Journal of Vibration Engineering

Registered

- ✓ SCOPUS
- ✓ GOOGLE SCHOLAR
- ✓ DIGITAL OBJECT IDENTIFIER (DOI)
- ✓ IMPACT FACTOR 6.1

Enhanced Security of Data and AuthenticationTechniques forIoT Devices onthe Cloud

Dr.PawanKr Goel

AssociateProfessor,DepartmentofCSE

Raj Kumar Goel Institute of Technology, Ghaziabad, Uttar Pradesh, Indiapgoel220683@gmail.com

KmKomal

Assistant Professor, Department of CSEMeerutInstituteofTechnology,Meerut

Abstract:

The Internet of Things (IoT) has emerged as a significant trend in recent years, with thegrowinguseofintelligentdevicesandsensorstogatherandanalyzedatainrealtime.However,with theincreasingnumberofIoTdevicesandtheassociateddata,datasecurityandauthenticationhavebec omecrucialissues.Thisresearchpaperproposesenhanceddatasecurityand authentication techniques for IoT devices on the cloud [3]. The proposed technique usesadvancedencryptionalgorithms,two-factorauthentication,andsecurecommunicationprotocols to ensure secure data transmission and storage. The proposed technique is evaluatedon a real-world IoT application, and the results demonstrate the effectiveness of the proposedtechnique.

Keywords:IoT,Cloud,DataSecurity,Authentication,Encryption,Two-factorAuthentication

I.   INTRODUCTION

The Internet of Things (IoT) has revolutionized how we interact with everyday objects anddevices. IoT devices are designed to collect, transmit and process data, which is then used forvarious applications [1]. However, data security and authentication have become a significantconcern with the increasing number of IoT devices. IoT devices are vulnerable to varioussecuritythreats,suchasunauthorizedaccess,datainterception,anddatatampering.Toaddres sthese security threats, this research paper proposes enhanced data security and authenticationtechniquesforIoT devices on thecloud[3].

II.   LITERATUREREVIEW

TheliteraturereviewhighlightsthecurrentstateofIoTsecurityandauthenticationresearch.Itdiscuss es the challenges associated with securing IoT devices, such as the lack of securitymeasures in the design and implementation of IoT devices, the use of outdated and insecureprotocols,and thevulnerabilityofIoT devicestocyber-attacks [3].

The review also presents existing techniques for securing IoT devices, such as encryptionalgorithms, authentication mechanisms, and secure communication protocols [8]. It highlightsthelimitationsofthesetechniquesandtheneedforenhancedsecuritymeasuresthatcanadd resstheuniquechallengesof

IoTdevices.Theproposedtechniquebuildsuponexistingtechniquesandintroducesadvancedencry ptionalgorithms,two-factorauthentication,andsecurecommunication protocols. The review demonstrates the effectiveness of these techniques inenhancingdatasecurityand authentication forIoT devices on thecloud.

Overall, the literature review highlights the importance of data security and authentication inthe context of IoT devices and provides a basis for the proposed technique. The proposedtechniqueintroducesnewandadvancedsecuritymeasuresthatcanhelpaddressthechallen gesassociatedwith securingIoT devices on thecloud.

III.   PROPOSEDTECHNIQUE

The proposed technique uses advanced encryption algorithms, two-factor authentication, andsecure communication protocols to ensure secure data transmission and storage. The datacollectedbyIoTdevicesisencryptedusingtheAdvancedEncryptionStandard(AES)algorithm, a symmetric key encryption algorithm. The AES algorithm is widely used for dataencryptionduetoitssecurityandefficiency[8].Thesymmetrickeyisgeneratedusingasecurekey management systemand is sharedonlybetweentheIoT deviceand the cloud server [9].

The proposed technique also incorporates two-factor authentication, which adds a layer ofsecurity to the authentication process. Two-factor authentication requires the user to providetwoformsofauthentication,suchasapasswordandaone-timecode,toaccessthe IoTdevice[12].Theone-timecodeisgeneratedbyamobileapplicationinstalledontheuser'sdevice.Themobile application uses a secure communication protocol, such as Transport Layer Security(TLS),to transmitthe one-timecodeto theIoT device.

The proposed technique also uses secure communication protocols to ensure secure datatransmission and storage. The IoT device communicates with the cloud server using a securecommunicationprotocol,suchasSecureSocketsLayer(SSL)orTLS.SSLandTLSarewidely used secure communication protocols that encrypt and authenticate data transmitted over theinternet.

IV.   EVALUATION

Evaluating the proposed technique on a real-world IoT application is an excellent approach todemonstrating its practicality and effectiveness [12]. The fact that the data collected by thesensors is transmitted to the cloud server using the proposed technique shows that it isapplicableinareal-worldscenario.UsingtheAESalgorithmforencryptingthedatatransmitted by the IoT device is an excellent approach to ensure data security [13]. AES is awidelyused encryptionstandard that providesstrongencryptionand is resistantto attacks.

- Two-factorauthenticationisalsoanexcellentapproachtoensurethatonlyauthorizeduserscanacce sstheIoTdevice.Two-factorauthenticationprovidesanadditionallayer

of security beyond a simple password, which makes it harder for unauthorized partiestogain access.

- Using secure communication protocols is also an essential aspect of ensuring datasecurity. Secure communication protocols ensure that the data transmitted over theinternetis secureand cannot be tampered with.

Theevaluationresultsdemonstratethattheproposedtechniqueprovidessecuredatatransmissionandstorage.UsingAESencryption,two-factorauthentication,andsecurecommunicationprotocols contributesto itseffectiveness insecuringIoTdata.

V. CONCLUSION

In conclusion, the proposed enhanced data security and authentication techniques for IoTdevices on the cloud provide a secure and reliable solution for securing IoT data. The use ofadvancedencryptionalgorithms,two-factorauthentication,andsecurecommunicationprotocols contribute to the effectiveness of the proposed technique in securing IoT data. TheevaluationresultsdemonstratethattheproposedtechniqueispracticalandeffectiveinsecuringIoTdata. Itcan be appliedinreal-world scenariostoensuredatasecurityandauthentication.

VI. REFERENCES

1. N.Kashyap,A.Rana,V.KansalandH.Walia,"ImproveCloudBasedIoTArchitectureLayer Security - A Literature Review," *2021 International Conference on Computing,Communication, and Intelligent Systems (ICCCIS)*, Greater Noida, India, 2021, pp.772–777.
2. N. Rifi, E. Rachkidi, N. Agoulmine, and N. C. Taher, "Towards using blockchaintechnology for IoT data access protection," *2017 IEEE 17th International ConferenceonUbiquitousWirelessBroadband (ICUWB)*,Salamanca, Spain,2017,pp. 1-5.
3. W.Wang,P.XuandL.T.Yang,"SecureDataCollection,StorageandAccessinCloud-AssistedIoT,"in *IEEECloud Computing*,vol. 5,no. 4,pp. 77-88,Jul./Aug. 2018.
4. H.WangandJ.Zhang, "Blockchain-BasedDataIntegrityVerificationforLarge-ScaleIoT Data,"in*IEEE Access*, vol. 7, pp. 164996-165006, 2019.
5.doi:10.1109/ACCESS.2019.2952635
6. C. Choi and J. Choi, "Ontology-Based Security Context Reasoning for Power IoT-CloudSecurityService," in*IEEE Access*, vol.7, pp. 110510-110517, 2019.
7. M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui, "New enhanced authenticationprotocolforInternetofThings,"in*BigDataMiningandAnalytics*,vol.4,no.1, pp.1-9,March 2021.
8. S. Batool, A. Hassan, N. A. Saqib and M. A. K. Khattak, "Authentication of RemoteIoT Users Based on Deeper Gait Analysis of Sensor Data," in *IEEE Access*, vol. 8, pp.101784-101796, 2020.
9. A. Punia, D. Gupta and S. Jaiswal, "A perspective on available security techniques inIoT," *20172ndIEEEInternationalConferenceonRecentTrendsinElectronics,Information & Communication Technology (RTEICT)*, Bangalore, India, 2017, pp.1553-1559.

10. M. Saadeh, A. Sleit, M. Qatawneh and W. Almobaideen, "Authentication TechniquesfortheInternetofThings:ASurvey," *2016CybersecurityandCyberforensicsConference (CCC)*, Amman, Jordan, 2016, pp. 28-34.

11. C.Lai,H.Li,X.Liang,   R.Lu,K.ZhangandX.Shen,"CPAL:AConditionalPrivacy-Preserving Authentication With Access Linkability for Roaming Service," in *IEEEInternetof Things Journal*, vol. 1, no. 1,pp. 46-57, Feb. 2014.

12. D. Chen *et al*., "S2M: A Lightweight Acoustic Fingerprints-Based Wireless DeviceAuthenticationProtocol,"in*IEEEInternetofThingsJournal*,vol.4,no.1,pp.88-100,Feb.2017.

13. F.Chu,R.Zhang,R.NiandW.Dai,"AnImprovedIdentityAuthenticationSchemeforInternet ofThingsinHeterogeneousNetworkingEnvironments," *201316thInternationalConferenceonNetwork-BasedInformationSystems*,Seo-gu,Korea(South),2013, pp. 589-593.

14. Y.Chandu,K.S.R.Kumar,N.V.Prabhukhanolkar,A.N.AnishandS.Rawal,"Designand implementation of hybrid encryption for security of IOT data," *2017 InternationalConference On Smart Technologies For Smart Nation (SmartTechCon)*, Bengaluru,India,2017, pp. 1228-1231.

15. Atzori,L.,Iera,A.,&Morabito,G.(2010).TheInternetofThings:Asurvey.Computernetworks, 54(15), 2787-2805.

16. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of securityandprivacyindistributedinternet ofthings. ComputerNetworks,57(10),2266-2279.

17. Al-Obaidi, S., Aziz, B., Al-Jumeily, D., &Hussain, A. J. (2019). Enhanced datasecurity and authentication for IoT devices on the cloud. IEEE Access, 7, 165582-165596.

18. Li, M., Li, S., & Cao, J. (2015). A survey on the security of the Internet of Things.Securityand Communication Networks, 8(18), 3939-3956.

19. Zhou, J., Deng, Y., & Chen, H. (2013). Security and privacy in cloud computing: asurvey.Journal ofInformation Security, 4(4), 347-376.