Ann. For. Res. 65(1): 4574-4586, 2022
ISSN: 18448135, 20652445

ANNALS OF FOREST RESEARCH
https://www.e-afr.org/

ENHANCING THE NETWORK SECURITY DURING THE IMPLEMENTATION OF SMART AGRICULTURE USING NOVEL SECURITY MECHANISM

Dr. Shanta kumar Patil[1], Dr. Chatrapathy K[2], Satwik Teotia[3], Dr. Naveen Kumar B[4]

[1]Professor and HOD, Department of Computer Science and Engineering, Sai Vidya Institute of Technology, Bengaluru, India, shantakumar.p@gmail.com.

[2]Professor, School of Computing & Information Technology, Reva University, Bangalore, India, pathykc@gmail.com.

[3]Assistant Professor, Department of Computer Science, ABES Engineering College, Ghaziabad, Uttar Pradesh, India, satwik.teotia@abes.ac.in

[4]Associate Professor, Sahyadri College of Engineering & Management, Mangalore, Karnataka, India, navkan24@gmail.com.

Abstract: Internet of Things (IoT) has been explored in terms of its purpose, breadth, and actual use. As aresult of this effort, the whole network is now safer. Many studies have looked at the security of the Internet ofThings; however, the security measures used in those studies have had a negative impact on the networkperformance. That is why prior studies only looked at certain types of data. Previous research has beenhindered by obstacles such as high error rates, sluggish speeds, and a large proportion of packets lost. Theneed for approaches that protect both text and visual content while using minimal system resources cannot beoverstated. IoT solutions might tremendously benefit from this research. In today's Internet of Things (IoT)technologies, data compression and security are routinely necessary. Whenusingthishybridstrategy,transmission is more reliable and error-free. This sort of research might benefit IoT-based systems, such ashealthcare and the commercial sector. Research on IoT and network security via encryption is essential.Investigate the security implementation issues of the IoT network such as the speed, accuracy, and latency oftheInternetofThingsmoredeeply.Suchresearchshouldconcentrateonmergingcompressionandencryptionapproachestooffer high-performanceandtrustworthynetworksecurityforIoTsbysolvingsecurity problems in the IoT network. This new approach of network security should be safer and moreefficientthanthecurrentone. Data is protectedfromhackersbya uniquesecuritytechnique.

Keywords:Networksecurity,IoT,Encryption,Performance,Accuracy.

I. INTRODUCTION

For IoT security, research has focused on improving network security. The Internet ofThings(IoT)hasbeenexaminedforitsneed,breadth,andfunctioning.Thepresentresearch looked on the hazards of transmitting data through a network. Efforts are made tokeep data secure from hackers by considering the security technique used. In the proposedeffort,reducingthequantityofmaterialwouldimprovetheencryptionoperation'sperformance. A great deal of study has been done in this area; however, the processes usedin those studies have

had a negative impact on the network's performance. Thus, previousresearch only applied to certain types of data. Due to problems such as high error rates,slow speeds, and a large proportion of packets lost, earlier study has been hampered. Textand visual data must be protected while using as little system resources as possible, andresearch into such methods is urgently needed. This research might have a significantimpact on real-world solutions. Data compression and security are essential in today'sInternet of Things world. It is more reliable and error-free to use hybrid technology in thetransmission. This sort of research might be beneficial to IoT-based systems, such ashealthcare and business. Encryption-based research into IoT and network security shouldbetakeninto consideration.

1.1 Internet of Things

In the Internet of Things (IoT), there is no need for direct human-to-human or computer-to-computercommunication.Computers,mechanicalanddigitaltechnologies,items,animals, and even humans themselves are all examples of this technology. The Internet ofThings (IoT) encompasses anything from implanted heart monitors to farm animals withbiochip transponders to automobiles with low tyre pressure sensors and any other naturalor man-made object that has an IP address and can communicate data over a network. Abroad variety of industries are using it to enhance operational efficiency, get a betterknowledgeoftheircustomers, andincreasetheoverallvalue oftheirfirm.

Fig.1:Internetofthings applications

1.2 Issues in network security

Due to hacking and cracking methods, the security of their remnants must be improved [3,4].Securitymanagementandthedifficultiesfacedbydiverseindustriesaremajorconcerns in rising countries. Intruders' hacking and cracking activities are a security issue.Additionally,theneedforaccessibilityalwaysisamajorchallenge.Studentsmaynow access their essential information at any time and from any location using cloudstorage [5]. Remote schooling is expensive; therefore, researchers looked at methods toreducethecosts.Studentsandyoungpeopleinimpoverishednationsfaceseveralchallengeswhileatte

mptingtoaccesscloud-basedonlineeducation.However,RSA,DNA Cryptography, and other security methods [10, 11] have been used to secure thecloudsystem[8,9].However, there are still performance issues. Pre-existing studies that ensured safety showed a 7% to 20% reduction in overall performance. Cloud speed is affected by several factors, including the size of packets, the time required to encrypt data, the time required to filter data through firewalls, and the time required to detect malware. As a result, a new technique is needed that may bothimprovesecurityandspeed.

1.3 Role of compression in performance enhancement

To minimize the amount of network system content, a compression techniquehas been developed. However, despite the presence of several compression techniques, theproblem of data loss persists. It is required to use a replacement table where larger words are substituted with words with high frequency. Shorter words can be used in place of longer ones to minimize packet size. The packet's transmission time is halved as a result.Thelikelihoodofapacketbeinglostisreducedsincesmallerpacketsgo through the network more quickly. The cloud-based online learning system mightbenefitfromacompressiontechniquethatreducespackettransmission time.

1.4 Influence Factors

In a cloud environment, viruses and external assaults have resulted in Security Treats. As a result, instructional information may be hacked through a network. Hackers are solely liable for unauthorized access to data. The cracker, on the other hand, is responsible for decrypting the encrypted data. In order to keep data safe, encryption and firewalls are routinely used. However, there have been several assaults that might have an impact on security, such as communication attacks, physical attacks, device software attacks, and lifecycle attacks.

Fig.2: Securityor Influence Factors

Performance Factors

Adopting time-consuming encryption techniques that also have an influence on the system's performance is necessary to increase system security. The following factors have an impact on how well the cloud environment performs:

1. The type of communication media utilized, whether wired or wireless, affects the system's performance. Compared to wired systems, wireless solutions frequently operate less well. Furthermore, wired, and wireless systems each have their own classifications.
2. Bandwidth: The amount of data that may be transferred in a specific length of time is known as bandwidth. When there is more bandwidth available, more data may be sent in a shorter amount of time.
3. Protocol usage: A network's data transmission is governed by protocols, which are set forth in this paragraph. A connectionless protocol like the user datagram protocol is quicker than a transmission control system that needs acknowledgement.
4. Security measures, which take time to ensure that data being delivered is valid, may impair cloud network performance.
5. The distance between the transmitter and receiving nodes has an impact on performance. Performance slows and transmission time increases as distance increases. As a result, a shorter distance yields an improved performance.
6. A signal loses energy as it moves from one location to another. Attenuation depends on the transmission medium and distance. A signal regenerator is still required for attenuation-related issues.
7. A compression approach has been developed in order to reduce the amount of content used in the online learning system. However, the issue of data loss still exists despite the availability of numerous compression algorithms. It is required to use a replacement table where larger words are substituted with words with high frequency. Shorter words can be used in place of longer ones to minimize packet size. The packet's transmission time is halved as a result.

Forinstructors,staff,andstudents,theissuesofIoTcompliancehavealreadybeenexamined [1, 2, 3, 4]. Researchers have also looked on security and risk divides. Thetechnology's potential influence on IoT security is investigated. Education security is amajor issue in many developing economies. Hacking and cracking activities by intrudersraises a security risk. Additionally, the need for accessibility always is amajorchallenge. Now, students need to access information at any time and from any place viaIoTspace [5]. [5] Remote learning may be made more affordable by examining severaloptions for reducing costs. In a poor country, it is challenging to offer kids and youth withonline cloud-based education. However, various security techniques, such as RSA [8, 9], DNA Cryptography [7], and others, have been employed in the past to secure the IoT system. There is still the issue of performance, though. The entire performance has been decreased from 7% to 20% byexisting research that has offered security. The IoT's performance is affected by several variables, including packet size, encryption time, firewall filtering time, and virusdetection time. As a result, a new technique is needed that may both improve security andspeed.

Theobjectivesofresearchareasfollows:

1. IoT'ssignificanceinremotelearningandthelimitationsofcurrentresearcharediscussedinthisfirststep.
2. Focusingonthesecurityand performanceissuesinthecurrent IoTparadigm,as well.

3. Developingasecureandhigh-performancemodeltoaddresstheperformanceandsecuritychallengesthathave beenencounteredinpriorstudies.
4. Considertheaspectswhilesimulatingthecomparisonchart.

II. Literature Review

Distance learning has been the subject of a wide range of studies. The scalability andvariety of material in an IoT-based security system have been the subject of other studiesas well. In this part, we have discussed security research in an IoT ecosystem. In addition, aresearch paper that provides security for IoT applications and compresses material via theIoTisalsoincluded.ResearchonIoT-basedsecurity,applicationperformanceimprovement,and datacompressionisthefocus of thisarea.

In 2016, Dr. Pranav Patil and his colleagues explored e-learning for distance education.TheyuseCloudComputingaspartoftheirtraining.Writingthisresearchrequiredconsideration of a modern e-learning system. They came up with the idea of employingcloudcomputingintheonlineeducationsystemaftercompletingstudy.[1]Thedesignofacloud computingsystemhas been studied viatheinclusion ofe-learning.

According to AsgaraliBouyer and colleagues in 2014, online education necessitates theuse of cloud computing. The researchers' research has shown that cloud computing is a dynamically scalable technology. The possibility of offering services online exists. Virtual technologies are playing a bigger role in online education as a result of recent technological advancements. Many academics have found that online instruction is quiteeffective.Studieshaveemphasizedtheimportanceofonlineeducation'squalityandquantity expansions. Research is beneficial to both academic institutions and students oftechnical science and engineering. The research focused on an online education systemthat relies on cloud computing.

On the characteristics of cloud-based education systems, AgahTugrul et al., a team ofacademics, published their findings in 2016. Data used in education is increasing in bothvariety and relevance as a result of technical improvements throughout the research. In theliterature, web technologies and their contributions to a system of distance learning havebeenextensivelyresearched.Mobilesystems,whicharewidelyutilizedindistantteaching, were also considered. A lot more people now have access to the internetbecause of it. Thanks to web technology, people may now get information via the internetregardlessoftheirlocationoravailabletime.Thisresearchexaminedthepotentialeducational applications of cloud computing. It examines the advantages of the cloud. [3]Thisresearch employed a survey method.

Researchers headed by AnanthiClaral Mary explored cloud computing's potential benefitsas well as its drawbacks this year. Cloud computing has offered a lot of benefits to theacademic arena. There are disadvantages to storing and processing sensitive data on thecloud. This research has revealed vulnerabilities in cloud computing security as well as amethodto guardagainstassaults onthecloud. [4]

TheMeslhysystemenforcedcloudapplicationsecurityasof2013.Cloudserviceprovidersshouldutilize onedefaultgatewaytoprotectsensitivecustomerdataacrossmany public and private cloud services, according to this research. Without crashing cloudapps, this gateway platform encrypts critical data before it is sent to storage in the cloud.With the help of this research, a fast encryption technique with file integrity has beendeveloped. Additionally, it provides anti-malware, firewall, and tokenization capabilities.Nevertheless, the security model has lowered performance by 7% as a result of blockingandslowingnumerousapplicationthreadsdue tomalwaredetectionandthefirewall[5].

An investigation on the implementation of performance analysis of cloud-dependent webservices for virtual Learning Environment Systems was given by Osman, Saife in 2016.Research has shown that web services via cloud environments may be used in diversecontexts, enabling applications. Soap and REST might be used to build these services.Protocolsprovideawiderangeofusefulfunctions.Theovercloudwebservicesenvironment is being optimized by the findings of performance study. Response time andthroughput during cloud access to quiz web services have been studied in detail. Securityprecautionshave resultedin a 5%increaseinresponsetime.

DNA Cryptography was introduced by Pandey, G. P. in 2019 to safeguard the cloudapplication. Huffman Algorithm has been shown to be effective in compression research.Socket programming was used by the author to facilitate transfer between sender andrecipient programs. The cloud has been utilized in research to safeguard compresseddata.

P.suresh presented cloud security research using the RSA ALGORITHM in 2016. AES,DES, RSA, and other encryption and decryption algorithms have been examined in thecontext of security research. An asymmetric key algorithm was used to implement RSA inthisstudy.Differentkeysizeswereusedforencryptionanddecryption.Securitymechanisms,on theotherhand, reducethe system's performanceby20% [8].

In 2016, Singh, S. K. presented research on data security for cloud applications utilizingthe RSA technique. According to the author's research, the RSA Algorithm's performanceisinfluencedbythreedifferentvariables.TheseareTimeComplexity,SpatialComplexity, and Throughput. This research used the RSA algorithm to encrypt data sothatonly authorized individuals could access it. In order to upload data to the cloud, itmustbe encrypted first. In order to send data to a user, the Cloud provider authenticatesthe user and allows the data to be transmitted. [9] The amount of time it takes to encryptdatahas dropped by15%.

Cybersecurity for the e-learning system wasprovidedby Bandara in 2014. The term"cyber security" refers to a set of guidelines for safeguarding electronic data. Securityconcernsinane-learningsystemarerapidlyexpanding.e-Learningsecurityisaparticularly difficult problem to solve since so many systems may now be accessed andoperated over the Internet. This study found that internal cyber-attacks are a commonoccurrence. Distributed e-Learning systems provide additional security problems [10],whichthe authorshave considered.

Analysis of protection problems was offered by Kumar, G. in 2011. To conduct the study,theoretical methods were used. Data gathered from several cloud-based websites of e-

learning solution providers was used to conduct empirical research. Text analysis hasbeen used to conduct a theoretical examination of cloud security research. Theoreticalfindings have been compared to actual findings in a procedure known as comparativeanalysis[11].

Arshad Ali et al. published a paper on cloud computing in 2015. In this article, we havepresented some of the current aspects of online education. Cloud computing has also beenexamined by researchers. E-learning aspects have been included into the design of cloudcomputing platforms detailed in this study. This study examines the benefits of cloudcomputingin distanteducation [12].

III. Proposed Methodology

Using encryption and compression methods, the proposed research aims to keep data safewhilealsocompressingit.Thedatawouldbecompressedandencryptedbeforetotransmissionforsecurityreasons.MATLAB(MatrixLab)isusedforsimulation.According to the flowchart, the secure material has been designated D. CD-R and CD-RWmanufacturing follow. Afterwards, the encryption is put in place. Once encryption hasbeen implemented, the data is delivered to the recipient client. In this case, the originalcontentis decrypted anddecompressed usingthesetechniques.

Theprocessflowofresearchconsistsofthefollowingsteps:

1. TheconstraintsofcurrentIoTimplementationresearchstudiesshouldbeconsidered and examined.
2. Compressionofprotectedcontentisbeingexaminedtoreducethesizeofthe object.
3. Thecompresseddataistobeencryptedusinganencryptionalgorithm.
4. Client-serversimulationofmaterial usingtheprovidedmethod.
5. Comparethesize,performance,andsecurityoftheoldandnewIoT systems.

Compression and encryption are performed on receiving end. The usage of this techniquemay help reduce network capacity and congestion issues. Outsiders would have no accesstothe system's data because ofthesecuritymeasuresin place.A large-sized packet is compressed using the XOR-based encryption process in this part,andthe contentsareprotected.

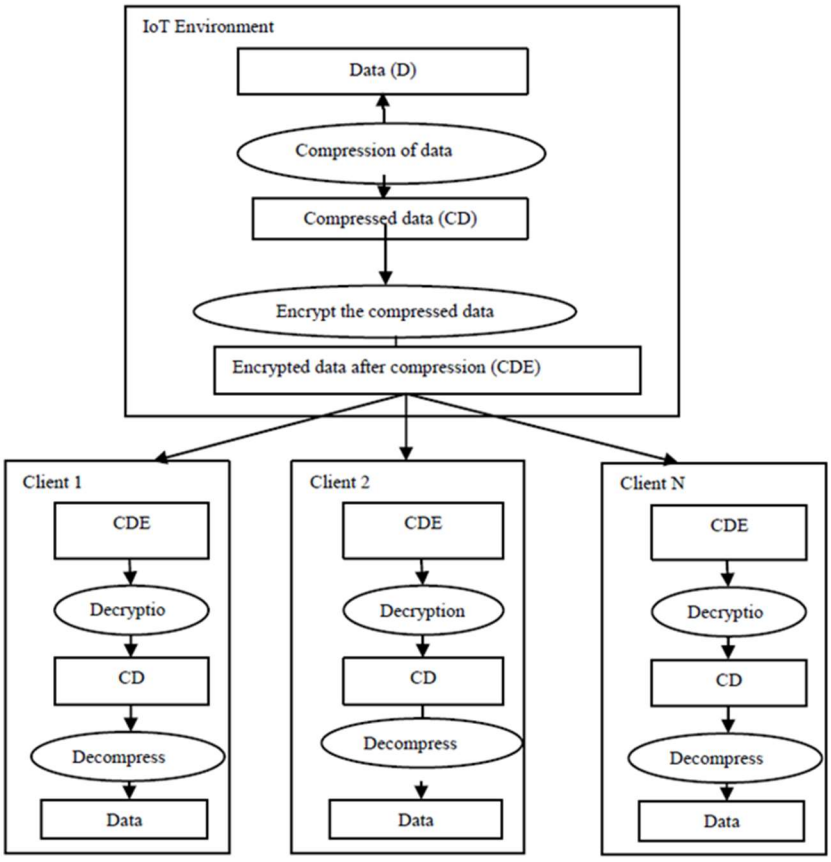

Fig. 3: Proposed System of the work

IV. ResultandDiscussion

A data packet's transit time between the sender and receiver modules is considered.

4.1 Consumption of Time

Figure 5 shows an advanced RSA and DNA encryption-based study. We simulated the time required for the proposed system as opposed to the traditional RSA. The proposed work uses exclusive ordering during encryption and encrypts compressed data. However, previous research used RSA, a DNA technology that takes longer to encrypt data. Furthermore, the material was not compressed before transmission in earlier studies. As a result of the data packets' reduced size compared to those of others, the time consumption is obviously lower.

Table1Consumption ofTime for distinguished algorithms

Number ofpacket	RSA	ADVANCE RSA	DNA Cryptography	Proposedwork
10	1	0.95	0.9	0.85
20	1.7	1.65	1.6	1.3
30	2.4	2.3	2.2	1.7
40	3.1	3	2.9	2.4
50	4	3.6	3	2.7
60	4.7	4.6	4.4	3.5

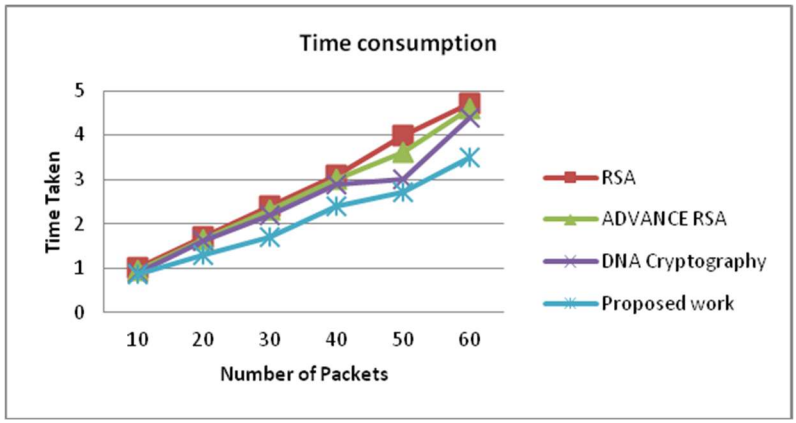

Fig 4 Time comparison during transmission of packets

4.2 ERRORRATE

There is always the possibility of data transmission errors. However, the smaller the packet size and the shorter the time it stays on the network, the less chance there is of an error. The substitution process shortens the string, thus reducing the risk of error. However, the packet size was not reduced by the RSA and DNA encryption [12, 13, 14] techniques used in previous studies. As a result, the current study can reduce the risk of accuracy. The figure below compares the error rates of RSA, Advance RSA, DNA cryptography, and the proposed method.

Table2Error rate with different algorithms

Number ofpacket	RSA	ADVANCE RSA	DNA Cryptography	Proposedwork
10	0.9	0.8	0.7	0.6
20	1.4	1.3	1.2	0.9
30	2.4	2.3	2.2	1.7
40	2.6	2.4	2.3	1.9
50	4	3.6	3	2.5
60	4.2	4	3.8	3.6

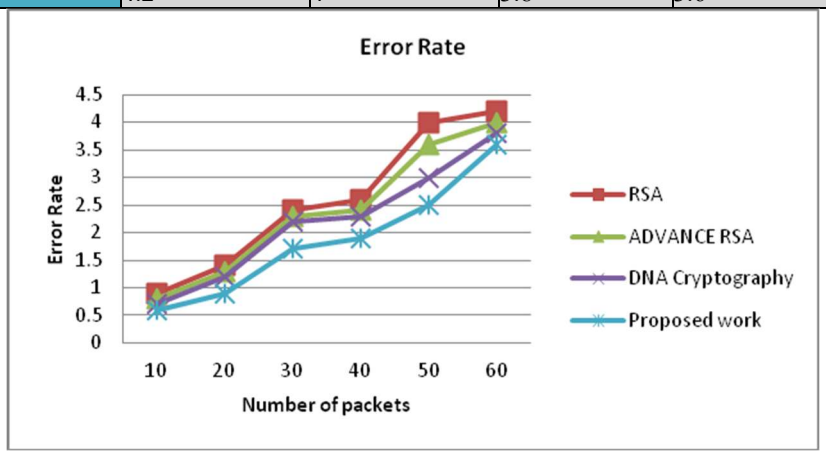

Fig 5 Error rates for distinguished Algorithms

4.3 PACKETSIZE

The suggested approach uses a replacement technique that reduces the content length,therefore reducing the packet size. The results demonstrate the smaller data packetsin compare to the past research. RSA and DNA cryptography did not compress datain previous study. The suggested approach has been used to compare the size of packets inRSA,Advance RSA, and DNAcryptography.

Table3Packetsize Comparison

Number ofpacket	RSA	ADVANCE RSA	DNA Cryptography	Proposedwork
10	9	8	7	6
20	14	13	11	9
30	21	20	18	12
40	26	22	18	16
50	31	28	25	20
60	42	36	32	26

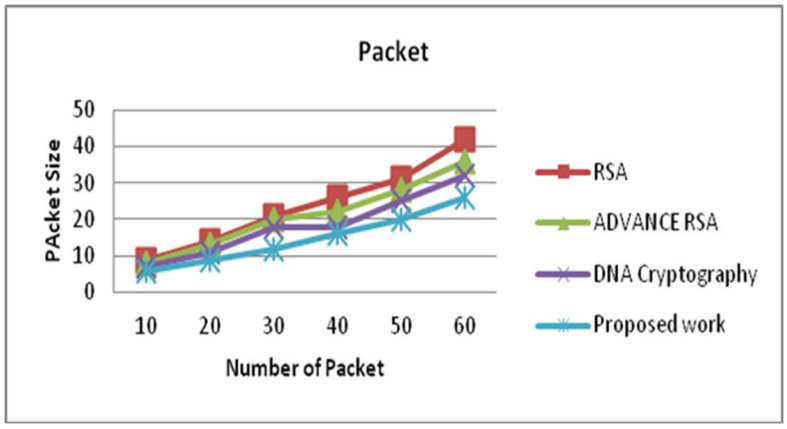

Fig 6 Packet size for different Algorithms

V. Conclusion and Future Work

The combined approach was investigated, where the XOR operation provided security through encryption while the content replacement technique decreased the size of the data packet.Simulations show that the cloud-based teaching system recommended beats traditionalmethods.Asaresultofdatacompressionandencryption,thedataisbothsecureandfastto deliver. Receiver decrypts and decompresses the encrypted and compressed data at theend. The issue of error rate and latency is no longer an issue during transmission since thedata volume is reduced. Additionally, the ratio of dropped packets drops. Various attacks, such as man-in-the-middle (MITM), denial-of-service (DDoS), brute-force, IoT service attacks, attacks by hostile insiders, and application layer attacks can more easily compromise conventional security solutions. The suggested method is more secure than RSA- and DNA-based cryptography-based approaches. The performance of priorbig data security technologies has been shown to be lacking. Because of

this, researchersuse lossless data compression methods. It is possible to employ a bespoke encryptiontechniqueotherthanthestandardRSA,DES,andAEStobetterprotecthugedata.MATLABis beingusedasa simulationtoolin thisstudy.There may be a better way to compress data in the future. Future studies may find ways tomakesystemsevenmoresecure.TheintegrationofsophisticatedIoTservicesandoptimization techniques in future research may deliver greater performance and a lowermistake rate. Soft computing approaches may be used to enhance service quality anddependability. Researchers may analyze the IoT's high availability and zero downtime inordertoincreaseits reliabilityinremote learning.

REFERENCES

[1] Patil, P.: A Study of E-Learning in Distance Education using Cloud Computing.International Journal of Computer Science and Mobile Computing 5(8), 110–113(2016).

[2] Bouyer, A. ,Arasteh, B.: The Necessity Of Using Cloud Computing In EducationalSystem.CY-ICERElsevier143, 581-585 (2014).

[3] Tugrul,A.,Atun,H.:TheCloudSystemsUsedinEducation:PropertiesandOverview. Engineering and Technology International Journal of Educational andPedagogical Sciences 10(4), (2016).

[4] Claral, A.: Implications, Risks And Challenges Of Cloud Computing In AcademicField – A State-Of-Art. International Journal of Scientific & Technology Research8(12),(2019).

[5] Ali, A., Bajpeye, A. : E-learning in Distance Education using Cloud Computing.InternationalJournalof Computer Techniques 2(3),(2015).

[6] Kumar, S., Goyal, N., Singh, M.: Distance Education Technologies: Using E-learningSystemandCloudComputing.InternationalJournalofComputerScienceandInformationTechnologies 5(2), 1451-1454 (2014).

[7] Shi, Y., Hao, H.: Trends of Cloud Computing in Education. In: Cheung S.K.S., FongJ., Zhang J., Kwan R., Kwok L.F. (eds) Hybrid Learning. Theory and Practice. ICHLLectureNotesin ComputerScience,vol.8595. Springer (2014).

[8] Karak,S.,Adhikary,B.:Cloudcomputingasamodelfordistancelearning.InternationalJournal of Information SourcesandServices 2(4),32-38(2015).

[9] Mishra,J.,Panda,S.:A NovelObservation onCloudComputing in Education.InternationalJournalof RecentTechnologyandEngineering8(3),5262-5274(2019).

[10] Balobaid, A., Debnath, D.: A Novel Proposal for a Cloud-Based Distance EducationModel.InternationalJournalfore-LearningSecurity6(2), 505-513(2016).

[11] Zhihong, X., Jun, Z.: Expand distance education connotation by the construction of ageneral education cloud. In: International Conference on Advanced Information andCommunicationTechnology for Education, (2013).

[12] Pandey, G. P.: Implementation of DNA Cryptography in Cloud Computing and UsingHuffman Algorithm, Socket Programming, and New Approach to Secure Cloud Data.Socket Programmingand New ApproachtoSecure Cloud Data, (2019).
[13] Suresh, P.: Secure cloud environment using RSA algorithm. International ResearchJournalofEngineeringandTechnology3(2), 143-148(2016).
[14] Singh, S. K., Manjhi, P. K., & Tiwari, R. K.: Data Security Using RSA Algorithm inCloud Computing. International Journal of Advanced Research in Computer andCommunicationEngineering 5(8), 11-16 (2016).
[15] Bandara, I., Ioras,F., Maher, K.:Cybersecurityconcerns in e-learning education.In:Proceedings of ICERI 2014 Conference,pp.728-734, Spain(2014).
[16] Kumar,G.,Chelikani,A.:Analysisofsecurityissuesincloud-basede-learning.UniversityofBoard/SchoolofBusinessandIT, (2011).
[17] Meslhy, E.: Data Security Model for Cloud Computing. Journal of Communication and Computer 10, 1047-1062, (2013).
[18] Osman, S.: Performance Analysis of Cloud-based Web Services for Virtual Learning Environment Systems Integration. International Journal of Innovative Science, Engineering & Technology 3, (2016).
[19] Garrison, G., Kim, S., Wakefield, R.L.: Success Factors for Deploying Cloud Computing. Communications of the ACM 55(9), 62–68 (2012).
[20] Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments Adoption of Cloud. Sales force, (2012).
[21] Venters, W., Whitley, E.A.: A Critical Review of Cloud Computing: researching desires and realities. Journal of Information Technology, 27(3), 179–197 (2012).
[22] Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Communication Association Info System 31, (2012).
[23] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J.: A Cloud computing- The Business Perspective. Decision. Support System 51, 176–189 (2011).
[24] Nirmala, V., Sivanandhan, R. K, Lalshmi R. S. : Data Confidentiality and Integrity Verification using User Authenticator scheme in cloud. In: 2013 International Conference on Green High-Performance Computing, IEEE, India (2013).
[25] Kumar, A., Lee B.G., Lee H., Kumari, A.: Secure Storage and Access of Data in Cloud Computing. In: International Conference on ICT Convergence, IEEE, India (2012).
[26] Tribhuwan, M., Bhuyar, V., Prizade, S.: Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management. In: International Conference on Advances in Recent Technologies in Communication and Computing, pp. 386-389, IEEE, (2010).
[27] Rewagad, P., Pawar, Y.: Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. In: International Conference on Communication Systems and Network Technologies, pp. 437-439, IEEE, (2013).

[28] Tadapaneni, N. R.: Cloud Computing - An Emerging Technology. International Journal of Innovative Science and Research Technology 5, (2020).
[29] Tadapaneni, N. R.: A Survey of Various Load Balancing Algorithms In Cloud Computing. International Journal for Science and Advance Research in Technology 6, (2020).