Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Cryptographic Law enforcement and advances in the Digital Rights Management

Dr. Tarun Kumar Kaushik[1], Rupendra Singh[2], Dr. Hemant Kumar Sharma[3], Dr. Aditya Tomer[4], Dr. Anurag Singh[5]

[1]Assistant Professor Sharda School of Law, Sharda University, Greater Noida.
[2]Assistant Professor, Amity Law School, Noida
[3]Professor and director - School of Law Pimpri Chinchwad University, Pune (Maharashtra)
[4]Additional Director & Professor, Amity Law School, Noida
[5]Professor Department of Law, Meerut College Meerut, Chaudhary Charan Singh University Meerut
Email. aa@gmail.com

This paper studies the emerging trends in cryptography and digital rights management (DRM) and their implications for the security and integrity of digital assets and communications. Throughout the presentation, the importance of resilient encryption algorithms as a way to respond to the threat of quantum computing posed by the development of post-quantum cryptography is highlighted. Moreover, this paper examines the role of homomorphic cryptography in the conduct of secure computations on encrypted data in order to preserve privacy during these secure computations. Block chain technology is analyzed as a way to integrate into digital rights management systems in an effort to explore the possibilities and shortcomings of its implementation. The study focuses on its potential to revolutionize this sector through its transparent and decentralized nature. A further discussion is offered on the connections between artificial intelligence (AI) and digital rights management (DRM) in order to illustrate how AI-driven solutions can be used to detect and mitigate unauthorized access and piracy of digital content. It is critical that stakeholders embrace this rapidly changing digital landscape so that they can facilitate innovation and creativity, while ensuring protection and fair distribution of digital content, in order to navigate the ever-evolving digital landscape with confidence.Mobile Ad-hoc Networks (MANETs) are inherently vulnerable due to its dynamic, decentralized structure and requirement for advanced solutions for security risk mitigation. It is suggested to use a machine learning (ML)-based strategy for effective attack detection and mitigation. Important characteristics are identified and standardized from the network traffic data, such as the time it takes to respond, how frequently replies occur, and the rates at which packets are dropped. The efficacy of six Machine Learning classifiers—Support Vector, Naïve Bayes, K-Nearest Neighbor, Logistic Regression, Machine, Multilayer Perceptron, and Extreme Gradient Boosting—in identifying black hole attacks is assessed through training. The mentioned outcomes exhibit the efficiency and efficacy of the recommended machine learning strategy in limiting black hole attack risks in MANNETs. These results are based totally on numerous factors including Packet shipping Ratio (PDR), overall time, accuracy and energy usage.

Keywords: Cryptography, Digital Rights Management, Emerging Trends, Post-Quantum Cryptography, Homomorphic Encryption, Block chain, Artificial Intelligence, Security, Privacy.

1. Introduction

1.1 Cryptographic Law Enforcement

Physical device storage and communications traffic are increasingly protected by end-to-end encryption (E2E). Service providers do not have keys for E2E encryption systems, as they are held by endpoints, typically end-user devices like smartphones or computers. Providers and manufacturers cannot access plaintext data, nor can attackers who compromise their systems access it [1]. The issue of privacy goes beyond politics and law. A certain equilibrium can also be achieved on a technical level. Business and financial regulations can be circumvented or evaded through privacy. Financial transactions allow hackers and thieves to operate more easily due to a lack of privacy. A high level of privacy facilitates criminal activity. Having too little privacy also makes crime easier. Several key questions need to be addressed in order to achieve a reasonable balance between privacy and law enforcement [2]. The use of cryptographic primitives—symmetric encryption algorithms, public key algorithms, hash functions, message authentication codes, digital signatures, etc.—is well known. Through the appropriate combination of them, specific (cyber) security services can be provided, such as: confidentiality, data and entity authentication, and non-repudiation (see, for instance, [4] for classical cryptography, [5], [6] for recent cryptography. In order to ensure the desired security level, the Transport Layer Security (TLS) protocol, which is being considered a somewhat de facto standard, highly relies on cryptography. Numerous legal instruments dealing with human rights and cyber security specifically mention cryptography. European Commission and high representative for foreign affairs and security policy, for instance, presented the new Cyber security Strategy in December 2020, which emphasizes the importance of strong encryption for protecting individuals' fundamental rights and digital security [7], so strong encryption should be developed, implemented, and used [3]. Various aspects of life, including legal systems, depend heavily on information, and its protection is of paramount importance. A crucial component of information protection is cryptography, a science that deals with encrypting and decrypting information. Cryptography plays a key role in modern legal systems, as discussed in this article. Cryptography is increasingly used by governments and organizations to protect their data, which raises questions about its impact on legal systems and citizens' rights [8].

1.2 Digital Rights Management

The Digital Asset Management (DAM) process helps organizations manage their digital rights and permissions, organize and store their rich media and find and retrieve them. It refers to multimedia assets including photos, music, podcasts, animations, and other digital content OR Digital Asset Management is a strategic approach to increase revenues and speed up processes. In this digital age, managing information is a requirement for businesses and individuals alike and has separate significance within various fields of human interests. The 21st century is a digital era where digitalization has impacted every aspect of life. It is crucial that laws are adapted so that each individual's fundamental rights are protected. It involves creating a log

and constructing an operational and validated framework in order to manage and secure digital assets, as well as probing an authentic functionality that enables terminal-users to identify, detect and redeem a digital asset [9]. As a functional area of law, law and digital technology, or IT law, has gained a foothold in both the legal profession and academia over the past decade. The development of new technologies such as big data, the Internet of Things, quantum computing, block chain technology and sophisticated algorithms raises questions regarding the regulation of these technologies, for example, with regards to what rights and protection citizens should have. There are three main types of legal issues involving citizens' rights:

- Use of new technologies to violate rights
- New technology and conflicting rights
- The emergence of new issues due to (the use of) new technologies that have not yet been granted rights.

Lawyers are familiar with problems in the first and second categories. One example of a first category concern is whether sophisticated data analytics violate one's privacy, or whether risk profiling is discriminatory in nature towards particular groups. Typically, questions in the second category pertain to wiretapping (privacy interest) or to insulting a religion (freedom of religion versus freedom of speech) or whether someone may be wiretapped for the purpose of criminal investigation (security interest). All of these questions have a lot of literature and case law. Despite this, literature, legal practices, and academic debates rarely touch on the third category. For example, the third category includes the 'right to be forgotten,' also called the 'right to oblivion,' which has been included in EU General Data Protection Regulation (GDPR) since 2018, or the (theoretical, non-existent) 'right to anonymity.

2. Methodology

The manufacturers of multiple products have applied productive and in-depth investigation work to evaluate the conventional regimes of cataloging and indexing computerized musical assets of composers. To secure digital assets against cyber-conflicts, it is necessary to understand speech, recognize different digital characters, and conduct conceptual analysis and many other intricate aspects. For these ideas to be fully realized, substantial processing power is required so that content can be ingested in real-time, one of the most critical aspects of audio-video applications, video content, and other media. This technology will be commercially viable with the introduction of low-co stand preponderance workstations [9].

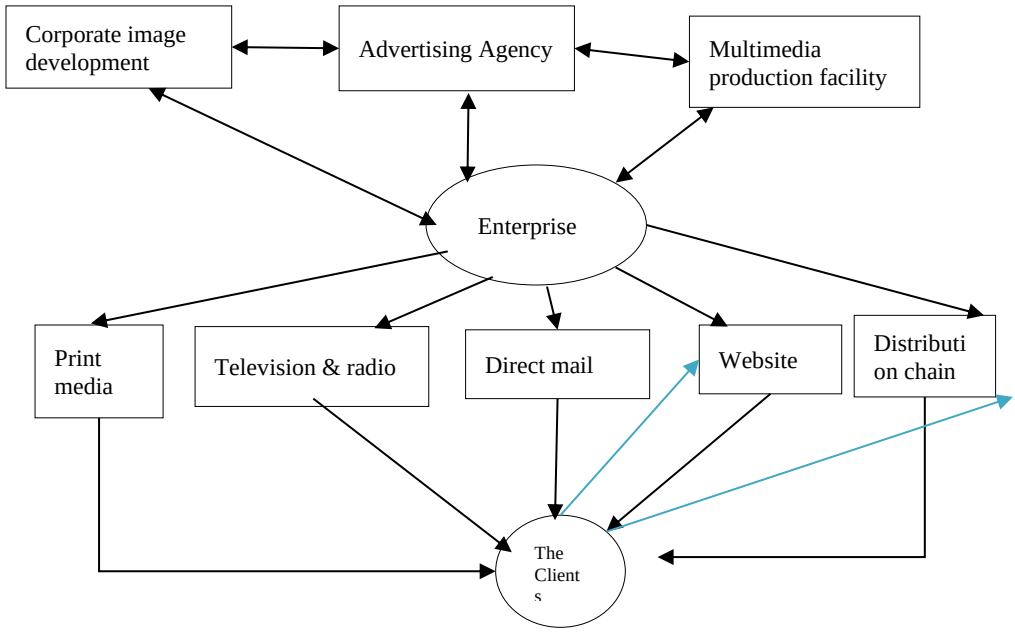

Figure 1: Content exchange within an organization [9]

Modern businesses create media content under various guises. Below is a figure that shows how various compartments within a collaborative organization develop data and content. There is usually some formalized filing structure in place for each department's media content. The criteria of global brand management require that all content on the website be shared with the enterprise-wide, so that there is no chaos, wrong logos, out-of-state corporate images, and link-rot.

3. Evolution of Digital Rights Management Technologies

Contemporary academic and practitioner conversations are increasingly focused on digital transformation (DT). Using Google Trends, we can see that interest has grown from 1 to 100 in six years. Additionally, it has strategic significance [12]. Managers across industries and contexts are challenged by DT (e.g. [13], [14], [15]). Organizations have been spurred to accelerate DT due to the challenges surrounding COVID-19 pandemic [16]. However, the extensive and diverse literature on DT lacks a common definition and understanding of exactly what it is [17, 18]. Generally, systematic reviews or meta-analyses are rare [19, 20] and narrowly focused. The current debate around the phenomenon is dominated by the fact that due to the proliferation of digital technology, there is a lack of clarity surrounding it. – In many ways, today's organizations are both affected and need to adapt to the explosion of information, communication, and computing (e.g. [15], [21], [22]). This phenomenon can therefore be considered as a modification of an organization's form, quality, or state over time. The widespread diffusion of digital technologies triggers and shapes DT as an organizational change. Using this view, we can potentially explain how the phenomenon of DT is managed and how it contributes to organizational change [11]. Figure 2 illustrates how interest in DT

has risen rapidly and recently. There have been an increasing number of publications on DT over the years. 50 percent of the 279 articles considered were published within the past five years. The figure below shows how many articles have been published on DT since 2000 [23].

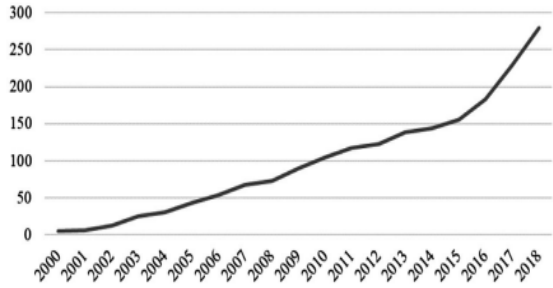

Figure 2: Articles on digital transformation published over time [11]

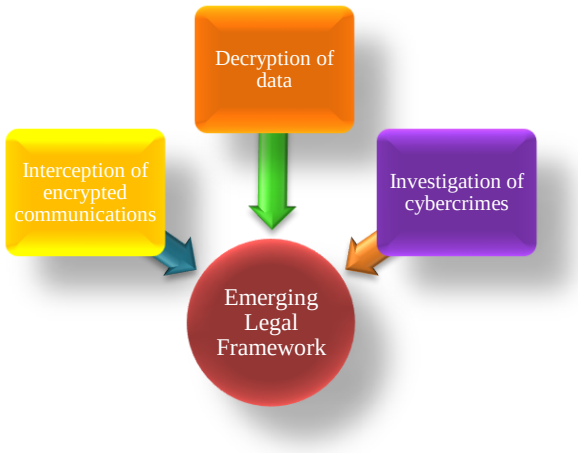

Figure 3: Emerging legal framework

4. Laws of encryption: An emerging legal framework

The legal framework for cryptographic law enforcement encompasses the regulatory measures and statutes governing the use of cryptographic techniques in the context of law enforcement activities. This framework establishes guidelines for the lawful interception of encrypted communications, decryption of data, and investigation of cybercrimes involving encrypted information. It delineates the rights and responsibilities of law enforcement agencies, as well as the privacy rights of individuals, ensuring a balance between security imperatives and civil liberties. Key components of this framework may include laws governing data protection, surveillance, wiretapping, and electronic communications, along with international agreements and treaties addressing cross-border cooperation in combating cybercrime. Law enforcement practices use cryptographic techniques in part based on legal precedents set by court rulings and judicial interpretations. The changing nature of the technology and the complex legal landscape surrounding encryption present ongoing challenges in maintaining

an effective and ethical legal framework for implying cryptographic law enforcement [24].

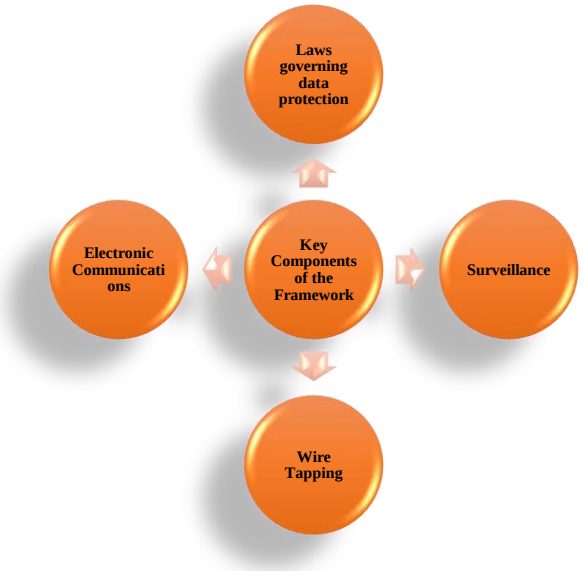

Figure 4: Significant Components of the framework

5. Challenges and Ethical Considerations in DRM (Digital Rights Management)

There are many moral issues related with IoT, Big Data, and AI governance, yet there are more this kind of challenges than advantages [25]. The process of Digital Rights Management has problems and issues, which make this process even complicated. The issue of digital rights management refers to the wide range of problems connected with the protection of digital content and access rights management in the world, which is quickly becoming fully and purely digital . One of the key problems and challenges of this process is balancing the interests of content developers, distributors, and customers while also protecting someone's intellectual property, which must be protected by law and other guarantees. Technological limitations and vulnerabilities pose major problems with Digital Rights Management from a practical perspective. In addition, the interoperability issues between different DRM systems and platforms can hamper seamless access to content across numerous devices and services. In Digital Rights Management (DRM) implementations, accumulating and using personal data give rise to ethical and legal apprehensions. In addition, the rapid pace of technological innovation and evolving consumer preferences necessitate continual adaptation and refinement of DRM strategies to persist essential and relevant. Confronting these challenges needs collaboration among stakeholders, innovative approaches to DRM implementation, and a careful stability between security, privacy considerations, and usability of data.

6. Emerging Trends in Cryptography and Digital Rights Management

An inclusive range of innovative trends in cryptography and digital rightsmanagement (DRM)

are emerging over the past few years, with the intention of improving security, privacy, and control over digital content and communications with the help of cryptography and Digital Rights Management (DRM). The progress of the post-quantum cryptography has been one of the most noticeable trends in cryptography over the past few years, which focuses on making algorithms that have better resistance to attack from quantum computers, which is a very important topic in cryptography. It is also becoming progressively more popular to use homomorphic encryption as a method of encryption, in part, because by preventing decryption of encrypted data, computations can be accomplished while retaining the privacy of data. With the help of block chains and smart contracts emerging as key tools for managing digital rights through an immutable, decentralized process, block chain technology has become a chief trend in DRM. Furthermore, the incorporation of artificial intelligence and machine learning into DRM systems strengthens content protection by detecting and minimizing unauthorized access and piracy of content, thereby also enhancing its protection. The trends emerging are generally seen as a continuation of the ongoing evolution of cryptography and data protection in an increasingly digital world, where digital assets and communications are increasingly digital, and the integrity and security of these assets and communications is crucial [26].

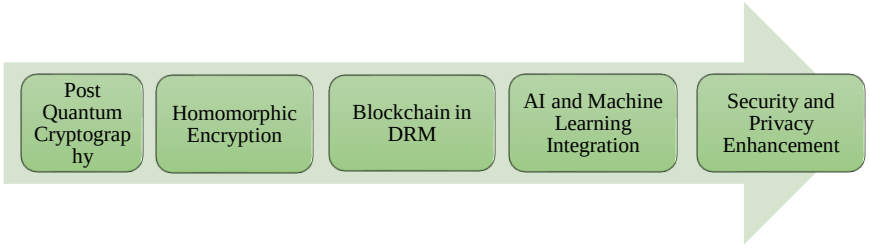

Figure 5:Emerging Trends

7. Future Directions and Innovations in Digital Rights Management

Digital Rights Management (DRM), a regulation which focuses on managing the rights of digital files and media, holds great promises for the future as technology continues to progress and create. Artificial Intelligence (AI) and machine learning (ML) algorithms have already been incorporated into DRM systems, but integrating these technologies into DRM systems is the next step. By constantly examining patterns and behaviors to identify potential threats, these advances will enable a strong detection and prevention of unauthorized access to digital content as it will be easier to detect and prevent unauthorized access to the digital content. Additionally, block chain technology holds great potential for revolutionizing digital rights management (DRM) through its ability to provide a decentralized, tamper-proof platform for the management of rights on digital property. With the aim to reduce piracy and ensure fair compensation for their work, content creators can leverage block chain-based technologies to build immutable and transparent records of distribution and ownership, Furthermore, Digital Rights Management (DRM) will be challenged as well as expanded by immersive technologies, such as virtual reality (VR) and augmented reality (AR). It will be obligatory to adapt DRM solutions as these technologies become more prevalent and as a result, the integrity of immersive experiences will need to be protected, as will the prevention of unauthorized copying or amendment of virtual content as an outcome of these technologies. As we move

further in an increasingly digital world, future innovations in DRM will focus on enhancing security, scalability, and usability so that they can meet the evolving needs of content creators, distributors, and consumers in order to comply with the increasing demands of businesses and consumers [27].

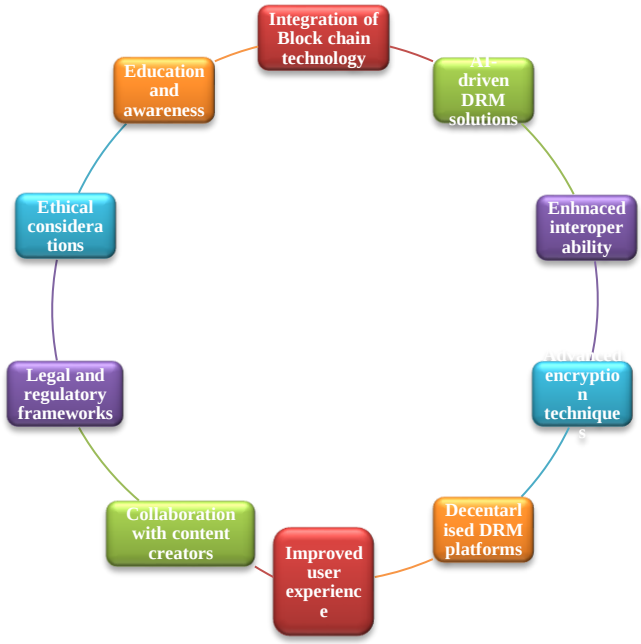

Figure 6:Future Directions

8. Conclusion

It can be culminated that the emerging trends in cryptography and digital rights management (DRM) are a key indicator of a pivotal shift in addressing the evolving challenges present in the digital domain. There has been a proactive response to the looming threat posed by quantum computation through the development of post-quantum cryptography, which has ensured that encryption algorithms remain resilient in the face of advanced computational capabilities that is an end result of quantum computing. It is broadly acknowledged today that homomorphic encryption stands out as a beacon of privacy preservation, as it provides the ability to perform secure computations on encrypted data while also maintaining safety at the same time. Block chain automation, in the form of DRM, can herald a new era of digital rights management that is transparent, decentralized, and crafted to foster trust, accountability, and transparency in transactions that take place digitally. Additionally, it is also expected that the synergy between artificial intelligence (AI) and digital rights management (DRM) systems will enhance security measures by taking advantage of AI's abilities to detect and mitigate the risk of unauthorized piracy and access. With the development of technology, these trends will continue to develop in the future and highlight the importance of ensuring the security, privacy, and integrity of digital assets and communications in an interconnected world. With the help of the adoption of

these innovations, stakeholders can navigate the digital landscape with confidence, ensuring that digital content is protected and distributed in a fair and equitable manner while fostering innovation and creativeness within the sector.

References

1. Green, M., Kaptchuk, G., Van Laer, G.. "Abuse Resistant Law Enforcement Access Systems". In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science(), vol 12698. Springer, Cham. https://doi.org/10.1007/978-3-030-77883-5_19.
2. Courtois, N. T., Gradon, K. T., & Schmeh, K. "Crypto currency regulation and law enforcement perspectives". arXiv preprint arXiv:, pp. 2109.01047, 2021.
3. Limniotis, K. "Cryptography as the means to protect fundamental human rights". Cryptography, vol. 5, no. 4, pp. 34, 2021. https://doi.org/10.3390/cryptography5040034
4. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. "Handbook of applied cryptography. CRC press.
5. Paterson, K.G. The Cyber Security Body of Knowledge, University of Bristol, 2021, ch". Applied Cryptography, version vol. 10, 2018.
6. Smart, N. The Cyber Security Body of Knowledge, University of Bristol, 2021, ch. Cryptography, Version vol. 1, pp. 01, 2021.
7. European Union. The EU's Cybersecurity Strategy for the Digital Decade.
8. Saidakhrarovich, G. S., & Rustambekovich, R. I. "THE ROLE AND IMPORTANCE OF CRYPTOGRAPHY IN MODERN LEGAL SYSTEMS", 2021.
9. Chimakurthi, V. N. S. S. "Digital Asset Management: A Lowdown on Intricacies of Digital Rights and Permissions". Global Disclosure of Economics and Business, vol. 9, no. 2, pp. 129-140, 2020. https://doi.org/10.18034/gdeb.v9i2.605
10. Custers, B. "New digital rights: Imagining additional fundamental rights for the digital era". Computer Law & Security Review, vol. 44, pp. 105636, 2022. https://doi.org/10.1016/j.clsr.2021.105636
11. Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. "A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change". Journal of management studies, vol. 58, no. 5, pp. 1159-1197, 2021. https://doi.org/10.1111/joms.12639
12. Singh, A., Klarner, P., & Hess, T. "How do chief digital officers pursue digital transformation activities? The role of organization design parameters". Long Range Planning, vol. 53, no. 3, pp. 101890, 2020. https://doi.org/10.1016/j.lrp.2019.07.001
13. Andriole, S. J. "Five Myths About Digital Transformation. Sloan review", 2017.
14. Benner, M. J. and Waldfogel, J. "Changing the channel: Digitization and the rise of "middle tail" strategies". Strategic Management Journal, pp. 1–24, 2020. https://doi.org/10.1002/smj.3130
15. Correani, A., De Massis, A., Frattini, F., Petruzzelli, A. and Natalicchio, A. "Implementing a digital strategy: Learning from the experience of three digital transformation projetcs". California Management Review, vol. 62, pp. 37–56, 2020. https://doi.org/10.1177/0008125620934864
16. Popova, R. "Space technology and cybersecurity: challenges and technical approaches for the regulation of large constellations". In Space Law in a Networked World pp. 102-128, 2023. Brill Nijhoff. https://doi.org/10.1163/9789004527270_005
17. Warner, K. S., & Wäger, M. "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal". Long range planning, vol. 52, no. 3, pp. 326-349,

2019. https://doi.org/10.1016/j.lrp.2018.12.001
18. Beebe, N. H. (2012). A Bibliography of Publications in the Journal of Discrete Mathematical Sciences and Cryptography. vertex, 344, 427.
19. Kumar, S., Srivastava, P. K., Srivastava, G. K., Singhal, P., Singh, D., & Goyal, D. (2022). Chaos based image encryption security in cloud computing. Journal of Discrete Mathematical Sciences and Cryptography, 25(4), 1041-1051.
20. Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind-Jensen, T. "Unpacking the difference between digital transformation and IT-enabled organizational transformation". Journal of the Association for information systems, vol. 22, no. 1, pp. 102-129, 2021. https://doi.org/10.17705/1jais.00655
21. Schallmo, D., Williams, C. A., & Boardman, L. "Digital transformation of business models—best practice, enablers, and roadmap". International journal of innovation management, vol. 21, no. 08, pp. 1740014, 2017. https://doi.org/10.1142/S136391961740014X
22. Vial, G. "JOURNAL OF STRATEGIC INFORMATION SYSTEMS REVIEW Manuscript title: Understanding digital transformation: A review and a research agenda", 2019.
23. Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. "Digital transformation: A multidisciplinary reflection and research agenda". Journal of business research, vol. 122, pp. 889-901, 2021. https://doi.org/10.1016/j.jbusres.2019.09.022
24. Weill, P., & Woerner, S. "Is your company ready for a digital future? MIT Sloan Management Review, Vol. 59, 2019.
25. Dizon, M. A. C., & Upson, P. J. "Laws of encryption: An emerging legal framework". Computer Law & Security Review, vol. 43, pp. 105635, 2021. https://doi.org/10.1016/j.clsr.2021.105635
26. Alam, M. N., Kaur, K., Kabir, M. S., Susmi, N. H., & Hussain, S. "Uncovering Consumer Sentiments And Dining Preferences: Legal And Ethical Consideration To Machine Learning-Based Sentiment Analysis Of Online Restaurant Reviews". In International Journal of Creative Research Thoughts Vol. 11, Issue 5, 2023.
27. Kabir, M. S., & Alam, M. N. "IoT, Big Data and AI Applications in the Law Enforcement and Legal System: A Review". International Research Journal of Engineering and Technology (IRJET), vol. 10, no. 05, pp. 1777-1789, 2023.