CHAPTER 7

CONCLUSION AND FUTURE SCOPE

Internet of things (IoT) has now become a fascinating system that improves information technology for its use in homes, cities and medical sectors. IoT works as an extension of internet to realize interconnections among every day object based on platform independent communication protocols. Object forming IoT must possess sensing, communication, and computation capabilities leading to a convenient as well as economical assistance for society. Interaction among heterogeneous objects enhances the security vulnerabilities in IoT. With security as a prime concern, communication in IoT need to maintained using a secure mechanism to protect the system from attacks.

7.1 Conclusion

In last few years, with gradual growth in Information and communication technology (ICT), the epoch of smartly operated things has evolved at exponential rate. Thus, IoT is taking its place in homes, office, cities, agriculture, business and many more at a very fast pace. One of the promising technologies using the things smartly is IoT. These smart things are capable of communication as well as can make decision depending on persuaded processing. IoT involving things for communication may belong to users of different functionalities, which raises a concern on privacy and security of data from the diverse users. Therefore, one of the significant contributions in the advancement of IoT is security.

IoT has evolved as an innovation of next generation in this world of smart devices. IoT intends to provide services for data collection, data management, data and device security for application development. IoT supports interconnection of various heterogeneous things such as sensors, cameras, devices, smart phones for offering automation in home, health care, industry, or military. Things or devices in IoT communicate and compute to make our lives comfortable and safe. In inventory automation, real time check on items, their information management, status
management, monitoring can be carried out using IoT. The huge amount of data that flows among the devices in the network demands for a security framework that ensures authentication, authorization, integrity and confidentiality of data. IoT has evolved as the fast adapted technology among the users due to its anywhere anything connectivity. As anything can connect, this may impose a serious impact of security of data for these connected devices.

Smart things in IoT are enabled to compute, communicate, and take decisions related to any network activity. Therefore, this requires a secure solution of communication between heterogeneous devices.

Number of security solutions is available in literature for IoT. Traditional security solutions like AES, DES, RSA, and many more do not fit at all in resource constrained IoT. These traditional solutions take much power and resources from the devices part of IoT scenario. Therefore, security algorithms that are lightweight are appropriate for IoT devices due to their less power requirements and optimum memory.

Security solutions when offered with IoT will add the trust of users. This call for a secure solution requiring less power for computation and is also less vulnerable to existing attacks. The security primitives expected from IoT scenario are authentication, confidentiality as well as data integrity. In order to offer these security primitives, this research work divides the whole work in three major objectives.

First, a Hybrid Lightweight Security Framework (HLSF) is proposed. This proposed HLSF consists of three phases; first phase is registration where credentials are allocated to every device that joins the network, second phase is authentication where device and server authenticate each other so that the later communication is from the legitimate user, third phase is data security that is provided by proposed Lightweight Data Security (LDS) algorithm. Therefore, HLSF offers authentication, confidentiality and integrity services to data flowing to and from devices.

Second objective of this research work, is compare the proposed HLSF with the existing security solutions. In order to achieve this objective, first existing lightweight security solutions like SPECK, SIMON, FANTAMOS, TWINE, LDS are compared on the basis of code length, memory requirements, execution time, throughput, avalanche effect and the number of CPU cycles. This comparison shows the LDS is
the better performing security algorithm among all these. Later, SPECK is compared with the proposed LDS with different variations in terms of block size, key size, code length, memory requirements, execution time, throughput, avalanche effect and the number of CPU cycles.

Third objective is to perform cryptanalysis of SPECK and LDS by implementing Differential attack on both. Results show that SPECK is compromised in 19 out of 27 rounds whereas LDS is compromised in 10 out of 20 rounds. The overall throughput, packet delivery ratio, and latency of LDS are compared with SPECK. Results prove that LDS outperforms SPECK as well is less vulnerable to differential attack. Later, the decision making is made by applying data mining on the data collected from HLSF. Effectiveness of data mining is evaluated by calculating the precision, accuracy, and recall of IoT scenario using HLSF and by comparing it with IoT scenario by using CoAP as a security mechanism.

7.2 Future Scope

IoT makes the life of user comfortable by offering a network that senses, collects, and makes decision effectively. Everything when connected to network is exposed to more number of attacks. Therefore security addition in IoT network will increase the trust level of user.

This research works in this direction only to offer an efficient lightweight security solution in IoT that can do effective data collection using sensor, performs data mining for decision making, and is less vulnerable to attacks.

The future scope of this research work can be to propose an efficient method for sensing on securely collecting the data from sensors. This will further chop down the power usage of sensor node. Moreover, this research work can be implemented in different application scenarios like smart homes, health care automation, or industry driven projects.