International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Difficulties with Internet of Things Security

Suraj Raj, SCSE, Galgotias University, Greater Noida,India

Rohit Raj, SCSE, Galgotias University, Greater Noida,India

Abstract:

Internet of Things is one of the most important things which is used in our dailey life styles. The internet of effects offers several benefits to associations, some benefits are assiduity-specific, and some are applicable across multiple diligence. It's also used in smart metropolises like roads, hospitals and in smart homes like controlling door or air conditioner unit or precluding fires and much further. The connectivity, networking and communication protocols used with these web- enabled bias largely depend on the specific IoT operations stationed. These bias that use IoT are connected to the internet and shoot and admit numerous of important data through thenetwork.This opens the bushwhacker's starvation to foray the IoT networks and got its precious data. The problem with the IoT bias is the limited performance factors that make it delicate to apply the being security system on it. This limitation requires a need to present featherlight algorithms which support the IoT bias. The check in this paper reviewed several proposed algorithms and authentication styles in IoT to stop numerous kinds of attacks with considering the limitation of the IoT system.

1.Introduction

Simultaneously, with billions of IoT gadgets, applications, and administrations currently being used, and more noteworthy numbers coming on the web, IoT security is of most extreme significance. Ineffectively got IoT gadgets and administrations can act as passage focuses on the cyberattacks,and compromising touchy information leaks,use as weaponizing information, and undermining the details of the wellbeing of a clients.

This types of dangers and prizes are by and large painstakingly viewed as by numerous state run administrations and worldwide associations. Notwithstanding, In the Internet's worldwide and their effect, that is important for its security be tended to cooperatively. For that reason the branch of the Canadian Multistakeholder Process: Enhancing IoT Security drive was sent off.

Recognizing the complexity of mitigating digital protection gambling from the global expansion of IoT and the subsequent need for Canadian-made strategies to address these risks, the Internet community has joined Innovation, Science and Economic Development (ISED).Working with the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Cleaner CIPPIC and CANARIE have adopted a deliberate multi-stakeholder process for a wide range of improvements leading up to proposals for upgrading Canada's IoT security.

This initiative brought together a multistakeholder group, recruited from the Canadian Internet user community, to explore the size of the challenges and also the range of possible solutions that would be pursued further to deal with them, guided by the subsequent standards:

The complexity of IoT security necessitates a bottom-up, natural cycle to make sure the solutions address all existing and anticipated problems. [1] The technique must be flexible and may be defined and improved through discussion with partners.
Long-term IoT security improvements rely on universally orchestrated specialised principles, but they're challenging to implement and take time. IoT security solutions should logically start at the general public level while cooperating with other governmental, provincial, and international entities.

It is crucial to start working on educating consumers and for organisations to start embracing best practises that will reduce the risks of consumer IoT device reception due to the rapidity of the risks and the lengthy time span of long-term advancements, such as upgrades to system strategies and the improvement of global norms.
In this particular instance, the emphasis was placed on consumer-level devices rather than those that are utilised at the venture level. The Enhancing IoT Security multistakeholder group participated in a series of in-person multistakeholder gatherings, centre events, online classes, and directed research between mid-2018 and mid-2019 to encourage the following:

an organisation of criteria and standards for the security of devices connected to the Internet.
shared guidelines to ensure the security of devices connected to the Internet over the course of their lifetime, including the decision-making, assembly, correspondences, and executive activities.
proposals to clarify Canadian public policy around IoT security.
The use of the multistakeholder approach in its association, administration, and direction was a distinguishing feature of the Canadian Multistakeholder Process: Enhancing IoT Security drive. The Oversight Committee and the Internet Society provided oversight and guidance, and they served as the executives. The role the multistakeholder model played in this effort is examined in reference section II, which also frames the cycle's most important lessons.

To clarify the cycle and encourage specific proposals, three thematic working groups—Network Resilience, Device Labeling, and Consumer Education and Awareness—were set up. These Working Groups' recommendations address the specialised, strategic, and societal facets of IoT security.

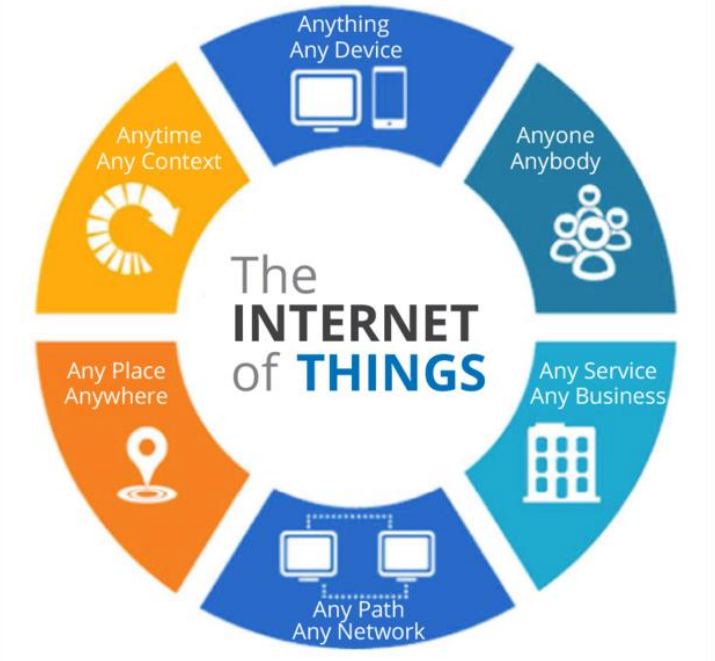

Fig. 1. Definition of IoT.

2.Problem faces in securtiy issue in iot

1. Erroneous access control

Administrations presented by an IoT gadget ought to be open by the proprietor and individuals in their nearby climate whom they trust. Notwithstanding, this is many times inadequately upheld by the security arrangement of a gadget.

IoT gadgets might trust the neighborhood organization to such even out that no further validation or authorization is required. Another gadget that is associated with a similar organization is likewise trusted. This is particularly an issue when the gadget is associated with the Internet: everybody on the planet can now possibly get to the usefulness presented by the gadget.

A typical issue is that all gadgets of a similar model are conveyed with a similar default secret word (for example "administrator" or "password123"). The firmware and default settings are typically indistinguishable for all gadgets of a similar model. Since the certifications for the gadget - expecting to be that, as is much of the time the case, they are not changed by the client - are public information, they can be utilized to get close enough to all gadgets in that series.

IoT gadgets frequently have a solitary record or honor level, both presented to the client and inside. This implies that when this honor is gotten, there could be no further access control. This single degree of assurance neglects to safeguard against a few weaknesses.

2. Excessively enormous assault surface

Every association that can be made to a framework gives another arrangement of chances for an aggressor to find and take advantage of weaknesses. The more administrations a gadget offers over the Internet, the more administrations can be gone after. This is known as the assault surface. Lessening the assault surface is perhaps the earliest move toward the most common way of getting a framework.

A gadget might have open ports with administrations running that are not rigorously needed for the activity. An assault against such a superfluous help could without much of a stretch be forestalled by not uncovering the help. Administrations like Telnet, SSH or a troubleshoot connection point might assume a significant part during improvement yet are seldom essential underway.

3. Obsolete programming

As weaknesses in programming are found and settled, it is vital to circulate the refreshed adaptation to safeguard against the weakness. This implies that IoT gadgets should transport with cutting-edge programming with practically no known weaknesses and that they should have updated usefulness to fix any weaknesses that become known after the organization of the gadget.

For instance, the malware Linux. Darlloz was first found in late 2013 and worked by taking advantage of a bug detailed and fixed over a year sooner.

4. Absence of encryption

At the point when a gadget conveys in plain text, all data being traded with a client gadget or backend administration can be gotten by a 'Man-in-the-Middle' (MitM). Any individual who is equipped for getting a situation on the organization way between a gadget and its endpoint can investigate the organization traffic and

possibly get touchy information, for example, login certifications. An ordinary issue in this class is utilizing a plain-text variant of a convention (for example HTTP) where an encoded form is accessible (HTTPS). A Man-in-the-Middle assault where the assailant furtively gets to, and afterward transfers correspondences, conceivably modifying this correspondence, without either party staying alert.

In any event, when information is encoded, shortcomings might be available on the off chance that the encryption is unfinished or arranged mistakenly. For instance, a gadget might neglect to check the realness of the other party. Even though the association is scrambled, it very well may be captured by a Man-in-the-Middle assailant.

Touchy information that is put away on a gadget (very still) ought to likewise be safeguarded by encryption. Commonplace shortcomings are the absence of encryption by putting away API tokens or qualifications in plain text on a gadget. Different issues are the use of feeble cryptographic calculations or involving cryptographic calculations in accidental ways.

f their gadgets by making it simple to safely arrange them. By concentrating entirely on convenience, plan, and documentation, clients can be pushed into arranging secure settings.

There is an incomplete cross-over between this classification and different classes recorded previously. For instance, the issue of mistaken admittance control referenced above incorporates utilizing perilous or default passwords. One method for tackling this is to make the client cooperate with the gadget to such an extent that it is extremely simple or even required to design a solid secret phrase.

For the majority of the above security classes, it is hard for a non-specialized client to assess whether a gadget meets the necessity. Nonetheless, client cooperation can, by definition, be seen toward the end client, thus the purchaser can assess how well a gadget performs on client collaboration.

Client association is a significant class to ensure executed safety efforts are initiated and accurately utilized. Assuming that it is feasible to change the default secret key, yet the client doesn't have the foggiest idea or can't find the usefulness, it is futile.

3.Ways To Solve IoT Vulnerabilities
And Protect Your IoT Device:

1. Change watchwords frequently And Make Them Strong

Evolving Watchwords, constantly, on web records, PCs and cell phones is a standard these days. At this point, it ought to likewise turn into a standard for Internet of effects units.
You ought to continuously take care of any outstanding enterprises and insure that
• Each IoT contrivance has a special secret word
• You change these watchwords principally a many times each time
• Keep down from normal and conventional watchwords
• Make these watchwords exceptionally mind boggling and violent to break
You can depend on secret crucial administrators to recall them for you, yet as that also can be addressed, a customary fashion for recording watchwords on a piece of paper is your sure thing.

2. Try not to Calculate On Cloud Technology

Pall invention is extremely helpful without a mistrustfulness, yet it's likewise a veritably weak arising invention inclined to assaults.
IoT directors for the utmost part furnish distributed storehouse space with each contrivance you buy. And keeping in mind that it's tempting to use commodity that comes for nothing, suppose about that

• You really want a performing association with access information and documents put down in the pall
• This association can be addressed into while you are getting to your pall account
Help yourself out and go through protection estimates that accompany your pall account fully. also, insure you secure your date or, far superior, store your documents and information locally, where they are past the range of fraudsters.
More deeply study the kinds of pall administrations.

3. Keep down from Universal Plug and Play Features

All inclusive Plug and Play point, that a lesser part of IoT units have, makes it workable for multitudinous widgets to interface with one another. This implies you do not have to arrange each contrivance each alone.
Albeit this gives an inarguable accommodation to Internet of effects natural system in your home or working space, be careful about that
• All inclusive Plug and Play conventions use near associations for associating
• These associations, as we have seen, are veritably inclined to outside assaults and can be painlessly gotten to
• Assuming that the assault occurs, it could impact multitudinous IoT widgets by raiders getting to them from a distance
Switching off the Plug and Play on Internet of effects widgets would give you tranquility of see any problems in similar manner.

4. use Secondary Network

WiFi guests constantly make colorful associations that incorporate one with access confined to themselves and their families.
This methodology of creating an redundant association can be applied to IoT widgets, as it serves to
• Forestall unapproved entrance to your nonpublic records
• Stop any trials of seizing IoT units and executing malware
• Completely place the IoT contrivance past the range of any external element, securing decoded information

5. Update Your IoT Device Regularly

As we have examined in the part about an absence of updates as one of IoT security issues, programmed refreshes should be set up to check for true updates by the contrivance patron.
This introduces security patches on your device(s) and prevents programmers from exercising new approaches to interposing them.
Customary IoT programming refreshes ultimately give
• Good in realizing that your fabrics are refreshed with the most recent safety sweats that can avert the freshest types of assaults
• A further elevated position of safety for your home or office overall
The Future Of Internet Of effects Security How Will IoT Evolve In 2020?
Web of effects security enterprises are the subject of examination inside the factual business as well as a section of the scholarly world that perceives and concentrates on the implicit these fabrics have.

In 2020, an ever adding number of trials will understand the capability of IoT as the business adventure will represent over half of the in general IoT spend in 2020. This suggests that makers should try harder with network protection to measure up to commercial hypotheticals.

The typical guests should do their part as well, by tutoring themselves and eventually depend on speed with IoT security developments and their significance.

As utmost advances, this bone also starts with coordinated trials on a further elevated position. In March 2019, the US Congress presented a pall network protection charge whose design was to make IoT units bought by the public authority accompany principally least security measures.

A many makers are now offering IoT particulars with implanted security. Likewise, remote correspondence and data handling are being bettered with specific streamlining ways, for illustration,

- Arched advancement
- Heuristic ways
- AI
- fake brain associations
- Transformative computations
- Cross types of AI and other enhancement strategies

We can likewise anticipate a development of assiduity- unequivocal fields of IoT security exploration that might concentrate and deliver enhancement in

- Start to finish frame security models
- Secure distributed computing in IoT
- IoT plan and prosecution security and protection issues
- Anticipation of assaults on IoT fabrics and position of interruption in view of AI
- Secure IoT fabrics design
- Protection of information and styles of IoT contrivance security

Action particulars On IoT Security Issues

The content of IoT security issues is extremely complicated. Implicit uprightness breaks can crop out of a many, completely unconnected sources. likewise, on the grounds that this invention is basically still in its early stages, the two guests and makers are as yet looking for the right arrangements.

We've seen that Internet of effects security difficulties can appear from

- Malware assaults and the seizing of widgets
- Unfortunate customer skill because of absence of awareness
- Absence of true updates
- crooked morals in assembling
- revolutionary IoT widgets

Fortunately, a many estimates guests can fall back on to limit the effect of terrible security are

- Keeping IoT network separate from the rest
- Staying down from Plug and Play highlights
- Not exercising distributed storehouse

4. IOT operations

The abecedarian pretensions of IoT devices are the design for a climate and reluctant free widgets like expertise abiding, shrewd effects, brilliant good, and shrewd civic communities among othersThe uses of the uses of IoT in businesses, clinical & medical field, and in everyone home robotization are examined about the accompanying member.

A. IoT in diligence-

The IoT have given a right an open door to construct critical ultramodern fabrics and operations(6) in a smart IoT transportation frame, the approved existent can screen the current area and development of a vehicle. The approved existent can likewise prevision its unborn area and roadtraffic.The acknowledgment and administrations of new IoT advances primarily calculate on the protection of information and security of data. The IoT licenses multitudinous effects to be associated, followed and checked so significant data and nonpublic information gathered accordingly. Since there are so many attacks on IoT, security is a more basic concern in the IoT environment compared to conventional relationships.

B. Bias with IoT in Personal Medical

The IoT widgets are frequently used in medical care settings to assess and check on patients. Personal Medical Biases (PMDs), which are furthermore established in cases' bodies or may link to cases' bodies at any time, are used to screen for diseases in instances. PMDs are tiny electrical devices that are becoming both well-known and extremely common. On account of medical care, the essential ideal is to guarantee the security of association to keep the protection of case from noxious assaults. At the point when raiders assault cell phones, they've their predefined objects. generally, their point is to take the data, assault on widgets to use their means, or may close down certain operations that are observing cases condition.

There are numerous kinds of assaults on clinical widgets that incorporate snoopping in which security of the case is revealed, uprightness boob

in this type of the communication is being modified, and availability issues which incorporate battery depleting assaults. Some of the network protection troubles connected with security, protection, and good of clinical information of case are examined as follows about that :

1) PMDs are the starting point for any battery-powered project. Consequently, these widgets ought to support a specified encryption. Bracket, availability, protection, and responsibility will be at high risk if the scheme is a component of vivid associations.

2) Since there is no remote correspondence verification system for PMDs. So that unapproved individuals might easily access the data stored in the device.

3) Lack of safe proof exposes the widgets to numerous other security issues that could lead to nocturnal attacks. A hostile party might use Denial of Service (DoS) attacks.

4) The distribution of case information across a medium that could be altered by unauthorised parties makes case protection potentially risky.

C. IoT in Smart Home

The IoT smart home administrations are continuously growing, and cutting-edge widgets can now communicate with one another using IP addresses. In a smart home environment, every clever home accessory is linked to the internet. The likelihood of nocturnal pursuits increases as the volume of widgets rises in the astute domestic environment. Assuming smart home widgets are worked autonomously the possibilities of nasty goes after also diminishes. As of now brilliant home widgets can be gotten to through the web wherever whenever. In this way, it expands the possibilities of nasty assaults on these widgets. A smart home comprises of four sections administration stage, shrewd widgets, home hall, and home.

A smart home comprises of four sections administration stage, brilliant widgets, home passage, and home association. In the smart home, multitudinous widgets are associated likewise, keenly shares data exercising a home association. latterly, there exists a home door that controls the sluice of data among shrewd widgets associated with the outside network. Administration stage utilizes the administrations of specialist association that convey colorful administrations to the home association.

5. Analysis of various attack types and potential outcomes

The IoT is resisting many attacks, such as dynamic and idle attacks that could effectively disrupt the utility and reduce the benefits of its administrations. A gatecrasher simply faculties the target in a detached assault or may collect the information, but it never actually proceeds. However, the rapid assaults actually disrupted the exhibition. Interior attacks and exterior assaults are the two further classes into which these dynamic assaults are arranged. Similar weak attacks can stop the widgets from conducting themselves keenly. Later, security restrictions should be implemented to protect widgets from retaliatory attacks. This member discusses the striking feathers of assault, the nature/conduct of assault, and the danger zone of assaults. According to how they are carried out, different degrees of assaults are divided into four categories, which offer implicit remedies for problematic assaults.

1) Attack from a low position If a bushwhacker tries to attack a group and his attack is unsuccessful.

2) Attack from a medium posture The fact that a gatecrasher, bushwhacker, or buttinsky is only observing the medium has no bearing on the veracity of the information.

3) High-level attack When an association is attacked, the information may change or be adjusted, depending on who is responsible.

4) Attack from a really high position If a gatecrasher or raider violates the terms of the association by gaining unauthorised entry and carrying out an illegal act, rendering the organisation unreachable, sending out mass mailings, or harming the association.

6.CONCLUSION

The primary focus of this article was to highlight key security challenges, with an emphasis on security assaults and their defences. Numerous IoT widgets become easy prey due to the lack of a safety system, and surprisingly, this is not in the casualty's information on being contaminated.

The security requirements, such as bracket, uprightness, and confirmation, are examined in this study. Twelve different types of assaults—low-position assaults, medium-position assaults, unquestionably substantial position assaults, and veritably significant position assaults—along with their tendency/conduct and suggested responses to experiencing these assaults are discussed in this overview.

Given the importance of security in IoT operations, it is absolutely crucial to integrate security system in IoT widgets and communication relationships. Incorporating dereliction watchwords for the widgets and reading the security criteria for the widgets before engaging them intriguingly is also advised not to, in order to protect

against any gatecrashers or security risk. Injury to the highlights that aren't in use may reduce the likelihood of security attacks. Additionally, it's important to focus on the vibrant security practises used by IoT groups and widgets.

7.REFERENCES:

[1] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.
[2] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.
[3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.
[5] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.

[6] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.
[7] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
[8] A. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
[9] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in iot environment," in Computer Science and its Applications. Springer, 2015, pp. 691–696.
[10] R. H. Weber, "Internet of things–new security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23–30, 2010.
[11] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot),"

in International Conference on Network Security and Applications. Springer, 2010, pp. 420–429.
[12] Y. H. Hwang, "Iot security & privacy: threats and challenges," in Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM, 2015, pp. 1–1.
[13] M. A. Qureshi, A. Aziz, B. Ahmed, A. Khalid, and H. Munir, "Comparative analysis and implementation of efficientdigital image watermarking schemes," International Journal of Computer and Electrical Engineering, vol. 4, no. 4, p. 558, 2012.
[14] M. Abdur Razzaq, R. A. Sheikh, A. Baig, and A. Ahmad, "Digital image security: Fusion of encryption, steganography and watermarking,"
International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 5, 2017.

[15] S. Singh and N. Singh, "Internet of things (iot): Security challenges, business opportunities & reference architecture for e-commerce," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 1577–1581.
[16] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," The Internet Society (ISOC), pp. 1–50, 2015.
[17] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2013.
[18]Surendran, S., Nassef, A., & Beheshti, B. D, "A survey of cryptographic algorithms for IoT devices", In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) , pp. 1-8, 2018.
[19] Roman, R., Zhou, J., & Lopez, J., "On the features and challenges of security and privacy in distributed internet of things", Computer Networks, 57(10), pp. 2266-2279, 2013.
[20] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A., "Security, privacy and trust in Internet of Things: The road ahead", Computer networks, 76, pp. 146-164, 2015.
[21] Andrea, I., Chrysostomou, C., &Hadjichristofi, G., "Internet of Things: Security vulnerabilities and challenges", In 2015 IEEE Symposium on Computers and Communication (ISCC) , pp. 180-187, 2015.
[22] Al-Omary, A., Othman, A., AlSabbagh, H. M., & Al-Rizzo, H. ," Survey of Hardware-based Security support for IoT/CPS Systems", KnE Engineering, 3(7), pp. 52-70, 2018.
[23] Sharaf-Dabbagh, Y., & Saad, W. (2016, June). On the authentication of devices in the Internet of Things. In 2016 IEEE

17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) , pp. 1-3, 2016.
[24]Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., &Ylianttila, "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications", International Journal of Distributed Sensor Networks, 10(7), 357430, pp. 1-14, 2014.

[25] Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., &Kayssi, A. (2016, June). Identity-based authentication scheme for the Internet of Things. In 2016 IEEE Symposium on Computers and Communication (ISCC), pp. 1109-1111, 2016.

[26] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R., "Proposed embedded security framework for internet of things (iot)", In 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace &Electronic Systems Technology (Wireless VITAE), pp. 1-5, 2011.
[27] Pacheco, J., & Hariri, S., "IoT Security Framework for Smart Cyber Infrastructures", 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W). doi:10.1109/fas-w.2016.58, 2016.
[28] Hernández-Ramos, J. L., Moreno, M. V., Bernabé, J. B., Carrillo, D. G., &Skarmeta, A. F., "SAFIR: Secure access framework for IoT-enabled services on smart buildings", Journal of Computer and System Sciences, 81(8), pp. 1452-1463, 2015.
[29] Zhang, C., & Green, R. (2015, April). Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In Proceedings of the 18th Symposium on Communications & Networking, International Society for Computer Simulation, pp. 8-15, 2015.
[30] Shafagh, H., Hithnawi, A., Dröscher, A., Duquennoy, S., & Hu, W. "Poster: Towards encrypted query processing for the Internet of Things", In Proceedings of the 21st annual international conference on mobile computing and networking, ACM, pp. 251-253, 2015.
[31]Yoshigoe, K., Dai, W., Abramson, M., & Jacobs, A.

"Overcoming invasion of privacy in smart home environment with synthetic packet injection. In 2015 TRON Symposium (TRONSHOW), IEEE, pp. 1-7, 2015.

[32] Al Salami, S., Baek, J., Salah, K., & Damiani, E., "Lightweight encryption for smart home. In 2016 11th International Conference on Availability, Reliability and Security (ARES), IEEE, pp. 382-388, 2016.