International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Authentication for Unified Software Architecture for Smart Computing IoT devices through Mobile App

Syed Faizan Haider[1], Syed Afzal Murtaza Rizvi[2]

Submitted: 26/05/2023 **Revised**: 04/07/2023 **Accepted**: 26/07/2023

Abstract— IoT devices play a significant part in the connectivity of everything to the internet in this century, making it possible for users to effortlessly access and control their gadgets from a distant location. The primary benefit of using Internet of Things devices is the ability to save time, have remote access to resources at any time and from any location, and have everything linked to the internet. Since its inception, the Internet of Things (IoT) industry has been plagued by a number of problems, most of which are concerned with data protection and security. Confidentiality and integrity both play an important part in the authentication process for security, which is necessary in order to create a robust security system. At this time, Internet of Things protocols also offer various levels of security, all of which are connected in some way to authentication and authorization. However, as time goes on, it will become increasingly important that the level of protection against various attacks, such as masquerade attacks, man-in-the-middle attacks, replay attacks, password guessing Impounder attacks, DoS attacks, and so on, requires more protection at different layers. We used a temperature sensor (DHT22) with Node MCU in this research to investigate security and develop a smart solution. We propagated data over the Internet of Things protocol and received it at the Mobile end. In this study, we examine the safe transmission of data from the Internet of Things devices to mobile devices and highlight the problems we faced and overcame while constructing the prototype. Additionally, we are concentrating on the level of security involved in the transmission of data from the Internet of Things devices to the cloud as well as from the cloud to mobile devices directly, and we are developing a prototype that is capable of operating flawlessly and that propagates data smoothly to the cloud.

Keywords: *IoT, security, Authentication, SSL, IoT devices, IoT Mobile Application.*

1. Introduction

The Internet of Things (IoT) is a technology that is now expanding at a rapid pace, and almost all experts in the relevant fields are of the opinion that IoT will be integrated with everything eventually, leading to a sharp rise in demand [1].

IoT is used in a variety of applications, each of which has its own unique set of obstacles; taken together, these challenges encourage study in the subject of IoT. Common applications include smart cities and smart homes, in which residents may remotely operate their home appliances and monitor their property for signs of prospective burglary. The ability to monitor patients, get real-time health status and prediction information in the field, or make policy choices in pandemic situations are all possible thanks to one of the most important applications of artificial intelligence, which is healthcare. In the military, emergency services may also benefit from the Internet of Things. This can include the remote monitoring of an army personnel's health and whereabouts, the administration and allocation of resources, and reaction preparation, among other things. Other applications of the Internet of Things include crowd monitoring and traffic management, both of which enable intelligent transportation by providing real-time traffic information and optimizing routes; water management encompasses water quality, leakage, usage, distribution, and waste management. The Internet of Things may be used for a variety of applications connected to the environment, including monitoring air pollution, noise, rivers, and even industry [2].

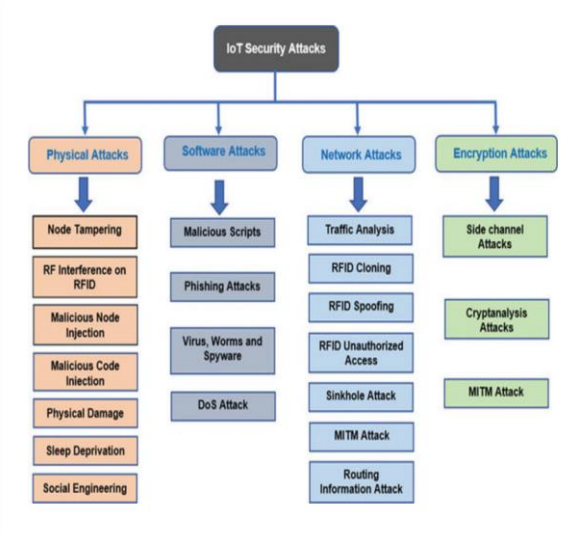

Fig. 1 Various security attacks in the IoT system

The Internet of Things (IoT) is a vision of the future in which everything is connected to one another and controlled

[1]*Department of Computer Science, Jamia Millia Islamia, New Delhi*
[2]*Department of Computer Science, Jamia Millia Islamia, New Delhi*

by means of intelligent gadgets; more precisely, we may utilize IoT technology to exercise control over any object we want. Connectivity to the internet is necessary for all devices that are part of the Internet of Things. People will experience an increase in convenience as well as savings of time as the number of devices connected to the Internet of Things (IoT) increases. In this day and age, if the internet is not operating well, then with the aid of LoRa devices, data may be transferred up to 5 kilometers without the internet [2]. It is a huge step forward in the ability to interconnect devices from the Internet of Things utilizing LoRa in locations that are distant or inaccessible and do not have internet connectivity. Because there are now more linked devices than at any other time in history, it may be challenging for a sector to either specialize in or adopt the Internet of Things (IoT). The security of devices connected to the Internet of Things, data collection, unauthorized access to devices, data hijacking, data manipulation, network penetration, eavesdropping, IoT firmware updates, and other concerns often present themselves as challenges. A lot of specialists in the sector have devised new methods and used technical breakthroughs in order to solve these problems. Over time, gadgets connected to the Internet of Things will also merge with artificial intelligence, which will result in the latter becoming more capable and sophisticated [26]. The Internet of Things is playing an increasingly important part in a variety of fields, including those in which individuals must be physically present in order to manage or monitor various devices. The best example of this would be monitoring machines that are capable of exercising full and remote control over the Internet of Things devices. As we all move from 4G Networks to 5G Networks over the course of time, the Internet of Things will see an exponential surge in demand, production, and consumption over the next few years [3]. Because of this new development, the Internet of Things technologies and the sector that helps support such technologies will get a boost. It is now much easier to carry out AI operations, edge-level data processing, and data management thanks to the high-level AI-based integrated circuits (ICs) that are now being manufactured by the hardware industry.

Devices connected to the internet of things (IoT) might make smart cities and smart houses even more desirable and technologically sophisticated in the future. A lack of Internet of Things technology in the past caused a range of resources to be wasted, but the routines of a smart society assist to improve and protect these resources [6, 7]. The Smart Agriculture system not only helps the crops develop more successfully but also saves the farmer time and money in the process. The use of technologies related to the Internet of Things also leads in higher earnings for a number of different sectors. In spite of the fact that security is the primary concern in every setting in which Internet of Things devices are utilized, the vast majority of customers are blissfully unaware of the potential risks associated with the use of these devices, and as a result, they are content to continue using them. Manufacturers of Internet of Things devices often fail to develop compliances for their products in order to make them secure in line with OWASP criteria. This is typically the case since doing so is not a very cost-effective endeavor. It is of the utmost importance to stick to the guidelines that have been set and to build a secure connection in order to prevent the possibility of any data breaches or hacking of these devices [5].

The format of the paper may be broken down into the following sections, as shown in the following outline: in the second part, we will cover the relevant work that has been done in the topic of Internet of Things security and privacy. The third part gives a description of the recommended model, the fourth section gives an analysis of the experiments, and the last section gives a summary of the research in the form of a conclusion along with some suggestions for the next work that should be done.

2. Related work

A. An acronym for the Internet of Things (IoT)

Certain gadgets are linked to others, and those connections allow for the devices to be directly connected to the Internet and controlled remotely from anywhere in the globe. The Internet of Things creates a new sort of network in which all the gadgets may be linked and managed with relative ease. [10]. Even as technology is adopted by industry and households, the Internet of Things makes it possible for devices to communicate with one another or with other machines in a very smooth manner. This occurs in conjunction with the adoption of other technologies that make the device smart and intelligent.

B. Obstacles to Safety and Security

Fundamental Safety: Because of the enormous demand, the majority of devices are deployed with weaker security, which makes assaults conceivable" [9]. However, Internet of Things (IoT) security is very important, and if a linear approach isn't taken, the whole system, as well as data security and privacy, is at risk of being compromised.

The additional issues that face the majority of the healthcare business, with the exception of COVID, are related to privacy. When it comes to the healthcare business as a whole, the use of this sort of technology necessitates a complete degree of security as well as privacy inside their networks. The proliferation of the Internet of Things devices in the market has also resulted in an update to both GDPR and HACCP rules. [10]. and "the Internet of Things is exposed to privacy and security risks due to a lack of internal security safeguards." [11]. According to Turgot et al., (2015), the most prevalent and well-known assaults over the last several years have been tied to the Internet of Things

(IoT) devices that have insufficient levels of security. These attacks include DoS and Man in the Middle attacks. Devices Data gathering, data management, data sharing, and data privacy and sharing Privacy and data security concerns are not just important for the healthcare industry but also for a variety of other sectors that involve the transfer of sensitive data.

Data Management: There are many industries that use multiple sensor data and equipment and data management that generate billions of data points continuously and in a single day is a major challenge for the industries and processing such data, meaningful information from such data Get a complete understanding of Extraction, Applied Machine Learning, and Deep Learning gives fruitful information from such data [25]. Data Management: There are many industries that use multiple sensor data and equipment and data management that generate billions of data points continuously and in a single day. Edge computing, a relatively recent technological development, alleviates many of the difficulties and time-consuming procedures that are associated with transporting data that is superfluous or redundant and obtaining the result after storing the data and processing it on the cloud. To get around this problem, IoT-based smart devices are adaptable and provide data with their full meaning to the cloud, making it possible for the cloud to do fewer computational tasks and use fewer resources. [12], [14].

C. Communication Protocols

The Internet of Things (IoT) devices are wholly reliant on the internet. IoT devices are unable to function if they are not connected to the internet; nevertheless, LoRA devices have a range of up to 5 kilometers without experiencing any loss of packets in transmission.

D. IoT security compared to more conventional IT security

IoT and conventional wireless networks in terms of how they deal with issues of privacy and security. IoT devices are readily susceptible to WiFi, as Frustaci, Pace, Aloi, and Fortino (2018) point out. Furthermore, during the last three to four years, the number of attacks carried out against IoT devices has steadily increased. Authentication problems, management problems, information storage problems, and a host of other problems are the root cause of this situation.

E. IoT Security Concerns

There are several problems associated with IoT, the most prevalent of which is only when devices are placed in open places are they vulnerable to assaults that include node capture. Attacks include injecting malicious code into the node's memory. These attacks are known as malicious code injection attacks. Eavesdropping and interference are two popular forms of assault. One of the most prevalent forms of attack is to monitor the target and then attack it. The act of interfering with communication through disrupting signals is known as jamming. This assault is very similar to a DoS attack, in which the attackers keep the server busy by flooding it with traffic by raising the strain on the computers that make up the cloud. SQL Injection Attack The goal of this attack is for the attacker to get access to the database or to reach it directly. Man-in-the-Eavesdropping, constant monitoring, and infiltrating the network are all aspects of a middle assault, which is very similar to eavesdropping. Theft of data in IoT applications is one of the most pressing concerns; sometimes, sensitive data calls for a higher security level, whether the data is at rest or in transit [21]. Codes that are malicious, such as viruses and worms, may compromise the system's integrity and spread across the network. In general, there are two methods of attack: one is active, while the other is passive. Active attacks can be readily detected, and at the application layer, we may trigger them if there is a possibility of an active assault on the target. Passive attacks are more difficult to detect. But when it comes to passive assaults like eavesdropping, it may be very challenging to defend against them. Attacks come in a wide variety of forms, and successfully defending against all of these forms is one of the most difficult difficulties. DoS attacks are among the most common types of cyberattacks, and they include repeatedly attempting to target or overload a server in order to prevent it from listening to other legitimate requests.

F. System Ports

One of the methods to support the degree of security at the Transport layer, which is one of the ways to make it secure, is via the use of network ports. In order for communications to properly transfer across encrypted tunnels, SSL is necessary to be used with a key size of at least 128 bits [8]. Despite the fact that the IoT protocol uses a variety of ports for secure communication, this mechanism's significance in ensuring the safe transmission of data cannot be overstated. Internet browsers will almost always choose HTTPS when dealing with online apps; the same is true for communication-based on the Internet of Things. The MQTTS protocol is superior than the MQTT protocol in both its capacity for communication and its degree of security.

Because of the increasing proliferation of smart gadgets in every environment, concerns about security and privacy are always growing. Earlier versions of WSN favored lightweight encryption due to concerns about power consumption. This kind of encryption is less secure for communication, and in the event that data is important, the outcome might have disastrous effects. Battery usage and battery backup of devices are both becoming much better as a result of improvements made to technologies such as IoT devices. These improvements are made possible by the

adoption of more recent technology and a variety of new strategies. According to the findings of our study, we need a robust authentication system in order to transport data from one device to another end. In the model that we have developed, the data are transmitted directly from the devices to the cloud, and subsequently from the cloud to the mobile device, without the need of any specialized platform or application.

3. Proposed Model

Applications based on the Internet of Things are very quick and simple to use. This study presents a paradigm that we have presented, in which we combine Internet of Things devices with mobile and employ temperature monitoring-based apps to measure parameters using mobile. Directly connecting Internet of Things (IoT) devices with mobile applications eliminate the need for an internet platform. Just certain settings were added, and then we linked it remotely. Our very own server, which reliably answers in a Pub/Sub fashion, has been put up by us. Users have the ability to switch subjects at any moment and remotely adjust the device setup. We demonstrate for you in the figures how users may take use of this service and get a great deal of profit from the application, which is now in the testing phase. The vast majority of apps that are used nowadays are web-based, and here we will launch with all of the required capabilities to ensure that people can simply access our product.

Hardware:

In order to put this into action, we are using an ESP8266 (microcontroller) and a DHT22 (Temperature sensor). The DHT22 is the most common instrument for detecting temperature and humidity, and its precision is noticeably superior to that of other instruments. For the purpose of better understanding the communication and security of Internet of Things applications, we have produced prototypes for this application. In order for the preceding component to function correctly, we have established suitable connections and uploaded our algorithm, which is the means by which it communicates with our server.

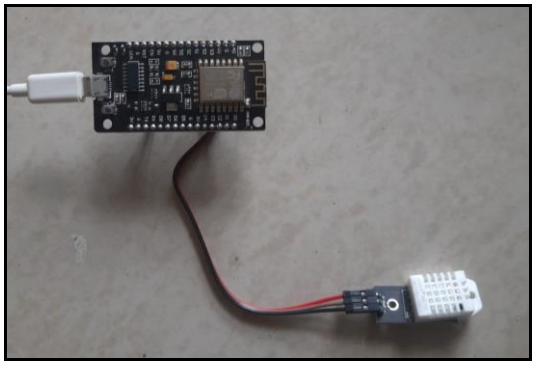

Fig 2: Prototype of IoT device

Software:

We have developed a mobile application in the software department that allows us to integrate devices together with all of the characteristics that are required, and the devices remain linked with it permanently. There is no need for customers to update their software, and the gadget continually transmits data that is easy to monitor and regulate. Within this program, data is kept locally on mobile devices, and users have the ability to access that data in an Excel format so that it may be analyzed at a later time. While pub/ sub-request handlers are the only ones allowed on the server. With this, we are able to simply connect with any device, and data may transfer extremely frequently and without any lag thanks to the MQTT protocol that we are using here. MQTT is one of the greatest and most prominent protocols used in IoT, which stands for the Internet of Things. The Publish/Subscribe protocol is one of the most effective methods available for subscribing to a number of different publishers and subscribers. In the illustration, a mobile application displays real-time data from IoT devices. The green line represents the most recent value, the red line denotes the highest level, and the yellow line indicates the lowest level.

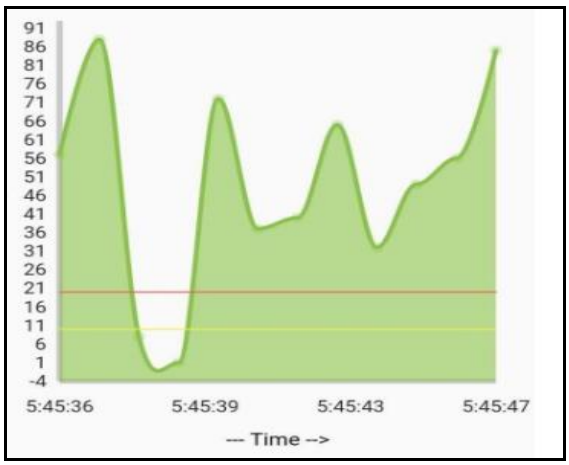

Fig 3: Mobile Application shows Live Temperature

4. Experiment Analysis

We are able to control and monitor live data from any location thanks to the Internet of Things. Our primary objective is to provide access to the Internet of Things devices in a manner that is secure, user-friendly, and portable. In order to provide consumers with access to our services at this time, we are now testing a prototype that functions correctly in every environment state and scenario. In order to conduct an analysis of experiments, we are making use of DHT22, which is more precise than DHT11. The error rate of the DHT22 is also extremely insignificant for common applications, which makes it suitable for measuring temperatures ranging from very cold to very hot. The DHT22's temperature measuring range is -40 degrees Celsius to 80 degrees Celsius. Using DHT22, we have carried out a number of experiments, and based on those

experiments, we have determined that data is transmitted in a safe manner, that the level of security identity is high, that the data is highly encrypted, and that there is a possibility of a DoS attack, but that a Man in the Middle attack is unlikely. For graphical analysis, we are utilizing Wireshark. If we are not using parameters, then the possibility of attack is very high; however, if we are using parameters, then the level of a security breach is less but with additional parameters such as SSL security and topic name encrypted f the possibility of attack is negligible and the result is shocking. In figure 4, we tested 1000 attempts through a python script and tested various types of attacks on the proposed IoT devices; the possibility is negligible and the result is shocking.

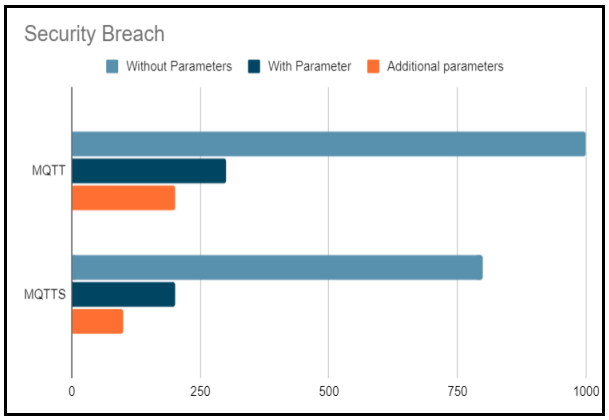

Fig 4: Security breach analysis on IoT devices

5. Conclusion

The Internet of Things (IoT) domain is one of the most popular domains. It will save time, cut down on losses, and enable instant connection from any location in any part of the globe. All of these benefits will contribute to the expansion of the industry. In this work, the study was carried out on the data security of IoT devices, as well as the data security of data propagated to Mobile Apps, and for that purpose, we made use of DHT22, which was capable of capturing ambient temperature extremely precisely. We are concentrating on developing easy-to-use and secure Internet of Things devices that can connect to servers and mobile devices. Because this connection provides the most reliable link between mobile and Internet of Things (IoT) devices, we decided to develop a smartphone application to which any device may connect. At the same time, we are coming to the realization that the degree of privacy and security is also quite significant. Therefore, attacks such as man-in-the-middle, denial of service, jamming, and tempering are not conceivable. Therefore, in order to integrate all different kinds of devices, protocols, apps, etc., the Internet of Things devices need to have defined standards in the form of standardization. In the future, we want to make use of AI in order to make it simple for users to get early alerts about temperature, and we also plan to build a variety of prototypes and platforms in order to ensure that users can make efficient use of the technology.

References

[1] Ray, Partha Pratim. "A survey of IoT cloud platforms." Future Computing and Informatics Journal 1.1-2 (2016): 35-46.

[2] Gaitan, Nicoleta Cristina. "A long-distance communication architecture for medical devices based on LoRaWAN protocol." Electronics 10.8 (2021): 940.

[3] Shah, Rushabh, and Alina Chircu. "IOT and ai in healthcare: A systematic literature review." Issues in Information Systems 19.3 (2018).

[4] Samie, Farzad, Lars Bauer, and Jörg Henkel. "IoT technologies for embedded computing: A survey." 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS). IEEE, 2016.

[5] Lee, Suk Kyu, Mungyu Bae, and Hwangnam Kim. "Future of IoT networks: A survey." Applied Sciences 7.10 (2017): 1072.

[6] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.

[7] Ishaq, Isam, et al. "IETF standardization in the field of the internet of things (IoT): a survey." Journal of Sensor and Actuator Networks 2.2 (2013): 235-287.

[8] Gilchrist, Alasdair. IoT security issues. Walter de Gruyter GmbH & Co KG, 2017.

[9] Shah, Sajjad Hussain, and Ilyas Yaqoob. "A survey: Internet of Things (IOT) technologies, applications and challenges." 2016 IEEE Smart Energy Grid Engineering (SEGE). IEEE, 2016.

[10] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

[11] Schurgot, Mary R., David A. Shinberg, and Lloyd G. Greenwald. "Experiments with security and privacy in IoT networks." 2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE, 2015.

[12] Safdar, Noreen, Hala Asif, and Fatima Farooq. "Energy Use and Human Health Nexus in Pakistan." Review of Economics and Development Studies 6.3 (2020): 661-674.

[13] Gravely, Shannon, et al. "Discussions between health professionals and smokers about nicotine vaping products: Results from the 2016 ITC Four Country

Smoking and Vaping Survey." Addiction 114 (2019): 71-85.

[14] Abu-Elkheir, Mervat, Mohammad Hayajneh, and Najah Abu Ali. "Data management for the internet of things: Design primitives and solution." Sensors 13.11 (2013): 15582-15612.

[15] Bohli, Jens-Matthias, et al. "SMARTIE project: Secure IoT data management for smart cities." 2015 International Conference on Recent Advances in Internet of Things (RIoT). IEEE, 2015.

[16] Zhang, PeiYun, MengChu Zhou, and Giancarlo Fortino. "Security and trust issues in fog computing: A survey." Future Generation Computer Systems 88 (2018): 16-27.

[17] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

[18] Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." Computer 50.2 (2017): 76-79.

[19] Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." Internet of Things 5 (2019): 41-70.

[20] Ramotsoela, Daniel, Adnan Abu-Mahfouz, and Gerhard Hancke. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study." Sensors 18.8 (2018): 2491.

[21] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." 2014 international conference on privacy and security in mobile systems (PRISMS). IEEE, 2014.

[22] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." IEEE Access 7 (2019): 82721-82743.

[23] Cerullo, Gianfranco, et al. "Iot and sensor networks security." Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. Academic Press, 2018. 77-101.

[24] Tang, Xiao, Pinyi Ren, and Zhu Han. "Jamming mitigation via hierarchical security game for iot communications." IEEE Access 6 (2018): 5766-5779.

[25] Thakkar, Ankit, and Ritika Lohiya. "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges." Archives of Computational Methods in Engineering 28.4 (2021): 3211-3243.

[26] Lin, Yun, Wei, Yi, Bing Lin, and Chun-You Liu. "AItalk: a tutorial to implement AI as IoT devices." IET Networks 8.3 (2019): 195-202.

[27] Gyawali, M. Y. P. ., Angurala, D. M. ., & Bala, D. M. . (2020). Cloud Blockchain Based Data Sharing by Secure Key Cryptographic Techniques with Internet of Things. Research Journal of Computer Systems and Engineering, 1(2), 07:12. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/5

[28] Prof. Sharayu Waghmare. (2012). Vedic Multiplier Implementation for High Speed Factorial Computation. International Journal of New Practices in Management and Engineering, 1(04), 01 - 06. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/8

[29] Mandal, D., Shukla, A., Ghosh, A., Gupta, A., & Dhabliya, D. (2022). Molecular dynamics simulation for serial and parallel computation using leaf frog algorithm. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 552-557. doi:10.1109/PDGC56933.2022.10053161 Retrieved from www.scopus.com