Energetic Data Security Management Scheme using Hybrid Encryption Algorithm over Cloud Environment

Quazi Warisha Ahmed[1], Dr. Shruti Garg[2]

[1]Department of Computer Science and Engineering, Birla Institute of Technology Mesra, Ranchi, India, phdcs10060.17@bitmesra.ac.in
[2]Department of Computer Science and Engineering, Birla Institute of Technology Mesra, Ranchi, India, gshruti@bitmesra.ac.in

Article History:Received:11 november 2020; Accepted: 27 December 2020; Published online: 05 April 2021

ABSTRACT : Now-a-days all documents are in a digital format as well as everyone need to maintain their data in electronic mode with the help of cloud servers. A cloud server provides lots of facilities to users such as remote data maintenance, huge data handling and so on. But in the case of security many cloud servers are providing probabilistic results alone. So, that a new cloud server data maintenance scheme is required to provide a high-level data security to the cloud system in an efficient manner. This paper introduces a new crypto-approach called Novel Hybrid Encryption Mode (NHEM), in which this algorithm integrates several latest approaches of crypto logics into it and provides a top-end security level to the cloud data. This NHEM is derived from the base factors of two cryptographic algorithms called Advanced Encryption Standard with 512-bit size of key frequency with Message Digest (MD5) algorithm. By using the integration of these two powerful approaches, a novel approach called NHEM is designed and it provides a huge support to preserve security on cloud medium. The cloud data needs to be protected from unwanted threats and intruders by means of raising an interruption attacks on server. The proposed approach of Novel Hybrid Encryption Mode concentrates more on access control logics and the crypto norms with respect to privacy measures. In this paper, the proposed scheme assures the data is too robust and no one can attack the data without proper credentials as well as the outcome proofs are clearly given on the resulting unit of this paper. The Advanced Encryption Standard algorithm is a well-known and powerful crypto scheme and the MD5 algorithm is also considered to be the unique unidirectional algorithm to provide security level in energetic manner. These two algorithms are combined together with the bit frequency of 512 to achieve the highest accuracy levels in data security over cloud environment as well as the resulting portion clearly illustrates that with proper graphical outcome.

Keywords: Cloud Data Security, Novel Hybrid Encryption Mode, NHEM, Advanced Encryption Standard, AES, Message Digest, MD5

I. INTRODUCTION

in this modern world, each and every data needs to be maintained in a digital format to avoid human errors and faults occurred by manual processing. The data maintained into the records manner with paper and pen concept does not need any special concern, but the data maintained into the digital manner needs high attention against protection of the data. In such manner the data protection is a consideration on this paper; cloud data maintenance is the best option to users to preserve the data in remote server with proper security norms. In literature, several researchers analyze cloud-oriented processing with diverse set of records and cryptographic methods. However, all these approaches are strucked up with certain level of security issues, so that the customers required high level of security to the data preserved into the cloud server. This leads an innovation of several innovative crypto algorithms against remote server attacks such as Data Encryption Standard (DES), Rivest Shamir and Adleman (RSA) algorithms and so on. The present system of cloud servers mostly utilized the enhanced version of Data Encryption Standard algorithm called Advanced Encryption Standard (AES) algorithm, in which it comes up with several frequency variations such as 128 bits, 192 bits and 256 bits key combinations [1]. But in this proposed approach the latest version of Advanced Encryption Standard logic with 512 bits of key frequency variation is utilized to make a hybrid logic, in which it processes the plain data with 512-bit key variations and provides a robust cipher data to maintain into the server. This makes the cloud users to feel error free and maintain the data with high level of security to the cloud servers [1]. But the classical access control logics are utilized over this approach, so that the concern of privacy needs to be improved further with cipher standards [6][7].

*Corresponding author: Quazi Warisha Ahmed
Department of Computer Science and Engineering, Birla Institute of Technology Mesra, Ranchi, India, phdcs10060.17@bitmesra.ac.in

The crypto algorithms are usually considered to be the technique for makes the plain text to cipher text and that will be used for the storage or processing. Based on the respective algorithm authorization modes, the decryption process will happen accordingly. The following figure, Fig-1 illustrates the logic of crypto process in detail with sample plain and cipher text outcomes [11].

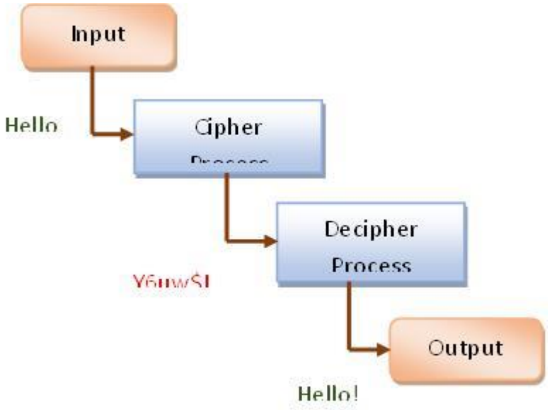

Fig.1 Proposed System Architecture

The key structure for those algorithms is Variate with respect to public and private. The concept of public key based encryption logics is usually called as asymmetric key encryption, in which it uses the pair of keys for encryption and decryption. The logic of public key is literally known to everyone but the private key is considered as the secret key, which is only known to the receiver end alone. The concept of private key encryption process is called as symmetric key encryption logic, in which it uses the single key for processing as well as this kind of private key based encryption process is considered to be the fastest encryption process, but the main issue to deal with the private key is to maintain the secrecy of the key, because the key can easily be stolen by anyone [8][9][10].

In this paper, a new hybrid data encryption scheme is followed to provide the top end security features to the cloud data with the help of two powerful crypto algorithms such as Advanced Encryption Standard (AES) and Message Digest (MD5) algorithm. These two algorithms are combinely worked together to provide a high end security to the data preserved into the cloud, these algorithms are integrated together and in which it is called as Novel Hybrid Encryption Mode (NHEM). The concept of NHEM is simple, to provide the top end security to the cloud data with high privacy norms by means of enabling the access control features in the proposed approach. The general crypto norms enabled cloud data maintenance scheme allows the user to preserve the records into the server with authentication schemes on several variations. In which the authentication schemes allows the user to login into the system with two-step verifications and other biometric norms. However, the data credentials maintained into the server end with any one of the service provider, so that the privacy is again a questionnaire over this approach [2][3]. This proposed approach is entirely different from the regular authentication norms and the standards of providing privacy are high with powerful and integrated crypto logics. The proposed approach of Novel Hybrid Encryption Mode provides MD5 authentication norms with user attribute enabled data key generation. This process accumulates the user attributes to generate the dynamic key for authentication credentials and that cannot be guess or break by anyone. These logics are clearly illustrated over the methodologies section of this paper as well as the data maintenance against vulnerabilities are the other concern to deal with, in which the AES algorithm is associated with the proposed logic to take care of such issues in order to attain the high end security with 512 bits frequency enabled key factors.

The rest of this paper describe regarding Related Study over section 2, further section of Section 3 illustrates the proposed system methodologies in detail with proper algorithm flow and the Section 4 illustrates the Result and Discussion portion of the paper and the final section, Section 5 illustrates the concept of Conclusion and Future Scope of the proposed paper. These all will be explained in detail over the further section summaries.

II. Related Study

In the year of 2020, the authors "AbhishekKumar'et al., [4]", proposed a related to computational estimation and data maintenance over cloud computing environments. In this paper [4], the authors illustrated such as cloud environments and the associated data maintenance schemes are developed in huge manner now-a-days. The advantageous identified from the cloud platforms are easily adaptable, compatible as well as easy accessing [4]. The main purpose of cloud environments are data communications and many different applications adapt this cloud for such purpose alone. The demanding need of cloud environment requires some sort of security features to provide privacy to the users. In this paper [4] the result section clearly proves the nature of cloud computing maintenance as well as the security achieved in that via the proposed experimental cloud maintenance logic. The main themes concentrated on this paper [4] are as follows: user security establishments, data communication facilitation and data maintenance scheme. This system [4] likewise covers the processing angle of the cloud and their relevance as well as the scientific view for the examination and investigation. It investigates the more extensive view and the region of relevance in various areas without any hurdles as well as safe information sharing procedures.

In the year of 2020, the authors "RajeevKumar'et al., [5]", proposed a related to the analysis of cloud computing environment security features, integrity maintenance and the adaptable nature. In this paper [5], the authors illustrated such as the cloud computing environments plays a vital role in many research areas and many corporate afford this cloud into their platform for easy data maintenance. The drastic development of cloud platforms requires high end safety measures with proper privacy preserving norms. In this paper [5] a detailed analysis of cloud oriented features and the related security metrics are analyzed in detail with the comparison of several literatures. Literally this paper [5] provides a detailed overview of the cloud environment with proper security metrics. The major features analyzed with this paper [5] are data maintenance with security, robust nature of data in the cloud server, data availability and privacy metrics. Cloud-Security issues in the new procedures of cloud privacy estimation are investigated in detailed manner as well as the difficulties in the cloud-privacy and security is investigated and conceivable future extent of the technique is examined. This paper [5] includes in dissecting the Quality-of-Service technique to research the points of interest and impediments in clear manner.

In the year of 2020, the authors "AdityaGarg'et al., [6]", proposed a related to cloud computing environment security metrics with respect to intrusion identification scheme by utilizing Honeypot-Network Platform. In this paper [6], the authors illustrated such as the drastic development of cloud environment and the related services requires more and more stability. As well as the increasing of number of users needs the powerful machines to overcome the faults occurred on cloud platform with rapid memory partitions. These issues cause the memory allocation problems and the reliability problems. Due to this kind of issues the cloud environment processing and performance is degraded suddenly without any indications, in which it indirectly leads to a permanent data loss. With this concern, a lots of intruders are trying to make the nodes presented into the network to weak state and retains the data literally without the knowledge of data owners. This kind of problems causes a severe affection to data maintained into the server. The demanding needs of cloud data maintenance require demanding security constraints to preserve the data from intruders and attackers. In this paper [6] a new methodology is introduced to overcome such kind of intruders from the cloud environment called Honeypot-Network Platform integration with cloud service nature. The process of this Honeypot based approach is activated while data sharing between the entities, but the third-party service providers cannot retain any specific benefits from such platform. This paper [6] clearly describes about the identification of intruders in cloud platform just as the utilization of Honeypot based network security features, along these lines proposing another method to do likewise.

III. PROPOSED SYSTEM METHODOLOGIES

In this paper, a new proposed methodology called Novel Hybrid Encryption Mode (NHEM) is introduced, in which it is derived from two powerful crypto algorithms called Advanced Encryption Standard (AES) and Message Digest (MD5) algorithm. The concept of Advanced Encryption Standard is standardized with several key metrics and associated features, but in this approach the key metric of 512 bits are considered to produce the high end security features to the NHEM. The proposed approach of AES-512 bits encryption logic is utilized for data encryption and decryption process and the MD5 logics are used for access control logics as well as the credential generation for data manipulations.

A. AES-512 bits – Data Substitution Phase

The data substitution phase of the Advanced Encryption Standard algorithm replaces the original characters with the proper substitutions as well as the block cipher processing utilize these kind of submission metrics while encryption phase [1]. The substitution phase of the proposed approach of AES 512 bit process in Novel Hybrid Encryption Mode process the information based on the following algorithm, Algorithm-1. In this algorithm, the different states of assigning the substitution characters to the actual plain text are defined in a clear manner with proper Pseudocode specifications. Simply, this algorithm provides the clear view of how the input is acquired from the user end, extracting the source content from the input based on number of rows and number of columns and the substitution assigning principles to the respective characters based on the defined substitution characters.

Algorithm: Substitution Phase

Input: *No. of rows and columns from the input plain data.*
Output: *Character Substitution Process result.*

1. Gather the input data from the user document.
2. Extract the content based on text features presented into it.
3. Split the word levels from 0 to n-1.
4. Create a integer variable called 'n' to store the words count.
5. Assign the words count to the variable for next processing.
6. Initiate the For loop from 0 to total number of rows in the given data.
7. Initiate the inner For loop from 0 to total number of columns in the given data.
8. Create an array object named 'st' with respect to available number of rows and columns.
9. Assign the Substitution variables to the created array based on the input data acquired over the loop.
10. Close the inner and outer For loops.
11. Return the resulting substitution array object for further processing.

Pseudocode:

```
Start;
Var RCnt← input.rows.count;
Var CCnt← input.cols.count;
for(i=0; i<=RCnt; i++)
{
   for(j=0; j<=CCnt; j++)
   {
      st(i)(j)←Subst(st(i)(j));
   }
}
return st;
End;
```

The following figure, Fig-2 illustrates the different levels of AES 512 bit crypto processing, in which the levels are categorized from level 0 to level 22. The levels are clearly processed with three different kinds of operations such as Row Shifting, Column Integration and Indexing. These features are clearly mentioned in the following figure.

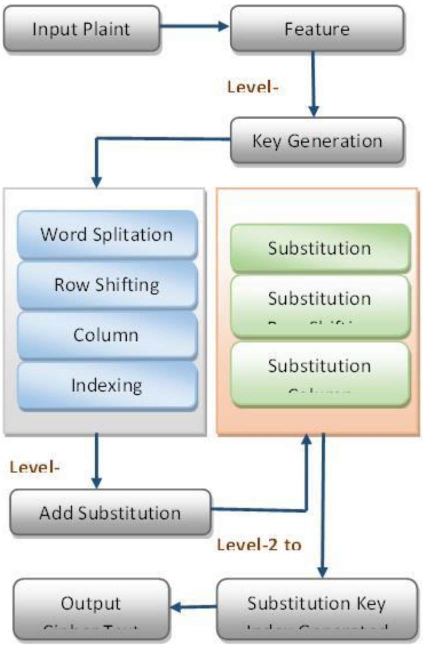

Fig.2 AES-512 bit Encryption Algorithm Working Model with Proposed NHEM

B. NHEM- Message Digest (MD5) Algorithm Integration

The MD5 is most important and well-known crypto algorithm used for unidirectional encryption process, in which the process of this MD5 crypto logic is acquiring the input text from the user and convert that to cipher text with data hashing principles. The data hashing principle generate the hashed content and that hashed detail will be stored into the server end for manipulation. The content is hashed based on the respective user identities, in which the key is generated instead of dynamic generation on other classical process of key generation, but in this approach the key generation is different. The user attributes such as name, contact details and the mail is considered for key generation of MD5 user credentials. Along with user attributes the dynamic random number is generated and merges it with the generated key to add the robust nature to the proposed algorithm, so that no one can interrupt or corrupt the data on the server end. The periodical back up process provides the system data to be safer and maintain the perfect level of integrity. The following equation is used to generate the user attribute based random key generation process with respect to the random class provided by the data processing tools.

$$\boldsymbol{R(mi, mx)} = \frac{\mathbf{Us^{attr}(1-n)+(Mi^{N}.Mx^{N})}}{\mathbf{{}_{1}^{n}X}} \quad \textbf{(1)}$$

Where $R(mi, mx)$ indicates the minimum and maximum value parameters of Random class R, $\mathrm{Us^{attr}}(1-\mathrm{n})$ indicates the user attributes from level 1 to n, $(\mathrm{Mi^N}.\,\mathrm{Mx^N})$ indicates the minimum numeric and maximum numeric level inputs and the ${}_{1}^{\mathrm{n}}\mathrm{X}$ indicates the overall user data from 1 to n. The following algorithm, Algorithm-2 illustrates the process of message digest algorithm implementations on this proposed approach MHEM.

Algorithm-2: Message Digest Process

Input: *User Identity Attributes (Name, E-Mail-ID and Contact Details).*
Output: *Manipulated Crypto Credentials for both Data Protection and Access Control.*

```
1. Obtain the user input from the client end web interface.
2. Check the input identities provided by the user are valid or not by send validation mails and OTP to the respective user.
Pseudocode:
   var val_str;
   Check the user name, contact details and e-mail-id portion of the identity attributes contains proper value or not. If the identities are proper and contains enough value ranges (word_length) then the approach allows the user to proceed further or else block the user.
   Ex.
   if(String[Is_Null_Or_Empty(User_Name && User_Contact && User_Mail)])
      {
         //Assign the missing attribute details to created String variable 'val_str'.
      val_str=missing_values;
      }
3. Initiate the connection bridge between client end and the server end by using internet services.
Pseudocode:
   Create a Connection object called 'Con'. (Ex. ServerConnection Con).
   Assign User identity attributes to variable called Obj. (Ex. Obj=User_Name + User_Contact + User_Mail)
   ServerCommand=new ServerCommand(Obj, DB_Con, User_Attributes)
If(Obj(1).Matched(DB[User_Attributes.Name])==true)
   {
      return Nm.true;
   }
ElseIf(Obj(2).Matched(DB[User_Attributes.Contact])==true)
   {
      return Cont.true;
   }
ElseIf(Obj(3).Matched(DB[User_Attributes.Mail])==true)
   {
      return Mail.true;
   }
```

```
Else
   {
      return Attribute.false;
   }
```

4. Once the return statement returns false attribute feature means, the user identity attribute is unique.
5. Create a new object for String Segregation. (Ex. String ObjStr).
6. Initialize the segregated content of the user attributes to the created string object.

Pseudocode:

```
   ObjStr=User_Name.Sub_String(0,4)+User_Contact.Sub_String(0,4)+User_Mail.Sub_String(0,4).
   return ObjStr;
```

7. User Identity attributes segregated and returned to further process of user attribute based key generation.
8. Apply the unidirectional data hashing logic to circulate the obtained ObjStr to hash values and generate the hashed key.
9. Acquire the created hashed key and stored into the cloud server based on the established connection 'Con' on step-3.
10. Return the hashed key for data processing and user access control requirements.

IV. RESULTS AND DISCUSSIONS

In this section, the experimental evaluation of the proposed approach Novel Hybrid Encryption Mode (NHEM) is discussed in clear manner with graphical proofs. The proposed approach of NHEM integrates the logic of AES 512 bits frequency processing logic to provide the high end data security and the Message Digest (MD5) algorithm to provide the user access control credential logics in an efficient manner. These two algorithm variants are properly worked together to provide the top security norms to the proposed approach with user attribute based key generation process, so that no one can guess or interrupt the keys at any case. The user attributes are integrated with random key generated dynamically on runtime, in which the dynamically generated credential is notified to the respective user via the input validated mail-id. The credential is not only enough for accessing the features of the proposed approach, while verifying the user identifies on authentication phase, system cross-verifies the credentials based on dynamic OTP generation process. Once the generated user credential and the dynamic high end password called OTP is correct, the respective user is allowed to proceed further or else the proposed approach blocks the user on that point. The following table, Table-1 illustrates the time estimations of different processing levels of the proposed approach NHEM.

Table-1 NHEM Time Estimation

Data (bits)	Key Generation (ms)	Crypto Process (ms)	Decryption Process (ms)
1000	50.26	39.52	56.33
1500	59.13	42.69	48.32
2000	63.56	50.06	56.32
2500	65.14	51.65	60.36
3000	66.92	53.29	60.96

The following figure, Fig-3 illustrates the graphical representation of the time estimations mentioned in the above table, Table-1 of the proposed approach Novel Hybrid Encryption Mode.

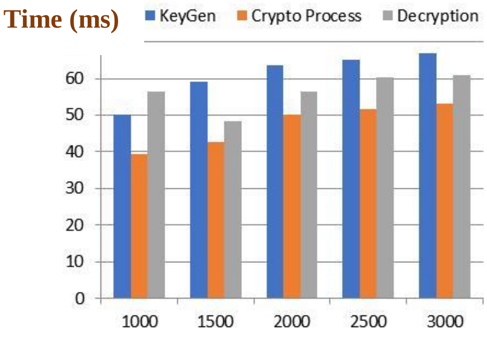

Fig.3 NHEM Time Estimations

The following figure, Fig-4 illustrates the graphical representation of the proposed approach NHEM accuracy levels over data collection range versus the relevant bit error ratio. This figure portrays the accuracy levels of the data collection with respect to error ratio, in which the x-axis shows the data collection range in bits and the corresponding bit error rate is shown in the y-axis. For better understanding of the BER, the accuracy range is constructed from the levels of 0 to 1 ranges.

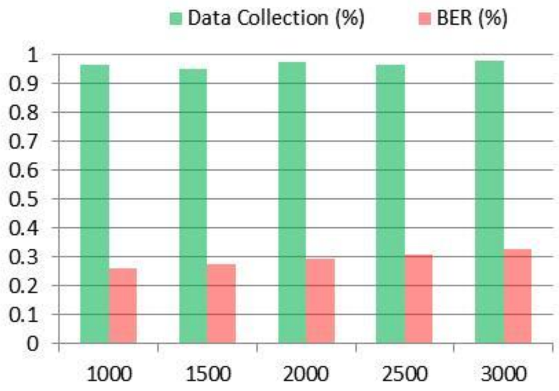

Fig.4 Accuracy Level vs. BER

The following figure, Fig-5 illustrates the graphical representation of the proposed approach NHEM encryption and decryption efficiency levels with respect to the AES-512 bit encryption standard of NHEM. The efficiency ranges are cross-verified with several bit frequency ranges mentioned in the literature [1].

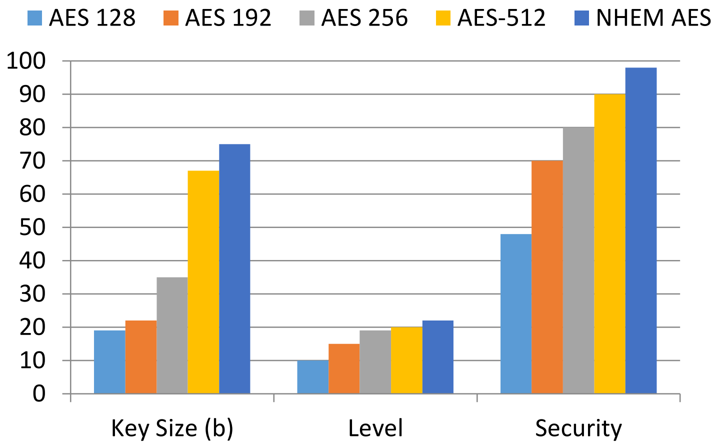

Fig.5 Performance Level Estimations of the Proposed Approach NHEM

V. Conclusion and Future Scope

In this paper, a new security logic called Novel Hybrid Encryption Mode (NHEM) is introduced to preserve the cloud data with proper credentials and privacy maintenance norms. This paper concentrates on data security, robust data maintenance, access control mechanism and the novel credential management schemes. The proposed approach of NHEM is a hybrid algorithm, in which it incorporates the two powerful algorithms called Advanced Encryption Standard (AES) and Message Digest (MD5) algorithm. The logics and individuality of the proposed approach of NHEM based AES and the MD5 is illustrated clearly on the algorithms 1 and 2 specified in methodologies section of the paper. The proposed approach of AES utilized 512 bits encryption logic to provide the high accuracy range in result and the figure, Fig-4 illustrate the same with the analysis of experimental results. The logic of NHEM attains highest accuracy in results and provides a top end security procedures to the cloud data as well as the data maintenance scheme in the proposed logic is simple as compared with the classical data maintenance schemes.

This proposed approach is extended further by means of crypto security features along with attack avoidance logic. This is a new logic introduced for avoiding the security threats caused by the intruders. This proposed approach NHEM clearly describes regarding the successful data maintenance but the appliance of this security threat elimination process improves the data protection level in rich manner.

REFERENCES

K. Anand, Dr. A. Chandra Sekar and Dr. G. Nagappan, "Enhanced AES Algorithm using 512 Bit Key Implementation", Asian Journal of Research in Social Sciences and Humanities, 2017.

Huang Shaohua and Xiao Nanfeng, "Abnormal Traffic Monitoring Methods Based on a Cloud Computing Platform", IEEE 5th International Conference on Cloud Computing and Big Data Analytics, 2020.

J. Divya and S. Shivagami, "A study of Secure cryptographic based Hardware security module in a cloud environment", Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020.

Satya Murthy Sasubilli, Ashutosh Kumar Dubey and Abhishek Kumar, "A computational and analytical approach for cloud computing security with user data management", International Conference on Advances in Computing and Communication Engineering, 2020.

Rajeev Kumar and M P S Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability", IEEE International Conference on Computing, Power and Communication Technologies, 2020.

Poorvika Singh Negi, Aditya Garg and Roshan Lal, "Intrusion Detection and Prevention using Honeypot Network for Cloud Security", International Conference on Cloud Computing, Data Science & Engineering, 2020.

Yi Sun, Qian Liu, Xingyuan Chen and Xuehui Du, "An Adaptive Authenticated Data Structure With Privacy-Preserving for Big Data Stream in Cloud", IEEE Transactions on Information Forensics and Security, 2020.

Fizza Shahid et al., "PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud", IEEE Access, 2020.

Roberta Terruggia and Fabrizio Garrone, "Secure IoT and Cloud Based Infrastructure for the Monitoring of Power Consumption and Asset Control", AEIT International Annual Conference, 2020.

Sarandis Mitropoulos and Alexandros Veletsos, "A Categorization of Cloud-Based Services and their Security Analysis in the Healthcare Sector", IEEE, SEEDA-CECNSM, 2020.

Quazi Warisha Ahmed and Dr. Shruti Garg, "A Cloud computing-based Advanced Encryption Standard", Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019).