International Journal of Computational Intelligence in Control

An Investigation into the Defensive Issues and Challenges with the Internet of Things

[1]G Siva Prasad , [2]Dr.K.V.S.R.P.Varma, [3]Dr.T.Nedunchezhian,
[4]Dr.B.Mouli Chandra, [5]M.Narendra
[1,2,3,5] Department of Computer Science and Engineering,
[4]Department of Electrical and Electronics Engineering,
[1,2,3,4]QIS College of Engineering & Technology, Ongole.
[5]CMR Engineering College, Hyderabad
[1]sivaprasad.g@qisit.edu.in,[2]varma.p@qiscet.edu.in,
[3]nedunchezhian.t@qiscet.edu.in, [4]moulichndra.b@ qiscet.edu.in,[5]narendra.m@cmrec.ac.in

Abstract— In recent years, the Internet of Things (IoT) has attracted a lot of research attention. Applications for the Network of Things span a numerous industries, including wearable technology, smart homes, smart cities, factory automation, and many more. With the powerful intelligence of IoT, there are many different types of issues and challenges. Protection is one of the main problems for IoT devices, software, and networks. This report describes how IoT research has advanced to handle this important IoT feature and concludes that a variety of safe issues & disquiets need to be addressed and identified right now. IoT (Internet of Things) fundamentally suggests that everything — or, to be more precise, all gadgets — are connected and can communicate with one another without the intervention of humans. Since the Internet of Things (IoT) has

Index Terms— *IoT, security flaws and difficulties with it, and solutions to such concerns.*

1. INTRODUCTION

The Internet of Things integrates cutting-edge sensors and circuitry into every real-world object that surrounds us. Each sensor sends information that is valuable. Understanding how gadgets work and how data is processed to make it useful to us is made easier with this understanding. Why these tools connect to one another and how we might use the data they provide present challenges. The sensors communicate with one another, connect securely to the IoT system, and use a global ground.

Through the widespread IoT system, the data from the sensors is acquired, combined with insights, and then deleted to make room for computer software that address specific demands of the company or consumers [1-3]. Imagine only a future in which your body is related with your automobiles after 10 to 25 years, and Your life is intertwined with home. Additionally, in order to anticipate this functional capacity and best serve our interests, each of these will interact with the other systems around them [4].

Implanted surgical tools and other tools to monitor us are connected to human organs. We may have riding automobiles that operate as safely as possible in the upcoming years. Therefore, an attack on our homes by reckless, irresponsible drivers or even a burglar is less serious than a software bug on one computer. There is no worry that they will become disconnected from or unconnected from these devices. But that wasn't the situation. Many of our computer systems are connected and interconnected, work together, and communicate with the internet [5], and if that happens, they become vulnerable and susceptible to manipulation.

IoT goods are being developed and released quicker by people [6]. However, they are unable to provide safety. Suppliers, superior firms, and raised companies are pressuring the top corporations to develop and deploy the IoT system more quickly. In order to compete with other companies, they develop and deploy the goods more quickly. They have no regard for safety. It is pointless to disclose 100 million lines of code if the individual's private information is not safe.

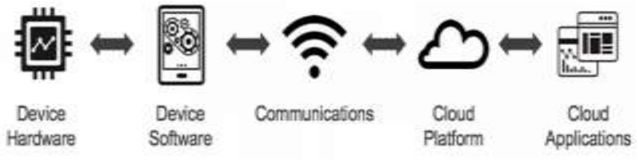
Consider a patient with cardiac disease. If someone has a condition that is controlled by implanting an intellectual pacemaker, such as heart disease. A person who has a smart pacemaker gets an android application to monitor the health and efficiency of both his heart and pacemaker. Both the patient and the physicians may access information on the patient's heart and pacemaker. When there is no encryption in pacemaker applications and the wearer assumes that their sophisticated pacemaker is in the hands of their adversaries because they have an adversary on the other side, the pacemaker may be swiftly penetrated and the hacker can control it without the wearer's knowledge. Therefore, someone's life might be at danger. IOT system protection is a serious problem because of this. Imagine if a car is totally connected to the internet. Additionally, if this car is vulnerable to malware, an attacker may utilise the vehicle's hardware to compromise its software, allowing it to exceed the posted speed limit and endangering the occupants.

Consider a car as an illustration. A car has several sensors installed that continuously track every bay and important part of the vehicle. The car's computational framework now receives information from the sensors and integrates and assesses it if there is a problem with the vehicle or engine. The computational framework then transforms the data into valuable information before sending it to the producer or the closest vehicle repair shop. When the customer returns to the car repair business, the technical specialist in machinery identifies the main problem and the vehicle may be quickly restored. When a component is damaged today, the vendor is now informed in full of the damaged part's information. Therefore, we may draw the conclusion that each sensor and computer communicate with one another and that the framework has a complete understanding of all there is to know about us. From the moment we wake up until the moment we go to sleep, a system is aware of everything about us.

The sensors keep a close eye on you, so we can't take this private information. This requires a secure connection between the device and the IOT platform [9]. The system maintains statistical records in a secure archive and keeps millions of sensor information.

2. IoT STRUCTURED FRAMEWORK

Figure 1 illustrates the IoT's organised framework. This organised framework [1, 2] may be broken down into five subsystems, and each component is covered individually here.



The IoT Technology Stack

Figure 1: **IoT STRUCTURED FRAMEWORK**

2.1 Sensor Interoperability Subsystem

The vast majority of sophisticated systems integrated with intelligent objects that gather and transmit data from the physical world to the electronic setting make up the Sensor Communication subsystem. Then, we may suppose that sensor systems obstruct the rest of the electronic world as well as the physical environment.

The following modules receive the data after which they analyse and assess the outcomes. There are sensors available that can measure a variety of variables, including exercise, humidity, pollution levels, health data, and much more. Higher capacity sensors are incorporated into such smart gadgets. They are sensors. referred to as body device, cold, and automobile sensors. Figure 2 depicts the sensor communication subsystem.

connectivity.

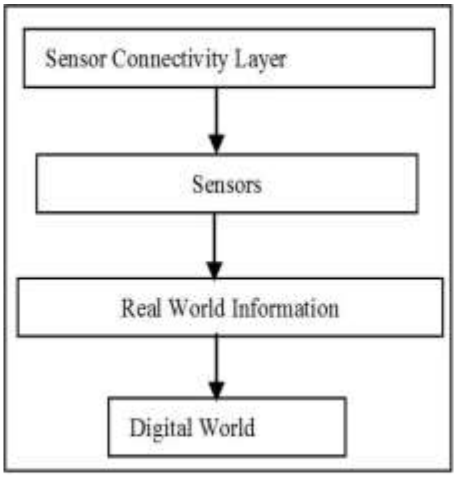


Figure 2**:** Sensor Connectivity Layer

2.3 Subsystem for Network Control

This subsystem handles network management, device administration, threat control, and data analysis. Figure 4 depicts the functionality of this subsystem. Actually, there are two types of data that this subsystem manages:

(a) Continuous: In this case, processing of sensor data from IoT devices is required. This suggests that we can use the proces data for sensor operation, analysis, and control. The processed data has been fully processed.

(b) Discreet: The data is handled, managed, or sent to the receiver without being processed beforehand. Certain IoT devices must transmit sensor data instantly and respond to it. for instance, patient-related data from the sensor. It's crucial that information is sent right away if a patient's heart delivers abnormal readings. (Fig.5).

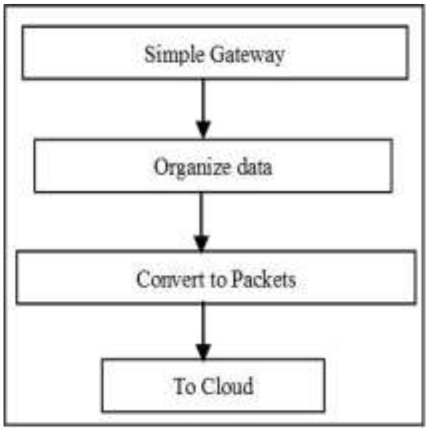


Figure 3: Simple Interface

Data management regulates data entry, fusion, power, and data flows. Figure 4 illustrates the Operations Support Framework. A common business model is data abstraction. There are a tonne of details. Therefore, it is essential to think carefully about taking a close look at your data.

2.4 Service Layer

The standardised IoT system's last element is the service subsystem. The saved data from the previous level will be transferred to this level. This component offers services to clients and final users. IoT can be used in almost every industry. The requests are grouped into two main categories.

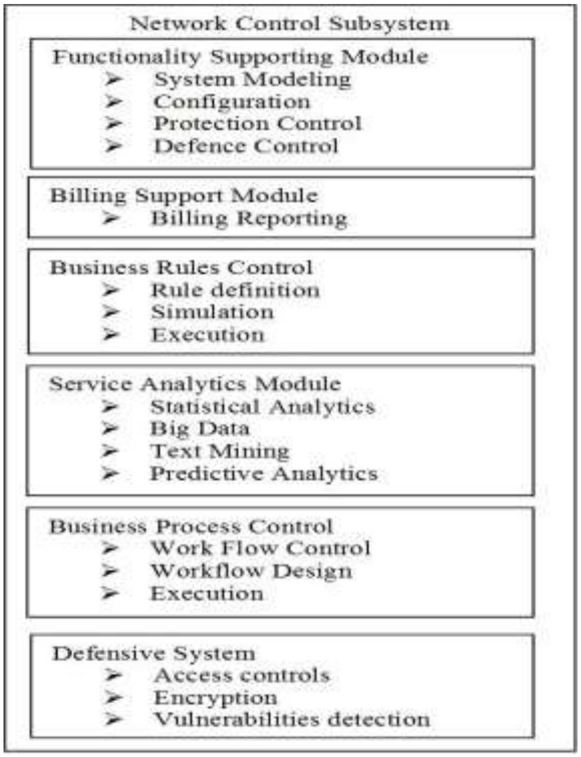


Figure 4: Network Control Subsystem

2.4.1 Partition Based Applications

IoT will have a positive impact on a variety of industries, including transportation, healthcare, business, power, and military services. IoT sensors may be used to monitor the effects of temperature alteration in various city settings. They techniques may be used to examine many aspects of the surrounding ecosystems, including the aquatic environment, the lithosphere, the sun, plants, etc. This mission makes use of a variety of sensors. All vehicles may communicate with one another on the road by being connected to IoT systems. The owner could have access to all car information. IoT-enabled medical devices will be utilised to safeguard patient safe. The evaluation of doctors will benefit as well. Smarter Plant may be an example of IoT in the retail sector. Skills like connected customers and sales forecasting are present in smart stores.

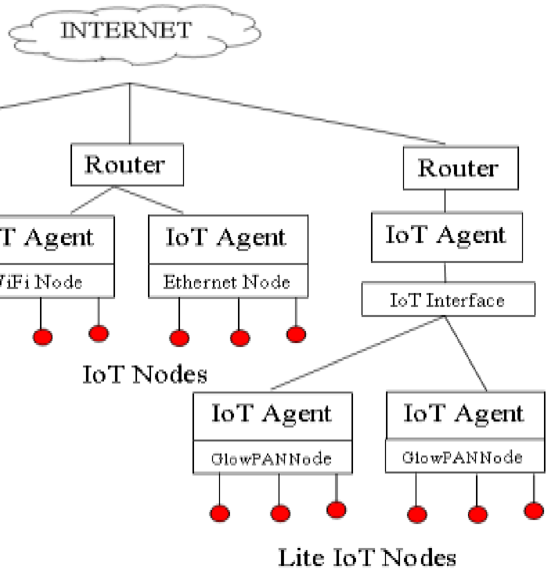


Figure 5: IOT Design Interface

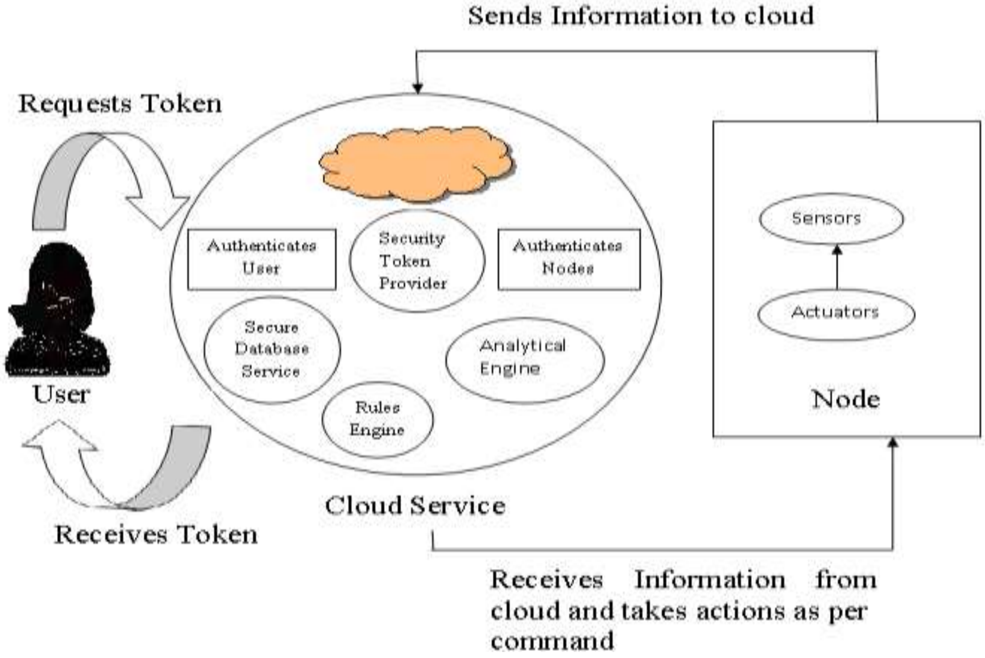


Figure 6: Cloud Service Architecture

Table 1: Implementation areas of Service layer

Home surveillance system powered by	Connection to the World Wide Web (WWW), entertainment

IoT based Smart cities	Urban management, resource management, transportation management, and crisis management.
IoT based Farming	Moisture detection, field detection, violations, water requirement warnings, and smoke detection.
Intelligent Transportation System	GPS services, smart device technology, smart vehicle technologies, and road traffic conditions are all examples of smart devices.
IoT for Smart energy Systems	Fluid level indication and refinery

2.4.2 Utilizing a horizontal marketing system, IoT applications

In this chapter, IOT is discussed in relation to citizen recording and surveillance, inventory control, commercial logistics management, and flood control. (Table 1).

3. SECURITY CONCERNS

The main issue here isn't web services; IoT devices may be utilised everywhere, in your home, car, or office, just by collecting your data and keeping an eye on things. But here, safety cannot be compromised. that if any of a computer's nodes or a sensor's nodes is compromised, it might mark a turning point for this industry. Consider a home security camera as an example. Both the server and portable devices received the acoustic and visual data.

Any of these places might have their data compromised. Not only can they view the contents of my camera, but if they can guess the passwords, they can also automatically access the camera without our knowledge. Therefore, developers must examine every second in order to construct trustworthy IoT systems. The user must have the ability to both approve and revoke special grants for entities, apps, and other devices. Additionally, the owner, those people, applications, and computers need to be verified. Every customer's information must be logged on sophisticated servers and computers, and most importantly, it must be possible to exchange information safely. In case of an issue, the systems should be repairable, fixable, and rectifiable [5].

Let's talk about the IoT use for smart homes. After providing your personal information to the virtual server, you will be given a secret code issued by the server. Additionally, a member of your network gathers the secret code. The secret code to your house is now visible on the virtual server, and you may now handle your computers and equipment. However, if a stranger or attacker breaks into the smart home or if he somehow obtains your secret code, he will take control of the property. But if a secret code is given to a reliable party, it implies that you believe in this system as well. Additionally, it gives confidence as to whether or not harmful malware has been installed on the machine. This system will request that since it currently has malware installed.

Additionally, it is recommended to use any kind of end-to-end authentication and cryptography model for all of your dependable transmission processes [5] and to not actually believe the other devices in the IoT network. Everyone is aware of and warned against using an unsecured or untrusted connection to another individual. However, if a hacker performs the right approach, he may publish a webpage from a bogus URL to release ransomware. An example would be a java runtime attack that could be loaded and mounted on a website without you knowing what was happening. Therefore, by using authentication encryption on computers, we can stop these assaults.

Even this threat's impact can be lessened. Ad blockers should be used because they prevent dangerous adverts from being shown on web browsers. It is protected from assaults like ransomware and identity theft by a browser. Your device will be disrupted and your credentials will be stolen. Client side programmes like Google Chrome develop "Sandboxing" features that increase client security. Every website we launch requires a separate browser operation. The opening of a new window or tab in the browser is a distinct action. The other tabs won't be impacted if one of them experiences issues or fails. Thus, sandboxing adds a protective layer to each of these systems. If you unintentionally open a hazardous door

We have firewall and antivirus settings for privacy on the laptops and desktop computers we use, but IOT does not. Successful websites like Youtube and other platforms have been offline for almost a day as a result of the DDOS attack [6]. These portals give users access to materials for service registration and use. The website server breaks when it receives an overwhelming amount of queries or fake visitors flood the site. It is a DOS attack. It's interesting that this assault didn't start on the computers, but rather on Internet of Things (IoT) devices like a security camera and some storage that were linked to the network. Let's use "Mirai" as an example of one of these malwares. Mirai

A cascade of Network Denial of Service assaults [6] hit a number of social media websites, including Facebook, Amazon Video, Youtube, and The New York Times. The 10/21 assaults have caused extremely high levels of congestion on the workstations that were targeted. A company called "Dyn" served as the mainstay of these workstations. DNS services are provided by the company to the other companies. This problem happened because there are so many internet-connected devices and there was no security. Due to default login credentials, DDOS enabler attacks have been made available. Cyberthreats and their evolution are displayed in Table 2. The intelligent systems are connected to Wi-Fi microcontrollers or spread spectrum wireless technology that uses frequency hopping. Either Linux or Real Time Operating Devices power these embedded systems.

of things is unquestionably a serious issue. Organizations that create should be concerned about the safety and security of these devices.

Table 2: IT Threats and its Progression.

Period	**Threats**
1985-97	Crackers, Phreaking on phones.
1997–05	Mail bomb Spyware, Malwares, Worms and Worms, Vines, Polymorphic bugs, Fake account generator.
2005–08	Spear phishing, corporate and governmental espionage, and denial-of-service
2008–11	harmful SQL code vulnerabilities, cyberwarfare, and destructive assaults.
2011–15	indiscriminate assaults, stealing login passwords, email addresses, financial information, and medical information.
2015-till date	Zero-day attacks, phishing emails, man-in-the-middle assaults, cryptojacking,

	poisoning of machine learning, Angular template injection, ransomware, Telegram hijacking, etc. Numerous more attacks are developing.

4. SOLUTIONS

IoT protection, which was formerly taken for granted, is now a very serious issue [1, 2].

Authentication: Cryptosystem [10] certificates will indicate that the machines are the proper ones and that the people identified by the certificates are who they say they are. With a default password set, no scheme can be the same on machines all over the world. The systems or apps created utilising IoT should have strong login credentials with a combination of lower- and upper-case letters, numbers, and special characters. This suggests that the only person who can log in is the authorised user.

Data Protection: To ensure data protection on computers, computational security procedures [11] to be put into practise. To maintain anonymity, no private information is instantly available.

Availability entails ensuring that the data is easily accessible when needed and that IT devices become correct.

Cryptography: Any web-based gateway can be protected from intrusion using efficient security protocols like Secure Sockets Layer/Transport Layer Security [12] and many others.

Threats to Websites: Malicious scripts and techniques, such as SQL code vulnerability attacks and client-side code injection attacks, can be used to target web interfaces and apps [13].
Additionally, it is necessary to protect websites against such assaults.

System Software Upgrade: Malicious programmes and viruses are obtrusive. Security flaws [14] pose a hazard to defence. Therefore, all IoT-based smart apps must support wireless internet connection updates. Before putting these changes into place, they should be evaluated. Therefore, if a privacy issue is found, computers can be updated and security flaws can be closed [15].

Privacy Protection The information cannot be updated while the aircraft is in flight in the interest of protecting privacy [16]. Computational encoding can then be used to guarantee this. It suggests that the data used in IT applications are trustworthy.

According to a Hewlett Packard study, "70% of IOT systems are vulnerable to threats." [17]

Machine Learning for IoT Security: Machine learning (ML) and deep learning (DL) approaches are being used increasingly often to secure IoT systems [20]. In order to train and construct Frameworks for supervised and unsupervised learning dependable and adaptable to a range of security frameworks and implementation settings, these approaches call for the generation and processing of enormous amounts of security data. Various machine learning (ML) and artificial intelligence (AI) techniques are now being applied in the IoT security industry. Recent developments have seen the introduction of many IoT infrastructures, including Wireless Sensor Networks (WSN) and smart grids, as well as various risks, including the detection of malicious software and penetration. There have also been used for a number of learning strategies, including DL and reinforcement learning. ML and DL techniques for spotting,

IoT frameworks built on the Software Defined Networking (SDN) protocol:

A network-level security strategy is recommended by studies in [21] to safeguard IoT devices. The protected system employs a secure channel that can identify different kinds of networked devices. The gadget also uses mitigation techniques to get rid of potential hazards. ML approaches are used to categorise a system as susceptible or unvulnerable. Recognition of the device type and information from vulnerability databases are given into a machine learning (ML) system that can forecast unsafe network nodes. Due to the network's widespread visibility, such methods are practical for brainy bionetworks that have the ability to make physical level decisions. The need for SDN-based IoT deployment is being supplemented by a number of proofs of concepts because SDN is a growing outline that isn't existence used to its full potential.

IoT security using FOG Computing:

Further down, we discuss the solutions that fog computing provides or may give to mitigate particular possible dangers.

Man-in-the-middle attack: Fog acts as a layer of protection between the user and the cloud or IoT device. IoT system vulnerabilities or intrusions must travel via the central fog layer, which can identify and reduce suspicious activity before it reaches the device.

1. **Data Transit attack:** Data management and collection on steady fog nodes are noticeably better than on IoT systems. Information is better protected when it is stored on fog nodes rather than end-user PCs. Information about users is also easier to get because to fog nodes.
2. **Eavesdropping:** Fog nodes only enable interaction between the end-user and the fog node, not route discovery throughout the entire infrastructure. Because there is little network activity, there is very little chance
3. **Constraints with IoT devices:**

   The majority of IoT devices have limited resources. which adversaries fully exploit. They try to destroy the IoT gadgets and utilise them as entry points by smashing them. Fog nodes can help IoT devices and shield them from such threats. A nearby fog node can carry out the far more intricate security actions required for safety.

Blockchain for IoT Security:

Blockchain is a potent, secure, decentralised, and open data foundation for IoT data. Blockchain technology is useful in IoT systems for a number of reasons. Table 3 lists a number of fundamental IoT security problems along with potential blockchain solutions. The key benefits of utilising blockchain in IoT systems are discussed in the sections that follow.

(1) IoT data may be archived using blockchain technology.

(2) The decentralised nature of blockchain enables secure data storage.

(3) Data is encrypted using the hash key, which is subsequently verified by miners.

(4) Attacks including impersonation, data loss, and security breaches are prevented.

(5) Using blockchain technology to prevent unapproved access.

(6) There is no longer a need for centralised cloud servers.

Table3: Block chain responses to IoT security issues

IoT	**BlockChain Solution**

Challenges	
Secrecy	Permissioned Blockchain
Circulation and price	Decentralized Block chain
Weighty Load	Records updation on network nodes.
Defective Architecture	Confirming the statistics cryptography

5. CONCLUSION

IoT will revolutionise the yet, if engineers don't focus on IoT protection, customer confidence in the security of IoT systems won't grow. IoT schemes may be protected against cyber threats with the use of measures that can be implemented. Data protection for people should be given importance, & data be seriously safeguarded.

REFERENCES

[1] Almolhis, N., Alashjaee, A. M., Duraibi, S., Alqahtani, F., & Moussa, A. N. (2020, February). The Security Issues in IoT-Cloud: A Review. In 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA) (pp. 191-196). IEEE.

[2] Swamy, S. N., & Kota, S. R. (2020). An Empirical Study on System Level Aspects of Internet of Things (IoT). IEEE Access, 8, 188082-188134.

[3] Sokolov, S. S., Alimov, O. M., Nekrashevich, P. S., Moiseev, A. I., & Degtyarev, A. V. (2020, January). Security Issues and IoT Integration for in Russian Industry. In 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 517-520). IEEE.

[4] Hasan, T., Adnan, A., Giannetsos, T., & Malik, J. (2020, June). Orchestrating SDN Control Plane towards Enhanced IoT Security. In 2020 6th IEEE Conference on Network Softwarization (NetSoft) (pp. 457-464). IEEE.

[5] Duangphasuk, S., Duangphasuk, P., & Thammarat, C. (2020, June). Review of Internet of Things (IoT): Security Issue and Solution. In 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 559-562). IEEE.

[6] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet of Things Journal.

[7] Das, S., Mohanta, B. K., & Jena, D. (2020, March). IoT Commercial Drone and It's Privacy and Security Issues. In 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA) (pp. 1-4). IEEE.

[8] Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge computing-assisted internet of things. IEEE Internet of Things Journal.

[9] Singh, S., Singh, K., & Saxena, A. (2020, October). Security Domain, Threats, Privacy issues in the Internet of Things (I oT): A Survey. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 287-294). IEEE.

[10] Portal, G., de Matos, E., & Hessel, F. (2020, June). An Edge Decentralized Security Architecture for Industrial IoT Applications. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[11] Niraja, K. S., & Rao, S. S. (2020, January). Security Challenges and Counter Measures in Internet of Things. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-3). IEEE.

[12] Li, Y., Li, Y., & Liu, J. (2020, August). Discussion on Privacy Issues and Information Security in the Internet of Things. In 2020 Chinese Control And Decision Conference (CCDC) (pp. 4968-4972). IEEE.

[13] Anwar, R. W., Zainal, A., Abdullah, T., & Iqbal, S. (2020, April). Security Threats and Challenges to IoT and its Applications: A Review. In 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 301-305). IEEE.

[14] Anwer, M., & Ashfaque, A. (2020, February). Security of IoT Using Block chain: A Review. In 2020 International Conference on Information Science and Communication Technology (ICISCT) (pp. 1-5). IEEE.

[15] de Oliveira Conceição, C. M., & da Luz Reis, R. A. (2020, June). Security Issues in the Design of Chips for IoT. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-5). IEEE.

[16] Khursheeed, F., Sami-Ud-Din, M., Sumra, I. A., & Safder, M. (2020, February). A Review of Security Machanism in internet of Things (IoT). In 2020 3rd International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-9). IEEE.

[17] Sharma, P., Kherajani, M., Jain, D., & Patel, D. (2020, February). A Study of Routing Protocols, Security Issues and Attacks in Network Layer of Internet of Things Framework. In 2nd International Conference on Data, Engineering and Applications (IDEA) (pp. 1-6). IEEE.

[18] Abuladel, A., & Bamasag, O. (2020, March). Data and Location Privacy Issues in IoT Applications. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE.

[19] Zaldivar, D., Lo'ai, A. T., & Muheidat, F. (2020, January). Investigating the Security Threats on Networked Medical Devices. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0488-0493). IEEE.

[20] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke and N. Kefalakis, "Scalable and Configurable End-to-End Collection and Analysis of IoT Security Data : Towards End-to-End Security in IoT Systems," 2019 Global IoT Summit (GIoTS), 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766407.

[21] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[22]. Fox, G.C.; Kamburugamuve, S.; Hartman, R.D. Architecture and measured characteristics of a cloud based internet of things. In Proceedings of the International

Conference on Collaboration Technologies and Systems(CTS), Denver, CO, USA, 21–25 May 2012; pp. 12.

[23]. Chang, H.; Hari, A.; Mukherjee, S.; Lakshman, T.V. Bringing the cloud to the edge. In Proceedings of the IEEE Conference on Computer Communication.

Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 27 April–2 May 2014; pp. 346–351.

[24]. Ponte: Connecting Things to Developers. Available online: http://www.eclipse.org/ponte/ (accessed on 12 September 2016).

[25]. Kura: OSGI-Based Application Framework for M2M Service Gateways. Available online: http://www. eclipse.org/proposals/technology.kura (accessed on 12 September 2016).

[26] P Ramprakash, M Sakthivadivel, N Krishnaraj, J Ramprasath. "Host-based Intrusion Detection System using Sequence of System Calls" International Journal of Engineering and Management Research, Vandana Publications, Volume 4, Issue 2, 241-247, 2014

[27] N Krishnaraj, S Smys."A multihoming ACO-MDV routing for maximum power efficiency in an IoT environment" Wireless Personal Communications 109 (1), 243-256, 2019.

[28] N Krishnaraj, R Bhuvanesh Kumar, D Rajeshwar, T Sanjay Kumar, Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks, 2020 International Conference on Inventive Computation Technologies (ICICT),201-204

[29] Ibrahim, S. Jafar Ali, and M. Thangamani. "Enhanced singular value decomposition for prediction of drugs and diseases with hepatocellular carcinoma based on multi-source bat algorithm based random walk." Measurement 141 (2019): 176-183. https://doi.org/10.1016/j.measurement.2019.02.056

[30] Ibrahim, Jafar Ali S., S. Rajasekar, Varsha, M. Karunakaran, K. Kasirajan, Kalyan NS Chakravarthy, V. Kumar, and K. J. Kaur. "Recent advances in performance and effect of Zr doping with ZnO thin film sensor in ammonia vapour sensing." GLOBAL NEST JOURNAL 23, no. 4 (2021): 526-531. https://doi.org/10.30955/gnj.004020 , https://journal.gnest.org/publication/gnest_04020

[31] N.S. Kalyan Chakravarthy, B. Karthikeyan, K. Alhaf Malik, D.Bujji Babbu,. K. Nithya S.Jafar Ali Ibrahim , Survey of Cooperative Routing Algorithms in Wireless Sensor Networks, Journal of Annals of the Romanian Society for Cell Biology ,5316-5320, 2021

[32] Rajmohan, G, Chinnappan, CV, John William, AD, Chandrakrishan Balakrishnan, S, Anand Muthu, B, Manogaran, G. Revamping land coverage analysis using aerial satellite image mapping. Trans Emerging Tel Tech. 2021; 32:e3927. https://doi.org/10.1002/ett.3927

[33] Vignesh, C.C., Sivaparthipan, C.B., Daniel, J.A. et al. Adjacent Node based Energetic Association Factor Routing Protocol in Wireless Sensor Networks. Wireless Pers Commun 119, 3255–3270 (2021). https://doi.org/10.1007/s11277-021-08397-0.

[34] C Chandru Vignesh, S Karthik, Predicting the position of adjacent nodes with QoS in mobile ad hoc networks, Journal of Multimedia Tools and Applications, Springer US,Vol 79, 8445-8457,2020