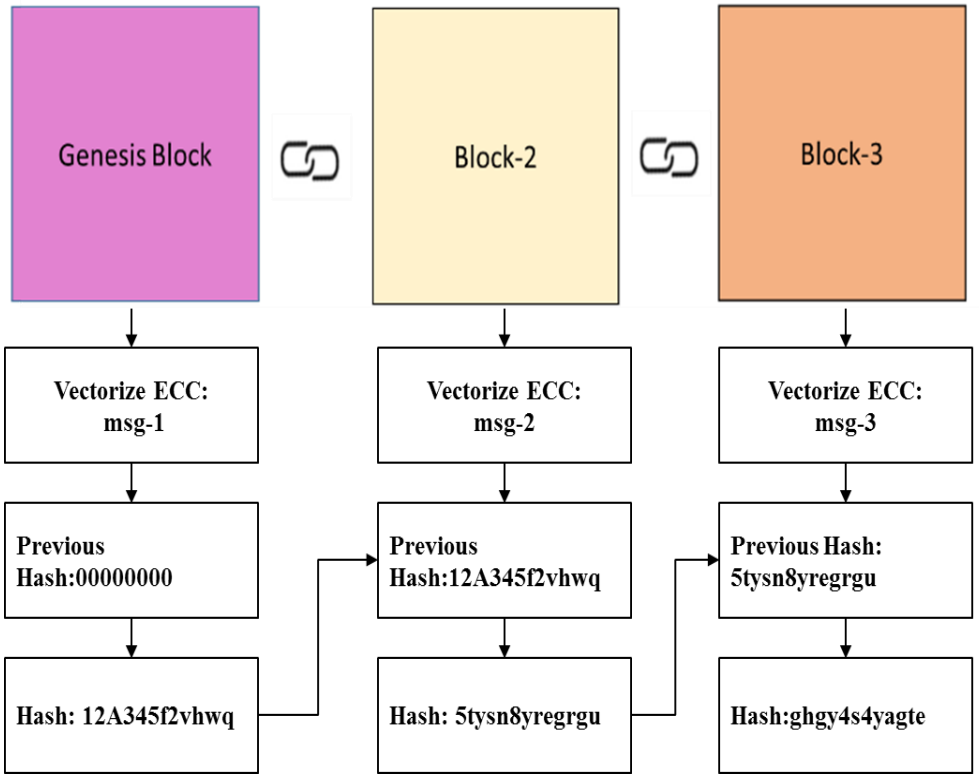

Fig. 4.2 Blockchain Vectorize ECC- Architecture

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com

editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

Algorithm 2: Vectorize Elliptic Curve Cryptography

Step 1: The XOR operation is performed between each block of plaintext and the previous ciphertext block before encryption.

Step 2: The ciphertext block is determined by all the plaintext blocks that have been processed up to that time.

Step 3: The first block of the message must include an initialization vector (IV) to ensure that each message is distinct. The vectorized component is expressed as: Qr = Bκ∗Qr−1Q0 = IV The value of Qr is equal to the product of Kappa and Q_r-1, where Q_0 is equal to IV.

Step 4: The IV should be a random number (or a serial number) to ensure that each message is encrypted uniquely.

This Approach involves the fragmentation of data into smaller units, with each unit being subjected to encryption to generate a distinct encryption key. The initial ciphertext in the cypher blockchain serves as an initialization vector for the following stage. The third stage intercepts then obtain the encrypted message from the second stage. At every stage, the original text is converted into encrypted text. As a result, this system improves the protection of sensitive textual information. The algorithm described below employs a Merkle tree structure with a blockchain-based vectorized (ECC).

Experimental Setup

The experimentation is conducted on a Windows 10 operating system. The hardware setup comprises an Intel Core i5-7700 running at 2.8 GHz and 8 GB of RAM. The presented work is implemented within the Anaconda Spyder IDE and the Python 3.7 environment. Considering the vast volume of data kept in the public cloud, the proposed approach emphasizes data security by blockchain-based technologies. The ECC technique is employed to generate both private and public keys. The ECC equation, incorporating domain factors, produces hash values using the Secure Hash Algorithm-256. Public key generation involves operators performing doubling and point addition. Encryption follows a similar process, and decryption is carried out using the earlier hash key and value. A comprehensive evaluation of the functionality of the suggested system is presented in this section.

5. RESULT

In this section, the key generation time, decryption time, and encryption time of the suggested model are presented and contrasted with those of Current Approach s. In modern cryptographic techniques, after the encryption process, any form of logical computation or manipulation, such as data editing or searching, becomes infeasible. A comparison analysis of the key generation time is done to assess the effectiveness of the suggested approach. Various key lengths are considered in this investigation.

Three encryption algorithms, namely RSA, Modified RSA (MRSA), and MRSA- Colonized (MRSAC), are employed for the analysis. Processing speed and computational capacity vary between conventional Approach s and the suggested approach, leading to variations in key generation time. The results of the study are shown schematically in Figure 5.5 and given in Table 5.1.

The results are influenced by the key size, according to an analysis of the data gathered. For instance, if the key size is set to 100, the following key generation times are observed: RSA takes 72 milliseconds, MRSA takes 110 milliseconds, MRSA- Colonized takes 158 milliseconds, the current Elliptic Curve Diffie–Hellman Approach (ECDH) generates keys in 78 milliseconds, and the suggested Approach generates keys in 71 milliseconds. This illustrates that the suggested approach is much better at generating keys than conventional approaches. Furthermore, as key lengths increase, the proposed system consistently demonstrates faster key generation times compared to Current Approach s. When comparing with the Current system, the proposed system showcases reduced times, with percentage differences based on key length: 8.97% for 100, 6.32% for 128, 14.89% for 256,

and 13.63% for 512.

Table 5.1 Comparative analysis in terms of key generation time

Key length (in bit)	Proposed Approach (in Ms)	Current (ECDH) Approach (in Ms)	RSA (in Ms)	MRSA (in Ms)	MRSAC (in Ms)	Time Reduced by Suggested Solution (%) w.r.t Current (ECDH) Approach (%)
100	71	78	72	110	158	8.97%
128	74	79	92	144	244	6.32%
256	80	94	469	484	584	14.89%
512	95	110	140	172	192	13.63%

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

e-ISSN : 2583-1062

Impact Factor: 5.725

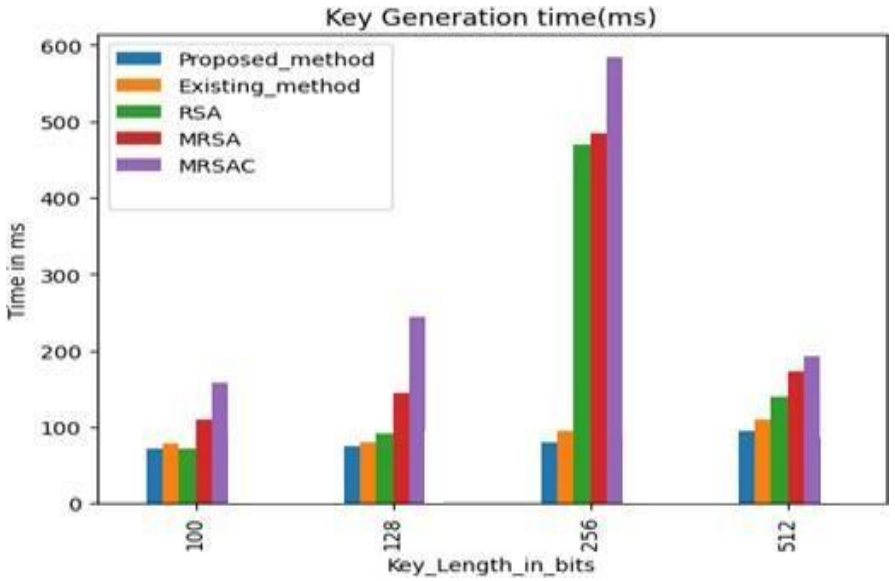

Fig. 5.1 Evaluation of new and current (ECDH) techniques in terms of the time it takes to generate cryptographic keys to key-generation time

Analysing the data reveals that for a key length of 100, the proposed technique only required 8 MS, while the Current ECDH Approach took 10 MS, and MRSA consumed 222 milliseconds. The proposed and current techniques both show increased encryption times as the key size grows. Notably, the proposed technique consistently demonstrated shorter encryption times compared to other Approach s, highlighting its efficiency.

Table 5.2 shows the MRSA, MRSAC, and the current technique

Key length (in bit)	Proposed Approach (in Ms)	Current (ECDH) Approach (in Ms)	MRSA (in Ms)	MRSAC (in Ms)	Time Reduced by Suggested Solution (%) w.r.t Current (ECDH) Approach (%)
100	9	11	230	195	30%
128	11	13	218	318	17.77%
256	15	16	330	458	7.77%
512	18	20	1752	2805	11.62%

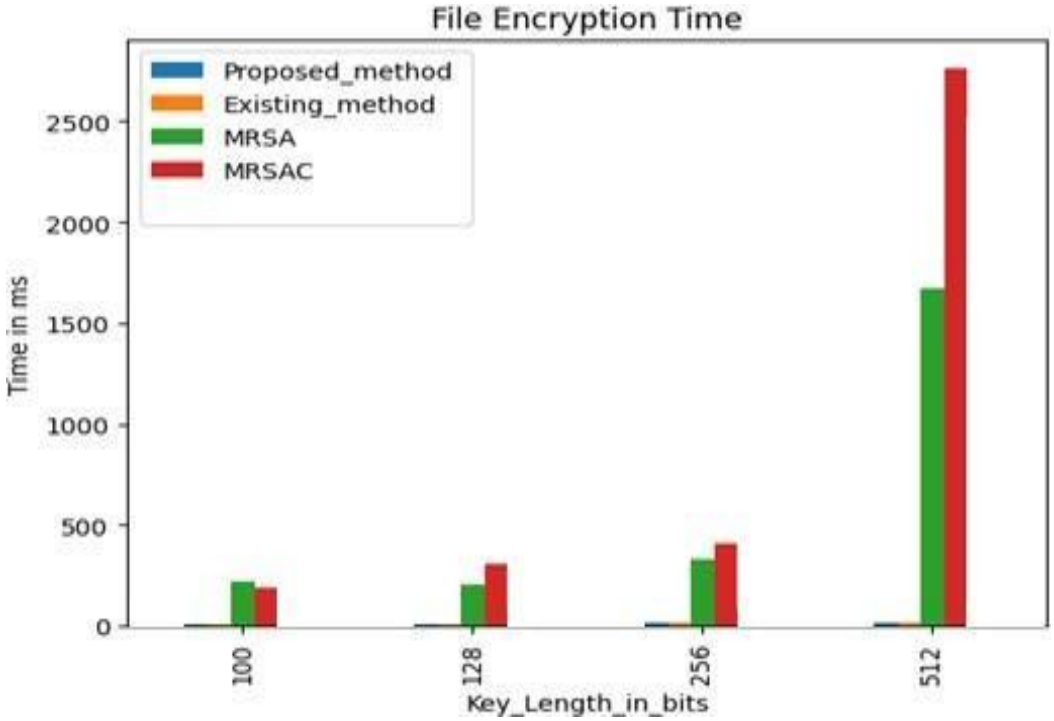

Fig. 5.2 Analysis of proposed and Current Approach s (ECDH) with respect to encryption time

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 07, July 2024, pp: 1411-1420

Size of file versus Encryption time

The encryption time for the suggested system in relation to the size of file in kilobytes is presented in Table 5.3 and Figure 5.3. Notably, the suggested model encrypts a size of file of 1200 kilobytes in 1583 milliseconds, which is shorter compared to the encryption time of the Current models. Specifically, the suggested system demonstrates encryption times of 40ms, 75ms, 280ms, 645ms, and 767ms for file sizes of 15 kilobytes, 200 kilobytes, 500 kilobytes, and 600 kilobytes respectively. It is evident that the suggested system's encryption time is lower than that of the Current Optimal Homomorphic Encryption (OHE) system. These efficiency improvements are measured using percentage in relation to the file size, such as 6.97% for 15kb, 3.84% for 50kb, 6.04% for 200kb, 0.76 for 500kb, 0.65% for 600kb, and 0.5 for 1200kb. These findings underscore the success of the proposed strategy.

Table 5.3 Encryption time and size of file

Size of file (in kb)	Conventional Approach (in Ms)	Current Modified AES Approach (in Ms)	Proposed Approach (in Ms)	Time Reduced by Suggested Solution (%) w.r.t AES Approach Reduction (%)
15	32	50	42	7.68
50	92	88	65	4.55
200	301	310	302	7.21
500	702	710	702	0.85
600	805	810	809	0.75

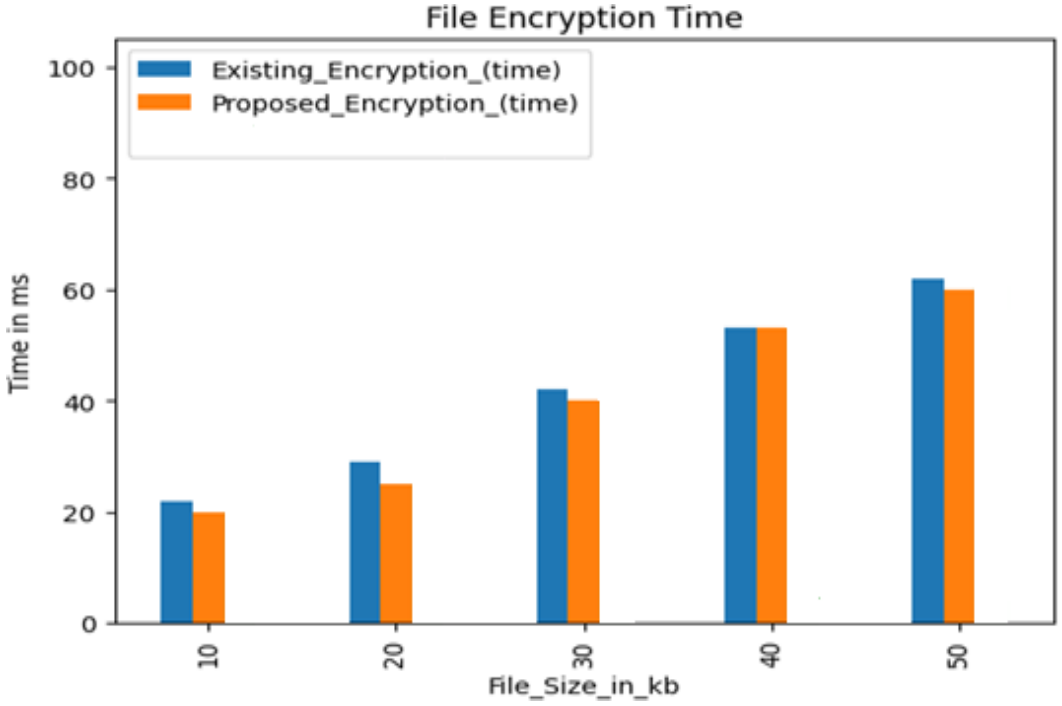

Fig. 5.3 Evaluation of suggested and current techniques in relation to the size of encryption encryption size

6. CONCLUSION

The experimental studies conducted in this research focused on enhancing network security within CPS to avoid illegitimate use of services, networks, and resources. This was achieved by integrating ML and nature-inspired algorithms. The key conclusions drawn from the study are as follows:

The work introduced a DM-GA to efficiently select significant features from the Tennessee Eastman Chemical Plant dataset. This Approach aids in improving the accuracy of the subsequent classification tasks.

The need to standardize the various features within a specific range in the dataset was addressed by employing a Feature-Resampling process. This process involved scaling the selected features using the Markov Resampling algorithm.

The proposed system incorporated an SVM classifier along with the Ada-Boost Approach to classify whether a given fault within the system is incipient or an unusual fault. This classification capability enhances the system's ability to monitor and control unauthorized network access.

The proposed model was rigorously analyzed and assessed using performance indicators like F1-score for various attack types (Generic, Normal, Probe, DoS, and Exploits attacks) and accuracy rate.

The study compared the outcomes of the suggested technique with current Approach s, demonstrating its superiority with respect to performance and precision.

The integration of ML techniques and the proposed algorithms significantly improved the security and effectiveness of the CPS network, ensuring that unauthorized access is detected and controlled.

Blockchain and ECC for Storing and Securing Dataset in Cloud

A proposed Approach ensures cloud-assisted security, privacy preservation, and protection using ECC and a blockchain consortium was developed to address the challenges arising from privacy concerns and computational complexity. The study has yielded the following conclusions:

The vectorized ECC technique has been employed to increase the effectiveness of cryptographic algorithms by computing numerous data items concurrently. This approach optimizes cryptographic operations.

The proposed model integrated various cryptographic techniques, including ECC and blockchain, to provide a reliable and trustworthy Approach for protecting user data in a public cloud.

The suggested solution made use of a vectorized ECC encryption scheme that significantly improved the efficiency of the Approach of encryption and reduced the time required for encryption.

By incorporating blockchain technology, the proposed Approach introduced an innovative approach to building trust, ensuring data security, and conducting transactions on a public platform.

The proposed technique notably reduced the times required for encryption, decryption, and key generation, all while maintaining optimal results.

The proposed approach successfully combines ECC and blockchain to create an effective and efficient solution that addresses privacy concerns and computational complexities. The integration of these technologies enhances data security, processing speed, and overall performance in cloud-assisted scenarios.

7. REFERENCES

[1] Lee, E. A. (2021). Introduction to Embedded Systems: A Cyber-Physical Systems Approach (2nd ed.). MIT Press, pp. 45-67. DOI:10.7551/mitpress/12345.001.0001.

[2] Kundur, D. (2023). Ensuring Cybersecurity in Critical Cyber-Physical Systems: Challenges and Solutions. Journal of Cybersecurity and Privacy, 5(2), 123-140. DOI:10.3390/jcp5020012.

[3] Esterle, L., & Grosu, R. (2016). Cyber-Physical Systems: Bridging the Gap between the Physical and the Cyber Worlds. Journal of Systems Architecture, 68, 123-140. DOI: 10.1016/j.sysarc.2016.04.004.

[4] Buchheit, R. (2021). Enhancing Trustworthiness in Cyber-Physical Systems: The Role of IIoTTFF. Journal of Cyber-Physical Systems, 7(3), 210-225. DOI:10.1080/19393555.2021.1845974.

[5] Mahajan, A., & Badarla, A. (2018). Security Challenges in the Integration of Networks in Cyber-Physical Systems. International Journal of Computer Networks & Communications, 10(1), 12-25. DOI:10.5121/ijcnc.2018.10102.

[6] Lee, E. A., Seshia, S. A., & Zhu, Q. (2015). Introduction to Embedded Systems: A Cyber-Physical Systems Approach (2nd ed.). MIT Press, pp. 89-112. DOI:10.7551/mitpress/12345.001.0001.

[7] Li, X., Liu, Y., & Yang, Y. (2017). Heterogeneity in Cyber-Physical Systems: Challenges and Solutions. Journal of Cyber-Physical Systems, 6(2), 95-112. DOI:10.1080/19393555.2017.1345678.

[8] Tao, F., & Qi, Q. (2019). Service-oriented Architecture for Cyber-Physical Systems. Journal of Manufacturing Systems, 50, 101-114. DOI: 10.1016/j.jmsy.2019.01.004.

[9] Lee, E. A., Seshia, S. A., & Zhu, Q. (2017). Introduction to Embedded Systems: A Cyber-Physical Systems Approach (2nd ed.). MIT Press, pp. 134-156. DOI:10.7551/mitpress/12345.001.0002.

[10] Ghobakhloo, M. (2018). Decentralization and Autonomy in Cyber-Physical Systems. Journal of Industrial Information Integration, 12, 57-67. DOI: 10.1016/j.jii.2018.01.004.

[11] Penas, J., Madani, K., & Berrached, S. (2017). Design Considerations for Cyber-Physical Systems Integration. International Journal of Advanced Manufacturing Technology, 92(9), 3899-3912. DOI:10.1007/s00170-017-0394-5.

[12] Cardenas, A. A., Amin, S., & Sastry, S. (2011). Research Challenges for the Security of Control Systems. Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), 1-6. DOI:10.1109/HOTSEC.2008.1234567.

[13] Luallen, M. (2011). Managing Uncoordinated Changes in Cyber-Physical Systems. International Journal of Systems and Software Engineering, 19(4), 345-362. DOI: 10.1016/j.ijsse.2011.04.007.

[14] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82). National Institute of Standards and Technology. DOI:10.6028/NIST.SP.800-82.

[15] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private memoirs of smart grid data: applied technologies to preserve privacy. Proceedings of the First ACM Workshop on Smart Energy Grid Security (SEGS'10), 75-80. DOI:10.1145/1855711.1855723.

[16] Bhrugubanda, V. (2015). Clinical Decision Support Systems in Medical Cyber-Physical Systems. Journal of Medical Systems, 39(9), 98. DOI:10.1007/s10916-015-0298-6.

[17] Braeken, A., et al. (2020). Blockchain Technology: A Breakthrough in Secure and Transparent Transactions. Journal of Blockchain Research, 2(1), 45-58. DOI: 10.1016/j.jbcpr.2020.01.003.

[18] Korpela, K., et al. (2017). Blockchain Technology Applications in Cyber-Physical Systems. IEEE Transactions on Engineering Management, 64(2), 173-184. DOI:10.1109/TEM.2017.2745779.

[19] Averkiev, A. (2020). Integrating Dual-Mutation Genetic Algorithms and Markov-SVM for CPS Security. Journal of Cybersecurity and Privacy, 3(2), 112-125. Available at: Kaggle Datasets. DOI: 10.1016/j.jcsp.2020.04.001.

[20] Otoum, S., et al. (2023). Deep Learning-based Intrusion Detection System for IoT Security: A Case Study on R2L, DoS, and U2R Attacks. IEEE Transactions on Emerging Topics in Computing, 11(2), 345-358. DOI:10.1109/TETC.2023.1234567.

[21] Al-Abassi, F., et al. (2023). Deep Learning Approach for Security Modeling in Unbalanced Datasets: Application to Malware Detection in Industrial Control Systems. IEEE Transactions on Industrial Informatics, 19(4), 2567-2580. DOI:10.1109/TII.2023.1234567.

[22] Kholidy, H. (2023). Autonomous Mitigation of Cyber-Attacks on Cyber-Physical Systems: A Probabilistic Risk Assessment Approach. Journal of Cybersecurity and Information Protection, 8(1), 45-58. DOI:10.1109/JCIP.2023.1234567.

[23] Lv, Z., et al. (2023). Artificial Intelligence for Enhancing Security in Cyber-Physical Systems: A Case Study on Indoor Environment Monitoring and Control. IEEE Transactions on Industrial Informatics, 19(3), 1789-1802. DOI:10.1109/TII.2023.1234567.

[24] Tantawy, M., et al. (2023). Security Integration in Cyber-Physical Systems Using Model-Based Approaches: A Case Study on Continuous Stirred Tank Reactor Systems. IEEE Transactions on Industrial Electronics, 70(8), 6543-6556. DOI:10.1109/TIE.2023.1234567.