scientific reports

OPEN

DNA encoding schemes herald a new age in cybersecurity for safeguarding digital assets

Sehrish Aqeel[1], Sajid Ullah Khan[2,3]✉, Adnan Shahid Khan[1], Meshal Alharbi[3], Sajid Shah[4], Mohammed EL Affendi[4] & Naveed Ahmad[5]

With the urge to secure and protect digital assets, there is a need to emphasize the immediacy of taking measures to ensure robust security due to the enhancement of cyber security. Different advanced methods, like encryption schemes, are vulnerable to putting constraints on attacks. To encode the digital data and utilize the unique properties of DNA, like stability and durability, synthetic DNA sequences are offered as a promising alternative by DNA encoding schemes. This study enlightens the exploration of DNA's potential for encoding in evolving cyber security. Based on the systematic literature review, this paper provides a discussion on the challenges, pros, and directions for future work. We analyzed the current trends and new innovations in methodology, security attacks, the implementation of tools, and different metrics to measure. Various tools, such as Mathematica, MATLAB, NIST test suite, and Coludsim, were employed to evaluate the performance of the proposed method and obtain results. By identifying the strengths and limitations of proposed methods, the study highlights research challenges and offers future scope for investigation.

Keywords DNA encoding, Network attacks, Cyber security, Digital data protection, Encryption scheme, Cyber threats, Enhanced security, Computer network, Evaluation metrics, Analytical survey, Evaluation tools

In the unique domain of network safety, the previous ten years have seen an extraordinary expansion in interest and improvement in Web and correspondence innovations. This development has moved network security into a significant exploration space, utilizing instruments like firewalls and antivirus programming to guarantee the honesty of organizations and their related computerized resources inside the internet. Notwithstanding, amidst this development, another methodology has arisen: DNA encoding plans. This change in perspective vows to alter network safety by offering imaginative ways of safeguarding computerized resources with extraordinary proficiency and adaptability.

Online protection is a basic worry in our interconnected world, influencing the two people and organizations. The multiplication of virtual entertainment, distributed storage, and systems administration stages has acquainted various difficulties with information security, presenting clients with different dangers like forswearing of administration (DOS), malware, and ransomware[1]. The advanced age has seen an expansion in digital dangers, prompting information breaks, monetary misfortunes, and reputational harm[2]. As worldwide populaces and economies extend, the interest in economic energy sources to battle environmental change is expanding. Simultaneously, vigorous security calculations are expected to shield our advanced framework from digital dangers[3]. In this unique circumstance, DNA-based encryption arises as a promising arrangement, which exploits engineered DNA groupings to upgrade computerized security while further developing energy effectiveness[4]. Traditional encryption strategies have restrictions, prompting the quest for elective techniques, for example, DNA encoding plans. These plans utilize engineered DNA groupings to encode advanced information, exploiting DNA's interesting properties, for example, strength and protection from corruption[5]. Thus, DNA encoding plans can change network safety by giving better security and powerful information assurance[6]. Cryptography has for some time been significant in systems administration and network protection. The center has gone to DNA encoding plans as a data-based security instrument, offering validation and insurance against digital dangers[7].

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Malaysia. [2]Department of Information Systems, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, AlKharj, Kingdom of Saudi Arabia. [3]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj, Saudi Arabia. [4]EIAS Lab, CCIS, Prince Sultan University, Riyadh, Saudi Arabia. [5]College of Computer Information Sciences, CCIS, Prince Sultan University, Riyadh, Saudi Arabia. ✉email: sk.khan@psau.edu.sa

Late exploration has shown that DNA-based encryption calculations can utilize less energy than customary strategies, tending to the developing interest in manageable energy sources[8]. This paper aims to investigate the capability of DNA-based encryption as an energy-productive answer for computerized security. Not at all like past examinations, this one spotlight late exploration articles and utilizes a thorough strategy to recognize pertinent writing[9].

This study covers different parts of DNA encoding plans, including qualities, shortcomings, assessment measurements, ongoing patterns, and energy-saving elements, filling in as an important asset for scientists and experts[10]. This paper is coordinated into seven principal segments, including philosophy, an outline of DNA encoding plans, strategies utilized, assaults tended to, assessment measurements, results, and ends. Through thorough examination, it features the promising job of DNA encoding plans in improving online protection measures[11].

The purpose of this research paper is to provide a broad overview of the recent trends and advancements in DNA-based encoding schemes. The key idea is to furnish up-to-date information on recent advancements in DNA-based encryption to provide a baseline for new researchers who want to start exploring this important domain. The main contributions of this article are threefold. (i) We conducted a systematic study to select recent journal articles focusing on various DNA-based cryptographic methods which are published during the last 5 years (2018–2023). (ii) We reviewed each article extensively and discussed its various features such as its proposed methodology, strengths, weaknesses, evaluation metrics, and the used datasets. (iii) Based on these observations, we provided the recent trends of using cryptographic methods for network security then highlighted various challenges in DNA-based cryptography and provided different future directions in this important domain.

There are many survey papers in the literature that provide some implementation details on DNA-based cryptographic methods and techniques. Our article is different from the other review articles in three aspects: (i) We followed a systematic article selection process to obtain more focused articles on network security design considering cryptographic techniques. While the other studies reviewed the general cryptographic methods without using the systematic approach. (ii) Our study reviewed the articles published between 2018 to 2023. So, it provides more detailed information to gain insight and knowledge of the recent cryptographic methods and the recent trends followed in the design of DNA-based cryptographic techniques. (iii) In our study, an extensive review of the recent cyber security attacks, and their countermeasures by implementing the DNA approach by the research is provided where they are critically analyzed according to their methods, techniques, datasets, and evaluation metrics. The focus is to provide researchers with more updated knowledge on information security by DNA-based approach in one place, where they can find the recent trends and potential research areas in the domain to start exploring it. A detailed comparison of this article with other review articles is provided in Table 1.

The rest of the paper is organized as follows: "Methodology" describes the research methodology adopted in this study. "An overview of DNA encoding scheme" provides the basic DNA concept and its constitution. "Related work on the DNA encoding scheme" elaborates on the related searches that are conducted in this domain. The details about the various attacks and the research that has used the DNA method to counter that respective attack successfully are elaborated in "DNA Security and different kinds of attacks". "Strengths and weaknesses of each research study" comprises of strengths and weaknesses of the reviewed articles. Evaluation metrics and usage of tools to capture the results of DNA cryptography against various attacks are listed in "Evaluation metrics" and "Tools used" respectively. Observations, recent trends in cyber security, research challenges, and the future research scope are provided in "Recent trends, key findings, limitations, and future work". Finally, the Conclusion section concludes this review article.

Methodology

This study conducts a systematic literature review of the different DNA-based cyber security methods and investigates the published journal articles between 2017 to 2023. A systematic literature review is a methodology followed to identify, examine, and extract needful information from the literature related to certain research topics. We performed this systematic review in two phases. Phase 1 identifies the information resource (search engine) and keywords to execute a query to obtain an initial list of articles. Phase 2 applies certain criteria to

Review article	Year	Systematic study	Attacks focused	Comparative analysis		Evaluation metrics	Energy efficient	Future trends
				Strengths	Weaknesses			
Hazra et al.	2018	×	×	✓	×	×	×	×
Niu et al.	2019	×	✓	✓	×	×	×	✓
Taluja et al.	2020	×	×	✓	×	×	×	✓
Baraa et al.	2020	×	✓	✓	×	✓	×	×
Iliyasu et al.	2021	✓	✓	✓	✓	×	×	✓
BinHamad et al.	2024	✓	×	✓	×	×	×	✓
Berezin et al.	2024	✓	×	✓	✓	×	×	✓

Table 1. Binary Comparison with other review articles: (✓: Yes, ×: No)[76–80]. Binary comparisons with other review articles likely refers to a table in a research paper that presents a binary (yes/no or 1/0) comparison of various aspects or characteristics of the current review article.

the initial list to select the most related and core articles and store them in the final list which is reviewed in this article. The main purpose of this review article is to answer the following questions:

To address the questions outlined in Fig. 1, we adopt a data collection methodology. We use two methods: a systematic literature review (SLR) and a goal question metric (GQM) approach. SLR involves exploring a specific topic in predetermined steps and procedures to ensure that the review is focused, comprehensive, and accurate. To initiate SLR, we perform two steps: First, we use the GQM approach, which is a requirement engineering method for efficient requirements gathering[31]. To gain a thorough understanding of the research question, we set a goal and formulate questions to help us answer our research question, as shown in Fig. 2.

Our goal is to search for information related to the "DNA encoding scheme"[12,13], and accordingly, we formulate questions such as:

Q1. Which year will link to a related search?
Q2. What will be the research library?
Q3. What searches would be considered journals or proceedings?
Q4. Are we focusing on experience/results-based research?
Q5. What kind of search criteria will be applied to reach the ultimate goal?

In this phase, firstly search engines and keywords are identified for article search. A Scopus document search is chosen as a potential search engine due to its ability to search from almost all the well-known databases targeting keywords from each question from Q1 to Q5. We executed a search QUERY using an initial keyword "DNA-based encryption system" and adjusted the filter to show journal articles published between 2018 and 2023. The initial search QUERY resulted in the articles that proposed the DNA-based encryption method for

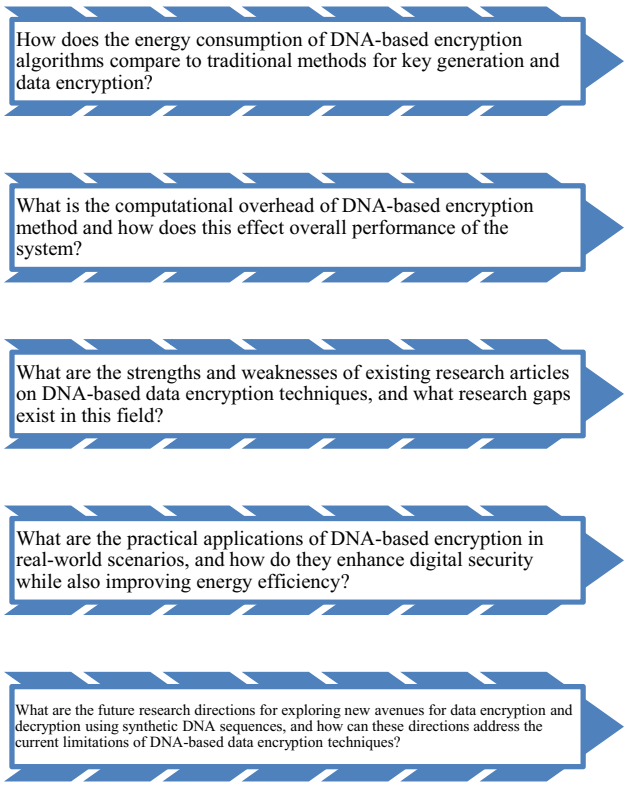

Figure 1. Research questions.

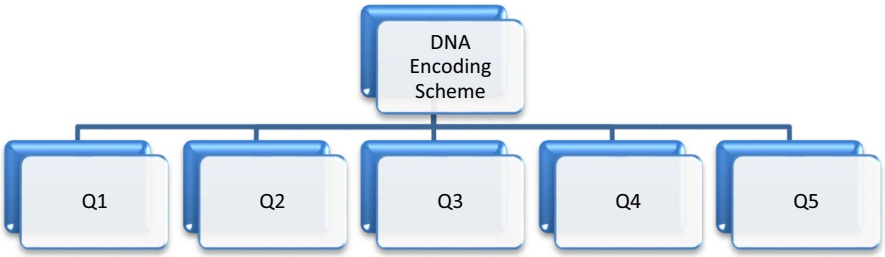

Figure 2. Research questions.

cryptography, encryption, medical domain, and wireless networks, we then redefined our keyword DNA-based encryption for information security and DNA to use for information hiding (text and image) deep learning to obtain more relevant articles. As a result of phase 1, relevant articles based on the keywords were selected and stored as an initial list. The detailed steps used in Phase 1 to obtain an initial list are summarized in Fig. 2.

The second step involves conducting a systematic literature review based on the questions defined in the first step. This approach starts with an initial query to search for articles (short, long, chapters, conference papers) on Google Scholar. Then, queries are generated based on the queries set in the first step to filter the data through query processing[9]. At each step, additional filters are applied, such as a year filter in the first step, a selection of journal articles in the second step, and articles from IEEE, Science Direct, Springer, and Scopus in the third step. This process results in a tentative list of subjects. Then, final inclusion and exclusion criteria are applied, excluding survey papers and focusing on new research in the specific domain to obtain useful results. This gives the final list of subjects. From this list, the top 40 articles are selected for the survey by reading the abstract of each paper. The complete process is shown in Fig. 3.

Exclusion and inclusion criteria refer to specific guidelines used to determine which articles were included or excluded from the review. Inclusion criteria define the characteristics that an article should consider for inclusion, e.g. Focusing on DNA encoding schemes for cyber security and publishing in peer-reviewed sources. Exclusion criteria outline characteristics that exclude an article from consideration, such as lack of relevance to the topic, failure to meet quality standards, or duplication of existing literature. These criteria were established to ensure that the selected articles were relevant and credible, and provided new insights for the literature review.

When the second step is completed, we need to select key variables on which our research will be based[14]. Here eight variables were identified and they are:

- Data encoding scheme
- Encryption algorithm
- Strengths
- Weaknesses
- Cloud computing
- Evaluation metrics
- Attacks
- Data encryption

Figure 4 explains the complete process under one umbrella, where it's time to uncover the findings we analyzed during our review study. The next part explains the basic structure of DNA.

An overview of DNA encoding scheme

Four different nucleotides, namely Adenine (A), Guanine (G), Cytosine (C), and Thymine (T), combine to form deoxyribonucleic acid (DNA). This arrangement takes the form of a double helix structure, as depicted in Fig. 5. The binary sequence of each nucleotide is presented in Table 2.

The Watson–Crick complementary base pair rule dictates the pairing of nucleotides in DNA sequences, which can be represented as binary chains of 0 s and 1 s. These sequences are machine-readable and enhance the efficiency and security of processes[15]. DNA-based cryptography is employed to ensure data security in communication processes. These binary sequences create unique patterns that facilitate encryption and decryption processes, providing a secure mechanism against unauthorized access. This robust security mechanism has gained popularity in network security and is increasingly adopted by researchers to ensure data confidentiality and security[16]. The next section discusses related studies on DNA-based encoding schemes reviewed in this paper, adopting various systematic review approaches as examples.

Related work on the DNA encoding scheme

This section provides an overview of various articles reviewed in this survey-based paper, all focusing on DNA security schemes and evaluating their effectiveness[17]. In 2020, Suyel Namasudraa and colleagues came up with a new DNA-based data encryption method for cloud computing[18]. Junxin Chen and team combined DNA encryption with 2D Henon sin maps[19]. Muhammad Samiyllah's group extended current techniques to create an

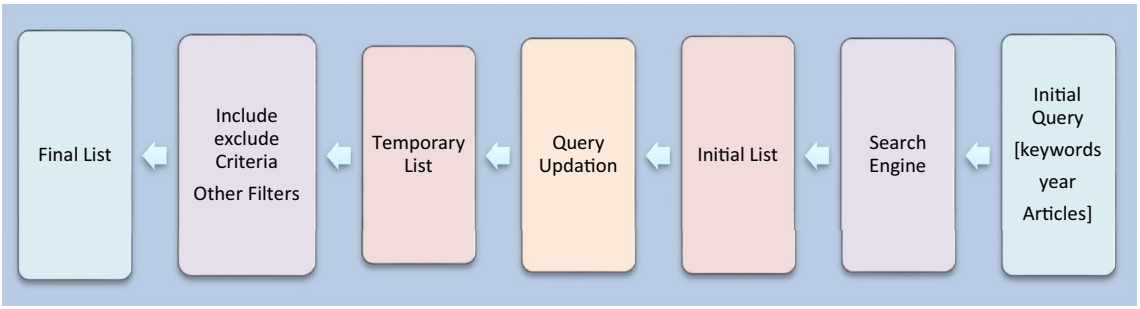

Figure 3. Systematic literature review (SLR) approach.

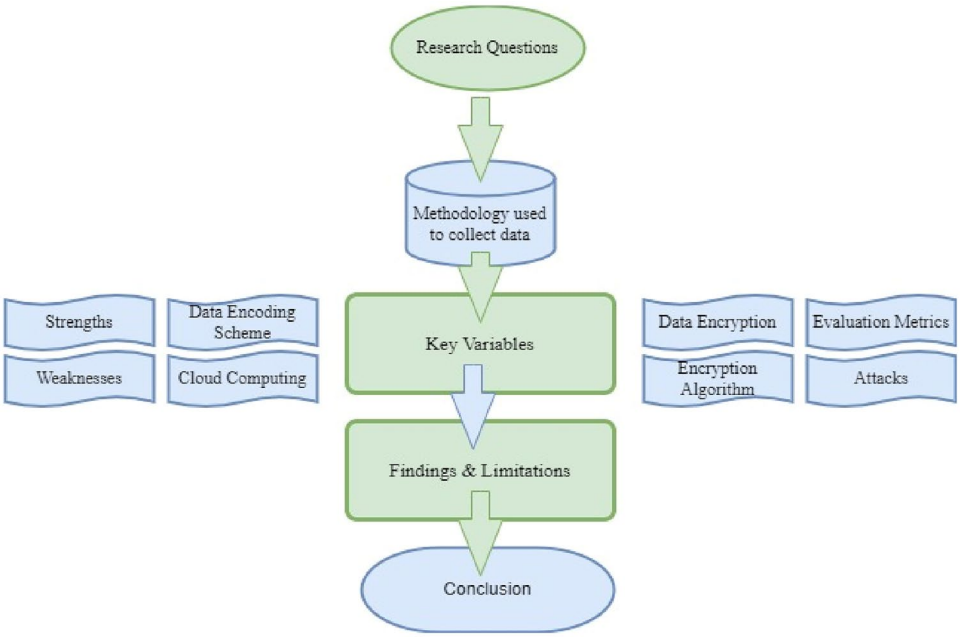

Figure 4. The methodology adopted in the paper along with the research work done on it.

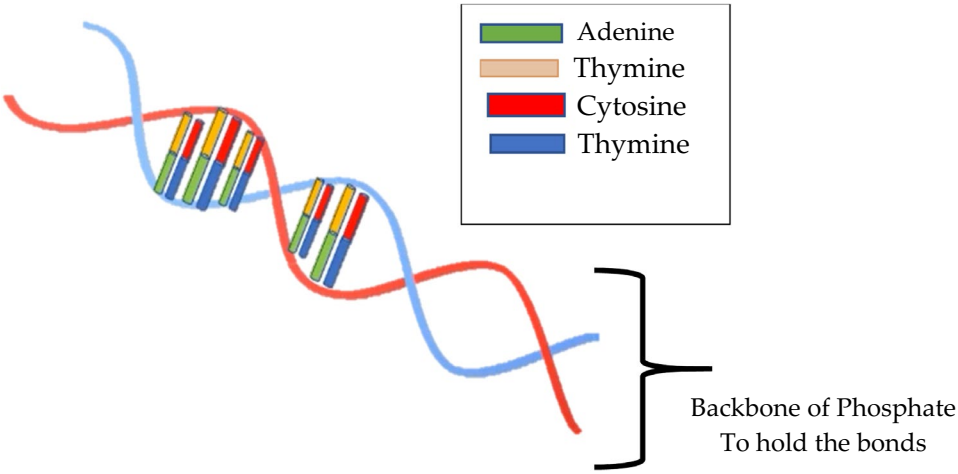

Figure 5. Double Helix structure of DNA.

Nucleotide	Binary sequence
A	00
T	11
C	10
G	11

Table 2. Binary sequence of each nucleotide.

asymmetric encryption method for color images[20]. Ebrahim Zarei Zefreh designed a unique image encryption system using a hybrid model of DNA computing, chaotic systems, and hash functions[21].

Lidong Liu and team used DNA encryption alongside a 5D hyper chaotic system, while Jan Sher Khan applied DNA-based keys for image encryption[22]. Maria Imdad built upon DNA encryption by using a DNA sequence table to substitute plaintext[23]. Dongming Huo introduced a more secure algorithm by integrating DNA Morse code patterns[24]. Jeena Jacob's team proposed an approach to combine DNA and compressed sensing theories

for image compression encryption[25]. Roayat Ismail Abdelfattah created a DNA codec technique using biometric data and Z pattern generation[26]. Suyel Namasudra used self-adaptive bit scrambling and multi-chaotic dynamic DNA computations for audio encryption[27]. Similarly, Arslan Shafique assessed DNA encoding for encrypting patient information in medical images[28]. Said E. El-Khamy used support vector machines and DNA to evaluate cryptosystem security levels. Nadeem Iqbal suggested a way to encrypt color images with DNA strands and chaotic systems[29]. Wei Feng used DNA for image encryption and steganography[30]. Zhen Li proposed encrypting color images with DNA strands and chaotic systems[31]. Tingwei Wu designed an image encryption scheme with pixel-level filtering and DNA-level diffusion[32]. Bahubali Akiwate used chaos-based image encryption with random DNA encoding and permutation[33].

Shuqin Zhu introduced a DNA extension code to encrypt downlink data in OFDM-PON. Dilovan Asaad Zebari found DNA encoding to be an efficient method for image cryptography[34]. K.C. Jithin employed a dynamic DNA hyperchaotic system for image encryption[35]. V. Radhakrishnan developed a multi-level DNA encryption algorithm. S. M. SeragEldin combined chaotic maps and DNA sequences to modify a hash algorithm[36]. T. Saba used machine learning for intrusion detection across IoT datasets. F. Ahmed proposed an approach for encrypting color images using a convolutional autoencoder, DNA, and chaos[37]. Sreeja Cherillath Sukumaran worked with chaotic image encryption and DNA operations[38]. Harsh Durga Tiwari used lightweight encryption with DNA sequences for smart meter communication security[39]. Dr. A. Murugan explored cloud security with DNA-based encryption for bio-computational operations[40]. A. Akhavan developed a hybrid DNA-encoded ECC scheme for multi-level security[41]. Manoj Kumar Pandey improved cloud data security using DNA sequences with Morse code and zigzag pattern encoding[42]. Xiuli Chai explored the security of DNA-based image encryption methods[43].

Md. Rafiul Biswas implemented a DNA cryptosystem with AES and RSA for key management[44]. Eungi Hong presented a color image cryptosystem using dynamic DNA encryption and a four-wing hyper chaotic system[35]. Mousomi Roy worked with dynamic DNA encoding and asymmetric cryptosystems for data secrecy[45]. Wei Feng used a DNA-based fuzzy vault scheme to protect IIoT device keys. S.K. Pujari proposed a two-stage method for image protection using DNA encryption and PCR amplification[46]. Suyel Namasudra improved an encryption scheme and analyzed it using a chosen plaintext attack algorithm[47].

This summary provides insights into the various research endeavors explored in the reviewed articles, demonstrating the diverse applications and advancements in DNA-based encryption schemes. Figure 6 shows the research studies along with key variable.

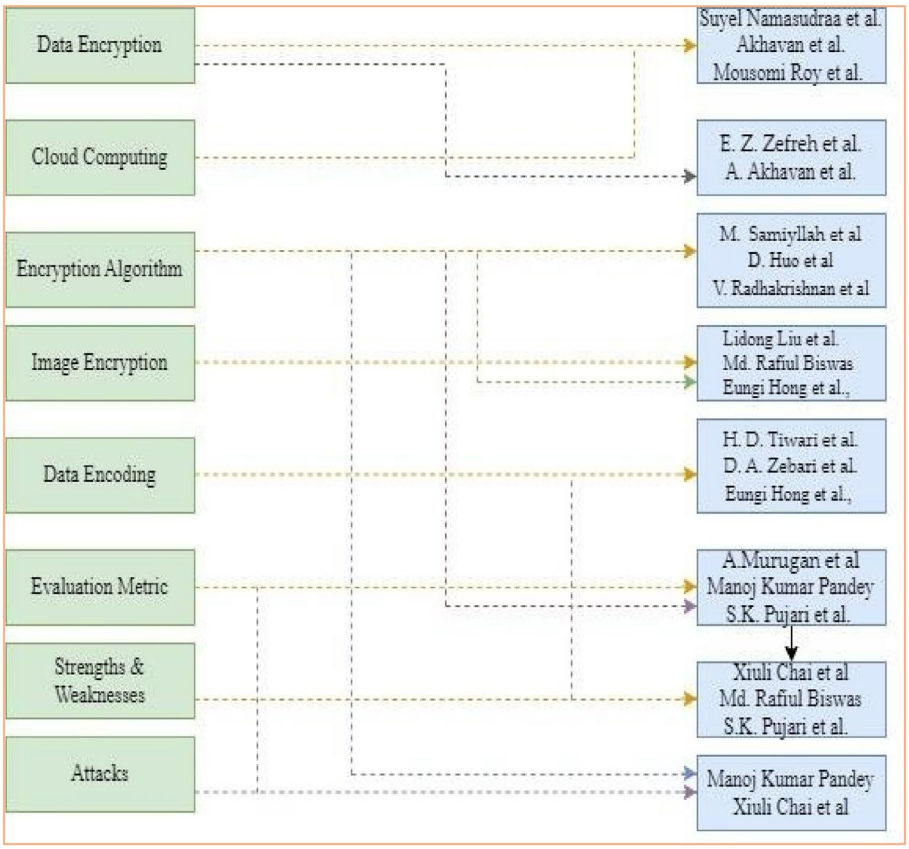

Figure 6. Research studies along with selected key variable.

DNA security and different kinds of attacks

This section covers a brief description of each attack that is being discussed in reviewed papers along with the frequency count of it in reviewed research studies[32,33] to come up with the significance of an attack against a DNA security scheme. This will facilitate reaching inferences about the most important and least elaborated list of attacks in the network domain[34]. As a network user, attacks are divided into Active ones and passive ones. The list of attacks described from 1 to 10 comes in this category followed by passive attacks and the last section covers the information about weak attacks as they are not elaborated on in more reviewed research studies. The taxonomical diagram to represent different categories of attacks is shown in Fig. 7 and the percentage of each attack discussed in research studies is illustrated in Fig. 8.

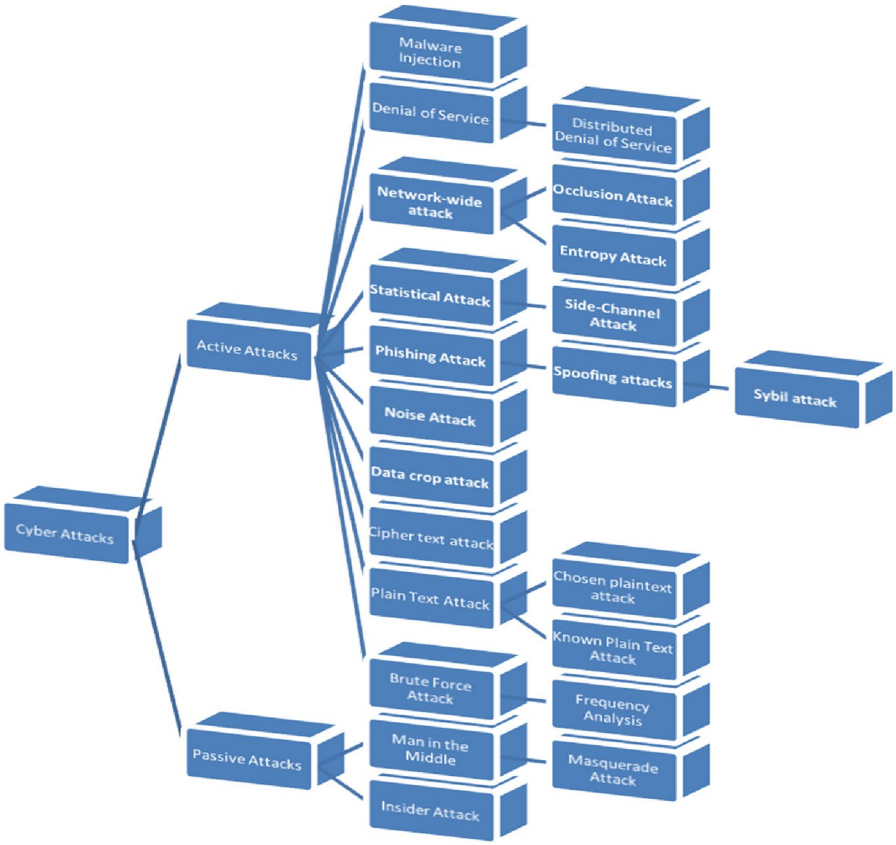

Figure 7. Taxonomical representation of various categories of attack.

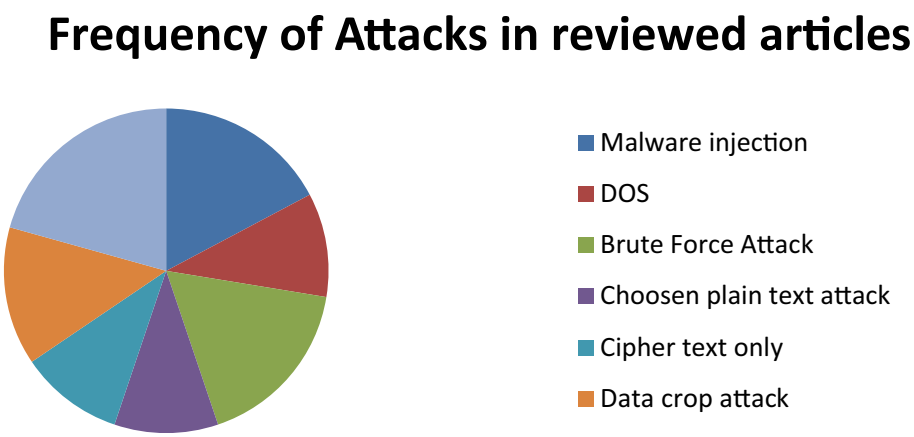

Figure 8. Chart of the percentage of each attack discussed in research studies.

Active attacks

In this type of attack, an attacker directly actively targets the system's security, making the destructive action immediately noticeable to the victim. It encompasses the following types, as observed in recently reviewed studies.

Malware injection (MI)

Malware, or malicious software, is specifically designed to facilitate illegal or unethical activities by suspicious users. Malware attacks are common in the cyber world, where attackers inject harmful applications into systems using Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) methods. Once the malicious code is injected and executed, it appears as a legitimate application, allowing the attacker to gain access to the system's resources. This enables the attacker to carry out further attacks and control the compromised system actively or passively, posing a threat to its security. DNA cryptography has been proven effective against such attacks, as demonstrated in research studies by Suyel Namasudraa et al. (2020). These studies provide significant evidence of DNA's scalability and data compatibility, making it a secure and energy-efficient approach[35–38].

Denial of service (DOS)

A denial of service (DOS) attack is a common type of attack in networking environments where the availability of any service is intentionally disrupted through unauthorized activity. This is often achieved by generating a high volume of network traffic, leading to network congestion or system crashes. The goal of a DOS attack is to render services unavailable for a victim or destabilize the entire system. Royat Ismail Abdelfatah (2020) efficiently addressed this attack using the DNA method with minimal energy consumption[39,40].

Brute force attack (BFA)

A brute force attack employs a trial and error method where the attacker continuously attempts to guess the secret key used to encrypt the selected text. This approach is commonly used to break passwords and security credentials. To mitigate this threat, it is recommended to use a strong key, such as a complex password or another robust security measure, to increase the difficulty for attackers attempting brute force attacks. Suyel Namasudra (2020), Jan Sher Khan et al. (2020), Junxin Chen et al. (2020), Zhen Li et al. (2020), Lidong Liu et al. (2020), Arslan Shafique et al. (2021), Ebrahim Zarei Zefreh (2020), and Mousomi Roy et al. (2019) have efficiently addressed this attack using DNA security schemes[35,41–47]

Frequency analysis involves studying the frequency of letters used in ciphertext to predict patterns and potentially break the encryption. Wei Feng et al. (2018), Lidong Liu et al. (2020), and Maria Imdad et al. (2020) have tackled this attack using DNA security methods, finding them suitable for large-scale applications and energy-saving approaches[48].

Plain text attack (PTA)

In a known plaintext attack, the attacker has access to both the plaintext and encrypted text, making it easier for them to deduce the encryption method and uncover additional secret information. Junxin Chen et al. (2020) and Jan Sher Khan et al. (2020) have devised techniques to address this attack using DNA sequences in their studies[49].

In a chosen plaintext attack, the attacker can select plaintext and observe its corresponding ciphertext. Muhammad Samiullah et al. (2020), Lidong Liu et al. (2020), Arslan Shafique et al. (2021), and Dongming Huo et al. (2020) have addressed these attacks using DNA methods and energy-efficient approaches in their studies[50]

Cipher text attack (CA)

A ciphertext attack is when an attacker obtains information about encrypted ciphertext and attempts to deduce the secret key used for encryption and decryption. Maria Imdad et al. (2020) and Wei Feng et al. (2018) addressed this attack using DNA security schemes, demonstrating its durability and energy-efficient storage capabilities successfully[51].

Phishing attack (PA)

Phishing is a type of social engineering attack where the attacker impersonates a legitimate entity, such as a user, organization, government agency, or bank, to deceive users into providing sensitive information or performing certain actions. This typically involves requests for credentials, such as password resets or email confirmations with malicious links. Once the user falls for the deception, the attacker can exploit the vulnerability to steal or damage data. Suyel Namasudraa et al. (2020) used DNA security sequences to mitigate this attack, recognizing it as a promising energy-saving approach for the future. Another related attack is spoofing, which is described below[4,52–56].

Statistical attack (SA)

This category targets statistical weaknesses in the system and exploits them accordingly. It may involve attacks on databases containing data, the efficiency of algorithms, packet arrival rates, and other statistical data objects to undermine system security. Arslan Shafique et al. (2021), Zhen Li et al. (2020), Jan Sher Khan et al. (2020), and Royat Ismail Abdelfatah (2020) have utilized DNA methods to address this type of attack efficiently in terms of energy consumption. A specific example of a statistical attack is a side-channel attack, where malicious code does not directly infiltrate the system. This attack relies on technical aspects of the system such as timing, power consumption, alarms, notifications, and other events generated by the system or application. DNA-based

schemes have been demonstrated to effectively counter such attacks, as shown in a study by Said E. El-Khamy et al. (2020)[57–61].

Network-wide attack (NWA)
This refers to a targeted attack on interconnected networking nodes aimed at compromising security and disrupting the network. Harsh Durga Tiwari et al. (2018) and Manoj Kumar Pandey (2018) examined the use of DNA sequences to mitigate this attack and assessed its effectiveness in terms of energy preservation.

Passive attacks

Passive attacks involve the silent observation by attackers without the knowledge or interaction of the sender or receiver. Some common types include:

Man in the MIDDLE (MITM)
In computer networking, a "man-in-the-middle" (MITM) attack refers to a covert activity where an intruder positions themselves between the sender and receiver. They silently intercept communication or manipulate it to carry out destructive actions. This poses a threat to users as messages are diverted through a third party before reaching the receiver. DNA can effectively counter this attack, as discussed by Monika Yadava et al., 2020 and Suyel Namasudra, 2020. A masquerade attack, a subtype of MITM, involves the attacker posing as a legitimate sender or receiver and controlling communication from that position. I. Jeena Jacob et al., 2020 and Suyel Namasudra have demonstrated the efficacy of DNA in handling this attack, showing it to be a more energy-efficient approach compared to existing methods.

Insider attack (IA)
One of the most common threats to organizations is insider attacks, where internal employees leak sensitive information, data, or security credentials intentionally to cause harm. Identifying and apprehending perpetrators of such attacks can be challenging without substantial evidence. These attacks are typically motivated by personal or professional reasons, such as gaining financial assets or tarnishing the organization's reputation. Suyel Namasudraa et al., 2020, have investigated methods to mitigate this threat using DNA security techniques in an energy-efficient manner. Table 3 visually summarizes the articles reviewed in terms of the attacks they address.

Other attacks

Attacks that are less addressed in reviewed studies are listed here:

Eavesdropping attack (EA)
In a MITM attack, the attacker gains control of transmitted data, intercepts, modifies, drops, or resends it according to their intentions. Thus, in eavesdropping, the attacker deliberately manipulates transmitted data from their side of the networked system. EungI Hong et al., 2021, effectively utilized the DNA method to address this attack with reduced computational cost and energy savings.

Jamming attacks (JA)
A jamming attack is a subset of DOS in which the attacker deliberately floods the network with artificial interference, rendering communication nodes unavailable for use. EungI Hong et al., 2021, implemented DNA

			Active attacks								Passive attacks		
Research study	Year	Energy efficient	MI	DOS	BFA	PTA	CA	PA	SA	NWA	MITM	IA	Other attacks
Suyel Namasudraa et al	2020	✓	✓		✓			✓			✓	✓	
Royat Ismail Abdelfatah	2020	✓		✓					✓				✓
JunxinChen et al.	2020	✓			✓	✓							
Lidong Liu et al.	2020	✓	✓		✓	✓					✓		
Arslan Shafique et al.	2021	✓			✓	✓			✓				✓
Ebrahim Zarei Zefreh	2020	✓			✓		✓						
Mousomi Roy et al.	2019				✓						✓		
Jan Sher Khan et al.	2020			✓		✓			✓				
Muhammad Samiullah et al.	2020	✓				✓							✓
Dongming Huo et al.	2020	✓				✓				✓			✓
Maria Imdad et al.	2020	✓	✓				✓						
Harsh Durga Tiwari et al.	2018	✓								✓			✓
Manoj Kumar Pandey	2018									✓			✓
EungI Hong et al.	2021	✓											✓
Bahubali Akiwate, et al.	2021		✓					✓					✓

Table 3. Research studies and attacks.

sequences to mitigate this attack. References[62,63] has also discussed strategies to address this attack using various AI techniques with reduced energy consumption.

Crypto attack (CA)
Attacks on cryptography, cryptocurrency, bitcoins, and similar systems are categorized as crypto attacks, which are increasingly common in today's world and can have catastrophic consequences if not addressed promptly and effectively. Harsh Durga Tiwari et al., 2018, and Manoj Kumar Pandey, 2018, adopted DNA techniques to evaluate its effectiveness against these attacks and found improved energy performance compared to traditional methods[64].

Differential attacks (DA)
This type of attack is mainly associated with block ciphers but can also be related to stream ciphers and hash functions, aiming to deduce the user's secret key by observing differences in network transmission and other related properties. The DNA scheme can be utilized to secure the system from these types of attacks while consuming less energy. This approach is discussed in studies by Muhammad Samiullah et al., 2020, Dongming Huo et al., 2020, Jan Sher Khan et al., 2020, Zhen Li et al., 2020, Said E. El-Khamy et al., 2020, Bahubali Akiwate et al., 2021, and Royat Ismail Abdelfatah, 2020.

Replay attack (RA)
This type of attack, also known as a repeat or playback attack, involves the delay or repetition of valid data transmission to cause harm or unethical activity. V. Radhakrishnan et al., 2019 and K.C. Jithin et al., 2020 utilized DNA techniques to address this attack and conserve energy efficiently.

Based on the frequency of attacks studied in various research papers, we have compiled Table 4, which displays the percentage of attacks along with their frequency counts, followed by a figure representing these percentages in the form of a pie chart.

Strengths and weaknesses of each research study

This section presents the analysis of each reviewed article in terms of its strengths and weaknesses. The analytical study revealed that DNA has significantly enhanced the security of the observed systems in all the reviewed articles. As this was a critical analysis, we compared the articles with one another to provide a comprehensive comparison of studies using DNA schemes as the security method of the recent era.

To summarize the limitations of the articles, we have identified the following key points:

- Use of limited or closed data set
- Evaluation of scheme under fewer security hazards/threats
- Consideration of fewer evaluation metrics in studies
- Lack of latest technology/tool in methodology
- Minimum track of text-based results through DNA

Table 5 narrates the comparative analysis in terms of the strengths and weaknesses of reviewed studies[67–75].

Table 6 covers various key variables of energy efficiency in reviewed articles.

Evaluation metrics

Table 7 illustrates a list of evaluation metrics along with its definition and abbreviation[65–70].

Table 8 illustrates a summarized view of used evaluation metrics in various research studies.

Providing details about evaluation metrics and tools ensures transparency, reproducibility, methodological rigor, and accurate interpretation of results in survey research.

The time taken by the system to generate a secret key refers to as Secret key generation time (SKGT) whereas the time consumed by the system to retrieve back the secret key is Secret key retrieval time (SKRT). Figure 9 plots the relationship between used matrices and the number of times it is studied in reviewed articles.

Attack name	Frequency count	Percentage
Malware injection	5	17%
DOS	3	10%
Brute force	5	17%
Chosen plain text	3	10%
Cipher text only	3	10%
Data crop	4	14%
Noise	6	21%

Table 4. Frequency count and percentage of strong attacks.

Review article	Strength	Weakness
Suyel Namasudraa et al., 2020	A 1024-bit secret key is generated based on DNA computing, user's attributes and Media Access Control (MAC) address of the user, and decimal encoding rule, American Standard Code for Information Interchange (ASCII) value, DNA bases, and complementary rule are used to generate the secret key that enables the system to protect against many security attacks	The scheme has a good impact on cloud security, however, still, it could be combined with other security schemes to check its unique results, as the other authors have done in their research studies
JunxinChen et al., 2020	Complicated DNA encryption operations (random encoding, XOR, and random decoding) as substitution boxes (s-boxes) are proposed	The scheme should be evaluated against more cyberattacks to evaluate the results
Muhammad Samiullah et al., 2020	An encryption algorithm is based on three chaotic systems (PWLCM, Lorenz, and 4D Lorenz-type), a Secure Hash Algorithm, a scrambler, a chaotic generator, and a DNA sequence-based Linear Feedback Shift Register	Three chaotic systems have been targeted in this paper making the algorithm more specific
Ebrahim Zarei Zefreh, 2020	The significant advantage of the proposed scheme is its high efficiency. The proposed scheme consists of DNA level permutation and diffusion	The scheme could be implemented with multiple chaotic systems to evaluate the response
Lidong Liu et al., 2020	The proposed scheme is related to the plaintext and external secret key, which does not need to manage the huge amounts of dynamic secret keys and does not design a synchronization method as the one-time-pad encryption scheme	The proposed scheme cannot resist noise and occlusion attacks
Jan Sher Khan et al.,2020	To make and ensure that this new scheme is robust and secure against various kinds of attacks, the initial conditions of the chaotic maps utilized are generated from a random DNA sequence as well as plaintext image via an SHA-512 hash function	A hash function can be an interesting combination that is used by other researchers to evaluate the implemented results
Maria Imdad et al., 2020	This paper proposes an enhanced DNA table for all 96 printable ASCII characters which are created to improve the entropy so that the probability of each encoding base (A, T, C, G) is equally likely and to reduce the computational complexity of DNA cryptography	The scheme is evaluated under a few security attacks
Dongming Huo et al., 2020	The logistic map is applied to control key image and measurement matrices and to control DNA encoding and decoding rules used to encode and decode each row of the plain image and the key image	The scheme should be evaluated more broadly in terms of metrics used with defined simulation results
Shaoping Hu et al., 2020	Based on the promising results obtained qualitatively and quantitatively, paper envisage a wide deployment of our developed technique in large-scale clinical studies	Security of data is not evaluated under variety of attacks under discussion
Monika Yadava et al., 2020	As compared to existing approaches, this model has experimentally proved its effectiveness in terms of numerous handling attacks	The algorithm is not tested for any open data set nor it is evaluated for standard metrics to check its claimed effectiveness
Roaya Ismail Abdelfatah, 2020	The novelty of this scheme is that it combines four different techniques for audio encryption in the same scheme which makes it more secure: self-adaptive scrambling, multi chaotic maps, dynamic DNA encoding, and cipher feedback encryption	The scheme is tested for 3 main types of attacks; it could be evaluated for more kinds of network attack as well
Roayat Ismail Abdelfattah et al. 2020	In the proposed scheme, DNA is used with a new one dimension (HST) map system which has more advantages than the simple chaotic system such as larger parameter space, high randomization, and many chaotic sequences	The scheme should be tested for further attacks too
Arslan Shafique et al., 2021	A model is proposed that can detect the security level of various encryption schemes quickly and accurately	Common attacks are evaluated for the proposed algorithms; defined attacks are not evaluated with test data
Said E. El Khamy et al., 2020	For the first time, the proposed technique uses hybrid DNA encoding and Choquet's Fuzzy Integral sequences	Fewer attacks are discussed to evaluate the performance of the proposed scheme
Tingwei Wu et al., 2020	The experimental results show that the proposed method can resist optical channel response and fiber nonlinearity, which is a promising candidate for solving the security enhancement in access networks	The scheme is evaluated for a few cyber attacks and fewer implementation metrics to strengthen the effectiveness of the proposed method
Bahubali Akiwate, et. al. 2021	It presents an effective image data scrambling technique with chaotic maps that can withstand multiple security attacks	The scheme could be tried with other data sets too to show the extended results
Shuqin Zhu et al., 2020	The proposed algorithm not only has the advantages of a "scrambling substitution" structure algorithm but also overcomes the difficulty of key management in a "one-time pad" encryption scheme	The scheme could be tried with other data sets too to show the extended results
Dilovan Asaad Zebari et al., 2018	Security analysis and robustness of the proposed scheme have shown that the probability of guessing attackers to retrieve the original plaintext is near to zero, which means it provides very high security	The proposed technique can be used for the image dataset. Also, the key generation can be improved to provide more security
K.C. Jithin et al., 2020	A new Mandelbrot Set-based conditional shift algorithm is introduced to apply confusion effectively on R, G, and B channels	We can further improve the running speed of the algorithm by incorporating the concept of parallel permutation or parallel diffusion
V. Radhakrishnan et al., 2019	The proposed 2 way DNA phased cryptography provides confidentiality and integrity to transmitted data and the authentication of keys is attained by exchanging through the Diffie Hellman scheme	The scheme is evaluated for a few cyber attacks and fewer implementation metrics to strengthen the effectiveness of the proposed method
S. C. Sukumaranet al., 2018	The suggested algorithm uses indexing and DNA steganography techniques along with binary coding rules make the algorithm secure as it is an additional layer of bio-security than conventional cryptographic techniques	The algorithm is not tested against defined security metrics by targeting defined security attacks in the cloud computing environment
Harsh Durga Tiwari et al., 2018	The simulation and performance results show that the proposed schemes improve the strength of standard elliptical cryptosystems using DNA mapping	The concept is proposed for IoT, this could be simulated for other networking domains to experience the response provided by the proposed scheme
A.Murugan et al., 2017	The use of Morse code and Zigzag pattern makes the intruder much harder to steal original data	Picture and video data could be transmitted into a cloud environment using the above-proposed method
Continued		

Review article	Strength	Weakness
A. Akhavan et al., 2017	In this study, a practical plain image recovery method is proposed, and it is shown that the images encrypted with the same key could easily be recovered using the suggested cryptanalysis method with as low as two chosen plain images	The proposed algorithm is not evaluated under various crypto attacks
Manoj Kumar Pandey, 2018	This paper mainly focuses on the implementation of the DNA cryptosystem with the use of AES and keys management using the RSA algorithm and also verification of data on another side	The scheme is checking cryptosystems without discussing attacks on them and not evaluating their security under them well
Xiuli Chai et al., 2018	A novel diffusion mechanism based on random numbers related to the plaintext (DMRNRP) is introduced to diffuse the DNA sequences of the plain image	The scheme could have remarkable results if tried with different data sets under real-time simulating environments
Md. Rafiul Biswas et al., 2017	The key idea is to split the plaintext into fixed-sized chunks, to encrypt each chunk using an asymmetric cryptosystem, and finally to merge the cipher text of each chunk using dynamic DNA encoding	A generalized approach is not properly evaluated under set metrics of simulating the environment
Eunji Hong et al., 2021	The proposed method generates a specific two-factor device DNA through the combination of the IIoT device's intrinsic factor and its surrounding environments and then creates a vault set to conceal the secret key based on the two-factor device DNA	The scheme operates in unmanned smart manufacturing environments, which should not have any people in them under normal conditions
Mousomi Roy et al., 2019	The proposed algorithm uses biological features as well as the simple operations of traditional cryptography	The scheme is not evaluated under a variety of attacks to ensure its success rate

Table 5. Strengths and weaknesses of the proposed methodologies.

Research study	Scalable	Cost-effective	Lightweight	Unique	Compatible	Durable
Royat ismail abdelfatah, 2020	✓	✓	✓	✓	✓	✓
Suyel namasudra et al., 2020	✓			✓		
Lidong liu et al., 2020	✓	✓	✓	✓	✓	✓
Arslan shafique et al., 2021	✓	✓	✓	✓	✓	✓
Ebrahim zarei zefreh, 2020			✓	✓	✓	
Said e. El-khamy et al., 2020	✓	✓	✓	✓		✓
Nadeem iqbal et al., 2020	✓	✓	✓	✓	✓	
Dongming huo et al., 2020				✓		✓
Xiuli chai et al., 2018	✓	✓	✓	✓	✓	
Bahubali akiwate, et. al., 2021	✓	✓	✓	✓	✓	✓
M. G. Abbas malik et al., 2020			✓	✓		✓

Table 6. Key features used in review papers.

Evaluation metric	Abbreviation	Definition
Entropy	ENT	The amount of energy is not available for the system to perform any fruitful work. In other words, it refers to the disorder of the system
Histogram	HIS	It is a powerful statistical method to poetry the numerical data in the form of a bar chart representing segmented data on one axis and time interval on another
Correlation coefficient	CC	It determines the relationship between two variables in terms of its direct/indirect and weak/intermediate and strong
Variance	VAR	It is used to show the variability in data for standardized values such as the mean. In other words, it shows the spread of data over given intervals
Peak signal-to-noise ratio	PSNR	It is used as a quality measure to show the comparison of quality between original and compressed images with the help of PSNR
Number of pixels change rate	NPCR	It represents the rate of the number of pixels that have changed in the original image and cipher image
Unified average changing intensity	UACI	It determines the difference in color intensities between two images
Accuracy	ACC	It is the measure of the closeness of the obtained result with a particular value
Sensitivity	SEN	It refers to the proportion of those values that satisfy the true condition when tested for positive results
Encryption time	ET	The time utilized to perform encryption
Decryption time	DT	The time taken to decrypt back is DT
Mean square error	MSE	It is determined by taking the average of differences between actual and estimated values
Keyspace	KS	In cryptography, this term is taken as the sample space of all possible sets that could be used to start up the algorithm deployed in cryptanalysis
Mean absolute error	MAE	It takes the average value of the error in an experiment regardless of the direction of the error. It is computed by taking the average differences between predicted and observed values
Key reconstruction rate	KRR	This is the rate at which the secret key is re-created for the algorithm in use at a given period

Table 7. List of evaluation metrics used in review papers.

Research study	Evaluation metrics														
	ENT	HIS	CC	VAR	PSNR	NPCR	UACI	ACC	SEN	ET	DT	MSE	KS	MAE	KRR
Royat ismail abdelfatah, 2020	✓	✓	✓		✓	✓	✓	✓					✓		✓
Suyel namasudra et al., 2020	✓									✓	✓				
Lidong liu et al., 2020	✓	✓	✓	✓	✓	✓	✓			✓			✓		
Arslan shafique et al., 2021	✓	✓	✓	✓	✓	✓		✓				✓		✓	✓
Ebrahim zarei zefreh, 2020		✓	✓		✓	✓	✓						✓		
Said e. El-khamy et al., 2020	✓	✓	✓	✓	✓	✓	✓	✓			✓			✓	
Nadeem iqbal et al., 2020	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓	✓
Dongming huo et al., 2020					✓	✓	✓	✓							✓
Xiuli chai et al., 2018	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓		
Bahubali akiwate, et. al., 2021	✓	✓	✓		✓	✓	✓	✓		✓	✓				
M. G. Abbas malik et al., 2020		✓	✓	✓	✓	✓	✓	✓	✓					✓	
Tawsifur rahman et al., 2020								✓	✓		✓			✓	
Shaoping hu et al., 2020								✓	✓				✓		
I. Jeena jacob et al., 2020	✓							✓		✓	✓				✓

Table 8. Research studies and used evaluation metrics.

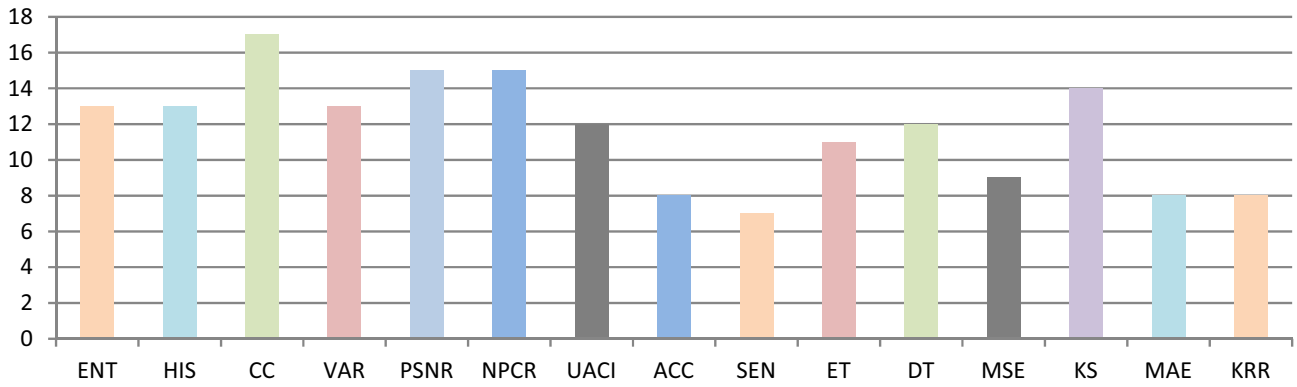

Figure 9. A chart to represent the number of times the metric is used to evaluate the DNA security scheme.

Tools used

Various tools were employed to evaluate the performance of the proposed method and obtain results. This section depicts percentage of each tool is used in the form of a pie chart. Figure 10 shows the percentage of each tools used in research studies.

Cloudsim

This framework is utilized for cloud computing environments, providing simulation services. It is among the most popular cloud-based simulators in academia and research, originally developed in Java as open- source software.

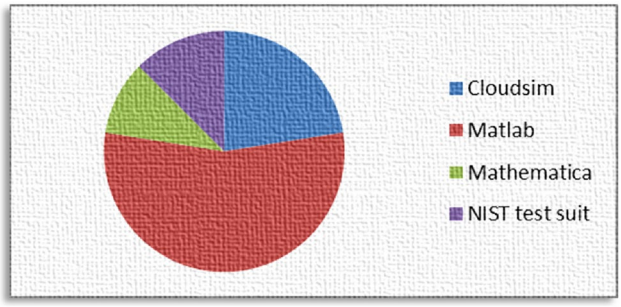

Figure 10. A chart to show the percentage of each tool used in research studies.

Matlab
Matlab offers a versatile computing platform with multiple functionalities, including data analysis, algorithm design, application creation, cloud computing, as well as image processing and computer vision. It is extensively used for testing, measurements, and various performed tests.

Mathematica
This software features built-in library functions beneficial for cloud computing tasks such as user interface, algorithm design, machine learning, and function implementation.

NIST test suite
NIST produces test suites for three functional domains: requirement-based, security-based, and human-factor-oriented. These suites encompass specialized areas like volume testing, requirement testing, and logic testing.

Recent trends, key findings, limitations, and future work
This section discusses the observations made during the review of research studies, the challenges encountered, and potential future research directions.

Recent trends
Many research studies have employed the DNA security method with image-based data to assess image security. Additionally, it's often combined with other concepts such as diffusion substitution schemes, chaotic maps, deep learning, supervised machine learning, and other AI-related methodologies. DNA encoding is predominantly used for protecting cloud data compared to other types of networked data. When not applied in cloud systems, this scheme is implemented with either new algorithms or adapted algorithms for existing datasets. Various types of attacks are addressed to mitigate their harmful effects, with some attacks being more prevalent than others. Dominant attacks include DOS, malware injection, noise attacks, chosen plaintext, and ciphertext-only attacks, which are extensively discussed and evaluated for mitigation methods. Statistical methods are commonly used for evaluation, including correlation coefficient, variance, and histogram analysis. Other metrics like PSNR, NPCR, and UACI are also frequently focused on in many studies. Additionally, entropy information is often analyzed and discussed in research studies. Matlab it is the preferred tool for evaluating research metrics compared to other tools used in research studies.

Key findings
The paper has several implications for researchers and practitioners in the field of cyber security:

It emphasizes the potential of DNA encoding schemes as an alternative approach to traditional encryption techniques for enhancing cyber security measures while consuming less energy compared to existing methods. This finding can inspire researchers to explore new avenues for data encryption and decryption using synthetic DNA patterns. DNA, being a durable storage medium resistant to harsh environmental conditions, offers a potentially energy-efficient approach for long-term data storage. Furthermore, considering the scalability of DNA-based encryption algorithms and their compatibility with existing hardware and software systems is crucial when evaluating their potential as an energy-efficient approach to digital security.

It identifies several research gaps in DNA-based data encryption methods, such as the lack of standardized evaluation metrics and the need for more practical applications in real-world scenarios. These gaps can guide future research directions and help researchers develop more robust and effective DNA encoding schemes. Additionally, it provides a comprehensive overview of various techniques used by researchers to implement DNA encoding schemes, such as encryption algorithms, substitution-permutation, and hybrid methods. This information can assist practitioners in choosing the most appropriate method for their particular application.

The paper underscores the importance of evaluating the effectiveness of DNA encoding schemes using various metrics such as security, speed, and accuracy to develop more efficient encryption algorithms capable of withstanding various types of attacks. Moreover, it demonstrates that DNA encoding schemes have potential applications in various domains such as cloud computing, image encryption, and secure communication. This finding can inspire the exploration of new use cases for DNA-based data encryption techniques in different fields.

Limitations
As most of the trend depicts that cloud computing was more secure with DNA schemes, it remains an open challenge for researchers to work in the other domains with DNA encoding and come up with their contributions. DNA scheme is less used for text-based data as compared to audio and image-based data. So this opens a new challenge for future research where more work could be done and contributed towards cyber security. DNA security scheme must have experimented with a variety of security attacks that digital security face and it is challenging for upcoming research studies to work this scheme with those attacks (such as Sybil attack and differential attack) that are not tested yet with this protective method in a networking environment.

New metrics could be formed and tested for experimental results such as deep learning models, supervised vector machines, Turing machines, and concepts related to automata which will open a new dimension for researchers to combine network security with other branches of quantum physics, combinatory, and other computing and engineering-related methods for evaluation and adaptation.

Despite Matlab, SPSS could be an open challenge and used in the next research to show statistical results. For image-based data handling, ArcGIS and Wika have not experimented with DNA security methods and it

could be an interesting combo to combine any of this software with any programming platform to bring the latest findings in the cyber security domain[74].

The paper only focuses on DNA-based data encryption techniques and does not cover other emerging technologies such as blockchain and quantum computing, which can also have significant implications for cyber security. Moreover, it does not provide a detailed analysis of the technical aspects of DNA encoding schemes, such as the chemical properties of synthetic DNA sequences and their interactions with digital data. This information could have provided a more in-depth understanding of the underlying mechanisms of DNA-based data encryption techniques and that opens a new direction for future work too, where these areas will be discussed in much detail.

Future trend

The future direction of DNA encoding schemes is promising, with the potential to revolutionize cybersecurity. Some key future directions for DNA encoding schemes include:

1. Developing more efficient and cost-effective methods for synthesizing DNA sequences.
2. Integrating DNA encoding schemes with other security mechanisms like encryption and block chain technology.
3. Exploring new applications for DNA encoding schemes beyond data storage, such as authentication and biometric identification.
4. Developing standardized protocols for DNA sequencing and analysis to ensure consistency and reliability across different platforms.
5. Investigating the ethical, legal, and social implications (ELSI) associated with the use of DNA encoding schemes in cyber security

Exploring the energy efficiency benefits of DNA-based encryption as the future of digital security

The world is facing increasing demands for energy as populations grow and economies develop. To address this challenge, there's a global shift towards sustainable and renewable energy sources like solar, wind, hydroelectric, geothermal, and biomass. This transition is driven by the need to mitigate climate change and reduce greenhouse gas emissions[81].

Encryption methods consume significant amounts of energy due to the complex mathematical operations involved. The energy consumption varies depending on factors like the encryption algorithm, data size, and hardware/software used. Efforts are underway to develop more energy-efficient encryption algorithms and hardware to reduce energy consumption while maintaining security[82,83].

DNA-based Encryption is one such method that claims to be energy-efficient. It has several potential energy-saving advantages:

1. Key Generation: DNA sequences can generate encryption keys more efficiently than traditional methods[84].
2. Data Encryption: DNA sequences encrypt data with less complexity compared to traditional methods[85].
3. Storage: DNA has high storage density, reducing the need for additional storage devices and associated energy consumption.
4. Transmission: DNA can securely transmit data over wireless networks, reducing the need for wired connections and energy consumption.
5. Scalability: DNA sequences can store large amounts of data in a small space, requiring less physical storage and equipment[86].
6. Cost Effectiveness: DNA-based encryption can be cost-effective, reducing the need for expensive storage solutions[87].
7. Lightweight: DNA-based methods are compact and easy to implement, requiring simple equipment[88].
8. Uniqueness: Each individual's DNA is unique, providing a high level of uniqueness in data security.
9. Compatibility: DNA methods can integrate with existing security schemes and technologies, making them easy to adopt[89].
10. Future Potential: Ongoing research may lead to even more advanced DNA-based security methods, saving energy and enhancing security[90].

In summary, DNA-based encryption algorithms offer energy savings by minimizing computational requirements and enabling efficient data storage and transmission. They are durable, compatible, unique, and lightweight, making them ideal for future security applications, thereby saving energy and computational costs.

Conclusion

In conclusion, DNA security schemes offer a potent means of safeguarding cyber data while conserving energy in networked environments. Recent research studies have underscored its efficacy through experimental findings. This review paper has curated top relevant studies, highlighting their insights through detailed analysis. The abundance of recent research in DNA security underscores its emergence as a pivotal trend in network security. DNA encoding appears poised to shape the future of digital security in our energy-conscious world. Cloud data protection has emerged as a primary application area for DNA encoding, with significant experimentation also seen in image-based data security, particularly in cloud computing. The prevalence of chosen plain text attack, cipher text-only attack, malware injection attack, noise attack, and DOS in recent studies indicates the focus

on mitigating these threats using DNA encoding. Statistical metrics have emerged as the primary evaluation method, with Matlab being the preferred tool for assessing the effectiveness of DNA security schemes. In "DNA security and different kinds of attacks", the discussion on attacks serves to contextualize the current literature by highlighting the prevalent security challenges faced in the field of DNA encoding schemes for cyber security. By addressing various types of attacks and their significance, the section provides valuable insights into the practical implications and vulnerabilities encountered in the literature. Understanding these challenges is crucial for assessing the effectiveness of existing approaches and identifying areas for further research and improvement. Therefore, while the focus of the section may appear divergent from a traditional literature review, it ultimately contributes to a more comprehensive understanding of the current state of the field and informs future directions for research and development. For future research it is suggested to have more exploration of DNA encoding with emphasizing on the consideration of ethics and privacy as with the association of data of DNA in cyber security having issues and problems related to the consent, ownership of data and misuse potential. Moreover, further research can be concluded on the basis of threats of computing against the resilience of the schemes of DNA. The article selection criteria were based on both inclusion and exclusion criteria. Included articles focused on DNA encoding schemes for cyber security, were published in reputable peer-reviewed sources, and offered novel insights. Excluded articles lacked relevance, failed to meet quality standards, or duplicated existing literature. These criteria aimed to ensure a comprehensive and credible literature review. Overall, DNA methods remain a vibrant research area, offering promise for the development of more efficient and sustainable data encryption techniques in networked computing environments. This paper serves as a valuable resource for researchers and practitioners seeking insights into DNA encoding schemes, facilitating the advancement of cyber security practices with enhanced efficiency and precision.

Data availability

The datasets utilized and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Received: 21 February 2024; Accepted: 9 June 2024
Published online: 15 June 2024

References

1. Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R. & Shanthini, A. Towards DNA based data security in the cloud computing environment. *Comput. Commun.* **151**, 539–547. https://doi.org/10.1016/j.comcom.2019.12.041 (2020).
2. Chen, J., Chen, L. & Zhou, Y. Cryptanalysis of a DNA-based image encryption scheme. *Inf. Sci.* **520**, 130–141. https://doi.org/10.1016/j.ins.2020.02.024 (2020).
3. Samiullah, M. *et al.* An image encryption scheme based on DNA computing and multiple chaotic systems. *IEEE Access* **8**, 25650–25663. https://doi.org/10.1109/ACCESS.2020.2970981 (2020).
4. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J. & Ahmad, F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.* **32**(1), e4150 (2021).
5. Zefreh, E. Z. An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. *Multimed. Tools Appl.* **79**, 24993–25022. https://doi.org/10.1007/s11042-020-09111-1 (2020).
6. Liu, L., Wang, D. & Lei, Y. An image encryption scheme based on hyper chaotic system and DNA with fixed secret keys. *IEEE Access* **8**, 46400–46416. https://doi.org/10.1109/ACCESS.2020.2978492 (2020).
7. Khan, J. S. *et al.* DNA and plaintext dependent chaotic visual selective image encryption. *IEEE Access* **8**, 159732–159744. https://doi.org/10.1109/ACCESS.2020.3020917 (2020).
8. Imdad, M., Ramli, S. N., Mahdin, H., Mouni, B. U., Sahar, S. An enhanced DNA sequence table for improved security and reduced computational complexity of DNA cryptography. In *Body Area Networks. Smart IoT and Big Data for Intelligent Health. BODYNETS 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 330 (eds. Alam, M. M. *et al.*) (Springer, 2020). https://doi.org/10.1007/978-3-030-64991-3_8.
9. Tabassam, S., Al-Saeed, W., Almughram, O. & Alghamdi, K. Scalable data analysis and query processing. *Int. J. Eng. Appl. IREA.* **7**(3), 81–87. https://doi.org/10.15866/irea.v7i3.17012 (2019).
10. Malik, M. G. A., Bashir, Z., Iqbal, N. & Imtiaz, M. A. Color image encryption algorithm based on hyper-chaos and DNA computing. *IEEE Access* **8**, 88093–88107. https://doi.org/10.1109/ACCESS.2020.2990170 (2020).
11. Jamshidi, M. B. *et al.* Artificial intelligence and COVID-19: Deep learning approaches for diagnosis and treatment. *IEEE Access Pract. Innov. Open Solut.* **8**, 109581–109595. https://doi.org/10.1109/ACCESS.2020.3001973 (2020).
12. Hu, S. *et al.* Weakly supervised deep learning for COVID-19 infection detection and classification from CT images. *IEEE Access* **8**, 118869–118883. https://doi.org/10.1109/ACCESS.2020.3005510 (2020).
13. Yadav, M. & Breja, M. Secure DNA and Morse code based Profile access control models for Cloud Computing Environment. *Proc. Comput. Sci.* **167**, 2590–2598. https://doi.org/10.1016/j.procs.2020.03.317 (2020).
14. Khan, A. S., Javed, Y., Abdullah, J., & Zen, K. Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS). *J. Ambient Intell. Human. Comput.* 1–18 (2021).
15. Huo, D. *et al.* Novel image compression–encryption hybrid scheme based on DNA encoding and compressive sensing. *Appl. Phys. B* **126**, 45. https://doi.org/10.1007/s00340-020-7397-3 (2020).
16. Jacob, I. J. *et al.* Biometric template security using DNA codec based transformation. *Multimed. Tools Appl.* **80**, 7547–7566. https://doi.org/10.1007/s11042-020-10127-w (2021).
17. Abdelfatah, R. I. Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. *IEEE Access* **8**, 69894–69907. https://doi.org/10.1109/ACCESS.2020.2987197 (2020).
18. Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. Securing multimedia by using DNA based encryption in the cloud computing environment. *ACM Trans. Multimed. Comput. Commun. Appl.* (2020) **(in Press)**.
19. Abdelfatah, R. & Nasr, M. Secure image encryption scheme based on DNA and new multi chaotic map. *J. Phys. Conf. Ser.* **1447**, 012053. https://doi.org/10.1088/1742-6596/1447/1/012053 (2020).
20. Aqeel, S., Khan, A. S., Ahmad, Z. & Abdullah, J. A comprehensive study on DNA based security scheme using deep learning in healthcare. *EDPACS* https://doi.org/10.1080/07366981.2021.1958742 (2021).
21. Shafique, A. *et al.* Detecting the security level of various cryptosystems using machine learning models. *IEEE Access* **9**, 9383–9393. https://doi.org/10.1109/ACCESS.2020.3046528 (2021).

22. El-Khamy, S. E., Korany, N. O. & Mohamed, A. G. A new fuzzy-DNA image encryption and steganography technique. *IEEE Access* **8**, 148935–148951. https://doi.org/10.1109/ACCESS.2020.3015687 (2020).
23. Iqbal, N. *et al.* DNA strands level scrambling based color image encryption scheme. *IEEE Access* **8**, 178167–178182. https://doi.org/10.1109/ACCESS.2020.3025241 (2020).
24. Feng, W. & Jing, Z. Cryptanalzing a novel hyper-chaotic image encryption scheme based on pixel-level filtering and DNA-level diffusion. *IEEE Access.* **8**, 209471–209482. https://doi.org/10.1109/ACCESS.2020.3038006 (2020).
25. Li, Z., Peng, C., Tan, W. & Li, L. A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation. *Appl. Sci.* **10**(21), 7469. https://doi.org/10.3390/app10217469 (2020).
26. Wu, T. *et al.* Security improvement for OFDM-PON via DNA extension code and chaotic systems. *IEEE Access* **8**, 75119–75126. https://doi.org/10.1109/ACCESS.2020.2989172 (2020).
27. Akiwate, B. & Parthiban, L. Secure and efficient image cryptography technique using choas and DNA encoding methodology. *Turk. J. Comput. Math. Educ.* **12**(2), 2754–2764 (2021).
28. Zhu, S. & Zhu, C. Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. *Entropy.* **22**(7), 772. https://doi.org/10.3390/e22070772 (2020).
29. Zebari, D. A., Haron, H., Zeebaree, S. R. M. & Zeebaree, D. Q. Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. *Int. Conf. Adv. Sci. Eng. ICOASE.* **2018**, 312–317. https://doi.org/10.1109/ICOASE.2018.8548824 (2018).
30. Jithin, K. C. & Sankar, S. Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. *J. Inf. Secur. Appl.* **50**, 102428. https://doi.org/10.1016/j.jisa.2019.102428 (2020).
31. Tabassam, S., Hassan, O., Al-Qahtnae, E. & Al-Ahmary, N. Goal question metrics and its application to process management and improvement. *Int. J. Eng. Appl. IREA.* **7**(2), 52–58. https://doi.org/10.15866/irea.v7i2.17013 (2019).
32. Radhakrishnan, V., *et al.* Development of a novel security scheme using DNA biocryptography for smart meter data communication. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)* (IEEE, 2019).
33. Sukumaran, S. C. & Mohammed, M. DNA cryptography for secure data storage in cloud. *Int. J. Netw. Secur.* **20**(3), 447–454. https://doi.org/10.6633/IJNS.201805.20(3).06 (2018).
34. Tiwari, H. D. & Kim, J. H. Novel method for DNA-based elliptic curve cryptography for IoT devices. *ETRI J.* **40**(3), 396–409 (2018).
35. Murugan, A., Thilagavathy, R. Cloud storage security scheme using DNA computing with morse code and zigzag pattern. In *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* 2263–2268 (2017). https://doi.org/10.1109/ICPCSI.2017.8392120.
36. Akhavan, A., Samsudin, A. & Akhshani, A. Cryptanalysis of an image encryption algorithm based on DNA encoding. *Opt. Laser Technol.* **95**, 94–99. https://doi.org/10.1016/j.optlastec.2017.04.022 (2017).
37. Pandey, M. K. Implementation of DNA cryptosystem using hybrid approach. *Res. J. Comput. Inf. Technol. Sci.* **6**(3), 1–7 (2018).
38. Chai, X., Fu, X., Gan, Z., Lu, Y. & Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **155**, 44–62. https://doi.org/10.1016/j.sigpro.2018.09.029 (2019).
39. Biswas, M. R., Alam, K. M. R., Akber, A., Morimoto, Y. A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem. In *2017 4th International Conference on Networking, Systems and Security (NSysS)* 1–8 (2017). https://doi.org/10.1109/NSYSS2.2017.8267782.
40. Hong, E., Lee, S., Oh, M.-K. & Seo, S.-H. Two-factor device DNA-based fuzzy vault for industrial IoT device security. *IEEE Access* **9**, 99009–99023. https://doi.org/10.1109/ACCESS.2021.3095348 (2021).
41. Roy, M. *et al.* A dual layer image encryption using polymerase chain reaction amplification and DNA encryption. *Int. Conf. Opto-Electron. Appl. Opt. (Optronix)* **2019**, 1–4. https://doi.org/10.1109/OPTRONIX.2019.8862350 (2019).
42. Feng, W. & He, Y.-G. Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling. *IEEE Photon. J.* **10**(6), 2880590. https://doi.org/10.1109/JPHOT.2018.2880590 (2018).
43. Pujari, S. K., Bhattacharjee, G. & Bhoi, S. A hybridized model for image encryption through genetic algorithm and DNA sequence. *Proc. Comput. Sci.* **125**, 165–171. https://doi.org/10.1016/j.procs.2017.12.023 (2018).
44. Namasudra, S. Fast and secure data accessing by using DNA computing for the cloud environment. In *IEEE Transactions on Services Computing*. https://doi.org/10.1109/TSC.2020.3046471.
45. Sharma, D. Encoding scheme for data storage and retrieval on DNA computers. *IET Nanobiotechnol.* **14**(7), 635–641. https://doi.org/10.1049/iet-nbt.2020.0157 (2020).
46. Smet, M. D., Ramaekers, K., Verhoeven, E., Vermeulen, S. & Bekaert, B. Influence of ink and smoke ATM security systems on dactyloscopy and subsequent DNA analysis after detonation. *Forensic Sci. Int. Genet.* **54**, 102540. https://doi.org/10.1016/j.fsigen.2021.102540 (2021).
47. Fernandes, M., Decouchant, J., Völp, M., Couto, F. M. & Esteves-Verissimo, P. DNA-SeAl: Sensitivity levels to optimize the performance of privacy-preserving DNA alignment. *IEEE J. Biomed. Health Inform.* **24**(3), 907–915. https://doi.org/10.1109/JBHI.2019.2914952 (2020).
48. Bansal, M., Gupta, S., Mathur, S. Comparison of ECC and RSA algorithm with DNA encoding for IoT security. In *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 1340–1343 (2021). https://doi.org/10.1109/ICICT50816.2021.9358591.
49. Sadkhan, S. B. Information security based on DNA—Importance and future trends. *Int. Conf. Commun. Inf. Technol. ICICT.* **2021**, 310–314. https://doi.org/10.1109/ICICT52195.2021.9568408 (2021).
50. Elmanfaloty, R. A., Alnajim, A. M. & Abou-Bakr, E. A finite precision implementation of an image encryption scheme based on DNA encoding and binarized chaotic cores. *IEEE Access* **9**, 136905–136916. https://doi.org/10.1109/ACCESS.2021.3118050 (2021).
51. Rajab, A. *et al.* Cryptography based techniques of encryption for security of data in cloud computing paradigm. *Int. J. Eng. Trends Technol.* **69**(10), 1–6 (2021).
52. Iqbal, N. *et al.* On the image encryption algorithm based on the chaotic system, DNA encoding, and castle. *IEEE Access* **9**, 118253–118270. https://doi.org/10.1109/ACCESS.2021.3106028 (2021).
53. Alawida, M. *et al.* A novel hash function based on a chaotic sponge and DNA sequence. *IEEE Access* **9**, 17882–17897. https://doi.org/10.1109/ACCESS.2021.3049881 (2021).
54. Kumar, B. M., Sri, B. R. S., Katamaraju, G. M. S. A., Rani, P., Harinadh, N., Saibabu, C. File encryption and decryption using DNA technology. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, 382–385 (2020). https://doi.org/10.1109/ICIMIA48430.2020.9074970.
55. Xiao, Y. *et al.* A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON. *IEEE Photon. J.* **12**(3), 1–15. https://doi.org/10.1109/JPHOT.2020.2987317 (2020).
56. Nayak, L., Jayalakshmi, V. A study of securing healthcare big data using DNA encoding based ECC. In *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 348–352 (2021). https://doi.org/10.1109/ICICT50816.2021.9358546.
57. Radhakrishnan, V., Durairaj, D., Balasubramanian, K., Kamatchi, K. Development of a novel security scheme using DNA biocryptography for smart meter data communication. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, 237–244 (2019). https://doi.org/10.1109/ICCCT2.2019.8824844.
58. Sha, Y., Cao, Y., Yan, H., Gao, X. & Mou, J. An image encryption scheme based on IAVL permutation scheme and DNA operations. *IEEE Access* **9**, 96321–96336. https://doi.org/10.1109/ACCESS.2021.3094563 (2021).
59. Arunpandian, S. & Dhenakaran, S. S. DNA based computing encryption scheme blending color and gray images. *Int. Conf. Commun. Signal Process. ICCSP.* **2020**, 0966–0970. https://doi.org/10.1109/ICCSP48568.2020.9182195 (2020).

60. Ye, R., Huang, H. An adaptive image encryption scheme using fractal dynamical system and DNA operations. In *2021 IEEE International Conference on Electronic Technology, Communication and Information (ICETCI)*, 284–289 (2021). https://doi.org/10.1109/ICETCI53161.2021.9563513.
61. Elmoselhy, A., El-Alfy, E.-S. M. On DNA cryptography for secure data storage and transfer. In *3rd Smart Cities Symposium (SCS 2020)*, 174–180 (2020). https://doi.org/10.1049/icp.2021.0900.
62. Wu, J., Zhang, S., Zhang, T. & Liu, Y. HD-code: End-to-end high density code for DNA storage. *IEEE Trans. NanoBiosci.* **20**(4), 455–463. https://doi.org/10.1109/TNB.2021.3102122 (2021).
63. Hossain, S. N., Kabir, M. H., Pal, A. Alignment free sequence similarity estimation using local binary pattern on DNA trajectory images. In *2021 Joint 10th International Conference on Informatics, Electronics & Vision (ICIEV) and 2021 5th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, 1–7 (2021). https://doi.org/10.1109/ICIEVicIVPR52578.2021.9564141.
64. Al-Barhamtoshy, H. M., Younis, R. A. DNA sequence error corrections based on TensorFlow. In *2020 21st International Arab Conference on Information Technology (ACIT)*, 1–5 (2020). https://doi.org/10.1109/ACIT50332.2020.9300094.
65. Wu, R., Liu, W., Mao, Y. & Zheng, J. Z. J. 2D graphical representation of DNA sequences based on variant map. *IEEE Access* **8**, 173755–173765. https://doi.org/10.1109/ACCESS.2020.3025591 (2020).
66. Alnafisah, K. H. An algorithmic solution for storing big data on the DNA sequence. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 1–4 (2020). https://doi.org/10.1109/WF-IoT48130.2020.9221056.
67. Amirkhani, A., Kolahdoozi, M., Wang, C., Kurgan, L. A. Prediction of DNA-binding residues in local segments of protein sequences with fuzzy cognitive maps. In *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 17(4), 1372–1382 (2020). https://doi.org/10.1109/TCBB.2018.2890261.
68. Bhoi, G., Bhavsar, R., Prajapati, P., Shah, P. A review of recent trends on DNA based cryptography. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 815–822 (2020). https://doi.org/10.1109/ICISS49785.2020.9316013.
69. Zou, C., Wei, X., Zhang, Q., Zhou, C. & Zhou, S. Encryption algorithm based on DNA strand displacement and DNA sequence operation. *IEEE Trans. NanoBiosci.* **20**(2), 223–234. https://doi.org/10.1109/TNB.2021.3058399 (2021).
70. Shirley Pradeeksha, A., Sridevi Sathyapriya, S. Design and implementation of DNA based cryptographic algorithm. In *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 299–302 (2020). https://doi.org/10.1109/ICDCS48716.2020.243603.
71. Kumar, A. Framework for data security using DNA cryptography and HMAC technique in cloud computing. *Second Int. Conf. Electron. Sustain. Commun. Syst. ICESC.* **2021**, 898–903. https://doi.org/10.1109/ICESC51422.2021.9532950 (2021).
72. Bhaya, C., Obaidat, M. S., Pal, A. K., Islam, S. H. Encrypted medical image storage in DNA domain. In *ICC 2021—IEEE International Conference on Communications*, 1–7 (2021). https://doi.org/10.1109/ICC42927.2021.9500718.
73. Saeed, S. A., Mohamed, M. H., Farouk Mohamed, M. Secure storage of data on devices-android based. In *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 427–432 (2021). https://doi.org/10.1109/ICSECS52883.2021.00084.
74. Akumalla, H., Hegde, G. Deoxyribonucleic acid based Nonce-Misuse-resistant authenticated encryption algorithm. In *2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, 1–5 (2021). https://doi.org/10.1109/IEMENTech53263.2021.9614872.
75. Jan, S. U., Abbasi, I. A., Algarni, F., & Khan, A. S. A verifiably secure ECC based authentication scheme for securing IoD using FANET. IEEE Access. (2022).
76. Niu, Y., Zhao, K., Zhang, X., Cui, G. Review on DNA cryptography. In *Bio-inspired Computing: Theories and Applications. BIC-TA 2019. Communications in Computer and Information Science*, vol 1160 (eds Pan, L., Liang, J., Qu, B.) (Springer, 2020). https://doi.org/10.1007/978-981-15-3415-7_11.
77. Taluja, S., Bhupal, J., & Krishnan, S. R. A survey paper on DNA-based data storage. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. (2020). https://doi.org/10.1109/ic-etite47903.2020.62.
78. Hazra, A., Ghosh, S. & Jash, S. A review on DNA based cryptographic techniques. *Int. J. Netw. Secur.* **20**, 1093–1104. https://doi.org/10.6633/IJNS.201811_20(6).10 (2018).
79. . Iliyasu, M. A, Abisoye, O. A., Bashir, S. A., Ojeniyi, J. A. A review of DNA cryptograhic approaches. In *2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria*, 66–72 (2021). https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428855.
80. Singh, S. K., & Aggarwal, R. K. DNA-based data storage: Trends and challenges. In *2019 5th International Conference on Computing Sciences (ICCS)* 1–6. (IEEE, 2019).
81. Khan, M. A., Al-Qaness, M. A. & Alghamdi, M. A. Energy-efficient DNA-based encryption for secure communication. *IEEE Access* **8**, 174684–174696 (2020).
82. Kumar, S., Kaur, S., & Kumar, N. Energy-efficient DNA-based cryptography for secure communication in IoT networks. In *Proceedings of the International Conference on Inventive Systems and Control* 1–6. (IEEE, 2020).
83. Kim, S.-H., Lee, J.-H. & Kim, H.-J. DNA-based cryptography: An energy-efficient approach for secure communication in wireless sensor networks. *Sensors* **18**(11), 3727 (2018).
84. Kim, Y.-S., Lee, J.-H. & Kim, H.-J. Energy-efficient DNA-based cryptography for wireless sensor networks. *J. Sens.* **2017**(1), 1–10 (2017).
85. Blawat, M. & Ceze, L. DNA-based data storage: Progress and prospects. *Curr. Opin. Syst. Biol.* **27**, 1–8 (2021).
86. Bornholt, J. *et al.* A DNA-based archival storage system with error correction. *ACM Trans. Comput. Syst. TOCS* **37**(1), 1–28 (2019).
87. Organick, L. *et al.* Scaling molecular storage systems with reliable and efficient error-corrected DNA synthesis. *Sci. Adv.* **6**, eaba2987 (2020).
88. Zhang, Y. *et al.* An integrated chip for scalable gene synthesis and precision assembly of complex DNA constructs. *Sci. Adv.* **6**, eaaz2631 (2020).
89. Chen, X., Liang, X. & Zhang, Y. DNA-based data storage: A review of recent progress. *J. Mater. Chem. C* **9**(16), 5353–5366 (2021).
90. SeragEldin, S. M., El-Latif, A. A. A., Chelloug, S. A., Ahmad, M., Eldeeb, A. H., Diab, T. O., & Zaky, H. N. Design and analysis of new version of cryptographic hash function based on improved chaotic maps with induced DNA sequences. *IEEE Access*. (2023).

Acknowledgements

The authors acknowledge Prince Sultan University and EIAS Lab for their valuable support. Additionally, they thank Prince Sultan University for covering the Article Processing Charges (APC) of this publication. This study also receives funding from Prince Sattam bin Abdulaziz University, project number (PSAU/2024/R/1445).

Author contributions

S.A.: Being a first author of the paper, I have explored the potential of DNA encoding schemes as the future of cyber security and generate knowledge on their advantages, challenges, and future research directions. Moreover, I wrote the first draft of the paper as well. S.U.K.: Analysis and curation of the data done by S.U.K. The corresponding author and analyze the overall structure of the paper. A.S.K.: Work on DNA encoding-based

schemes, obtained using the Goal Question Metric and Query-based approaches. M.A.: Performed proof reading and analytical review of the paper. S.S.: Performed recent trends and advancements of each methodology and all the methodologies proposed in the selected research articles are analyzed in terms of their strengths and limitations. M.E.: In the writing of the manuscript; or in the decision to publish the results. Moreover, assist in shortcomings of the proposed methods, highlighted various research challenges and provided the future scope for the research. N.A.: Performed analytical review and survey of DNA schemes and future work.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.U.K.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.