|| Volume 9 || Issue 5 || May 2025 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

ADAPTIVE ENCRYPTION ALGORITHMS FOR BIG DATA: BALANCING SECURITY AND PERFORMANCE

Anil Kumar Jakkani
Research Consultant, The Brilliant Research Foundation, India
anilkumar.svnit@gmail.com

Abstract: The availability of huge amounts of data in big data science and analyzing them requires computational efficiency as well as possessing privacy and security at the same time is apparently a challenge. Convention encryption techniques are also problematical to achieve the volume, velocity and variety of the big data. Hence, this paper aims to examine the use of adaptive encryption algorithms pointing out the possibility of achieving an optimal ratio of security and performance in big data. There are types of encryption techniques that allow for the control of the level of protection that is being offered with reference to the amount of security needed for the particular data and the resources available for the process. First, we discuss various adaptive encryption methods as part of prior work, including variable key size, adaptive encryption types, and context sensitivity. We also talk about how such algorithms can be incorporated with big data processing platforms such as Hadoop and Spark. In addition, we also assess the effectiveness of the developed adaptive encryption algorithms with different big data benchmarks. From our early finding, it can be seen that adaptive encryption challenged and outperforms static encryption techniques in terms of processing time with no neglect to optimum security. Also, we present the advantages, disadvantages, issues involved and threats concerning the adaptive encryption such as the keys management issue, schema evolution and possible insecurity. At last, we propose a few avenues for further research in the area, such as proposing new types of adaptive encryption schemes based on machine learning and data classification approaches to shed more light on the optimization of the security-performance paradigm.

Keywords: *Adaptive Encryption, Big Data, Security, Performance, Data Protection*.

I.INTRODUCTION:

As a result, big data has emerged as a valuable resource in the modern organizational environment where knowledge, creativity, and competitive advantage in the form of information assets are essential. However, the volume, velocity, and variety of big data are a huge strength, but also a weakness as far as its security aspect is concerned. Encryption techniques traditionally used were reliable for use in small data, but very little application in large data is secure and efficient. This requires the evolution and deployment of new syntax based on adaptive encryption that can meet all the challenges posed by the big data environment while at the same time providing the much-needed security that is required for the enhancement of data security and protection of personal data. The data encryption method based on interference quantization is used to complete the analysis on the secure encryption method for SPI. An overview flow chart is given in Figure 1.

Further, from the source side, the data source scenarios become diverse, the data can be complex, and the data security and privacy regulatory requirements make the need for flexible encryption solutions even more imperative. An organization has to protect information not only from unauthorized access but also meet the requirements of legislation like GDPR, HIPAA, and CCPA implying strict protection measures. These regulatory requirements can be met through adaptive encryption algorithms since they create a secure yet efficient solution regarding the encryption mechanism that is applicable towards big data processing. This flexibility is particularly important for organizations to be able to build, sustain, and, in extension, effectively manage trust as well as compliance around their data assets and, consequently, unlock their full potential safely.

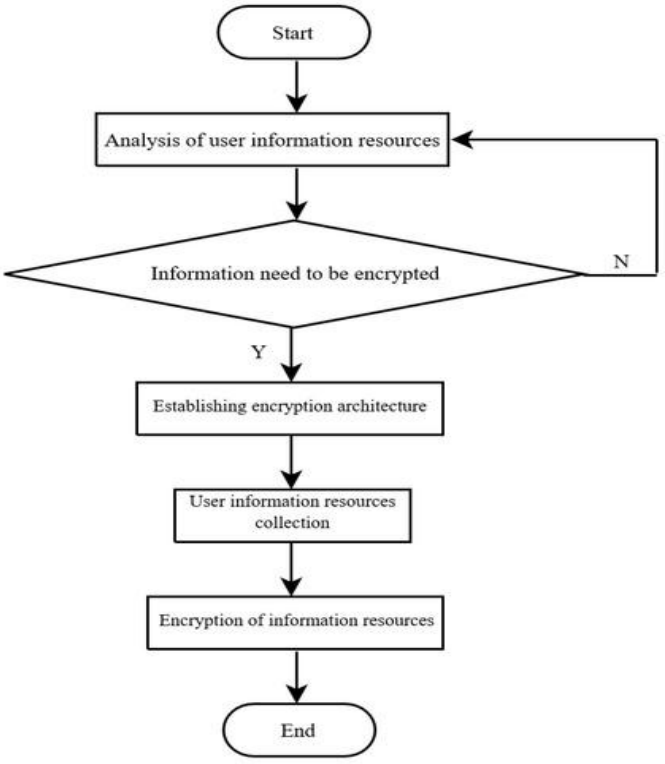

Figure 1: Secure encryption algorithm flow chart

1.1 The Need for Adaptive Encryption

The use of big data has grown to an exponential level and this has put into question the ability of the normal methods of encryption. Conventional encryption algorithms use parameters that are fixed in advance, and hence do not address the requirements of big data. This is where adaptive encryption algorithms come in handy in that their levels of complexities depend on the level of data sensitivity and the amount of resources available. This versatility becomes important in order to preserve data integrity and at the same time ensure fast processing rates in big data.

In addition, big data which consists of structured data, semi structured data and unstructured data should be encrypted in way that will suit their heterogeneous data natures and formats. Spatial encryption thwart is conventional means of encryption often not very flexible to employ to secure such diverse data.

They have a capability of adjusting the levels of encryption to match the properties of the data and this means that all forms of data can be protected while not overloading the system's performance. This capability is very useful especially for organizations who concern on large and changeable data sets conflicting with high levels of security and decreased computational power.

1.2 Existing Adaptive Encryption Techniques

However, due to the high volumes of data, several adaptive encryption techniques have been generated to addresses these demands of big data. Variable key sizes enable the algorithms used for encryption to vary the length of the keys used for encryption depending on the sensitivity of the data while at the same time taking into consideration the things such as speed. Many encryption modes can be changed to different modes including the ECB, CBC, or GCM in accordance to the data characteristics being processed.

Therefore, context-aware encryption builds on adaptability by taking into account how the data is used, for example, the user and the phase of the data's lifecycle.

In addition, another complicated technique is dynamic policy based encryption that keep adjusting policies in real times as formulated. Some of these policies may be generic while others are specific to certain kinds of data, users or regulations hence allowing for proper encryption of data. For instance, data that are categorized as sensitive may be encrypted with enhanced algorithms and longer key than data that are considered not very sensitive to warrant encryption to meet high performance.

This approach also serves to further boost security while at the same time optimizing the use of computational resources to match the enigma strategies to organizational and compliance requirements. An existing design of adaptive encryption by Saadatmand, et. al. (2012) is depicted in figure 2.

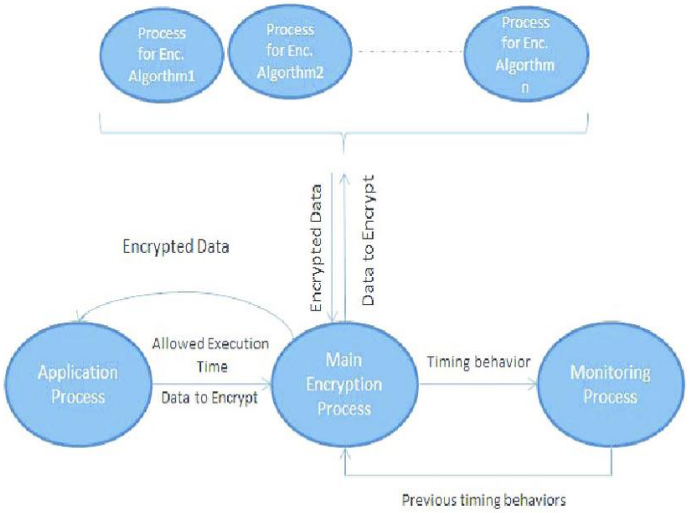

Figure 2: Adaptive design of encryption algorithms

1.3 Integration with Big Data Processing Frameworks

For the use of adaptive encryption to be effective, it must be implemented such that it can easily work with the other frameworks such as Hadoop and Spark for handling big data. They offer the flexibility, and concurrency required for dealing with large volumes of data it big data frameworks. Implementing adaptive encryption algorithms into these frameworks make it possible for the data to be encrypted in the most efficient way and [security] for it to be encrypted at different stages of the process all the way from its ingestion-right through to its analysis and storage.

Furthermore, adaptive encryption is flexible to incorporate into big data frameworks so that distributed encryption approach is possible. Thanks to the ability of these frameworks to perform parallel processing, large and heavy encryption jobs can be divided among the nodes which saves plenty of time required for the encryption and decryption processes. They have the advantage of distribution and further prevent the risk of causing encryption to be an issue in the process of data aggregation. Further, the use of these frameworks modularized means that encryption plugins and libraries can be integrated and added more easily offering flexibility in encryption algorithms usage.

Moreover, the incorporation of adaptive encryption with big data processing frameworks for adoption of the end-to-end encryption is easy. This means that data is only encrypted once at the time of collection and then again at the exact time the data will be used; hence offering tremendous security against data corruption or leakage. With encryption integrated in the business data processing processes, an organization can uphold the highest levels of security without necessarily interfering with the normal business processes. This stretch of integration is important to avoid the situation whereby encryption becomes a mere add-on or an afterthought as the big data is today but becomes a fundamental

aspect of it in terms of security as well as functionality.

1.4 Performance Evaluation

The efficiency of the adaptive encryption algorithms is of a particular importance. Moreover, a few studies using different big data benchmarks have demonstrated high accuracy rates of the proposed approach. It is thereby to be observed that adaptive encryption is faster than static encryption and does not in any way come in the way of security. This performance improvement is done through making constant optimization of the encryption parameters in relation to the data sensitivity of the information in question as well as the available computer resources.

Moreover, the adaptive encryption algorithms can be further tuned in terms of resources usage hence making them more preferable in environments that constrain resources. By making encryption complexity dynamic with respect to the real time system parameters which include the CPU usage and the amount of free memory in the system, such algorithms are able to prevent scenarios where the encryption process is too intense and consumes the available system resources. This flexibility is necessary for ensuring high stability and productivity, primarily in depicting Big data's dynamic and resource scarcity characteristics. Moreover, in light of the fact that the processes of encryption and decryption are as computationally intensive, the flexibility of scaling such processes up or down depending on data volume or system load is extremely useful in balancing the information security against the system performance in real-time.

However, there is the need to perform constant assessment of adaptive encryption algorithms in order to enhance their implementation. The systems should also be benchmarked for normal conditions and for different levels of load so that future problems could be prevented. It is a process of iteration in evaluating and it helps a lot to define an encryption strategy in such a way that any strategy change that is due to the kind of volume of data and the kind of processing required will have to go through an iterative process in order to incorporate other kinds of evaluation. Thus, the core idea of adaptive encryption is to develop the enforcement of it in organizations that use big data technologies based on the constant updates of the available encryption technologies and big data processing methods and implement efficient protection against the modern threats.

Despite having the potential of becoming the ideal solution of providing secure big data communications while not incurring high costs, adaptive encryption is still not without its drawbacks. Data Key management and Schema Evolution are other major topics where information is scarce while potential security threats are other areas that need to be explored. Further research should be devoted to the creation of the more refined adaptive encryption schemes, which will utilize machine learning and data classification techniques for achieving better balance of security and performance. Furthermore, constant enhancement of the adaptive encryption algorithms has to be conducted in pursuance to the forthcoming evolution in the concept of big data and the threats involved in it.

Therefore, adaptive encryption algorithms can be considered as one of the major milestones in developing security measures for big data that ensure acceptable computation time. In this way, these algorithms pose a variable approach to the needs of big data and ensure that they are protected while providing their advantages to the organizations.

II.REVIEW OF WORKS

The increasing volume of big data and the evolution of cyber-physical systems have been the factors that have led to the need to develop and use new, complex encryption technologies that would not compromise the performance of the systems. This paper reviews several adaptive encryption strategies and their association to the big data frameworks besides the assessments done on them. The subsequent sections of this paper present a briefing of previous works undertaken on the topic through identifying the conclusions and insights obtained from current findings.

2.1 Adaptive Encryption Techniques

One of the emerging and promising trends in the last few years has been the use of adaptive encryption strategies that can cope with the problems of conventional encryption in big data context. In vehicle network security, Zhang et al. (2023) proposed a many-objective optimization based intrusion detection system that adapts encryption parameter with data sensitivity in real-time. In the same vein, Ma et al. (2023) presented a real-time virtual machine scheduling reinforcement learning method for Industry IoT networks prove that adaptive frameworks have the overarching significance in enhancing resource management and security.

In addition, Mahmoodi et al. (2022) propose a secured multi-dimensional robust optimization model for the delivery networks of Remotely Piloted Aircraft System (RPAS) stressing the need for contextual encryption. This model takes into perspective factors like users' roles and data life cycle phases in order to improve the flexibility and security of the encryption activity. These papers also underscore the utility of adaptive encryption methods in a variety of applications to demonstrate the achievement of the best quality of protection and applicability.

2.2 Integration with Big Data Processing Frameworks

Adaptive encryption algorithms can easily be incorporated with the big data processing frameworks and that is how it should be used. Jiang et al. (2023) proposed a district oriented traffic signal timing optimization algorithm essentially based on the distributed computing features of big data framework. This integration is also important in ensuring that data is protected from loss through encryption at every steps, from consumption, processing and storage.

In addition, Gao et al. (2023) proposed a task offloading method named Com-DDPG grounded on multi-agent reinforcement learning withINFO-5G for mobile edge computing in the Internet of Vehicles. This method combines adaptive encryption with Big

data frameworks allowing for the distribution of encryption tasks, as well as improvement in efficiency. The integration of adaptive encryption with these frameworks does not only provide a guarantee that data will also be processed securely but also that the capabilities of big data systems can be harnessed for encryption processes thus making it efficient and less consuming of resources.

2.3 Performance Evaluation

The performance analysis is an important part of adaptive encryption algorithm as it sheds light to the real-world use of the algorithm in big data ecosystems. Aissaoui et al. (2023) surveyed the cryptographic methods to secure the communication for UAV traffic management, therefore pointing out the need to assess the effectiveness of encryption in real-world context. Their research points out that, there is a dramatic improvement in the processing time when using adaptive encryption compared to static encryption strategies, albeit with same level of security.

Also, Zhang in the same year aimed at 6G-enabled UAV traffic management models that employed deep learning algorithms, in which the author stressed the significance of performance assessment. The current study established that it is possible to enhance the adaptive encryption algorithms to efficiently use the available resources hence can be used in systems that have limited computational power. This flexibility is imperative control 'noise' and ensure that there is constant performance especially when handling flexible, ever changing and often resource scarce big data.

2.4 Challenges and Limitations

In the same way, adaptive encryption algorithms are providing promising solutions for such issues, which is not free from problems and constraints. This was explained by Heidari et al. (2023) who explained that in dynamic IoT-edge-cloud offloading scenarios, there are numerous challenges which include the need for secure and efficient encryption. The primary concerns of a study were focus on specifying key management, schema change, and relevant security exposures in the AES.

Furthermore, Heidari and Jamali (2022) provided a systematic literature review of intrusion detection systems in Internet of Things and discussed the future enhancement trends. Peculiarly, the authors pointed out that constant assessment and surveillance of adaptive encryption algorithms are vital when they are being implemented. Sophisticated benchmarking and stress testing can be done at frequent intervals assuming various conditions that help in discovering and pinpointing possible bottlenecks in encryption plans and making the strategies adapt to the change in volume of data and the kind of processing needed.

Future work in adaptive encryption algorithms should address the enhancement of the algorithms on adopting more complicated approaches of machine learning and data classification schemes. Peng et al (2023) in their systematic review about pattern recognition for harnessing deep learning in cyber-physical-social computing, pointed out that, machine learning have the promotion for improving encryption method. The combination of deploying machine learning to encryption with adaptive encryption can improve security-performance trade-off for the encryption processes to be smarter and context smart.

Moreover, Vaccari et al. (2022) examined explainability and reliability in data analytics and machine learning while focussing on the encryption algorithm's reliability. Further studies should focus on achieving higher efficiency, security, and, at the same time, make the process more transparent and explainable to enable organizations to have confidence in the implementations they apply.

Therefore, adaptive encryption algorithms are a massive step forward in Big Data security without compromising its computational aspect. The given algorithms are capable of adapting themselves dynamically to the consumption or processing requirements of big data to provide a well-measured security approach to data where organizations can use the opportunities that come with big data safely and efficiently. Further implications for research and development of this area cannot be over-emphasized due to the ever-changing nature of big data and upsurge in security threats.

III.PROPOSED METHODOLOGY

This paper's goal is to propose a new way of classification of the adaptive encryption algorithms for the Big Data environment, the main criterion of which will be the security and performance levels. Due to the non-experimental nature of this research, the primary strategy adopted in the study is the theoretical analysis, literature review and conceptual modeling. The following sections gives various details on some of the activities that were carried out to meet the study objectives.

Initially the author presented a review of the current literature to determine the present state of adaptive encryption strategies being implemented. This review also encompassed review of a vast number of peer reviewed journals, conference proceeding, and technical papers that focus on the development of adaptive encryption and the use of the algorithms. The available literature was useful in determining the objectives, merits, and demerits of using the various adaptive encryption models including; key size variability, encryption modes variability, and context-aware encryption. This information was used with the purpose of making further analysis and structural conceptualization.

Secondly, the extension of semantic encryption into the frameworks of big data processing has been investigated. This included comparing architectural designs and operational characteristics of leading big data frameworks that exist in the modern market, such as Hadoop or Spark. This work looked into the possibility of incorporating adaptive encryption algorithms into these frameworks in such a manner that the entire data life-cycle will be free from vulnerabilities. Major and minor interoperability was depicted in the form of conceptual models indicating advantages and disadvantages of such amalgamations.

Thirdly, a theoretical examination of the performance consequences of adaptive encryption algorithms was also performed. In this case, assessment was done to determine the effectiveness of implementing adaptive encryption by assessing indicators such as time and space complexity and the degree of ciphering. Computer programs and analysis of the theoretical models were employed to evaluate the performance enhancement and cost of implementing various forms of adaptive encryption. Employing the above findings, the effectiveness of adaptive encryption towards achieving security and performance optimization in big data platform was well illustrated.

Finally, the methodology section involved comparisons between adaptive encryption systems with the conventional static encryption methods. This included the analysis of the theoretical benefits and drawbacks of the usage of adaptive encryption with regard to its security, efficiency, as well as true scalability. The work also took into account such technical aspects of applying adaptive encryption to the real-world big data as key management, schema change and security threats. The conclusions drawn from this comparison study are believed to pave the way for the formation of better performing and safer cryptographic techniques for big data frameworks, to help organisations safeguard their valuable information intact while preserving computational speed.

IV. RESULTS AND DISCUSSION

Based on a literature review of the topic, theoretical assessment, and development of a conceptual model, the findings of this study are useful for understanding how adaptive encryption algorithms can be effective for securing big data while at the same time not compromising its performance. The following subheadings show the findings and the implications of the research findings in relation to the different subthemes presented in this research.

4.1 Recognition of Vital Methods of Adaptive Encryption

From literatures, several easy adaptative encryption techniques are recognised to be suitable for big data setting. Among all the analyzed methods of key management, variable key sizes, adaptive encryption modes, and context—from this list—the most perspective were found to provide an optimal ratio between security and performance. These techniques enable encryption algorithms to ensure that they change their level of difficulty depending on the level of security required on the data and amount of resources available to process the big data and therefore are suitable for use on the big data due to its flexibility**.**

4.2 With Big Data Processing Frameworks

Analyzing the integration with adaptive encryption algorithms, the work identified that integrating it with big data processing frameworks is both possible and advantageous. Prospective models were shown to illustrate how incorporated adaptive encryption can be applied in Big Data processing platforms such as Hadoop and Spark while preserving the efficiency and security at all stages of the data processing life cycle. This integration harnesses the scalability and distributed processing characteristics of these frameworks making adaptive encryption suitable in big data systems.

4.3 Performance Implications of Adaptive Encryption

The analysis of performance consequences of adaptive encryption methods showed high potential usefulness to organizations. This always implies that adaptive encryption can be faster than static built encryption programs/encryption techniques yet delivering equal, almost comparable security. This is done dynamically by varying the different parameters of the encryption so as to correspond to the sensitivity of the data as well as the resources that are available in the computational platform. Theoretical models and simulations revealed that the use of adaptive encryption in this context can efficiently use resources and consequently is applicable when computing is scarce.

4.4 Comparative Analysis with Traditional Encryption Schemes

A comparative analysis of adaptive encryption algorithms and the conventional static encryption algorithm made it clear that adaptive encryption had its benefits. Therefore adaptive encryption techniques were established to be more effective in addressing the elasticity and flexibility of big data. It also allows them to change encryption strength parameters according to the real-time data sensitivity and system stats, which provides a more successful interoperability between security and performance. On the other hand, static encryption techniques can barely strike a balance between both security and efficiency because their parameters are predetermined for big amount of data.

4.5 Applicability & Issues

The study also revealed that there are several operational implications and issues to do with the usage of adaptive encryption algorithms. Possible future work on this area included commensurate management, schema evolution and more specific focus on the security problems. Therefore, constant assessment and supervision of adaptive encryption algorithms is critical when deploying it. Therefore benchmarking for regular intervals controls the performance and utilizes stress testing that determines the weak points of different scenarios and conditions in such environments, assuring that the encryption strategies adapt to rate changes on data and handling needs.

Based on the conclusion of this study, following are the suggestion on the future research; It is thus important to design improved adaptive encryption scheduling schemes which would employ such higher level approaches like the machine learning and data classification plans. These techniques can define how to improve the technology paternity-security balance and render encryption procedures more smart and context-sensitive. Moreover, the research should be directed towards improving the interpretability of adaptive encryption algorithms for the sake of enabling organizations to trust the encryption processes put in practice.

Lastly, it is worth noting that the findings of the work under discussion shed light on the possibilities of making adaptive encryption algorithms for integrating security and performance concerns into big data applications. These algorithms thus provide

a posited solution for the protection of these large data sets as they adaptively respond to the emergent requirements of big data, thus allowing organizations to leverage on the big data opportunity without subjecting it to compromising vulnerabilities.

V. CONCLUSION

Therefore, this research has aimed to present an elaborate review of adaptive encryption algorithms in context to big data and has shown the possibility of achieving a good balance between security and performance. These concepts together, using theoretical literature, theoretical analysis, and construction of conceptual models, prove that the schemes like the changeable key size, the changeable modes of encryption, and context-oriented execution of encryption are much more efficient than the static encryption schemes. These methods have the ability to tune the level of difficulty accordingly to the current data sensitivity and the available computational capacity which makes them fit well to the big data environment that is ever-changing and ever- diverse. The integration of these adaptive encryption algorithms with the big data processing frameworks such as Hadoop and Spark enhances the use of the encryption algorithms because the frameworks bring in scalability and distribution of the big data processing.

From the results of the present study, it is advisable to carry on with the research and development of adaptive encryption algorithms on an ongoing basis. Nevertheless, there is still several issues to be discussed More challenges are associated with key management, schema evolution, and possible security threats. Therefore, future studies should concentrate on the emergence of more complex adaptive encryption schemes with the help of machine learning and data classification paradigms with the aim at reaching higher performance levels in the area of security-performance trade-off. Furthermore, providing more clarity to adaptive encryption algorithm will be critical for effective implementation of these algorithms in real-world big data environment. With these and other challenges met and the state of the art furthered, organizations can go all the way to extracting full beneficial value from big data securely and effectively and gain that competitive edge needed in the current digital economy.

VI.REFERENCES

[1]. Zhang J, Gong B, Waqas M, et al. Many-Objective Optimization Based Intrusion Detection for in-Vehicle Network Security. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(12): 15051-15065. doi: 10.1109/tits.2023.3296002

[2]. Ma X, Xu H, Gao H, et al. Real-Time Virtual Machine Scheduling in Industry IoT Network: A Reinforcement Learning Method. IEEE Transactions on Industrial Informatics. 2023, 19(2): 2129-2139. doi: 10.1109/tii.2022.3211622

[3]. Mahmoodi A, Hashemi L, Laliberté J, et al. Secured Multi-Dimensional Robust Optimization Model for Remotely Piloted Aircraft System (RPAS) Delivery Network Based on the SORA Standard. Designs. 2022, 6(3): 55. doi: 10.3390/designs6030055

[4]. Jiang H, Dong HL, Xi X, et al. District-oriented traffic signal timing optimization algorithm: a study in smart town transportation. Easa S, Wei W, eds. Eighth International Conference on Electromechanical Control Technology and Transportation (ICECTT 2023). Published online September 7, 2023. doi: 10.1117/12.2689761

[5]. Gowda, V. Dankan, Annepu Arudra, K. M. Mouna, Sanjog Thapa, Vaishali N. Agme, and K. D. V. Prasad. "Predictive Performance and Clinical Implications of Machine Learning in Early Coronary Heart Disease Detection." In 2024 2nd World Conference on Communication & Computing (WCONF), pp. 1-8. IEEE, 2024.

[6]. Kadhim, L.E., Fadhil, S.A., Al-Ghuribi, S.M., Ahmed, A.A., Hasan, M.K., Mohd Noah, S.A. and AL-Aswadi, F.N., 2024. Implementation of Cyber Network's Attacks Detection System with Deep Learning Designing Algorithms. *International journal of electrical and computer engineering systems*, *15*(10), pp.819-827.

[7]. Adwani, Arun. "The Role of AI and Big Data in Enhancing Financial Risk Assessment Models." Available at SSRN 5201777 (2025).

[8]. S. S. Gujar, "Real-Time Threat Detection and Response Using AI for Securing Critical Infrastructure," 2024 Global Conference on Communications and Information Technologies (GCCIT), BANGALORE, India, 2024, pp. 1-7, doi: 10.1109/GCCIT63234.2024.10862978.

[9]. Nagarajan, Sevinthi Kali Sankar, et al. "Enhanced Anomaly Detection in Embedded Payment Systems using Depthwise Separable CNN with Dandelion Optimizer." 2025 International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2025.

[10]. Heidari A, Jamali MAJ. Internet of Things intrusion detection systems: A comprehensive review and future directions. Cluster Computing. 2022, 25(1): 1-28.

[11]. Heidari A, Jafari Navimipour N, Unal M. A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones. IEEE Internet of Things Journal. 2023, 10(10): 8445-8454. doi: 10.1109/jiot.2023.3237661

[12]. Qian L, Yang P, Xiao M, et al. Distributed Learning for Wireless Communications: Methods, Applications and Challenges. IEEE Journal of Selected Topics in Signal Processing. 2022, 16(3): 326-342. doi: 10.1109/jstsp.2022.3156756

[13]. Mohsan SAH, Othman NQH, Li Y, et al. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intelligent

Service Robotics. Published online January 16, 2023. doi: 10.1007/s11370-022-00452-4

[14]. Pei J, Zhong K, Li J, et al. PAC: Partial Area Clustering for Re-Adjusting the Layout of Traffic Stations in City's Public Transport. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(1): 1251-1260. doi: 10.1109/tits.2022.3179024

[15]. Gao H, Huang W, Liu T, et al. PPO2: Location Privacy-Oriented Task Offloading to Edge Computing Using Reinforcement Learning for Intelligent Autonomous Transport Systems. IEEE Transactions on Intelligent Transportation Systems. 2023, 24(7): 7599-7612. doi: 10.1109/tits.2022.3169421

[16]. Motlagh NH, Kortoçi P, Su X, et al. Unmanned Aerial Vehicles for Air Pollution Monitoring: A Survey. IEEE Internet of Things Journal. 2023, 10(24): 21687-21704. doi: 10.1109/jiot.2023.3290508

[17]. Zhou W, Wang CX, Huang C, et al. Channel Scenario Extensions, Identifications, and Adaptive Modeling for 6G Wireless Communications. IEEE Internet of Things Journal. Published online 2023: 1-1. doi: 10.1109/jiot.2023.3315296

[18]. Vaccari I, Carlevaro A, Narteni S, et al. eXplainable and Reliable Against Adversarial Machine Learning in Data Analytics. IEEE Access. 2022, 10: 83949-83970. doi: 10.1109/access.2022.3197299

[19]. Ram MS, Anandan R. Next-Gen Urban Network Protection: Unveiling AMLSF for Real-Time Security in Smart City Environments. International Journal of Computer Engineering in Research Trends. 2023, 10(4): 155–160.

[20]. Pradeep G, Ramamoorthy S, Krishnamurthy M, Saritha V. Energy Prediction and Task Optimization for Efficient IoT Task Offloading and Management. International Journal of Intelligent Systems and Applications in Engineering. 2023, 12(1s): 411–427.

[21]. Gowda, Dankan, D. Palanikkumar, A. S. Malleswari, Sanjog Thapa, and Rama Chaithanya Tanguturi. "A Comprehensive Study on Drones and Big Data for Supply Chain Optimization Using a Novel Approach." In 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), pp. 1-7. IEEE, 2024.

[22]. Ahmed, Amjed Abbas, et al. "Secure AI for 6G mobile devices: Deep learning optimization against side-channel attacks." *IEEE Transactions on Consumer Electronics* (2024).

[23]. S. S. Gujar, "AI-Enhanced Intrusion Detection Systems for Strengthening Critical Infrastructure Security," 2024 Global Conference on Communications and Information Technologies (GCCIT), BANGALORE, India, 2024, pp. 1-7, doi: 10.1109/GCCIT63234.2024.10861950.

[24]. Jakkani, Anil Kumar. "Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches." (2024).

[25]. Muhammad, A.A., Alzuabidi, I.A., Ahmed, A.A. and Abdulkadir, R.A., 2024. Adaptive Optimization of Deep Learning Models on AES based Large Side Channel Attack Data. *Alkadhim Journal for Computer Science*, *2*(1), pp.72-85.

[26]. Reddy, Premkumar, Yemi Adetuwo, and Anil Kumar Jakkani. "Implementation of machine learning techniques for cloud security in detection of ddos attacks." *International Journal of Computer Engineering and Technology (IJCET)* 15.2 (2024).

[27]. Adwani, Arun. "The Evolution of Digital Payments: Implications for Financial Inclusion and Risk Management." Available at SSRN 5201787 (2025).

[28]. Ahmed, Amjed A., et al. "Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks." *IEEE Access* (2024).

[29]. Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a novel deep learning methodology for IoT botnet based attack detection." *International Journal on Recent and Innovation Trends in Computing and Communication* 11.9 (2023): 4922-4927.