BioGecko

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

INTERNETOFTHINGSINVESTIGATIONS AND DIGITALFORENSICSCHALLENGES

K.VenkatagurunathamNaidu
Dept.ofComputerSciencendEngineering Dr.M.G.R.E.R.I, Chennai,India.
Email: venkatspmvv@gmail.com

Dr.V.N.Rajavarman
Dept.ofComputerSciencendEngineering, Dr.M.G.R.E.R.IChennai,India.
Email: nrajavarman2003@gmail.com

Abstract
The Internet of Things(IoT) has evolved into adaily technology component that unifies all of the disparate systems and data into one process that is integrated and cohesive. Digital world currently lacking the favourable capacity for Inetnet of Things digital forensics despite the introduction of cutting- edge technologies offering precise solutions. As a result, the extraordinary growth in the number of electronic devices and the vastgathering and consumption of data have made Internet of things forensics necessary inthescenario of cybercrimes.We summarise the distinctions among IoT and traditional digital forensic techniques inthisstudy and also provided a list of three types of IoT-related computer crimes.

Keywords: IoT Investigation, IoTdevices, DataIn- tegrity, digital forensics,IoT Forensics

I. INTRODUCTION

Productivityandconnectivityhaveincreasedwiththeonline interconnection ofnumerouselectronicdevices,suchasIoT. Thesethingshavecreated asystem thatisbeingusedto orchestrateandcontroldevicesincrucialinfrastructures in- cludingnuclearaswellaspowerplants,thebuilding industry, andthehealthcare industry,amongotherplaces.Therearean increasingnumberofthesedispersedevicesinthenetworked environment, commonlyknownascyberspace.Hence,digital evidence,suchasinformation fromsocialnetworks,mobile SIMcards,CCTVcamerafootage,andmore,hasbeenused insomewayinthemajority ofcriminalactivities acrossthe public,privatesectors.Acompelling casestudyfordemon- stratingthevalueofmultilayered digitalforensicsinidenti- fyingculpritsistheBostonMarathon Bombing incident[1]. Despitechangesindataandtechnology, forensicsprocesses have not changed.The tools used to commit the crime or theobjectsonwhichitiscommittedhavebeenidentified as eyewitnesses.Theinterconnectedness oftoday'stechnologies hasmadeitsimpler forhackers toexploitprivateinformation, whichreducesthedependability ofmisusedequipment.IoT forensics mustbetriggered asaresultofthis.Gartnerpredicts thatbytheendof2020,therewillbe5.8million IoTdevices supportingvarious industries,resultinginasignificantamount ofunsafedata[2].IoTforensicsis abranchofdigitalforensics andinvolvesgatheringevidencefromallconnected devices throughavarietyofmethods. IoTincludesdataintermsof quantity,variety,andspeed.IoTtechnologies usesensorsand trackingtagstocontinuouslygatheractivitylogs,whichisanexcellent sourceofwitness.IoTforensics istherefore of utmostsignificance.Hereisalistofwhatwecontributedto thiswork:

- Thedistinctionsbetweenconventional andInternet-of- thingsdigitalforensicmethodsarehighlighted.
- Internet-of-thingsrelatedcomputercrimesarelisted.
- R&D contributionsto the fieldof IoT forensics are categorised.

II.IOTANDDIGITALINVESTIGATION PROCEDURE

Ittakes severalyears foratraditionalcourt toacceptandin- tegratedigitalevidence.Withtheadvancement oftechnology, growingrelianceon,andcomprehension of,thePolicieshave beenupdated forthedigitalagetohastenthelegalsystem's acceptance.Digitalforensicsisindeedanscientific discipline thathelpstoidentifyanoccurrence,gather evidence, examine, analyse,andreportfindings,accordingto NIST[3].According tothedefinition givenabove,therearefourmajorstagesor stepsthatmakeupdigitalforensics:

- Identification,whichentailstheidentificationoftheinci- dentandtheidentificationoftheevidence;
- Digitalinvestigatorcollectsallforensicdatafromvarious media,suchasaharddisc,duringthecollection process; and
- Inspectionandanalysisareaspartoforganisation.As partoftheevaluation,alldataandattributesareextracted andlookedat.Thefactsandinformation obtainedduring theanalysisphaseareanalysed andreviewed bythe investigator.
- Thepresenterthencontinuesontothepresentationphase, whentheycreateawell-organizedreportthatissubmitted tothepropercourtorprocess.

TheInternetofThings(IoT)differsfromtraditional (normal) devicesinanumberofways.IoTdevicesarefirstmotivated bybusiness, whichindicatesthat,atleastforenterprises,thepurpose ofitsdeployment istolowercostsandboostproductivity. Second,becauseIoTdevicesaremuchmoredispersed and diverseinnature,theyproduce atonneofdataofalldifferent kinds.Finally,IoTmakesitpossibletolinktooperational technology(OT)aswellasotherITequipment.Finally,the IoTrequirescompleteautomation andnearreal-timeincident monitoringdue to the geographicallydistributednature of itscomponents. Ourprojectionassumesthatthedetectionof evidencewithinInternet ofthingswillbemoredifficultinthis situation.The identificationstep ofany digitalforensicinquiry wouldbemorechallengingduetothemanykindsofelectronic gadgetsandsensors,aswellasthevariousdatatypesproduced by these IoT pieces. For instance, network forensics will bemostlyusedwhileexaminingacyber-attack thataffected numerousfirewalls androuters.HoweverinanIoTsituation, sensors[4]thatmightbeinstalled inapowerplant'sSCADA systemwillalsobeinvolved. Asaresult,tryingtogainaccess tosuchgadgetsthatarehousedinessentialinfrastructuremay bechallenging.Criticalinfrastructure ismoreovertypically segregatedfrom,disconnected from,orconnectedonlinevia secureconnections viaVPNtunnelling.Asaresult,detecting orfingerprinting suchexternaldevicesismoredifficultthan doingsoforpubliclyaccessible ITassets.Inthisinstance, specialauthorization isneededtogainaccesstosuchequip- mentforadditionalresearch.IoTdevicecollectionwillalso bemoredifficultthanwithtraditionaldevices.AsIoTdevices areincludedinthedigitalinquiry,weanticipate seeingmore challengesfromtheperspectiveofthecompany.Thisisdue tothepreviously notedfactthatIoTdeviceswillbemore widelydispersed andproducemoredatainawiderrangeof formats.Asaresult,howeveraddition tothenovelunderlying technologiesinIoT,researcherswillrequireadditionaltimeto developtheirskillsandcomprehend thenecessaryresources (suchastoolsthatinterpret thedatafrommultiple sensors), whichwillultimatelymaketheorganisation phasemorecom- plex.Finally,becauseitisautonomous ofhardwareanddata, weforecastthatthepresentation phasewon'tbeimpactedby theIoTtrend.Table1summarisesthekeydifficultydifferences betweentraditionalandIoTdigital forensics.Inthesameway,

TABLEICOMPARINGTRADITIONALANDINTERNETOFTHINGS(IOT) INVESTIGATIONS,ANDTHERESULTINGCOMPLEXITY.

Process ofDigitalInvestigation	Traditional	IoT

Identification	MediumtoHigh	High
Collection	LowtoMedium	MediumtoHigh
Organization	MediumtoHigh	High
Presentation	LowtoMedium	LowtoMedium

thekeydistinctions betweenevidencetypes,datautilisation, networklimits,anddatastoragearehighlightedinTable2.

III. ATTACKSONDIGITALFORENSICSANDIOT

Theperceptionlayer,networklayer,andapplicationlayerarethethreelayersonwhichtheIoTdevicesoperate. Barcodes,RFID oressentiallysensorsthatgatherdatafromthe outside environment and transmit it to the network layer makeupthephysical layer.Thenetworklayer'sgoalisto transmittheperceptionlayer'sfindings toaninformation processingsystemover the Internetor anothertrustworthy

TABLEIIKEYDIFFERENCESBETWEENTRADITIONALANDIOTINVESTIGATIONS

DigitalForensics	Traditional	IoT
Provenance of the evidence	Electronic devices including portable and stationary computers	Sensors and tags embedded in electronics; RFID; Internet ofThings gadgets
UseofData	Terabyte	Exabyte
Network	determined bound-arybasedonthecir-cumstances orown- ership	Due to the large number ofdevices, IoTforensics does haveablurry and
Storage	DiskAnalysis	Torecordthedisk's present state,micro cards, memory, and RAM-based systems are used [7].

network.Lastly,usersuseIoTintelligenceandanalyticsat theapplication layertoaccomplish theirobjectives(suchas increaseproductivity,connectivity,scalability,etc.).Security of these levels has become a difficultproblem in modern timesduetothegrowingusageandinclusionofinterconnected devices. Eachfeaturechangeacrossallthreelevelshasthe potential to jeopardise any essential security aspect, such asIntegrity,confidentiality&availability[6].Threetypesof assaultsorcybercrimesagainstIoTtechnologyarelistedin thissection.

A.PHYSICALATTACKS

Nodetampering:Itincludesphysicalaccessbyanattacker to a node in order to recoverkeys, node destruction,and operating onanIoTnode.ThisattackcanbestoppedwithauthenticationandcryptographyAuthenticationandcryptography[21].

-Sleepdeprivationattack:Theattackerattemptstodrainpower, whichultimatelycausestheIoTnodetoshutdown.Theassault includeskeepingthenodeconsciousforaverylongtime, whichultimatelycausesthenodetoshutdown.IoTsensors arebattery-

poweredandhaveafiniteamountofpower.Such attackscanbeidentifiedandpredictedbyusinganintrusion detectionsystemandtechniqueslikedeeplearning[14].
Maliciouscodeinjection:Whenanattackerinjectsmalicious code into a node, the node may be shut down or, in the worstsituation,theattackermayhavecompleteaccesstothe node.Thesensitivedataoftheattacker'snodereplicatingand injectionwillbesavedifthereiscollusionwiththeinjected attack[15].
Physicaltheft:Theassailantsneaks intothephysicalhardware orvaluable items.IoTdeviceswillbeputinseveralindustries andlocations,makingaccesstothemsimple.Thisisespecially truewhensensorsaredispersed overopenandpublicspaces (suchasagriculturalfields, roadways,andtransportationsys- tems).

B.SOFTWAREATTACKS

-Phishingattacks: Byemailspoofing,theattacker gainsac- cesstousernameandpasswordinformation. WithIoT,where credentials aretheentrancetoprivatedata,theinformation collected canbeutilisedbytheattackertogainunauthorised accesstoavictim'saccount,whichmayhaveaccesstoan IoTdevicemanagement system.Oneofthebeststrategiesfor thwartingphishingattacksisawareness.
-MaliciousScript:Script thatismaliciousViatheinjectionof malicious script,theattackeraccessesthesystem.TheRan- domisedWatermarkingFilteringScheme(RWFS)hasasensor thatdetectsandremovesfraudulent data.Thismethodology generatesanall-encompassing watermarkthatcanbeusedin forensics[12].
-Malware: Theattackercanharmthecomputerbyusing harmful code, such as viruses, worms, and Trojan horses. Thesecodesspreadthemselves viaemailanddownload from theinternet.Maintaining arepositoryofallvirusesand attemptingasignature-baseddetectionareforensicmethods toaddressthismalwareassault[14].Additionally, malware attackdetection maybeaidedbymachinelearningandthe developmentofzero-daycapabilities.

C.NETWORKATTACKS

DenialofService:Inthisattack,theattackerfloods the networkwith largeamountsof traffic(for example,band- width),exhaustingthe systemand renderingit unavailable to legitimateusers. This has an impacton all IoT layers, butparticularly theperceptionlayer.Inordertodistinguish betweenattackandreal-timetraffic,packetsmightbe captured usingthe forensictechniqueknownas JPCAP(networkpacket capturelibrary).CEPID(ComplexEventProcessing Intrusion Detection),adifferentforensictool, alsosuggestedamultilay- eredarchitecturetoconducttrafficmonitoring,packetanalysis, andevent handlingtorestrictsuspiciousactivity[14].// -Man- in-the-middle attack:Anintruderhorriblyeavesdropsonor manages two parties' private communication.The attacker also might deceivethe victim in order to learn more. By usingadigitalsignature-based authenticationmethodand continuouslymonitoringthe IoT nodes,this attackcan be prevented[14].A roguenodethatmayassumetheidentitiesof numerous IoTnodesisknownasaSybilattack.Redundancy andincorrect informationaretheeffectsofthis[13].AnRSS- baseddetectionmechanism canbeembeddedtoconducta forensicstudyinto theSybilattack,and networkheterogeneity topologiescanbeusedtogaugeperformance[11].

IV.IMORTANTIMPLEMENTATIONSINIOT FORENSICS

Theterm"LoRa"standsfor"long-range," anditreferstoa lowpowertechnologythatallowsforcommunicationbetween remotesensingdevicesandLPWANs. Thistechnology is absolutelyessentialsinceit offerssecurity,precisepositioning, andtwo- waycommunication.End-to-endencryption,aunique andspecialized 128bitAESkey,andapervasiveglobal identityareallimplementedbyLoRa.Lora WANisextremelyimportantforprovidingsecurity,howeverifthesafetykeys arenothandledeffectively,thereisachancethatthesecurity of networkdevicescouldbe compromised[10].

Sincethe InternetofThingsreliesondatafromsensors.Thetracing ofconstellationtracefigure, whichshowsinformationabout theradiofrequency propertiesofLoRadevicesandtheir distinctivefeatures,isasecuritymethodforthephysicallayer.
Thisfunctionalityaidsforensicinvestigationsinunderstanding thesensorassault[16].

V. DISCUSSION

IoT technologygenerallyfaces a numberof difficulties, including key management, an essential responsibility for IoT security. The absence of suitable forensic tools, how- ever, continuesto be the biggest problem facing the field andcommunity ofdigitalforensics.Althoughtechnology has greatlyevolved,thecommunity ofdigitalforensicexpertshas noteffectivelyusedthecapabilities toitsadvantage. Itisa necessitytochoosecloudstoragegiventheuniqueparadigm ofrisingspaceutilisation. Storageissuesmaybelessofa concernifthe forensiccasehasadedicated cloudspace. Anotherdifficultyisstronglyrelatedtotheaforementioned; theforensictoolsmustbeadaptable tothelevelofknowledge oftheforensicteamanduser-friendly. Aprogrammethatcan handleavastnumberofIoTintelligence, extractskeywords, andanalysesthegatheredevidenceisanimportant discovery [4]sincedataanalysisisacrucialandtime-consumingphase.

VI. CONCLUSION

Thepaperprovidesabriefoverview ofdigitalforensics and investigations inIoTsystemsandtechnologies.Devicesecu- rityandattack-relatedforensicsarecrucialduetothegrowing interconnectednessofdevices.Aboutthenormalprocedure andkeyvariances,we’veidentified theprimarydistinctions betweenconventional andInternetofThingsinvestigations. excludingthepresentation stage,ourdataindicatethatthe complexityofIoTstudieswillexpandinnumerousways.Also, welistedthemostcommoncybercrime(orattacks)against bytheInternetofThingsandsuggested someinvestigative strategiestoaddresssomeoftheirdifficulties. Wehavetaken intoaccount thefactthatInternet -of-thingsdigitalforensics andinvestigations arestillarelativelyrecentdevelopmentin technologyforbothpublicandcommercial sectorinvestiga- tors.

REFERENCES

[1] JohnnyNhan,LauraHuey,RyanBroll,Digilantism:AnAnalysisof Crowdsourcingand the BostonMarathonBombings,The BritishJournal ofCriminology,Volume57,Issue2,1March2017,Pages341361.
[2] Egham,U.K.,GartnerForecastsGlobalDeviceJanuary(2020)
[3] Patel,KeyurK.,andSunilM.Patel.Internetofthings-IOT: definition, characteristics, architecture,enablingtechnologies,application&future challenges.Internationaljournalofengineeringscienceandcomputing6,no.5(2016).
[4] NicoleLangBeebeandJanGuynesClark.AHierarchical,Objectives-BasedFrameworkfortheDigitalInvestigationsProcess(2005).
[5] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E.K.Markakis, ASurveyontheInternetofThings(IoT)Forensics: Challenges,Approaches, andOpenIssues,inIEEECommunications Surveys&Tutorials,vol.22,no.2,pp.11911221.
[6] Internetof Things-IOT:Definition,Characteristics,Architecture,En- ablingTechnologies, Application&FutureChallengesKeyurKPatel, SunilMPatel
[7] M. A. M.Sadeeq,S. R. M. Zeebaree,R. Qashi, S. H. Ahmed and K.Jacksi,InternetofThingsSecurity: ASurvey,2018International ConferenceonAdvancedScienceandEngineering(ICOASE),Duhok,2018,pp.162-166
[8] SimsonLGarfinkel.2010.Digitalforensicsresearch:The next 10years.Digitalinvestigation7(2010),S64S73.

[9] H.RajabandT.Cinkelr,IoTbasedSmartCities,2018International SymposiumonNetworks,ComputersandCommunications (ISNCC), Rome,2018,pp.1-4.
[10] B.Hammi,R.Khatoun,S.Zeadally,A.FayadandL.Khoukhi,IoTtechnologiesforsmartcities,inIETNetworks,vol.7,no.1,pp.1-13,12018.
[11] Abbas,Sohail&Haqdad,Muhammad &Begum,S.&Khan,Muhammadzahid.(2018).Detectingsybilattacksusingheterogeneous topologiesinstaticwirelesssensornetwork.JournalofTheoreticalandApplied InformationTechnology.96.49284940.
[12]Alromih,A.,Al-Rodhaan, M.,&Tian,Y.(2018).ARandomized WatermarkingTechniqueforDetectingMaliciousDataInjectionAttacks in HeterogeneousWireless Sensor Networks for Internet of Things Applications.Sensors(Basel,Switzerland),18(12),4346.
[13] Abbas,Sohail&Haqdad,Muhammad &Begum,S.&Khan,Muhammadzahid.(2018).Detectingsybilattacksusingheterogeneous topologiesinstaticwirelesssensornetwork.JournalofTheoreticalandApplied InformationTechnology.96.49284940.
[14] Imdad, Maria&Jacob, Deden &Mahdin,Hairulnizam&Baharum, Zirawani&Shaharudin, Shazlyn&Azmi,Mohd.(2020).Internetof things:securityrequirements, attacksandcountermeasures.Indonesian JournalofElectricalEngineeringandComputerScience.
[15] Kandah, Farah&Singh,Yashaswi&Wang,Chonggang.(2011). Colluding injectedattackinmobilead-hocnetworks.2011IEEEConference onComputer CommunicationsWorkshops,INFOCOMWKSHPS 2011.235 240.
[16] Jiang,Y.,Peng,L.,Hu,A.etal.Physicallayeridentification ofLoRa devicesusingconstellationtracefigure.JWirelessComNetwork2019,223(2019).
[17] Liu, X., Abdelhakim, M., Krishnamurthy,P., &Tipper, D. (2018).IdentifyingMaliciousNodesinMultihopIoT NetworksusingDualLinkTechnologiesandUnsupervisedLearning.OpenJ.InternetThings,4,109-125.
[18]]H.Achi,A.HellanyandM.Nagrial,Network securityapproach for digitalforensicsanalysis,2008International ConferenceonComputer Engineering&Systems,Cairo,2008,pp.263-267.
[19] Boztas,A.&Riethoven,A.R.J.&Roeloffs,Mark.(2015).SmartTVforensics:Digitaltracesontelevisions.DigitalInvestigation.
[20] S.Becirovic andS.Mrdovic, ManualIoTForensics ofaSamsung Gear S3FrontierSmartwatch, 2019International ConferenceonSoftware, Telecommunications andComputerNetworks(SoftCOM),Split,Croa- tia,2019,pp.1-5.
[21] Messai,Mohamed-Lamine.(2014).ClassificationofAttacksinWirelessSensorNetworks.
[22] Sutherland,Iain&Read,Huw&Xynos,Konstantinos.(2014). Forensic analysis ofsmartTV:Acurrentissueandcalltoarms.DigitalInvesti- gation.