An Insight of Existing Research Methods towards Securing IoT Communication System

Nasreen Fathima, Reshma Banu, G.F Ali Ahammed

Abstract**: *IoT is an advanced analytics system that incorporates physical devices, intelligent technologies, and internet services to provide automation services and cost-effective productivity. The IoT oriented framework offers effective control, stabilized execution, and translucent services when it is applied to any enterprise. However, IoT devices are at risk of many security threats because they communicate and operate smart device services over wide distributed networks (i.e., insecure Internet channels). Over the past few years, it has been witnessed that several types of malicious activities have been tried to undermine the security and privacy of sensor networks as well as Internet-based applications. In order to protect IoT devices, many research works have been carried out to address potential security attack and to find an optimal way to overcome and limit the risk factors that affect security requirement and individual privacy. Therefore, this paper carries an assessment of the existing research works in order to understand better the root cause of the new possible threat and the challenges associated with IoT security. The paper also reflects the research trend to demonstrate the current status of security methods being developed till date. The prime motive of the present work is to reveal the current research gap and make an effective contribution to the future research direction.***

Keywords: Internet of Things, Privacy, Security, Authentication, Adversary, Ransomware, Cryptography.

I. INTRODUCTION

The IoT (Internet of Things) is a set of an automated system composed of smart and intelligent features that include small devices, sensors, storage unit, artificial intelligence, internet connectivity, and active engagements. It visualizes a self-configurable, complex network that connects things to the Internet through the use of standard communication protocols. In the IoT, the term ‘things will mean that various smart devices that are highly interconnected with each other, latched with programmability features that have sensing and actuation.

Revised Manuscript Received on February 28, 2020.
* Correspondence Author

Nasreen Fathima*, Assistant Professor, Department of Computer Science Engineering, ATME College of Engineering, Mysuru, India, Email: nasreen16fathima@gmail.com

Dr. Reshma Banu, Professor & Head, Department of Information Science & Engineering, GSSSIETW, Mysuru, India, Email: reshma127banu@gmail.com

Dr. G.F Ali Ahammed, Department of Computer Science Engineering, VTU Post Graduate Centre, Mysuru, India, Email: aliahammed78@gmail.com

These interconnected devices have physical as well as a virtual portrayal that contains different and unique information such as identity, status, location, etc. and offers flexible services with or without human involvement.

The ‘things' could be smart shoes, Bluetooth key tracker, smart watch, smart glasses, smart rings, etc. [1- 4]. Therefore, in IoT, the term ‘thing’ is any device that is connected to the internet. The adoption of IoT oriented application in Industries conveys an enormous transformation in the quality of services and product deliveries. It is believed that the concept of IoT will change the human lifestyle and various form of technical aspects. With the increasing use of various smart devices, it has been observed that IoT has proved to be an important contribution to supporting such forms of comprehensive technologies [5-7]. Some of the practical examples of the IoT based application are automatic-vehicle and transport system, smart refrigerator, implantable medical devices, robotic system, wearable devices, etc. However, there is a potential need for securing such forms of distributed network system called as an IoT. The extent of the security breach is quite higher when it comes to the internet. However, these security issues open up increasing opportunities for cyber-criminals, ethical hackers, and the security researchers [8-9]. Therefore, it is found that losing security will seriously affect the economy, companies, business transactions, personal privacy, etc. There are also evolutions of different forms of threats evolving in the area of conventional cybersecurity. There are also various official reports of the attacks (e.g., data breach, vulnerability, etc.) towards the conventional cybersecurity system. It will mean that there is already evidence of a large number of potential attacks over the cyber system in present times. (e.g., Facebook-Cambridge Analytica, Cathay Pacific data breach, breaches at eBay, Github, etc.) [10-13]. All these examples just proved that our security potentials are extremely sub-standard and hence it also creates more opportunity to carry out a further investigation for exploring an effective solution.

Therefore, the contribution of this research article is to provide a quick insight into the effectiveness of existing IoT security techniques. Section II presents a critical concern for IoT security. Section III presents essential attributes of IoT security followed by a detailed discussion of existing security techniques in Section IV. Research pattern is discussed in Section V followed by brief research gap in Section VI. Finally, section VII concludes the summary of this paper.

II. CRITICAL CONCERNS TOWARDS IoT SECURITY

The security issues related to Things (IoT-devices) seems to be very large. As the number of devices associated with the IoT increases, they become more consistent targets for attackers The Things are the potential gateways to any individual enterprise system because they are widely distributed, and many devices have not yet established on the security standards. According to IT-professional views, it is expected that the rate of attacks will increase every year.

The followings are the importation concerns on which IT-professionals will struggle to maintain the IoT-security in an enterprise.

- **Wide intervals and different endpoint:** In IoT, each associated device communicates through a network within very large intervals that means each one is an endpoint for different organizations. Through the research prediction score, it is expected that IoT is a future of automation services for both machines and humans. By 2020, the IoT devices are expected to increase by more than 20 billion. Hence, it is reasonable to believe that as IoT devices increases, it will create a frenzy opportunity for the cybercriminals. Another factor is that as the IoT technology becomes stable, the things will become more secure, but it will take time and hence it very difficult to update or replace the older IoT based Units.
- **Business interoperability:** A voluntary connection between the IoT application and an organization can be controlled through an IT-management system. However, the policy of bring your technology such as portable devices and smart devices in the industry may bring an additional opportunity to perform a un-intentional act that results to cause security loop-holes and cause to loss of business, economic as well as the reputation of individuals. It also seems a big challenge for a management team controlling such unintentional behavior by company employees.
- **Variants of devices everywhere:** In the present network, there are different kinds of devices used in industry. However, the IoT devices are quite different from many devices used in the present systems. The IoT devices are smart as well as intelligent whereas the other devices are based on the mechanical support, and few are only smart. Therefore, it necessary for network engineers and tech experts to learn the advanced networking and security layer management concept such as IoT6, IPV6, RFID, Zigbee, and other advanced protocols. These procedures do not entirely replace the existing system, but it will help to extend and connect with the advanced feature of IoT application with enhanced security and privacy enforcement.
- **Link-up of the Digital world to Physical world:** Adopting IoT technology offers a promising result to connect the digital world to the physical world. IoT supports rich digital library and versatile access technologies to serve various application-based facility and links things to the physical world. The IoT provides real-time service, intelligent service, and flexible remote access services that can be very use-full in various real-time systems such as in the healthcare department, automobiles, industrial controls, education, etc. The IoT devices are vulnerable to security risk because the IoT devices are battery operated, sometimes placed in a hostile area and having a computational operation which can be manipulated and access by the unauthorized party. For instance, IoT based healthcare systems are attacked in an attempt to steal or destroyed essential data information that can cause huge loss to the medical organization, patient privacy, and hacking medical wearable devices lead to cause patient death. Therefore, IoT based application requires qualified management program in order to maintain and secure its operations such as long connections, sensors devices.

III. ESSENTIAL ATTRIBUTES OF IOT SECURITY

As the adoption of the IoT is exponentially growing, it is reasonable to accept that recent cyber attacks are also IOT-enabled. The attacker initially explores some vulnerable points so they can put the IoT node in a compromised situation and fulfill their intentions anyway. According to a survey of DigiCert-firm [14], the efforts towards securing IoT-devices in an enterprise are vastly different from the attacker's viewpoint that they focused on unsafe IoT endpoints. Based on reported it is found that in the past two years, 25% of the underlying companies suffer the loss of at least $34 million due to IoT security-related issues. To avoid this kind of attacks, researchers must analyze all possible way of attacks in order to design a powerful attack mitigations approach. A brief discussion of devices that are more vulnerable to IoT attacks are as follows:

- **Routers:** The router used in smart home automation is one of the common weak points that open a way for various security attacks. The reason behind this is that these devices came with basic credential which can easily be manipulated and hacked.
- **IoT-HUB:** Similarly, IoT Hub for smart-home is a device that connects and manages several of IoT assets. According to a report[15] researchers have found that there are 20 bugs in Samsung Smart Things Hub, then can allow intruders to take control over on individuals smart locks, remotely monitor the home, etc.
- **Smart Home Appliances:** The existing smart home devices are operated on unsecured internet channel and are controlled by the apps. This also opens a gateway to perform an adverse behavior because hacking and manipulating configuration setting of things over the internet is not a difficult task in the present days.
- **Network Connected Vehicles:** The advancement in sensor technology and electrical equipment has made it possible to connect, control and operate a vehicle through a cloud. However, due to the lack of efficient authentication mechanism, it is not so difficult to break in the security of these vehicles. For instance, it can lead to cause death if the failure of the braking system is done by an adversary from the remote point.

IV. EXISTING RESEARCH APPROACHES

This section carries an assessment of the existing research studies to address and solve the security issues in IoT applications.

After exploring the existing IoT security techniques, we found that there are three basic categories on which IoT security is implemented, namely i) security implementation based on network devices, ii) security implementation based on authentication, and iii) security implementation based on optimization.

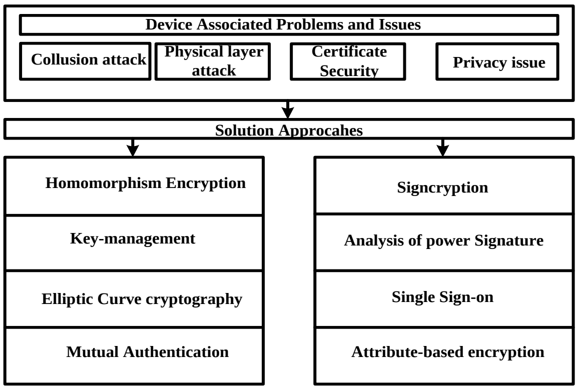

Fig.1 Taxonomy of Device-based security

- **Device-based Security Approach:** Since a few decades the wireless sensor networks have been extensively studied to obtain better possibilities for secure communication with resource constraints things. The integration of the IoT with cloud technology is believed to be profit enabler tool of many industries and organization. However, the evaluation of the security level required for the different application seems an important issue in the current market of advancement. One of novel security assessment framework based on SDN-(Software Define Network) for cloud-oriented IoT application is designed by Han et al. [16]. The authors have constructed their framework containing 23 indicators to evaluate the security level according to the application requirement. In order to analyze their designed framework potential, the authors have carried different interviews from various enterprise and industries and found that their framework meets the required objective that can help clients to grow their business in a fearless manner.

Existing device-based security studies should tend to address the threats often encountered on IoT devices (Figure 1). Unlike the actual threats to IoT devices, such as ransomware, most existing researchers have investigated different forms of security issues such as physical layer security, collusion attacks, etc. The existing security mechanism provides the use of core cryptographic algorithms to defend different forms of uncertain attacks.

Various existing research efforts have been made to address cloud security issues with the development of highly diverse solutions. After a careful review of existing research work, it is believed that the existence of distributed computing in cloud resources is the main cause of security breaches. Diaz et al. [17] investigated the integration of cloud and IOT technology. The authors have summarized the existing security recommendations for both technology and reveal challenges and open research issues related to it. Similarly, the work of Botta et al. [18] has reviewed the existing literature survey on cloud and IoT integration, with a demonstration of research trends and associated research challenges. A closer look towards the term 'Things' is drawn by the Voas et al. [19] in which the authors have carried in-depth studied of the special publication named as NoT((SP 800–183) to understand what IoT is. The authors have found that there is still no existence of IoT definition which can be accepted at the universal level. They noticed that the proper understanding of the IoT is still evolving and more specifically, any term that includes "smart" automatically becomes a part of the IoT. The authors have shown their concerns that the practitioners and researchers are consistently evolving up with new strategies. The motive of the presented work is to make readers aware of the current situations and focus on developing standard and secure architectures.

Most of the problems still exist in the IoT-nodes which are always less considered by various researchers. The explosion of IoT nodes may be more vulnerable to attacks and may lead invite botnet attacks and Mirai attacks in IoT networks. These threats lead to open vulnerable services at a higher level in the network, physical security, authentication process, etc. To deal with this kind of serious threat the work of meidan et al. [20] presented the anomaly detection model based on deep auto-encoders technique in order to map the behavior of the network periodically. In order to analyze a potential feature of the given technique, the authors have performed an experiment where some IoT devices are injected with botnet and Mirai attack. The experimental performance reveals that the presented approach efficiently detects the adverse behavior by the compromised IoT nodes. A mathematical transform-based technique approach is used by Zhang et al. [21] in which they have emphasized implementing security on the physical layer. Another discussion by Bertino and Islam [22] highlighted the potential capabilities of botnets threat in IoT devices. Wang et al. [23] have discussed the study of physical layer security. They designed a security system that enhances defense operation against attacks by adding upper layer protocols with physical layer information. We have come across that encryption technique is used primarily to provide security for the physical layer; however, there are some unconventional methods for protecting the IoT physical layer. Many IoT systems are constructed on the existing framework of middleware, and these systems use the fundamental security feature of the existing middleware. A survey work carried out by Fremantale and Philip Scot [24] has focused on the IoT middleware to analyze the challenges associated with IoT security and privacy. Initially, they have constructed a matrix pattern illustrated with an extensive analysis of existing works to identify cause and security requirement in IoT middleware and drawn a significant conclusion to contribute in the future research area. Similarly, Tiburski et al. [25] discussed the lightweight techniques for the IoT middleware security consistency. They also studied the existing work and presented important challenges associated with IoT middleware to achieve integration of standard security model and elimination of security risk and threats occur in IoT middleware systems.

There is also a general discussion on fog computing, which is reported to provide enhanced safety performance and cost-effective channel utilization such as decreased bandwidth, and reduced latency.

It has been introduced as a method to reduce the gap limitation between IoT devices and remote data centers. Alrawais et al. [26] discussed security vulnerabilities related to IoT oriented fog computing. The authors reveal that IoT suffers from authentication issues, privacy issue, data protection, and the presence of malicious nodes. The author uses the bloom filtering concept to enhance the certificate revocation mechanism of connected devices in IoT.

A fuzzy trust-based security trust model is designed by Soleymani et al. [27] for self-organizing vehicular networking in fog computing.

The fog calculation is also used to verify the accuracy of the location of the event. The proposed trust model performs security verification to ensure that the message received from the authorized vehicle is correct or not. The experimental performance exhibits that the presented approach not only detect adversary but also eliminates the uncertainty factor and inaccuracy of data in the vehicle network. Wang et al. [28] showed that the compression sensing concept could be utilized to provide a better security feature in IoT application. The author has highlighted data leakage issues in static environments. The authors applied matrix dependent solutions to improve data security. The performance evaluation of the presented approach is carried through the root mean square that shows a matrix dependent approach. Roman et al. [29] surveyed to analyze security challenges and threat risks in the field of mobile edge computing. The authors have an analyses trust issue in edge computing security and privacy. They point out that the trust mechanism is a very important security factor for the edge paradigm.

At present, it is reasonable to say that IoT has improved our quality of living-style by facilitating personalized service. However, in IoT, a huge amount of services and smart-devices connected over the internet every day due to this it faces very serious challenges that directly belongs to user's privacy and security. The research community on IoT mostly considers enhancing the communication process and IoT framework standardization. We also observe that existing security techniques based on two-factor authentication is not efficient to provide reliable and secure end-to-end communication among the varied services and IoT-devices. A biometric-based security system is now pulling the attention of the security researchers to implement unique trait-based authentication mechanism IoT application. The work carried out by Hossain et al. [30] has designed an integrated security model based on the biometric technique and cryptographic approach. The author has constructed a case structure based on facial biometric in which smart sensor nodes captures the image and transmit it securely to the dedicated destination. It has also been found that there are very fewer reports that have talked about security issues using biometrics [31, 32]. According to the author [33], biometric-based security is expected to replace the traditional password-based security by 2020 and will cover more than 70% of the smart devices market. Some other research studies have concentrated on adoption power signature concept towards securing IoT-devices and addressing the threat risk challenges associated with it.

In the same way, a survey of Park and Tyagi [34] talked about threats associated with side channels and highlight some vulnerable points of power signatures. Similarly, the work of Kittur et al. [35] discusses and analyses various batch verification mechanism to avoid unauthorized access of Information via IoT nodes. Xu et al. [36] concentrated on the optimal allocation of power resource to the IoT nodes and introduced a unique relaying scheme based on multi-hop communication and single-antenna environment.

Adoption of elliptical curve methodology has also been reported in some research works towards securing IoT nodes. It is considered that the complex nature of the elliptic curve algorithm puts the adversary into a struggle to analyze and understand the pattern of elliptical curve cryptosystem. Such usage of elliptic curve technique is reported in the study of Bai et al. [37] have designed an improved security model for cloud-based IoT application based on elliptic curve cryptography to achieve fundamental security principle. The study outcome suggests that the presented technique offers robust security with flexible adaptability in IoT and cloud ecosystem. The work of Park [38] uses a bootstrapping technique to secure data generated from the IoT device. Usage of DNA-based security has also been proven reliable to offer good security. Tiwari and Kim [39] have used the joint approach of DNA and ECC to construct multi-layered security framework for preventing data and IoT device from unauthorized control. In this, the author has used the concept of DNA sequences along with the sorting algorithm and ECC-encryption. The experimental result shows that by using DNA sequences with existing ECC provides double fold type security and more resistive to side channel attack and timing attacks. The study of Yan et al. [40], have tried to improve existing cryptographic-based approaches by utilizing pairing-based encryption. Now-days, nano-electronics technologies seem a promising approach to provide energy-efficient and security aware hardware implementation in resource constraints IoT devices [41]. Work on a similar concept is reported in a study of Uddin et al. [42] in which the author used PUF- (physically non-cloning function) with nanoelectronics memory technology at the hardware level. The PUF implementation enables efficient authentication and key generation mechanisms on IoT applications.

- **Authentication-based Security Approach:** In IoT authentication is the next top approach used to established secure communications between different entities. The authentication is done to recognize the validity of both the user and the device.

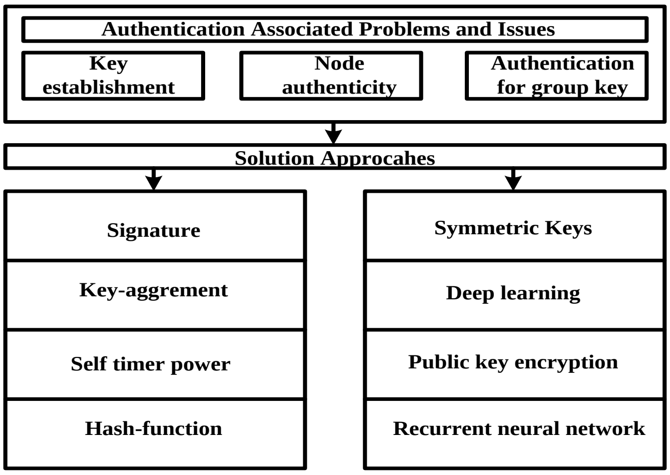

Fig.2 Taxonomy of Authentication-based security

Talking about authentication refers to a certification that ensures the reliability and verifiability of any individuals or things. The authentication process includes design and planning of the key management techniques.

The above figure 2 represents a map of existing authentication research work that has primarily addressed security issues affiliated to the IoT (node or things) mutual authentication schemes, key establishment, signature-based schemes, and traditional public key cryptographic approaches.

Recent work of authentication Protocol design based on self-adapted powered timers has been carried by Affifi et al. [43] for RFID based IoT application. In this author have presented various improved authentication protocols to mitigate the security defects in the existing protocols. This technique incorporates autonomous oriented powered timers to support robust synchronization to RFID tags without taking any external power resource. The experimental results show that the presented protocol achieves a potential feature to defend various kinds of attacks with less usage of storage memory. It is also showed that this technique is much efficient regarding security when compared to existing protocols. Challa et al. [44] developed a new authentication protocol based on the signature scheme. For analysis, the author has used the BAN logic system. The technique uses a key agreement strategy for developing a robust authentication model in IoT. The study outcome was evaluated using parameter delay and throughput that shows the presented technique quite efficient to secure IoT devices. The IoT applications are largely implemented on the resource constraints devices such as wearable devices. These devices are mainly used for monitoring, surveillance, etc. where lots of data are communicated with different devices. However, due to the constraints nature of sensors, the security and longevity of devices are not many stables. A recurrent neural network has shown useful results for the speech-processing task of resource constraints IoT applications. Based on the similar concept a work carried out by Chauhan et al. [45] introduced a breath print system in which the authors studied the performance of in-depth learning approach based on recurrent neural network (RNN) can be efficiently used in resource-constrained devices or not. Experimental analysis shows that the introduced technique is not only powerful but also lightweight enough to be effectively executed on various resource-constrained IoT devices. Porambage et al. [46] have introduced a methodology for establishing group key based on cryptographic hash function and signature scheme followed by multicast routing for securing communication performed through IoT- Sensor. Chien et al. [47] address the overhead problem of aggregated authentication and trust challenges associated with the key agreement in IoT oriented mobile system. In order to solve these issues, the author has developed a cluster oriented secure key agreement scheme. Qin and Ma [48] have presented a mutual authentication mechanism exclusively for low-powered communication devices in IoT. The process of authentication in IoT mainly uses public key encryption to offer better key management services for its nodes. It was discussed in the work of Raza et al. [49] that symmetric key management could potentially assist in a key establishment in IoT applications to overcome the limitation of pre-provisioning of the trusted keys in IoT.

- **Optimization-based Security Approach:** The entire framework of the IOT based on the combination of various hardware and software elements. In order to improve the user experience and benefits from IoT, one of them needs to take advantage of optimal design and architecture. Optimization indicates the options to achieve the desired goal. Generally, software-based implementation is selected as the priority for the insertion of any new features. However, this sometimes requires an additional resource as well as supportability of advance hardware components. Therefore, optimization of IOT components is also one of the challenges for research communities.

Bed for extracting security loopholes is constructed by Form figure 3 it is found that some of the research works focused on optimizing the performance of security protocols in the IoT domain. However, most of the existing optimization approaches involve enhancing the traditional encryption mechanism, improving routing operation, query processing, etc. The techniques proposed in existing systems are mainly based on hardware optimization, homomorphic encryption, asymmetric encryption, fuzzy logic, neural network, etc.

The work of Mukhdeep Singh Manshahia [50] has considered the problem of network congestion for IoT virtualization in a smart city. In order to mitigate this issue, the author has used the PSO algorithm to analyze traffic pattern and applied energy aware routing in the transport layer of sensors and actuator networks.

The validity of the study outcome is demonstrated concerning packet drop ratio and network lifespan.

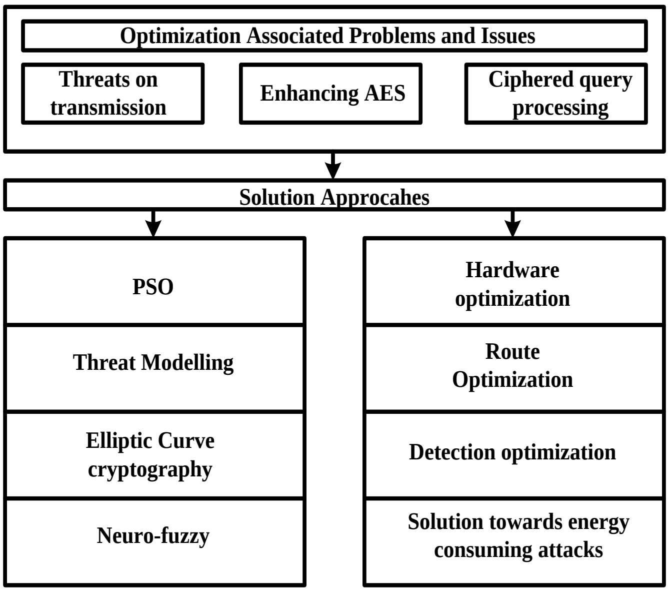

Fig.3 Taxonomy of optimization problem in IoT

In the study of Bui et al. [51], path optimization strategies were created with the help of AES algorithms. The study has also talked about the issues related to energy dependencies on the AES algorithm by presenting a hardware optimization approach. A work carried out by Chen et al. [52] focuses on optimization of intrusion localization. The authors have used fiber Bragg grating sensor for intrusion localization.

The presented approach uses deflection curve analysis for intrusion localization and particle swarm optimization algorithm is used to improve the identification accuracy.

The performance of the presented technique is compared with the existing technique, and the comparative outcome demonstrates that the introduced technique achieves short run-time with great stability. A cryptographic-based approach is used in the work of Shafag et al. [53] to perform cipher request execution in IOT. The study has also utilized an optimization algorithm for energy constraint IOT devices. Another work towards optimization can be seen in the work of Rahman et al. [54] where the author has introduced a neuro-fuzzy logic-based security approach to protecting against an intruder at physical and mac layer. Neural network architecture helps in optimizing the identity of intruders. A novel work towards optimization of energy consumption for power constraints IoT-devices is conducted by Mohd and Hayajneh [55] where the authors have optimized design of lightweight block cipher to prolong network life by managing energy consumption under an attack of energy drainer such as DoS. The study outcome is explored with the throughput, network lifetime and reduced latency.

Therefore, from the above discussion, it can say that there are various methods introduced in the field of IOT to improve security features. Existing approaches are more focused on securing the device. The study towards authentication is just an initial step. In the end, there is a small number of current studies that carries an optimization in IOT. Hence it is still an emerging research stage. Table 1 summarizes above discussed existing research works to secure IoT network and application.

Table 1 Summary of Existing Security Approaches in IoT

Authors	Problems	Techniques	Advantages	Limitation
Han et al. [16].	Securing communication between sensor and cloud	SDN based security evaluation model	Efficiently evaluates security requirements	No analytical/numerical results discussed.
Diaz et al. [17]	Security issues in IoT, and cloud	Qualitative discussion and analysis	Highlighted essential points	No analytical/numerical results discussed.
Botta et al. [18]	Security issues in IoT, and cloud	Extensive reviewed	Demonstrate research trend in IoT	No analytical/numerical results discussed
Meidan et al. [20]	Security threat in the network and physical layer	Anomaly detection model	Effective intrusion detection	Not benchmarked
Zhang et al. [21]	Security issue on the physical layer	Emphasized to implement security on the physical layer	Simpler implementation	Not as much sufficient
Bertino and Islam [22]	Botnets threat	The highlighted potential of botnets threat	Simpler discussion	No analytical/numerical results discussed.
Wang et al. [23]	Physical layer security	Encryption technique	Resistive to avoid malware propagation	Not benchmarked
Fremantale and philip scot [24]	IoT middleware	Matrix pattern-based analysis	Drawn a significant conclusion	Not benchmarked
Tiburski et al. [25], Alrawais et al. [26]	Security issues in IoT, fog computing, IoT device security, botnets device	Secret key generation based on time, qualitative discussion	Good theoretical discussion	No analytical/numerical results discussed.
Soleymani et al. [27]	Trust issue	Fuzzy trust model	Good authentication feature	Not efficient
Hossain et al. [30]	Integrity issue	Biometric technique and cryptographic approach	Better authentication feature	No benchmarking
Xu et al. [36]	Energy allocation	Relaying scheme	Good power management	Not as much sufficient
Bai et al. [37]	Cloud-based IoT security	Elliptic curve cryptography	Achieves good security level	No benchmarked
Park and Tyagi [34]	Analysis of power side-channel	Analysis of power signature	Single test-bed to assess multiple attacks	No analytical/numerical results discussed.
Uddin et al. [42]	Security implementation resource constraints hardware	Nanoelectronic memory technology	Simpler approach	Only limited to energy optimization
Affifi et al. [43] for	Authentication in RFID tags in IoT	Self-powered timers	Achieves efficient properties for resource constraints devices	Not as much sufficient
Challa et al. [44]	Authentication, key establishment	Mutual authentication, signature, key-agreement	Applicable for various adversaries	No benchmarking
Chauhan et al. [45]	Speech processing resource-constrained devices	Deep learning, recurrent neural network	Powerful and lightweight	Not performed Comparative analysis
Porambage et al. [46]	Authentication for group key	Signature, group-key, multicast	Scalable algorithm	Leads to computational complexity.
Chien et al. [47]	Overhead problem	Cluster oriented secure key agreement scheme	Increased throughput	Not performed Comparative analysis
Qin and ma [48]	Node authentication	Key establishment, mutual authentication	Can resist different attacks	Associated with complexity for real-time data
Raza et al. [49]	Key establishment	Symmetric keys, certificates	Reduced overhead	No benchmarking
Mukhdeep Singh manshahia [50]	Network congestion	PSO algorithm	Reduced packet drops ratio and increased network lifespan	Not focus on energy optimization

Bui et al. [51]	Enhancing AES	Hardware optimization	Lightweight, energy consumption reduced	Narrowed benchmarked
Chen et al. [52]	Intrusion localization	Deflection curve analysis and PSO	Achieves short run-time	No benchmarked
Shafagh et al. [53]	Ciphered query processing	Homomorphic encryption	Suitable for low-powered devices	No benchmarked
Rahman et al. [54]	Identification of intruder in physical and mac layer	Neuro-fuzzy model of detection	Efficient detection of an intruder	No applicable in real-time network owing to dependencies on the dataset
Mohd and hayajneh [55]	Network lifetime	Optimized design of lightweight block cipher	Enhanced network lifetime and reduced latency	No benchmarked

V. RRESEARCH TREND

We have reviewed recent literature on all research work to address security issues related to the Internet of Things. We have found lots of work carried in the domain of IoT security. Research publications have always provided a means of access to information that can facilitate the development of technological innovation and development concepts or technologies. We present works in last eight years research trend (i.e., 2012 to2018) as shown in (figure 4, figure5, figure6) followed by keyword *"Security in the Internet of things."*

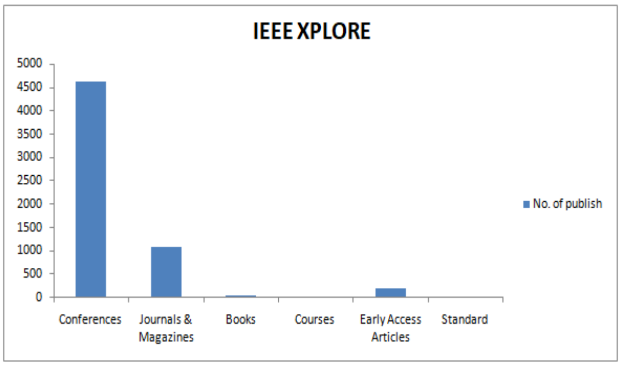

Fig.4 Number of publications in IEEE

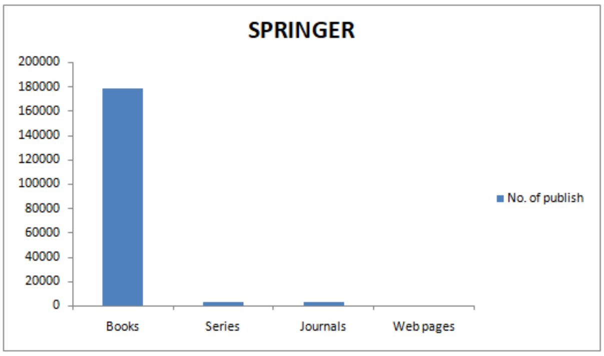

Fig.5 Number of publications in Springer

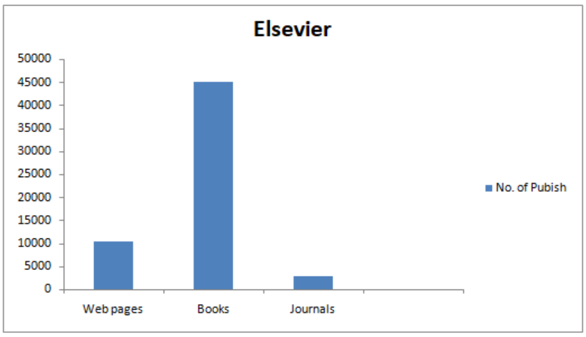

Fig.6 Number of publications in Elsevier

VI. RESULT AND DISCUSSION

In this result section, we have found out some techniques based on security protocols in the IoT from 2015 to 2019 (in table 2). The papers collected from the IEEE Xplore after that we have calculated the percentage of those techniques and demonstrated as a pictorial view point.

Table 2 presents the statistic data of security protocols in IoT

Years	Techniques	Numbers of Publications	Average	Percentage
2015-2019	Automatic Vehicle	106 Papers	48 Month	220.84
2015-2019	Transport System	848 Papers	48 Month	1716.66
2015-2019	Wearable Devices	940 Papers	48 Month	1958.33

Figure 7 present work done in last four years (i.e., 2015 to 2019). This figure talks about usage of security protocols techniques based on IoT .

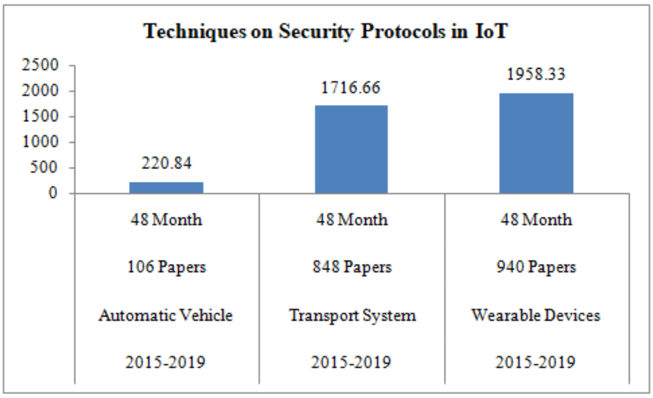

Fig.7 Shows the usage of security protocols in the IoT

VII. RESEARCH GAP

Research on an IoT security has been tended to utilizing different procedures where device security was always given preference in the existing research work. Existing security research techniques have been focused on understanding the security issues associated with RF tags, sensors, diverse layers, etc. The more significant part of the research exploration work that concentrated securing hardware component suffers from high computational complexity and increased cost. Some of the research work concentrating on network layer protection against serious threats is observed to be resolved by utilizing the access control mechanism that does not seems effective. It has also been found that existing work towards protecting application layer experiences the overhead problem.

- **Issues Associated with hardware-based Security:** An intensive analysis at existing research progress in the direction of device security demonstrates that there is the absence of benchmarked techniques. A different mechanism such as signcryption, single-sign-on, common verification, homomorphic encryption, circular bend cryptography has been accounted for delivering computational complexity and suffers from processing time. Subsequently, such security mechanism can't be utilized into IoT application because IoT based application includes fast query processing with delivering lower response time. There are few research works that have conducted power signature schemes for security. However, there is no standard yet been distributed for its utilization for a variant of IoT devices.
- **Imperfect IEEE Standard:** Existing investigations towards the security of the physical layer is limited by usage of IEEE 802.15.4 principles. Such standards are not accounted to execute any keying operation and also it doesn't guarantee the non-reusability of the protected nonce enabling the adversary to acquire the plaintext effectively from the secret content. Another big security risk is that such IEEE standard doesn't guarantee message integrity.
- **Difficulties in Authentication Schemes:** Existing verification approaches in IoT is done by commonly used security mechanisms such as key management, key agreement, etc. In short, the degree of novelty and improvement is minimal in introducing strong authentication mechanisms. This is because a crucial traditional management scheme does not ensure the security of new forms of attacks IoT devices. The use of such key-based policies is not much effective in current IoT sensing devices because these devices are resources constraints and needed external support to process them.
- **Less consideration to network layer:** The existing network layer frameworks, has less emphasis on network layer security and ultimately they are claimed to be protected by Internet Protocol Security (IPSec).
- **Less focus on data security:** Most of the research procedures have focused on device security and made cryptographic strategies to guarantee the security of it. There has been less advancement made in research progress tending to the data security issue.
- **Emerging stage of Security Optimization:** It has been found that existing technology that claims to optimize security technology in IoT cannot be expressed as a true optimization technique because there is less evidence in IoT, regular use of iterative encryption process, utilization of complex cryptography model during optimization and less consideration on cost of threat localization and modeling. Thus, existing research offers great a dependable balance to start optimization and enhancement towards IoT application security.

VIII. CONCLUSION

The risk of security attacks on IoT application is more, and there is a more chance that it will continue to increase. In spite of that, there has been a dynamic pathway for cryptographic-based methodology in numerous different technologies; it has not gotten that flow in IoT. Since, there are many progressive methods for cryptographic-based approaches in many other techniques, although it has not received the flow in IOT. The main cause behind this non-achievement area i) the use of variant devices in IoT application, ii) huge and complex data aggregation operations iii) shortfall of built-in security in devices. Many organizations and researchers have a good start to address security threats in the domain of IoT by using different techniques. However, form existing literature we came to know that there is a large gap between the actual events of the IoT attack and attacks discussed in the existing literature. Researchers have recognized different types of threats and addressed them in their exploration work. After reviewing the existing systems, it can be concluded that research efforts require further more research on data security. There are various IoT security mechanisms are introduced by the researchers, but none of them are based on the mathematical modeling approach. We additionally find that the authentication based security procedure also needs furthermore enhancement and improvement for the IoT ecosystem. Finally, the future work should put more focus on building efficient optimization techniques that able to provide lightweight security implementations resource-constrained IoT devices.

REFERENCES

1. Ray, Partha Pratim. "A survey on the Internet of Things architectures." *Journal of King Saud University-Computer and Information Sciences* 30.3 (2018): 291-319.
2. Fleisch, Elgar. "What is the internet of things? An economic perspective." *Economics, Management & Financial Markets* 5.2 (2010).
3. V. Angelakis, E. Tragos, H.C. Pohls, A. Kapovits, A. Bassi, “Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions”, Springer, Technology & Engineering , pp. 336, 2017
4. Zeinab, Kamal Aldein Mohammed, and Sayed Ali Ahmed Elmustafa. "Internet of Things applications, challenges and related future technologies." *World Scientific News* 2.67 (2017): 126-148.
5. Maksimović, Mirjana, Vladimir Vujović, and Enisa Omanović-Miklićanin. "Application of internet of things in food packaging and transportation." *International Journal of Sustainable Agricultural Management and Informatics* 1.4 (2015): 333-350.
6. Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, Stefanizzi ML, Tarricone L. An IoT-aware architecture for smart healthcare systems. IEEE Internet of Things Journal. 2015 Dec;2(6):515-26.
7. Kodali, Ravi Kishore, et al. "IoT based smart security and home automation system." *Computing, Communication and Automation (ICCCA), 2016 International Conference on*. IEEE, 2016.
8. Kamble, Ashvini, and Sonali Bhutad. "Survey on Internet of Things (IoT) security issues & solutions." *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. IEEE, 2018.
9. Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal. 2017 Oct;4(5):1250-8.
10. K. on Security, “Ddos on dyn impacts twitter, spotify, reddit,” 2016.
11. "Cathay Pacific Says Data Breach Exposed Personal Information of 9.4 Million Passengers", http://time.com/5434171/cathay-pacific-data-breach/, Retrieved on 11th December, 2018

12. Baby Monitor Exposures and Vulnerabilities",Rapid, Retrieved 19th September, 2017
13. 17 top cyber attacks in 21 centaury https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, Retrieved on 11th December, 2018
14. "The Security Ledger", https://securityledger.com/2018/11/survey-finds-attacks-find-insecure-iot-devices, Retrieved on 11th December, 2018
15. "Bugs in Samsung IoT Hub Leave Smart Home Open to Attack", https://threatpost.com/bugs-in-samsung-iot-hub-leave-smart-home-open-to-attack/134454/, Retrieved on 11th December, 2018
16. Han, Zhuobing, et al. "A Software Defined Network-Based Security Assessment Framework for CloudIoT." *IEEE Internet of Things Journal* 5.3 (2018): 1424-1434.
17. M. D´ıaz, C. Mart´ın, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," Journal of Network and Computer Applications, pp. 1–19, 2015.
18. A. Botta, W. de Donato, V. Persico, and A. Pescap´e, "N/A - On the Integration of Cloud Computing and Internet of Things," Future Generation Computer Systems, vol. 56, pp. 23–30, 2013.
19. J. Voas, B. Agresti and P. A. Laplante, "A Closer Look at IoT 's Things," in *IT Professional*, vol. 20, no. 3, pp. 11-14, May./Jun. 2018.
20. Meidan, Yair, et al. "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders." *IEEE Pervasive Computing* 17.3 (2018): 12-22.
21. Y. Zhang, Y. Shen, H. Wang, J. Yong and X. Jiang, "On Secure Wireless Communications for IoT Under Eavesdropper Collusion," in IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1281-1293, July 2016.
22. E. Bertino and N. Islam, "Botnets and Internet of Things Security," in Computer, vol. 50, no. 2, pp. 76-79, Feb. 2017.
23. Wang, Wei, et al. "Securing On-Body IoT Devices By Exploiting Creeping Wave Propagation." *arXiv preprint arXiv:1801.09224* (2018).
24. Fremantle, Paul, and Philip Scott. "A survey of secure middleware for the Internet of Things." *PeerJ Computer Science* 3 (2017): e114.
25. Tiburski, Ramao Tiago, et al. "The role of lightweight approaches towards the standardization of a security architecture for IoT middleware systems." *IEEE Communications Magazine* 54.12 (2016): 56-62.
26. A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," in IEEE Internet Computing, vol. 21, no. 2, pp. 34-42, Mar.-Apr. 2017.
27. S. A. Soleymani, A. H. Abdullah, M. Zareei, et al., "A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks with Fog Computing", IEEE Access, vol. 5, pp. 15619-15629, 2017.
28. N. Wang, T. Jiang, W. Li and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," in IET Communications, vol. 11, no. 9, pp. 1431-1437, 6 22 2017.
29. R. Roman, J. Lopez, M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges", Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.
30. Hossain, M. Shamim, et al. "Toward end-to-end biomet rics-based security for IoT infrastructure." *IEEE Wireless Communications* 23.5 (2016): 44-51.
31. Ren, Chun-xiao, et al. "When biometrics meet iot: A survey." *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation*. Atlantis Press, Paris, 2016.
32. Al-alem, Fatimah, Mohammad A. Alsmirat, and Mahmoud Al-Ayyoub. "On the road to the internet of biometric things: a survey of fingerprint acquisition technologies and fingerprint databases." *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*. IEEE, 2016.
33. Gartner, "Internet of Things Will Redefine Identity Management, http://www.planetbiometrics.com/article-details/i/2534/, Mar. 2015.
34. J. Park and A. Tyagi, "Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly.," in IEEE Consumer Electronics Magazine, vol. 6, no. 3, pp. 92-102, July 2017.
35. Kittur, Apurva S., Ashu Jain, and Alwyn Roshan Pais. "Fast Verification of Digital Signatures in IoT." *International Symposium on Security in Computing and Communication*. Springer, Singapore, 2017.
36. Q. Xu, P. Ren, H. Song and Q. Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations," in IEEE Access, vol. 4, no. , pp. 2840-2853, 2016.
37. Bai, T. Daisy Premila, A. V. Jerald, and S. A. Rabara. "Elliptic curve cryptography-based security framework for internet of things and cloud computing." *Int. J. Comput. Sci. Technol* 6 (2015): 223-229.
38. C. S. Park, "A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications," in IEEE Sensors Journal, vol. 17, no. 7, pp. 2215-2223, April1, 1 2017
39. Tiwari, Harsh Durga, and Jae Hyung Kim. "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices." *ETRI Journal* 40.3 (2018): 396-409.
40. Z. Yan, M. Wang, Y. Li and A. V. Vasilakos, "Encrypted Data Management with Deduplication in Cloud Computing," in IEEE Cloud Computing, vol. 3, no. 2, pp. 28-35, Mar.-Apr. 2016
41. A. Sengupta, "Hardware security of CE devices [hardware matters]," IEEE Consum. Electron. Mag., vol. 6, no. 1, pp. 130–133, 2017.
42. Uddin, Mesbah, Badruddoja Majumder, and Garrett S. Rose. "Nanoelectronic Security Designs for Resource-Constrained Internet of Things Devices: Finding Security Solutions with Nanoelectronic Hardwares." *IEEE Consumer Electronics Magazine* 7.6 (2018): 15-22.
43. Afifi, M. H., et al. "Dynamic authentication protocol using self-powered timers for passive Internet of Things." *IEEE Internet of Things Journal* 5.4 (2018): 2927-2935.
44. S. Challa et al., "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," in IEEE Access, vol. 5, no. , pp. 3028-3043, 2017.
45. Chauhan, Jagmohan, et al. "Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks." *Computer* 51.5 (2018): 60-67.
46. P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila and B. Stiller, "Group Key Establishment for Enabling Secure Multicast Communication in Wireless Sensor Networks Deployed for IoT Applications," in IEEE Access, vol. 3, no. , pp. 1503-1511, 2015.
47. Chien, Hung-Yu. "Group-Oriented Range-Bound Key Agreement for Internet-of-Things Scenarios." *IEEE Internet of Things Journal* (2018).
48. Y. Qiu and M. Ma, "A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks," in IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2074-2085, Dec. 2016.
49. S. Raza, L. Seitz, D. Sitenkov and G. Selander, "S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things," in IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1270-1280, July 2016.
50. Manshahia, Mukhdeep Singh. "Swarm intelligence-based energy-efficient data delivery in WSAN to virtualise IoT in smart cities." *IET Wireless Sensor Systems* 8.6 (2018): 256-259.
51. H. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X. T. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Thing Applications," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. PP, no. 99, pp. 1-10, 2017
52. Chen, Yong, Li-Xin Zhou, and Huan-Lin Liu. "A Fiber Bragg Grating Sensor Perimeter Intrusion Localization Method Optimized by Improved Particle Swarm Optimization Algorithm." *IEEE Sensors Journal* 18.3 (2018): 1243-1249.
53. H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Talos: Encrypted query processing for the internet of things." In Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, pp. 197-210, 2015
54. S. Rahman, S. A. Mamun, M. U. Ahmed and M. S. Kaiser, "PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 2531-2536.
55. Mohd, Bassam J., and Thaier Hayajneh. "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques." *IEEE Access* 6 (2018): 35966-35978.

AUTHORS PROFILE

Nasreen Fathima received MTech from National Institute of Engineering, from Visvesvaraya Technological University, India in 2009. She is currently serving as Assistant Professor in Department of Computer Science and Engineering at Academy for Technological & Management Excellence College of Engineering, Mysuru, India and have a total teaching experience of 15 Years. Her research areas are Wireless Networks and Internet of Things. She has published 6 papers in International Conferences, Journals and National Conference. Life member of ISTE and CSI.

Dr. Reshma Banu, is Professor & Head, ISE Dept at GSSS Institute of Engg & Technology for Women, Mysuru. Has 19 yrs of Teaching and Research Experience. She has won Best HOD of the year by CSI, Best Paper Award by *CSI, National Level*, Young Scientist Award from AUFAU,VIRA-2016. Has received Best Accredited Student Branch" by CSI and Funds for Best Projects by KSCST for 3 consecutive years also received VGST, Karnataka, SMYSR Fund by VTU TEQIP1.3 in 2020. Is Organizing Chair for IEEE- ICEECCOT during 2016,2017,2018 & 2019. Is Senior IEEE member, ISTE, CSTA,IAENG,CSI,SDIWC.

Dr. G. F Ali Ahammed received Ph.D. degree from Sri Krishna Devaraya University, Anantapur (A.P) in 2011. Presently he is guiding six Ph.D. scholars. He has 17 years of Academic, Research and Administrative experience and has published more than fifty research papers in National, International Journals and Conferences. He is currently working as a Associate Professor, in Department of Computer Science & Engineering at VTU Centre for Post Graduate Study, Mysuru .