www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

SECURING CLOUD COMPUTING WITH DNA CRYPTOGRAPHY

[1] Mrs. B. Himabindu, [2] P. Neha Reddy, [3] M. Rithika, [4] M. Siddartha Reddy, [5] M. Sathvik Reddy
[1] Assistant Professor, [2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology, Sheriguda, Ibrahimpatnam

ABSTRACT

Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services and etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services provider's servers. To address this issue, there have been several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.

Cloud computing is the type of technology preferred to maintain computing power, computer resources, and majorly used to handle the cloud storage process. Also, it helps to manage the data security process during different applications. The data encryption, data classification, and feature extraction approaches are majorly considered for increasing the data security process. The main aim of the work is to review the DNA based cloud computing process for improving data security. The main purpose of this work is to review the current research article focus on the data security and computing process. Further, taxonomy is introduced that helps in the evaluation and analysis process. The secondary research approach is used during review work. Further, the deep learning with sequencing and modification process is reviewed in the work to manage the security and sequence analysis process. In addition, the block-chain-based random technique is reviewed to manage data detection and probability rate. The data optimization and data indexing process with block-chain is preferred to enhance data security and handle the feasibility, accuracy, and transfer time. Moreover, the OPNET model, Dynamic and static model approach, and data access algorithms are used together for maintaining the data mining security process. The IoT network topology and attributes based encryption process are reviewed in developed methods for maintaining data optimization and data security process.

I. INTRODUCTION

Cloud computing has recently reached popularity and developed into a major trend in IT. We perform such a systematic review of cloud computing and explain the technical challenges facing in this paper. In Public cloud the "Pay per use" model is used. In private cloud, the computing service is distributed for a single society. In Hybrid cloud, the computing services is consumed both the private cloud service and public cloud service. Cloud computing has three types of services. Software as a Service (SaaS), in which customer prepared one service and run on a single cloud, then multiple consumer can access this service as per on demand. Platform as a Service (PaaS), in which, it provides the platform to create application and maintains the application. Infrastructure as a Service (IaaS), as per term suggest to provides the data storage, Network capacity, rent storage, Data centers etc. It is also known as Hardware as a Service (HaaS) .

Contextual social networks (CSNs) have gained prominence in recent years as specialized platforms connecting individuals based on shared interests, activities, or contexts. Unlike traditional social networks, which cater to a wide range of interactions, CSNs provide niche communities where users can engage in meaningful conversations and share content relevant to their specific interests. As CSNs continue to grow in

popularity, it becomes increasingly crucial to prioritize the safeguarding of user information and privacy within these platforms. This comprehensive guide will explore the key strategies and considerations for safeguarding user information in contextual social networks.

The rise of contextual social networks has provided users with specialized spaces to connect andinteract with others who share similar passions, hobbies, or professional interests. These platforms offer a personalized and tailored user experience, enhancing engagement and fosteringmeaningful interactions. Nevertheless, in the pursuit of creating a personalized experience, CSNscollect, process, and store vast amounts of user data.

Protecting user information within CSNs is of paramount importance due to several reasons. Firstly, it upholds user trust and confidence, crucial for the success and sustainability of any socialnetwork. Users are more likely to actively participate and share content when they feel their personal information is handled securely. Secondly, privacy breaches can have severe consequences, including identity theft, financial fraud, or emotional distress, potentially tarnishing the reputation of the CSN and resulting in legal and regulatory challenges.

Safeguarding user information in contextual social networks is not only a legal requirement but also an ethical imperative. By prioritizing user privacy and implementing robust security measures, CSNs can foster a safe and trusted environment, encouraging users to engage activelyand authentically within their chosen communities. In the subsequent sections of this guide, we will delve deeper into each of these strategies, providing actionable insights and best practices toensure the protection of user information in CSN.

II. LITERATURE SURVEY

TITLE: Use of Digital Signature with DiffieHellman Key Exchange andAES Encryption Algorithm to Enhance Data Security in Cloud Computing

AUTHOR: PrashantRewagad, YogitaPawar.

ABSTRACT:

Cloud computing is the relevant technology for this decade. It allows users to store huge amount of data in cloud storage and use as and when required, from anywhere in the world, through any kind of terminal equipment. Since cloud computing relies on internet, cloud data will be forced to contend with security issues like privacy, data security, confidentiality, and authentication. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. This paper, introduces use of hybrid cryptographic algorithm blended with digital signature and Diffie Hellman key exchange.. The hybrid algorithm is designed using the combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of hybrid algorithm makes it tough for hackers to crack the security and integrity of the system, thereby protecting data stored in cloud.

TITLE: Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing.

AUTHORS: Uma Somani, Kanika Lakhani, ManishaMundra

ABSTRACT:

The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing.Close computing is the Concept Implemented to decipher the Daily computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud computing is the

Cloud security and the appropriate Implementation of Cloud over the Network. . In this Research Paper, we have tried to assess Cloud Storage

Methodology and Data Security in cloud by the Implementation of Implementation of digital signature with RSA algorithm.

TITLE: Efficient robust private set intersection

AUTHORS: D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung

ABSTRACT:

Computing Set Intersection privately and efficiently between two mutually mistrusting parties is an important basic procedure in the area of private data mining. Assuring robustness, namely, coping with potentially arbitrarily misbehaving (i.e., malicious) parties, while retaining protocolefficiency (rather than employing costly generic techniques) is an open problem. In this work thefirst solution to this problem is presented

TITLE: Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing.

AUTHORS: Mehdi Hojabri& Mona Heidari

ABSTRACT:

The Cloud Computing is the next generation platform that provides dynamic resources pools, virtualization, and high availableness. Today, with the assistance of those computing, we are able to utilize ascendable, distributed computing environments among the boundary of the web, It provides several edges in terms of low value and accessibility of information, conjointly offers associate degree innovative business model for organizations to adopt It's services while not forthright investment. Except for these potential gains achieved from the cloud computing, there are plenty of security problems and challenges related to it and conjointly knowledge privacy protection and knowledge retrieval management is one in all the foremost difficult analysis add cloud computing.

TITLE:High Confidential Data storage using DNA structure for cloud environment

AUTHORS:R. Pragaladan; S. Sathappan

ABSTRACT:

Cloud Computing is a modern paradigm that can facilitate organizations to share several transaction services in a more secure way. The cloud system is infected with a lot of security issues and threats over transactional process which could outlaw the entire system.Cryptogra

system.Cryptographic techniques usingDNA structure are being utilized on a large scale for transmitting transactional data secretly, with DNA as an informational and computational carrier.To design a technique on transaction database systems, Watson-crick Hoogsteen base Confidential Data Transaction (WHO-CDT) mechanism is used in cloud infrastructure. WHO-CDT mechanism employs transactional information storage, in a more ultra-compact form using the DNA confidentiality structure form. The DNA confidentiality structure converts the user provided transactional data into the binary storage data. The binary data storage of information used in WHO-CDT is next encoded using the thick oligonucleotide sequences. This sequence of encoded data improves the confidentiality level on the OLTP system and business analytics. In the DNA structure, WHO-CDT follows one-time component pad encode method for different types of transactional data. Finally, WHO-CDT follows a series of user transaction with high confidentiality using the Polymerase Chain Action procedure. The series of DNA based security level maintenance to the cloud infrastructure attain the best solution with limited cost factor. Experimental studies show that the DNA-based Information Storage algorithms achieve good performance in terms of data confidentiality, execution time and communication overhead for encoding and decoding.To supply security a range of cryptography algorithms and mechanisms are used. Several researchers opt for the simplest they found and use it numerous combinations to supply security to the information in cloud. In this paper, we've got planned to form use of Digital signature and Kerberos with Advanced Encryption Standard cryptography (AES) algorithm program to guard Authentication, Confidentiality, and Integrity of information hold on in cloud.

TITLE: Enhancing security in cloud computing using Bi-Directional DNAEncryption Algorithm.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

AUTHORS: Ashish Prajapati, Amit Rathod.

ABSTRACT:

Cloud computing is the latest technology in the field of distributed computing. It provides various online and on-demand services for data storage, network services, platform services, etc. Many organizations are unenthusiastic to use cloud services due to data security issues as the data resides on the cloud services providers' servers. To address this issue, there havebeen several approaches applied by various researchers worldwide to strengthen security of the stored data on cloud computing. The Bi-directional DNA Encryption Algorithm (BDEA) is one such data security techniques. However, the existing technique focuses only on the ASCII character set, ignoring the non-English user of the cloud computing. Thus, this proposed work focuses on enhancing the BDEA to use with the Unicode characters.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

The most recent innovation in distributed computing is cloud computing. It offers data storage, network services, platform services, and other services online and on demand. Because the data is stored on the servers of the cloud services provider, many businesses are hesitant to use these services.Before cloud computing, companies had to store all their data and software on their own hard drives and servers. The bigger the company, the more storage they needed. This way of treating data is not scalable at speed.However, cloud technology adoption rate is low because of security, compatibility, loss of control, security, data protection, performance and uptime, to the risk of vendor lock-in Cloud computing services.

DISADVANTAGES OF EXISTING SYSTEM

1) The current method doesn't take into account cloud computing users who don't speak English because it only looks at the ASCII character set.
2) Data loss or theft
3) Data leakage
4) Account or service hacking
5) Insecure interfaces and APIs
6) Denial of service attacks
7) Technology vulnerabilities, especially in shared environments.

PROPOSED SYSTEM

Previous section describes the study about the cloud computing, basics of cloud computing and security problems occurs in cloud. Here in this paper, the Bi-serial DNA encryption algorithm is performing, that providing the two level of security.Proof of concept: George Favaloro poses with a 1996 Compaq business plan. The document is the earlies known use of the term "Cloud Computing".

Describe our proposed system model for resources allocation and scheduling. Resources and users in the proposed system are located at different locations. Users can access a particular service in an uninterrupted manner from different locations and share the valuable resources by pay per service.Since the resources are located at different locations , a meta scheduler is also included which will coordinate the scheduling of various resources among users.

ADVANTAGES OF PROPOSED SYSTEM

1. One such method is the Bi-directional DNA Encryption Algorithm (BDEA) we are using to provide more security.
2. Faster time to market
3. Scalability and flexibility
4. Cost savings
5. Better collaboration
6. Advanced security
7. Data loss prevention
8. Less control over underlying cloud infrastructure.

SYSTEM ARCHITECTURE

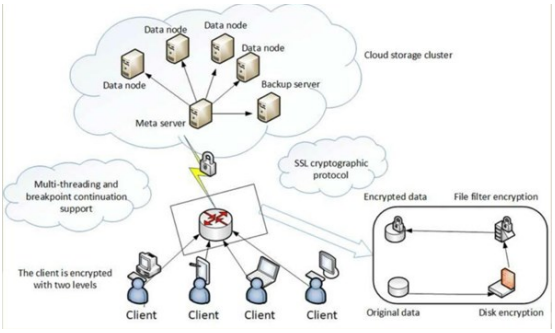

Fig: System Architecture

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

IV. IMPLEMENTAIONS

MODULES

- Sender
- Receiver
- Admin
- Cloud

MODULE DESCRIPTION ADMIN

Sender:

Here sender is a module, sender should register to the application then only he can able to login into the application. After successful registration he must authorized by admin thenonly he can able to login into his account after login he can perform some operations such as can view his profile,

Here the sender can send the message in the form of DNA Encode

Step1: select receiver and write message
Step2: convert original message to ascii code
Step3: convert ascii to hexadecimal
Step4: convert hexadecimal to binary
Step5: convert binary to DNA encode

Then send the message to receiver and can view all his messages and logout

Receiver:

Here receiver is a module, receiver should register to the application then only he can able to login into the application. After successful registration he must authorized by admin then only he can able to login into his account after login he can perform some operations such as can view his profile,

Here the receiver can decode the encoded DNA

Step1: verify decode key Step2: convert DNA to binary
Step3: convert binary to hexadecimal
Step4: convert hexadecimal to Ascii
Step5: convert ascii to original

Then read the message and logout

Admin:

Here admin is a module can able to login directly with the application, after successful login he can perform some operations such as view all senders and authorized them, view all receivers and authorize them and logout.

Cloud:

Here cloud is a module should login directly with the application after successful login he can perform some operations such as view original to ascii, view ascii to hexadecimal, view hexadecimal to binary, view binary to DNA and logout.

V. SCREENSHOTS

FIG-1 Home Page:This is home page for website.

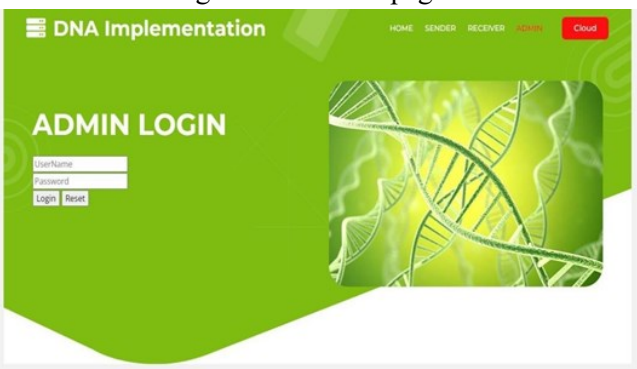

FIG-2 Admin Login:This is Admin Login page for website.

FIG-3 Admin Home Page:This is admin home page for website

Index in Cosmos
JUNE 2025, Volume 15, ISSUE 2
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

FIG-4 Sender registration

FIG-5 Sender Login:This is senders login for websites.

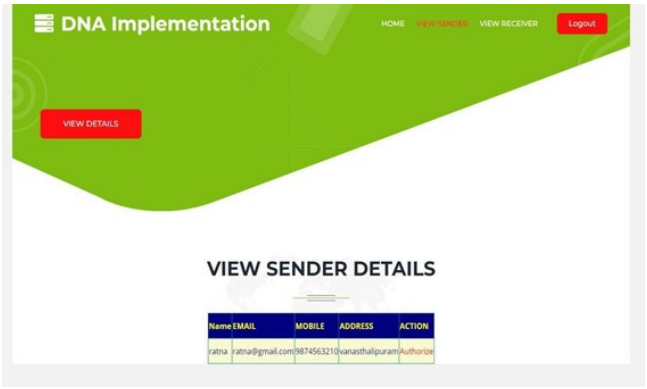

FIG-6 Sender Details:The admin can authorized or acceptance the sender request

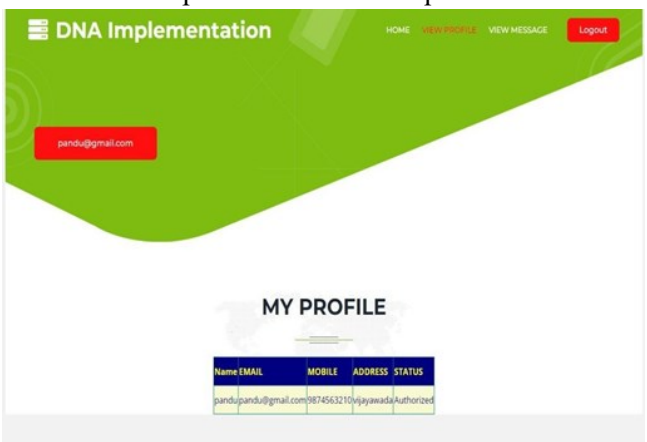

FIG-7 view the admin authorised request

FIG-8 Receiver registration : this is newly can be register

FIG-9 This is receiver login for websites

FIG-10 Receiver Details:The admin can authorized or acceptance the receiver request

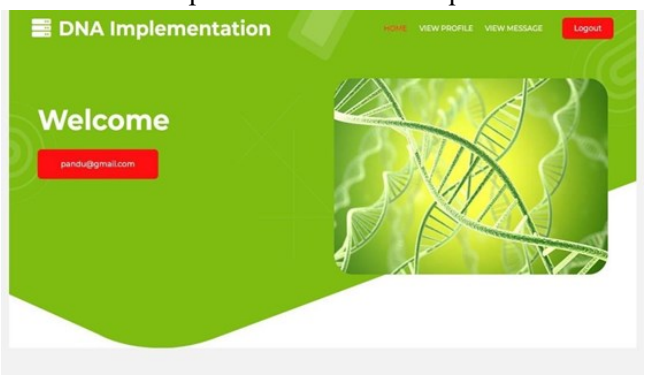

FIG-11 Receiver Home PageThis is receiver home page for website

Index in Cosmos
JUNE 2025, Volume 15, ISSUE 2
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

FIG-12 DNA Implementation Implementation of DNA

FIG-13 Cloud Login This is cloud login for website

FIG-14 This is cloud home page for website

FIG-15 Cloud Home Page converting to ASCII

FIG-16 Converting the ASCII to Hexadecimal

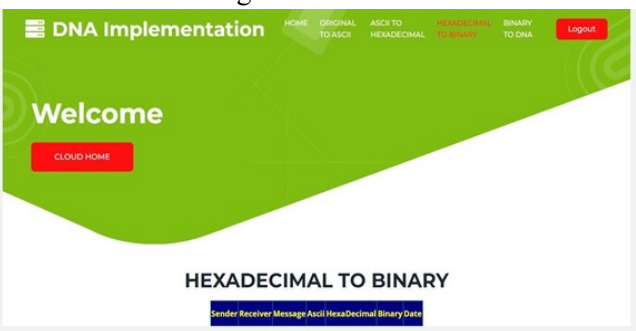

FIG-17 Converting the Hexadecimal to Binary

FIG-18 Converting the Binary to DNA

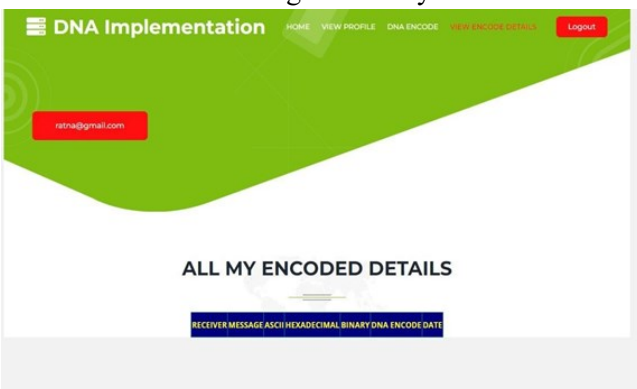

FIG-19 All encoding details are visible

Index in Cosmos
JUNE 2025, Volume 15, ISSUE 2
UGC Approved Journal

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

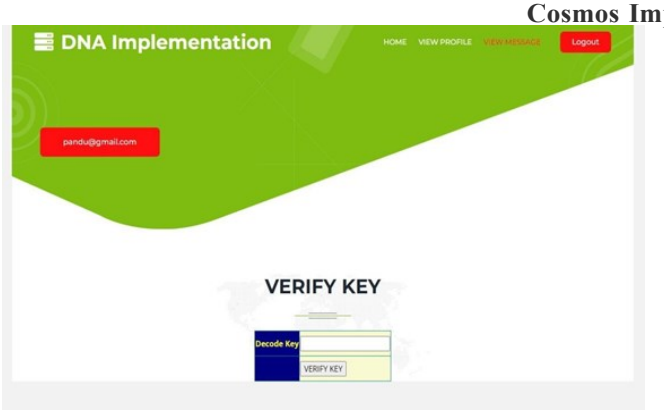

FIG-20 Verification of decoding details from senders

VI. CONCLUSION

CONCLUSION

Data security is the main challenge for cloud usability. Various algorithms like RSA, Diffie-Hellman, DNA encryption etc. are available to provide data security for the data stored on cloud. Digital signatures, Extensible Authentication Protocols are used for authentications. Using BDEA algorithm, we achieve 2-layer security for ASCII character sets. The proposed system focuses on extending the BDEA algorithm to be used with Unicode character set. This can help reach to the wider community of the cloud users. The future work will focus on the possible attacks and crypt analysis of the cipher text and measure its strength.

FUTURE SCOPE

1. Continued progress in DNA synthesis techniques will enable the generation of custom DNA sequences tailored for specific encryption purposes. This could lead to more efficient and secure DNA-based crypto graphic algorithms.
2. As DNA-based security matures, efforts will focus on seamlessly integrating it into existing cloud computing infrastructure. Scalability challenges related to data storage, retrieval, and processing will be addressed to accommodate large-scale adoption.
3. Research into DNA encryption methods resilient to quantum computing attacks will gain prominence. Developing algorithms that leverage the unique properties of DNA to withstand quantum threats will be a crucial area of exploration.
4. Collaboration between biotechnology, computer science, and cybersecurity disciplines will accelerate advancements in DNA-based security. Multidisciplinary research efforts will drive innovation and overcome technical hurdles.

REFERENCES

1. T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang and M. Xie, "Edge- based differential privacy computing for sensor–cloud systems", Journal of Parallel and Distributed Computing, vol. 136, pp. 75-85, Feb. 2020.
   Show in Context Google Scholar
2. .H. Taleb, K. Khawam, S. Lahoud, M. E. Helou and S. Martin, "A fully distributed approach for joint user association and RRH clustering in cloud radio access networks", Computer Networks, vol. 182, pp. 107445, Dec. 2020.
   Show in Context CrossRef Google Scholar
3. A. Dwivedi, S. Dhar, G. Srivastava and R. Singh, "Cryptanalysis of Round-Reduced Fantomas Robin and iSCREAM", Cryptography, vol. 3, no. 1, pp. 4, Jan. 2019.
   Show in Context CrossRef Google Scholar
4. A. D. Dwivedi, P. Morawiecki and G. Srivastava, "Differential Cryptanalysis of Round-Reduced SPECK Suitable for Internet of Things Devices", IEEE Access, vol. 7, pp. 16476-16486, 2019.
   Show in Context View Article Google Scholar
5. A. Asghari M. K. Sohrabi and F. Yaghmaee, "A cloud resource management framework for multiple online scientific workflows using cooperative reinforcement learning agents", Computer Networks, vol. 179, pp. 107340, Oct. 2020.
   Show in Context CrossRef Google Scholar
6. S. Namasudra, S. Sharma, G. C. Deka and P. Lorenz, "DNA computing and table based data accessing in the cloud environment", Journal of Network and Computer Applications, vol. 172, pp. 102835, Dec. 2020.
   Show in Context Google Scholar

7. S. Meng, Z. Gao, Q. Li, H. Wang, H.-N. Dai and L. Qi, "Security- Driven hybrid collaborative recommendation method for cloud-based iot services", Computers & Security, vol. 97, pp. 101950, Oct. 2020.
Show in Context CrossRef Google Scholar
8. M. Tahir, M. Hayat, I. Ullah and K. T. Chong, "A deep learning-based computational approach for discrimination of DNA N6- methyladenosine sites by fusing heterogeneous features", Chemometrics and Intelligent Laboratory Systems, vol. 206,pp. 104151, Nov. 2020.
Show in Context CrossRef
9. J. Al-Muhtadi, K. Saleem, S. Al-Rabiaah, M. Imran, A. Gawanmeh and J. J. P. C. Rodrigues, "A lightweight cyber security framework with context-awareness for pervasive computing environments", Sustainable Cities and Society, vol. 66, pp. 102610, Mar. 2021.
Show in Context CrossRef Google Scholar
10. I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities", Sustainable Cities and Society, vol. 56, pp. 102080, May 2020.
Show in Context CrossRef Google Scholar
11. X. Chi, C. Yan, H. Wang, W. Rafique and L. Qi, "Amplified locality-sensitive hashing-based recommender systems with privacy protection", Concurrency and Computation: Practice and Experience, Feb. 2020.
Show in Context Google Scholar
12. H. Lv, "iDNA-MS: An Integrated Computational Tool for Detecting DNA Modification Sites in Multiple Genomes", iScience, vol. 23, no. 4, pp. 100991, Apr. 2020.
Show in Context CrossRef Google Scholar
13. Q. Tang, "DNA4mC-LIP: a linear integration method to identify N4-methylcytosine site in multiple species", Bioinformatics, vol. 36, no. 11, pp. 3327-3335, Feb. 2020.
Show in Context CrossRef Google Scholar
14. H. Geng, Z. Yin, C. Zhou and C. Guo, "Construction of a simple and intelligent DNA-based computing system for multiplexing logic operations", ActaBiomaterialia, vol. 118, pp. 44-53, Dec. 2020.
Show in Context CrossRef Google Scholar
15. M. Imran, M. H. Durad, F. A. Khan and A. Derhab, "Toward an optimal solution against Denial of Service attacks in Software Defined Networks", Future Generation Computer Systems, vol. 92, pp. 444- 453, Mar. 2019.
Show in Context CrossRef Google Scholar.