International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 443-451 www.ijaem.net ISSN: 2395-5252

Security Enhancing Techniques for Data in IoT Cloud – Analysis

Mr. Sunil Raj Y, Mrs. Helen Parimala, Mr. Lucas L

Assistant Professor, Dept. of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli – 2
Research Scholar, Dept. of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli – 2
Assistant Professor, Dept. of Mathematics, St. Xaviers Catholic College of Engineering, Chunkankadai, Nagercoil – 3.

Submitted: 01-10-2021 Revised: 10-10-2021 Accepted: 12-10-2021

ABSTRACT: Internet of Things integrated with Cloud makes revolution in every field, starting with business, home, and medicine. IoT is playing a major role by connecting living and non-living via Internet forming a network. Cloud residing at the virtual corner and serving IoT via Internet. If Internet is detached both the technologies may not be named so. Here data from IoT devices were processed and may be preserved on Cloud. Providing numerus benefits and spanning their service they have few issues to be fixed. Dealing with the security issues present, IoT and Cloud would be more trusted and could replace the present workforce. While providing benefits this may help business improve by limiting the time and economy. Therefore, it is clear that security issues if fixed would enhance the growth of these technologies. Such an improvement would help the business and the society grow to a greater extend. The paper presents the existing security mechanism in a multidimensional perspective. The detailed study is conducted on the IoT security schemes and Cloud based security techniques present. Here cloud have to be taken a little more care as it is going to handle the data largely. Therefore, different storage-based schemes, encryption schemes and audit-based schemes where analyzed. Finally, a clear picture on the pits and holes in the existing IoT Cloud based security schemes have been presented. This will help researchers improve the security of data in IoT Cloud.

KEYWORDS: IoT, ECC DNA, Cloud Computing, TPA, Security

I. INTRODUCTION

Internet of Things (IoT) allows the devices connected and controlled over the Internet. This allows the devices to communicate between them for solving a problem in real-life. As objects are coming out with intelligent sensors, and a number of connectivity protocols available help connecting things over the internet easily. As the networked IoT devices are of low capability the connecting protocols allowing the communication includes CoAP, MQTT, AMQP, and XMPP [1, 2, 3].

Data generated by this IoT network, will be sent to the internet as it takes up another form HTTP. Now the gateway being the central part of making the communication successful over the internet. This does translate the request from the IoT's into HTTP. This will be understood by the remote server, and the data thus collected and translated by the gateway would reach the Cloud for processing, analysis or storage.

Cloud Computing (CC) provides distinct services in a distributed fashion despite of the geographical locations. It is great that it could lent hardware/software on a metered basis. Major transactions here will be using the protocols including HTTP, POP, SMTP, FTP and so on, based on the purpose. Most of these services will have direct link with the IoT's, where they will send request on their own (CoAP/ MQTT) language and Cloud would respond with its own (HTTP) language. In this scenario at any point of time eavesdroppers or malicious users may enter the cycle leading to security issues [4].

As it is lending every IT infrastructure as service, business/ firms, are safe from investing huge amount while saving the space and time. Providing a lot of advantages, the problem to the growth of Cloud is its security threats.

The security issues that arise as CC leads to lack of manual control and implements virtualization. This may read to the integrity, consistency and other privacy issues. A number of research's going on in the field of Cloud and IoT are actually indenting to enhance the security of these technologies. Looking at the cloud at any point of application, the major issue to be fixed would be the storage issue. Cloud Storage (CS) is holding the private data on the Internet, and it is nearer to any user on the Cloud. Therefore, proper security mechanism is to be devised to enhance the authentication, encryption and monitory schemes to prove the proof of ownership such as Third-Party Audit (TPA) should be employed [4, 5].

Authentication can be done at two levels, device and user level. Also, it is not better to relay only on authentication. Enforcing the monitory mechanism to users and devices will enhance the security. Furthermore, the encryption schemes can be enhanced, as the recent Hybrid encryption schemes perform more better in both IoT and Cloud. The researchers have found that DNA coding-based encryption is performing better with ECC. This actually strengthens the security as the cycle of substitution is increased and ECC does the rest.

As data from IoT network being stored on Cloud and used for analytics or other purposes. Being present various security mechanisms providing security in the multidimensional aspects. The paper is intended to have a detailed review on the certain security mechanisms employed in IoT Cloud as mentioned.

The paper is organized as follows: Section (ii) presents the detailed review of the literature, Section (iii) present the detailed analysis on the existing mechanisms, Section (iv), concludes the work with a brief summary to enhance the security in IoT Cloud integrated platform.

II. REVIEW OF LITERATURE

IoT a global network with devices of multiple capability to be connected together, uses interfaces, and are integrated forming a network. Devices such as sensors or actuators connected together forming a network could be known as IoT network where communication, and information processing technologies are involved [6, 7]. Being used in various applications such as health, production, and surveillance, as the data generated is more sensitive. The anomaly in the data generated may lead to serious risk. In order to handle the data without being replaced or manipulated it have to be protected. The review here exhibits the recent security techniques that exists to protect the IoT network.

2.1 IoT Security

After the study on the security concerns in IoT Cloud [8] have proposed a novel method to enhance security of data in IoT Cloud. Authors have used Huffman algorithm for generating keys along DNA coding for the security of the data. The proposal involves two level of encoding the data. Here the plain text is encoded by the proposed DNA algorithm and then by Huffman scheme which is symmetric in nature.

[2] Have proposed a method to enhance the security in IoT integrated Cloud platform using DNA and Huffman based hybrid scheme. DNA coding scheme have an advantage of authentication, storage, digital signatures and so on in a secure manner. Authors have used variable size key. As it was intended by the authors the symmetric crypto system is used as the calculation involves low memory while performing faster. The asymmetric RSA is utilized to encode the symmetric key.

To secure the IoT [9] proposes a cryptographic technique based on stream cipher. The data between IoT's were encrypted with One Time Pad (OTP) along with DNA codes. Furthermore, the key generation was using a linear feedback shift register (LFSR). The data from publisher is encrypted and the receiver decrypt the data back.

[10] have proposed a methodology for securing the data with digital signatures and DNA cryptography. The digital signature is a public-key cryptographic technique which adopts the scheme of both public and private keys. This public-key cryptographic algorithm is implemented by the DNA cryptography in the form of DNA sequencing. This DNA sequencing can store the data and is transferred in more secured way. The data from the IoT sensors is collected through the machine learning algorithms and is secured by this digital signature algorithm by DNA Cryptography and is stored and sent in more secured way.

Authors in [11] have proposed a DNA based method realized on IoT's. The analysis on the proposed scheme was done and it proves that DNA mapped ECC provide better security. The system was implemented and the energy consumption was found that the energy consumption was as that of existing systems without DNA coding.

In [12] authors have presented DNA and ECC based hybrid scheme. After the DNA sequence selection, an algorithm for sorting used. After sorting the data is replaced with DNA codes. Now the data is converted into binary after which they are encrypted using ECC. The performance analysis is conducted evaluating the energy and time taken. Authors have proved that DNA combined with ECC provide strong security.

To provide to IoT environment another approach by [13], have used DNA encoded ECC to reduce processing time. The technique was also intended for reducing the memory size in IoT devices. These two levels of hybridization add security to IoT Cloud.

2.2 Security in Cloud

The data generated by the IoT may travel inside the network communicating with other devices. The data then may have to reach a point where it will be stored for future processing. Here comes the Cloud which will hold data or services for a long time. Virtualization being the backbone it can be seen as a virtual hard disk where the generations may be forgetting the use of magnetic disks for transferring the data. It can also be assumed that the recent IT infrastructures such as computing devices may be using cloud for processing and storage. In such a technology, security must be enhanced. As CC is already in use the future AI based generations may require data to be safer from various attacks. The remarkable problems comprise Data Integrity (DI) [14]. Here in the study, the analysis is made on the existing techniques to protect the data from various attacks.

[15] Twin MDS code is robust against passive eavesdropper and data repair process. After the analysis the authors derive that using regenerating code-based scheme performs more better than MSR/ MBR.

In [16] authors have proposed an architecture for Object Storage (OSt) system. The OSt as it is on the Cloud could handle static data which is also unstructured. This architecture could also replace the archived storage which is a more recent scheme. Providing such an architecture the expectation of the authors is to enhance the scalability, flexibility and security.

In [17] authors proposes a pipelined Cloud-of-Clouds (CoC) storage approach, which speed up the dispersal algorithms, calculation operations executed with transmission operations in parallel. The author’s intention is to propose a pipeline-based system to speed up the operation on cloud. Here the dispersal algorithms in the CoC storage paradigm after the analysis have been found to perform better enhancing the speed.

In [18] authors have introduced, private Cloud infrastructure-based design, for providing security in access and sharing of files and easy maintenance. It adds time efficient storage and sharing of files while nod disturbing easiness and security. For better functionality compression methods can be introduced. Design best suits in situations like fairly unused storage centres over which a cloud is built.

For making up a secure and reliable system [19], proposes a twin code framework which is most suitable for distributed storage, by which it may efficiently handle data reconstruction and efficient node repair.

To secure the CS [20], introduces biometric based framework. Techniques such as chaotic maps, key generation and reed-solomon decoding are used in various levels of security aspects.

2.3 DNA Based Hybrid Approach

DNA based encryption is becoming popular for the recent IoT Cloud transactions. Here the data will be converted into a genomic sequence which will be a DNA of the IoT Cloud data. Though it requires subsequent substitutions as caesar ciphers, they are reducing the computational complexity would keep the data more secure. Hence mixing it with the classical cryptographic scheme such as symmetric or asymmetric would provide strong security [21, 22].

In [23] authors have reviewed security algorithms such as DNA, ECC and RSA algorithms in hybrid form. DNA with ECC makes difference in IoT framework as it reduces time and space. This also ensures the security as the length of the key is more modest. The framework proposed by the authors is employed with double layered security. The first layer is DNA and second layer is ECC. Authors after the study have revealed that such algorithms are more efficient with low capable IoT devices.

Authers on their work [14] have devised a data encryption scheme using bi-serial DNA. The scheme converts the data into hex codes and then into binaries. Data is then split in two parts by the authors. From thus separated keys one of them is used as key and other as actual data for transfer. XOR operation included along this scheme by the authors have increased the compression rate. The performance analysis indicates that the proposal increases the security, with the computational complexity as for amplification two prime numbers where used.

In [24] authors have used DNA along with Binary (OTP) to enhance the security of data. The random nucleotides are made to form a sequence of DNA, generating a key. The length depends on the data size. A binary sequence is used for OTP where the length is twice that of DNA key. Now the process of encoding is done which actually puts at the risk of finding the length of the key, only after this the actual data could be decrypted.

[25] One of the most emerging techniques in the world of cryptography is DNA cryptography which works on the concepts of DNA computing. Multiple DNA algorithms that have been studied and researched are Symmetric and Asymmetric Key crypto System using DNA, DNA Steganography Systems, Triple stage DNA Cryptography [30]. So, a combination of BREA and DNA sequence is used to make the encryption more secure.

For enhancing the security [26] authors have used AES and RSA with DNA algorithm. After the three level of encryption a message digest is generated with SHA256. As per the proposal digest is employed in confirming the DI.

Combining both cryptography and steganography [27] have proposed a hybrid scheme where SHA512, ECC, DNA and CM-CSA were used. Intended to hide the data behind a video, authors have initially let the data to undergo IHE compression. Followed by this process the DNA coding and then passed on through SHA512 and ECC. Thus, multilevel encrypted input now put behind in pixel points which is behind the frames. The CM-CSA does the steganographic process there by enhancing the security of the Cloud data.

In [28] suggesting a double level of encryption authors have enhanced the security of the data. Here authors have used two keys for encoding the data. The first key is generated using ECC, and Gaussian kernel (GKF). The other key being generated based on random injective mapping. As per the authors intention the encrypted data arbitrarily hidden in behind the second DNA series based on GKF.

Authors to enhance the security in [29] have proposed an ECC based technique for hiding the data in DNA. This technique provides solution for secure communication between the nodes. Authors have implemented the scheme as two parts, where the first is encrypting the data with play fairs. And the second, is hiding the encrypted data behind DNA in a random location using ECC.

Therefore, the DNA based security schemes could serve the IoT Cloud by providing strong security irrespective of the data being transferred.

2.4 TPA based Security Approach

TPA being a more predominant scheme where the users or data blocks may be continuously monitored. This can be seen of as a separate component independent of any DU or DO or CSP's. The study reveals the major TPA based schemes proposed to monitor the DI.

In [11] authors have proposed a Trusted TPA (TTPA) based framework to enhance security in Cloud. TTPA increases the security that is gained by using DNA cryptography and Digital Signature. Cloud User and CSP gain confidence that their data is safe with the help of TTPA. Data confidentiality is ensured by DNA Cryptography, DI by Digital Signature and TTPA ensures data authenticity.

[30] have suggested an auditing technique using TPA for verifying the integrity of data. The proposal makes use of AES for verification of data. Authors have used SHA2 for deriving metadata that is meant for verification process. Also, it is found that message digest (MD) is employed for integrity checking.

[31] have introduced TTP who checks for the integrity of cloud data and its validity. Public audits provide the third party intending to ensure the stored data is correct against external attacks. Authors have introduced three entities for ensuring the data security. The entities included Cloud Users (CU), Cloud Service Providers (CSP)/Admin, and TTPA. After the analysis of the scheme authors have inferred that the work performs better solving the problems of security.

In [32] authors have presented their work on managing the control by registering. The proposal comprises of a translucent customer, a verification server, and a translucent server. Combined verification done between authentication servers and the TPA, is arranged by TC and TS. Authentication server verifies the authorized individual and check for the access permissions.

[33] have proposed an architecture with two parts depicting the services provided. Th proposal comprises of a dashboard describing an overview of the risk status. It also describes the actions that could protect the data to be executed. It also has a back-end that automates risk-mitigating safeguarding the client from the risks.

[34] have proposed an architecture containing two-phase, the setup phase, and an audit phase. Here authors have used a TTP server to verify DI. This reduces the computation to a greater extent. It also reduces the communication complexity enhancing the DI.

[35] have proposed a framework to minimize the physical size of the organization called Distributed TPA on Cloud (DTPAC). Here the author has proposed a module called CSP Helper, which can be deployed in any level of service models. As per the proposal TPA residing inside could backup critical data from CSP Helper.

The data about the provenance of audit will be totally monitored by the TPA.

[36] have proposed a model which includes, CSP, DU, and TPA. TPA here is a Semi-TTP verify the DI on request. CSP is assumed to be an untrusted entity. Author describes that CSP may delete or update the data on the storage. TPA could run verification algorithm periodically to monitor this process. The model has been proposed to withstand the attacks such as Forge Attack or Replace Attack that may be launched by CSP.

III. ANALYSIS AND DISCUSSION

Security being the major concern, based on the review conducted the analysis is being conducted. The analysis is recorded on the major aspects such as, IoT security, Cloud Security, TPA and DNA based schemes.

3.1 Security in IoT – Analysis

IoT Cloud dominating every field such as science and engineering. It is very rare to find a field that not use IoT or Cloud. In this scenario it is the duty of these technologies to protect the sensitive of their clients/users. Though artificial intelligence is employed most cases the security enhancement schemes is to be enhanced. As the study conducted the analysis on the recent schemes proposed to enhance the security of IoT is reflected here below.

Tabel 3.1. Analysis on Security in IoT

	Proposal	Components	Issues
[2]	Hybrid Scheme	DNA, RSA & Hufman	Transport
[8]	Hybrid Algorithm	DNA, Huffman	Security
[9]	Hybrid Algorithm	DNA & OTP	Security
[10]	Hybrid Scheme	DNA & Digital Signatures	Security
[12]	Hybrid Algorithm	DNA & ECC	Security
[13]	Hybrid Algorithm	DNA & ECC	Security

As IoT is highly exposed to attacks, a large number of works have been proposed to enhance the security. The Table 3.1, show few recent proposals, of which all includes DNA based hybrid algorithm. It is revealed that DNA is more efficient and would be predominantly used in IoT Cloud security.

3.2 Security in Cloud – Analysis

Protecting the Cloud becomes another major task next to IoT. Here as data on the Cloud Storage is at rest may be exposed to various attacks. This may have to be seen of as in two major aspects. First is by the physical disasters. In order to overcome such risks a number of security proposals exists. Scattering of data to n different nodes may help safeguarding a portion of data with which the others can be recalculated.

Tabel 3.2 Analysis on Security in Cloud

	Proposal	Problem	Approach
[11]	Algorithm	Security	DNA & TPA
[15]	Twin MDS	Passive Eavesdropping, Node Recovery	MDS / MSR
[16]	Architecture	Unstructured digital static data	Object Storage
[17]	Architecture	Dispersal algorithms	Calculation & Transmission
[18]	Architecture	Security in file	Compression

		access and sharing	
[19]	Framework	Reconstruction & Node Failure	Twin Code
[20]	Framework	Security	Read-solomon, chaotic maps

Encountering the first way of lost data from cloud, Table 3.2, shows the existing mechanisms that safeguard the data on Cloud. Among which it is understood that splitting the data and storing it in multiple nodes will serve more. The second way of threat that is encountered with the data on Cloud is by anonymous users, malicious CU's or malicious CSP's This is being handled with the help of various security algorithms and TPA based techniques, are discussed in the following sections.

3.3. DNA based Security – Analysis

DNA Cryptography is performing better while converting the data using genetic code. The length of cipher text higher than plaintext will be better in this case. Methodology adopted includes converting plaintext into ASCII then converting into binary. Binary is then encoded in to sequences and one of the sequences is selected as a key and grouped in blocks of 8 characters. With respect to positions of characters in key, table is created and with the help of table and key, data gets converted [21, 22].

Tabel 3.3 Analysis on DNA based Hybrid Schemes

	Proposal	Problem	Methodology
[23]	Framework	Security	ECC, RSA, DNA
[14]	Algorithm	Security	Bi-Serial DNA, XOR
[24]	Algorithm	Security	DNA, OTP
[25]	Algorithm	Security	Symmetric, Asymmetric DNA
[26]	Algorithm	Integrity	AES, RSA, DNA, SHA256
[30]	Algorithm	Security	BREA, DNA
[27]	Algorithm	Security	DNA, SHA512-ECC
[28]	Algorithm	Security	DNA, ECC, DES, GKF
[29]	Algorithm	Security	DNA, ECC

Hybrid encryption schemes being the security experts, table 3.3, shows the way it is mixed with other algorithms for enhancing the security in IoT Cloud. The attacks that are raised by the anonymous or malicious users can be dealt with these schemes. As it could provide better security to the data avoiding eavesdropping as the encoding followed may not be able to recalculated. In order to provide better security to the data preserving it from malicious CSP's or CU's, another technique may also be employed as in the following section.

3. 4. Analysis on TPA

Auditing solves the problem of ensuring the DI. This will be done with the help of a common log that will be maintained to record the access. This cannot be neglected as the data can be used for analysis of the malicious activities that takes place on the Cloud.

Tabel 3.4. Analysis on TPA based Security

	Proposal	Problem	Methodology
[30]	Auditing Technique	Integrity	AES, SHA-2, Message Digest

[11]	Trusted Third Party Auditor	Integrity, confidentiality, Authenticity	DNA, Digital Signature
[31]	TTPA Framework	Integrity	Validation, Audit
[32]	TPA Framework	Integrity	Authentication & Verification
[33]	Architecture	Security	Auto Risk Monitor & Mitigation
[34]	Architecture	Integrity	Setup, Audit
[35]	DTPAC	Integrity	CSP Helper Audit
[36]	TPA	Forge Attack or Replace Attack	Audit using semi TTPA

As depicted in Table 3.4, it is clear that auditing can also help the Cloud keep track of freshens of the data. As the sole control is on the Cloud a monitory mechanism is always essential. Therefore, as it could identify the attacks such as forge and replace it is very much essential.

IV. CONCLUSION

The analysis made on the study reflects various security techniques used in IoT Cloud. Here security to handle data at rest is handled with a separate mechanism and the security of data in transit have been handled using different techniques. Among which Hybrid algorithms have been used in both the places IoT and Cloud. Along with the predominant security schemes such as ECC various other algorithms were used. Among which [2, 9, 10, 11, 12, 13] DNA based encoding is becoming popular with the classical schemes such as ECC.

In emergency-based applications such as medical and military as other such applications, the data integrity has to be preserved largely. The study reveals in-order to preserve the integrity a part in security authentication scheme is employed. Also, authors have introduced [30, 11, 31, 32, 34, 35] TTP based techniques where data at rest is monitored for their integrity. DNA cryptography can be used in CS, signatures and authentication. While authors have also used DNA based scheme for enhancing the integrity of data [26, 2]. Therefore, it is clear that using schemes such as TTP and Hybrid encryption could enhance the security in IoT Cloud. In future the work will be extended towards proposing a security enhanced IoT Cloud architecture.

REFERENCES

[1]. Y. Wu, Q. Z. Sheng, S. Zeadally, “RFID: Opportunities and challenges,” in Next-Generation Wireless Technologies, N. Chilamkurti, Ed. New York, NY, USA: Springer, 2013, pp. 105–129.

[2]. Vidhya Vijayan, Eldo P Elias, “Hybrid Method for Securing Data in IoT Cloud”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019.

[3]. Sowmya Nagasimha Swamy, Dipti Jadhav, Nikita Kulkarni, “Security Threats in the Application layer in IOT Applications”, International conference on I-SMAC, 2017.

[4]. Joel J. P. C., Dante B. R., Heres A., Murilo H., Rafael M., Jalal Al-Muhtadi, Victor Hugo C., “Enabling Technologies for the Internet of Health Things”, IEEE, 2018, ISSN: 2169-3536.

[5]. Samhita Kanthavar, “Design of an Architecture for Cloud Storage to Provide Infrastructure as a Service (IaaS)”, IEEE, 2017.

[6]. R. van Kranenburg, "The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID", Amsterdam, The Netherlands: Institute of Network Cultures, 2007.

[7]. L. Tan, N. Wang, “Future internet: The

internet of things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), Chengdu, China, 2010, pp. 376–380.

[8]. Harish Kumar N, Rajshekhar M Patil, Deepak G, Murthy B M, "A Novel Approach for securing data in IoTCloud Using DNA Cryptography and Huffman Coding Algorithm", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017.

[9]. Noor A. Hussein, Mohamed Ibrahim Shujaa, "DNA computing-based stream cipher for internet of things using MQTT protocol", International Journal of Electrical and Computer Engineering (IJECE), Vol. 10(1), February 2020, pp. 1035 – 1042.

[10]. Naga Saranya Cherukupalli, Sesha ShayeeMaruvada, "Securing Data in IoT Devices using DNA Cryptography", International Journal for Modern Trends in Science and Technology, 6(8S), 2020.

[11]. Nayna Agarwal, Anand Mahendran, Ramanathan Lakshmanan, "Trusted Third Party Auditing for Cloud Security Using Digital Signature and DNA Cryptography", IJSTR, Vol 8(12), 2019.

[12]. Harsh Durga Tiwari, Jae Hyung Kim, Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices, ETRI Journal, Vol. 40 (3), 2018. (http://wileyonlinelibrary.com/journal /etrij)

[13]. Barman, P., Saha, B. "DNA encoded elliptic curve cryptography system for IoT security". International Journal of Computational Intelligence & IoT. 2, 2019.

[14]. D. Prabhu, M. Adimoolam, "Bi-serial DNA Encryption Algorithm" [Online]. Available: https://pdfs. Semantic scholar. org/ 1754/ f0eb5 85 25005 98 a70af 4002 e186 cd2f 3c6 ce.pdf

[15]. Samundiswary.S, Nilma M Dongre, "Object, Storage Architecture in Cloud for Unstructured Data", International Conference on Inventive Systems and Control, IEEE, 2017.

[16]. Saswati, Anirban, "A Parallel Technique for Storage Defragmentation in Cloud", 2016 Second International Conference on Research on Computational Intelligence and Communication Networks, IEEE, 2016.

[17]. Jiajie, Jiazhen, Yangfan, Xin, "Cloud-of-clouds Storage Made Efficient: A Pipeline-based Approach", IEEE International Conference on Web Services, 2016, pp724–727.

[18]. Marina, Velkaska, Paunkoska, "Efficient distribution and improved security for reliable cloud storage system", IEEE EUROCON 2017–17th International Conference on Smart Technologies, 2017, pp727 – 732.

[19]. Nakouri, Hamdi, Kim, "A New Biometic Based Security Framework for Cloud Storage", 13th International Wireless Communication and Mobile Computing Conference, 2017, pp390 – 395.

[20]. Carvalho, Castro, Andrade, "Secure Cloud Storage Service for detection of security violations", 17th IEEE/ ACM International Symposium on cluster, cloud and grid computing, 2017, pp715 – 718.

[21]. Kang Ning, "A Pseudo DNA Cryptography Method", arXiv:0903.2693 [cs.CR], Cornell University Library, 2009.

[22]. Kritika Gupta, Shailendra Singh, "DNA Based Cryptographic Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3 (3), 2013.

[23]. Malti Bansal, Shubham Gupta, Siddhant Mathur, Comparison of ECC and RSA Algorithm with DNA Encoding for IoT Security, Proceedings of the Sixth International Conference on Inventive Computation Technologies [ICICT 2021], IEEE Xplore, 2021.

[24]. Shreyas Chavan, "DNA Cryptography Based on DNA Hybridization and One Time pad scheme", International Journal of Engineering Research & Technology, Vol. 2 (10), 2013.

[25]. Mansi Rathi, Shreyas Bhaskare, Tejas Kale, Niral Shah, Naveen Vaswani, "Data Security Using DNA Cryptograph", International Journal of Computer Science and Mobile Computing, Vol.5, 2016, pg. 123-129.

[26]. M. Kumar, "Implementation of DNA cryptosystem using Hybrid approach", Research Journal of Computer and Information Technology Services, Vol. 6(3), 2018.

[27]. Asha Jose, Kamalraj Subramaniam, "DNA based SHA512-ECC cryptography and CM-CSA based steganography for data security", Materials Today: Proceedings, Elsevier, 2020.

[28]. Eman I. Abd El-Latif & M. I. Moussa "Information hiding using artificial DNA sequences based on Gaussian kernel function" Journal of Information and Optimization Sciences, 2019, ISSN: 0252-

266.

[29]. Zena Ahmed, Saher Adil, Saif M. Kh. Al-Alak, ECC Based Blind Steganography-DNA for Hidden Information. Journal of Engineering and Applied Sciences, 14, 2019.

[30]. Soumya Shinde, Ramya V. Shinde, Priyanka Kamadhenu, “A Novel Data Auditing Approach to Achieve Data Privacy and Data Integrity in Cloud Computing”, International Conference on New Horizons in Science Engineering Technology (NHSET-2018), IJSRCSEIT, Vol. 4 (5), 2018.

[31]. Nayna Agarwal, Anand Mahendran, Ramanathan Lakshmanan, “Trusted Third Party Auditing For Cloud Security Using Digital Signature And DNA Cryptography”, IJSTR, Vol 8(12), 2019

[32]. Dinesh R , Ezra Vivin A, Dr. Srinivasan N, Albert Mayan J, “A Multi-server Data Security With Public Auditing in Cloud Computing”, International Conference on Frontiers in Materials and Smart System Technologies, IOP Publishing, 2019.

[33]. Ciarán Bryce, Security governance as a service on the cloud, Journal of Cloud Computing: Advances, Systems and Applications, Springer, 2019.

[34]. Mai Rady, Tamer Abdelkader, Rasha Ismail, “Integrity and Confidentiality in Cloud Outsourced Data”, Ain Shams Engineering Journal, Science Direct, 2019.

[35]. S. Mahdavi-hezavehi, Y. Alimardani, R. Rahmani, “An Efficient Framework for a Third Party Auditor in Cloud Computing Environments”, Computer Science Theory, Methods and Tools, The Computer Journal, 2019.

[36]. Imad El Ghoubach , Rachid Ben Abbou, Fatiha Mrabti, “A secure and efficient remote data auditing scheme for cloud storage”, Journal of King Saud University – Computer and Information Sciences, Elsevier, 2019.