IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 8, August 2019

# User Activities and Location Based Authentication in IOT Automation

**Sangeeta Kol[1], Prof. Deepak Pranjpe[2]**

P.G. Student, Department of CSE, Global Nature Care Sangathan Group of Institutions, Jabalpur, MP, India[1]

Assistant Professor, Department of CSE, Global Nature Care Sangathan Group of Institutions, Jabalpur, MP, India[2]

**Abstract:** Recently, advanced technologies in the semiconductor process have a great developed with nano technology. It enabled cost effective solutions to directly integrate wireless network connectivity with embedded processors and sensors. From the improved technology, IoT lead to great interest in the field of information and communication technology, it is defined as integrated, fused and networked interconnection with objects. Security challenges in IoT include privacy, authentication and secure end-to-end connection. In addition, with the presence of multiple smart home standards currently used in market, any security scheme needs to consider inter-compatibility among the multiple standards. We analyzed and surveyed critical issues for technologies and securities of IoT, and discussed the applications and challenges of smart home network and related to IoT systems. Finally, to provide secure authentication procedure, we proposed the security protocol in IoT service in this paper which is based on user activities and locations.

**Keywords:** Internet of things, Authentication, Security, GPS, User Activities, Confidentiality, Integrity

## I. INTRODUCTION

IoT was first introduced in 1980s, but at that time it was not popular, and its increase rate was low, however a decade ago, IoT started to increase exponentially, there are many reasons behind that increase such as: Internet which is cheap and almost accessible all over the world. Over the last few decades, the number of internet users has exponentially increased in all countries, even in low income countries, people can access internet. Electronic manufacturers are developing new chips which are so small, consume low power and they are cost effective. Computer software and network technology have developed dramatically over the last few decades. Implementation of IPv6 which will allow each object on the earth to have its own Internet protocol (IP) address is another precursor to the growth of IoT. All those factors made IoT to experience a rapid growth and popularity.

For IoT vendors selling hardware and software products, their annual revenue will reach 470 billion of US dollar by the year 2020. For consumers, there is an area where IoT has played more important role; that is healthcare. By implementing IoT in healthcare, patients, medical doctors, and hospital have benefited from it. For example, a remote healthcare monitoring is an application of IoT where doctors can monitor their patients remotely and get to know the status of their diseases without physical contact. Another example of IoT in healthcare is a heart rate monitor; what if my phone can monitor my heart speed rate and if there is something wrong it will call ambulance and it will give the ambulance the exact location of where I will be, it will reach there and pick me to the hospital then doctors will take care of me. It sounds amazing. For wearable's devices, these devices have played a tremendous role by helping individuals to keep track on their body weight balance and stay healthier, wearable's devices are very popular due to their low cost and they are fashionable. For homes, IoT has created what is called a smart community. It connects entire house with all appliances such fridge, door, gates, camera, light bulb, kitchen. Those appliances are connected to the internet and they can be controlled via application installed on a smartphone or any computer. That helps the owners to control their entire home remotely whenever they want wherever they are. For example, a person who is in Maldives for a vacation can see and control what is taking place in real time at his house located in Kiev, Ukraine.

### 1.1. Security and Privacy challenges in IoT

IoT has contributed a lot in different areas such Business infrastructure, industrial control systems where the entire factory can be connected to the internet be controlled via smartphone. IoT has also played a tremendous role in healthcare sector. Despite all mentioned achievements, security and privacy remain a big challenge in IoT. But the question is why security and privacy are so challenging? Here are the answers:

- many IoT systems have both hardware and software vulnerability that remains unpatched. If a hacker exploits those vulnerabilities, there will be zero-day attacks. That could be a disaster for the entire organization; it will be hard to mitigate those attacks because the manufacturers were not aware of vulnerabilities.
- IoT is exposed to larger attack surface. Because devices are connected each other, many attacks are possible not to one device but to the entire network.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 8, August 2019

Consumers have low knowledge of IoT; people enjoy IoT, but few understand how it works and they don't pay attention to the security issues.

### 1.2 CIA TRIAD IN IOT

IoT will reach its full potential and full popularity only if interactions between connected devices fulfill the fundamental security model which is known as CIA triad (confidentiality, integrity, and availability)

#### *A. Confidentiality*

IoT manufacturers and vendors must make sure that data being transmitted in connected devices will be accessed only by authorized people, i.e. consumers. But confidentiality has remained a challenge to IoT because so many devices were discovered exchanging data in cleartext in IoT system. The other issue is the misconfiguration of wireless access point (WAP), sometimes users choose the password which is not strong without mixture usage of upper case, lower case, numbers and special characters. IT experts discovered that most of users prefer to use weak password such as 1234, this is a big mistake because attacker with a password cracking tool can easily break that password and gain access to the IoT system. Confidentiality between IoT can successfully be achieved by using updated and strong encryption such as Advanced Encryption Standard (AES).

#### *B. Integrity*

Data being transmitted among IoT systems must remain unchanged during the entire life cycle. For example, imagine a patient with implantable cardioverter defibrillator, that device reports the status of a patient to the medical doctor who is located at a different remote location. Imagine what could happen if the data is being sent from a patient to the doctor has been tempered by a hacker. That could be catastrophic, because such situation can even cause the death of a patient. The doctor will receive the information from patient and he will not be aware if the data has been tempered or not, as a result he will treat the patient according to the false information. That situation could be a worse scenario in healthcare; it could happen if data integrity was not highly considered. Integrity in IoT can successfully be verified by using hash function, such as SHA 256 (Secure Hash Algorithm 256).

#### *C. Availability*

Availability in critical devices must be 99.999%, i.e. the downtime will be as minimal as possible. Availability can be achieved by removing any single point of failure, it could be considered a worse scenario if connected devices in critical systems run over a single point of failure. If that single point failure fails, the entire system will be down. We achieve a high availability by applying redundancy. The following Fig. 1.2 shows how to remove a single point of failure by applying redundancy.

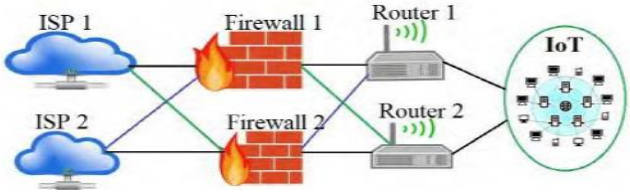


Figure 1.1: Redundancy system applied to IoT.

Security is one of the major players in the IoT environment. In recent past the numbers of cyber-attacks and cybercrimes have risen exponentially. Attackers mostly exploit constrained devices because these devices have low or no security at all. In not very distant past several cases were reported where an attacker took control of such constrained devices using bots and used them to mount DDoS attacks. Network as well as security protocols that were used in traditional internet cannot be used for the IoT because of the constrained nature of the devices and low throughput of the network. IoT requires new protocols for communication and security purpose that have low computational complexity, less throughput, low power consumption, etc. In other words, light weight security protocols are needed for IoT environment. For Networks and Devices to be secure, they require strong authentication protocols. Authentication is the process of verifying an entity's identity. Best security practices state that authentication protocol should involve at least two different types of credential. Authentication in IoT is challenging because the entities involved in the IoT environment cannot afford to include cryptographic primitives which have high computational complexity as in traditional internet. Although, the threshold of computational complexity can be increased by using schemes which utilize middle-ware such as gateways for computation. The gateway nodes are slightly more powerful than the IoT devices. Over the years several authentication schemes have been proposed for constrained devices and networks.

### 1.5 Security in the Internet of Things

Internet of Thing (IoT) is an entity -to- entity communication in which devices, or things, associate with the system to give data they accumulate from the environment through sensors, or to permit different frameworks to connect and follow up on the world through actuators. The IoT is a developing idea that contains a developing number of

advancements and displays a scope of evolving elements. Among these, we witness an explosion in the amount of smart things and better methodologies for collaboration with frameworks. Instances of such IoT frameworks are inescapable medicinal services, propelled assembling administration frameworks, smart city administrations, public surveillance and data acquisition or participatory detecting applications [1, 2]. The universe of IoT is simply beginning, these scenarios emerges a set of common challenges and patterns. The Heightened security dangers is one of the critical issue which ought to be resolve or give cautious thought towards it, deadness of those issues can have undesired outcomes, e.g. dissatisfaction and frustration of new administrations, harm to notoriety, or exorbitant claims.

Security is a fundamental requirement of IoT system and it becomes more and more important with the rapid development of network attacking techniques. Security means that the identities of communication entities need be authenticated and the data integrity and secrecy must be guaranteed. Although traditional IP-based security protocols can be applied in IoT systems, new issues arise and need be investigated thoroughly. One issue is related to the protocol performance. As many wireless sensors may be battery powered and have limited computing, storage and communication capabilities, simple and efficient techniques and protocols are expected by users. Traditional IP security protocols like the IPSec, SSL, TLS, and HTTPs [3] are assumed to work on the Internet hosts which have strong computational power and rich storage. They rely on the public key infrastructure (PKI) to support the authentication of public keys and digital certificates. The drawback of the PKI is that we need to manage digital certificates for a large number of sensors in a large-scale IoT system. The storage, transmission, authentication and updating of digital certificates will incur great overheads. Thus, it is argued that the identity-based cryptography (IBC) is more suitable for WSNs and IoT systems.

## II. RELATED WORK

The Internet is a network of networks, connecting computers and other gadgets together to share information. What has changed increasingly over the past two decades is the ability to connect remote and mobile “things, “objects”, “utilities” or “assets” to the Internet and the cloud using wireless communications and low-cost sensors/computing/storage [4]. Johnson in his view make an allusion that when all these things are interconnected within the network of networks it is called the Internet of Things (IoT). IoT is growing at an exponential rate while its connected components are becoming cheaper and more flexible to use. Kouns [5] indicated that by 2020 there will be over 26 billion connected devices. Others such as, Gartner, quoted by Kouns [5] predicted that by 2017, given the rate at which IoT is growing, 50 percent of employers may ask their employees to bring their own devices to work. The growth in the IoT is primarily fuelled by a lot of characteristics. Within this ambit, Holdowsky et al. [6] puts it clearly that this could be attributed to the improved computational power of microprocessors which is doubling every three years. Within the academic panoramic view, Kambies et al. [7] attributes this to the price of sensors that have consistently reduced over the past years with expectation that the price reductions will continue to reduce well into the future. For example, Johnson indicated that the average cost of an accelerometer is now 40 cents, compared to 2USD in 2006. Sensors vary widely in price, but many are now affordable enough to support IoT and businesses that come with it. Accuracy is also increasing. Holdowsky et al. gave an example, of water meters that are able to report more accurately than before. In terms of storage capacity, IoT devices have big storage and ability to collect huge amounts of data and even to transport it using high speed networks than traditional internet or computers. Notwithstanding the above advantages, devices connected to the IoT may, however, expose sensitive information and become potential security risks such as:

(1) Enabling unauthorized access and misuse of personal information;
(2) Facilitating attacks on other systems; and
(3) Creating safety risks.

For example, new smart televisions allow users to search the internet, make online shopping, and share videos and data [8]. With these security vulnerabilities, such televisions could expose the information stored or transmitted at risk [9]. Intruders could exploit vulnerabilities to facilitate identity passwords, credit card number theft or fraud. Holdowsky et al. [5] discovered that there are many implementation and configuration flaws in the IoT deployments and developments. For instance in [5] Holdowsky et al. states that flaws such as Denial of Service (DoS) can occur on machines connected to the IoT. DoS are when an intruder manipulates functionality of service on network infrastructure [10]. DoS attack is a concern due to the fact that it adds to the number IoT devices under the risk of being attacked, including remote IoT devices such as sensors, which are less unlikely to be properly secured, making them easier to be exploited [6]. For example, a compromised IoT device could be used to launch a DoS attack. DoS attacks are more effective; the more devices are interconnected the more intruders have access to it. As more and more devices become connected to the IoT, vulnerabilities could increase allowing these intruders to connect to some devices that could also be used in such attacks.

Fundamentally, the IoT creates ubiquitous digital presence connecting different equipment such as sensors which are very vulnerable to attacks. Security within the IoT is of prime importance so as to protect the information crossing through the network. As such, a lot of scholars and academics have proposed different security mechanisms for the IoT.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 8, August 2019

It is indicated that the more devices connected to the IoT, the more chances of security flaws exists, allowing unauthorized person to intrude the connection [11]. It is also indicated that, there are bit errors that occur in the ciphertext when it transferred over the IoT, same as over any other platforms of any wireless communications. When the cipher text is decrypted on the receiver side, it may cause half of the plaintext bits to be in error because of insufficient avalanche effect of algorithm used [12]. Protecting communication on the IoT is still very hard, not only in application data, but also when routing and other metadata. IoT has a lot of vulnerabilities ranging from the installation of algorithm in devices to weak crypto algorithms design and cross-site. Also, there are problems or concerns of privacy, lack of transport encryption, insecure software and firmware, insufficient authentication and authorization. Several methods have been proposed in order to combat this.

Different algorithms used on the IoT have been enhanced so as to secure the devices connected to the IoT. Fundamentally, these algorithms have been used to, based on extant research and practical implementations, have been used to secure the IoT. In line with the above, the avalanche effect is usually satisfied when changing of one bit in a text is complimented with an avalanche effect with a probability of more than 50%. The avalanche effect is used to test the strength of different algorithms used on the IoT. On a rather plausible academic research, Zibideh [13] showed that the avalanche effect is a desirable property for traditional algorithm like AES, DES and other well-known algorithm used on the IoT. Others such as, Ramanujam et al. [14] used ancient cryptographic algorithms (Playfair, Ceaser and Vigenere algorithms) to scramble input bits with modern cryptographic algorithms blocks of DES and Blowfish to make new algorithm. They used ciphertext of ancient algorithm as the plaintext of modern algorithm blocks. They found out that the average avalanche effect of standard Blowfish algorithm was 28.71%. Similarly, they found that the avalanche effect of standard DES algorithms was 54.68%. Khan et al. [15] compared Secure Force (SF), DES and AES algorithms. SF algorithm was non-complexity algorithm used on the IoT. It is usually used when installation space is limited on a specific device. SF 64, 128 and 192 gave the avalanche effect of 58.2%, 51.55%, and 45.70% respectively after one bit plaintext or key was flipped. Scholars such as Maaita et al. [16] published a paper where pseudo random number generator (PRNG) was used as to increase complexity of the key generation of DES and AES. Dewangan et al. [17] modified AES by changing the form of plaintext and encryption key. They mapped plaintext and encryption key in different binary codes before being used as the inputs of the AES algorithm. Paul et al. [18] applied matrix based key generation on AES instead of using standard key generation of AES. In their proposed method they indicated that there was an enhancement of avalanche effect of AES from 50% to 55% after 10 rounds. Within the ambit of this literature review, no one has ever tested avalanche effect using initial vector XORed with plaintext and final vector XORed with cipher text. In this paper we will use initial vector XORed with plaintext and final vector XORed with cipher text and test the avalanche effect of all the algorithms researched herein. The vectors will be extracted from irrational digits of PI after the digit 3.

## III.PROPOSED ALGORITHM

In the proposed method we are working on user authentication in Smart environment. This is based on two factor authentication. The first level authentication is based on user's gmail account that he or she already is using to get login or to access the services of smart phones. After the first level authentication the user will be prompted for second level authentication. User has to perform second level authentication when triggered for devices in the smart environment.

When user will perform the devices on/off for first time, the geographical co-ordinates will be registered with particular gmail address in the data table of database. Then the status of the devices is also sent to device history table. When the user will triggered action on the same location, the devices performs automatically because the co-ordinates are same. Here the learning is performed on user's location parameters. The security of the communication is done by using SSL.

In this work we have proposed a novel OAuth based authentication scheme (Gmail), by means of which user delegates a IoT application (Device) to access the data on behalf of resource owner. The proposed work provides a system (Device) might want to send an alert message. The location sensor is connected to device, it will generate the alert whenever there is change in location that should be mitigated, and then it notifies the Gmail whenever there is a incident or emergency. The architecture of open authorization shows the authenticated service. The data from service provider should access by the device on behalf of resource owner. Devices gets generates OAuth request that will be authenticated whether the username and password supplied is correct or not by service provider (Gmail).

**Figure 3.1** illustrates the proposed IoT based authentication system. The system consists of 4 major components: An IoT device, an IoT service provider cloud server (Cloud Server), Cloud Server for data storage and a user interface. The IoT device is responsible for triggering switches for smart home. The IoT device communicates with the cloud server through IoT network. This IoT system is accessible to the user using a mobile interface. In proposed system devices as well as user has direct cloud access. It's mean no local gate-way and no local database have to sync with server. Along with we will implement learning algorithm, by which once machine learns the behavior of the user. It may perform accordingly.

1) Parameter1: Gmail

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 8, August 2019

3) Parameter 3: Activities (Implementation as per logged in user).

**Proposed Algorithm for First level Login into system:**
Step 1: Login/Sign up with Gmail Auth. (First Authentication)
Step 2: Check Mobile GPS location and store it in cloud. (For second authentication).
Step 3: User patterns are recorded into cloud.
Step 4: End Process.
After completion of above process user can manage his IoT devices. Very next time when the owner wants to switch IoT devices from his smart phone, then the device list is available for owner without any authentication, because of ones the smart phone authenticate by gmail auth, the credential has been reused for every further logins. But when the cloud receives unknown location which is not stored in its cloud, then machine will ask for thumb impression for authentication. This increases the home automation security from remote access.
The figure below represents the above mentioned scenario.

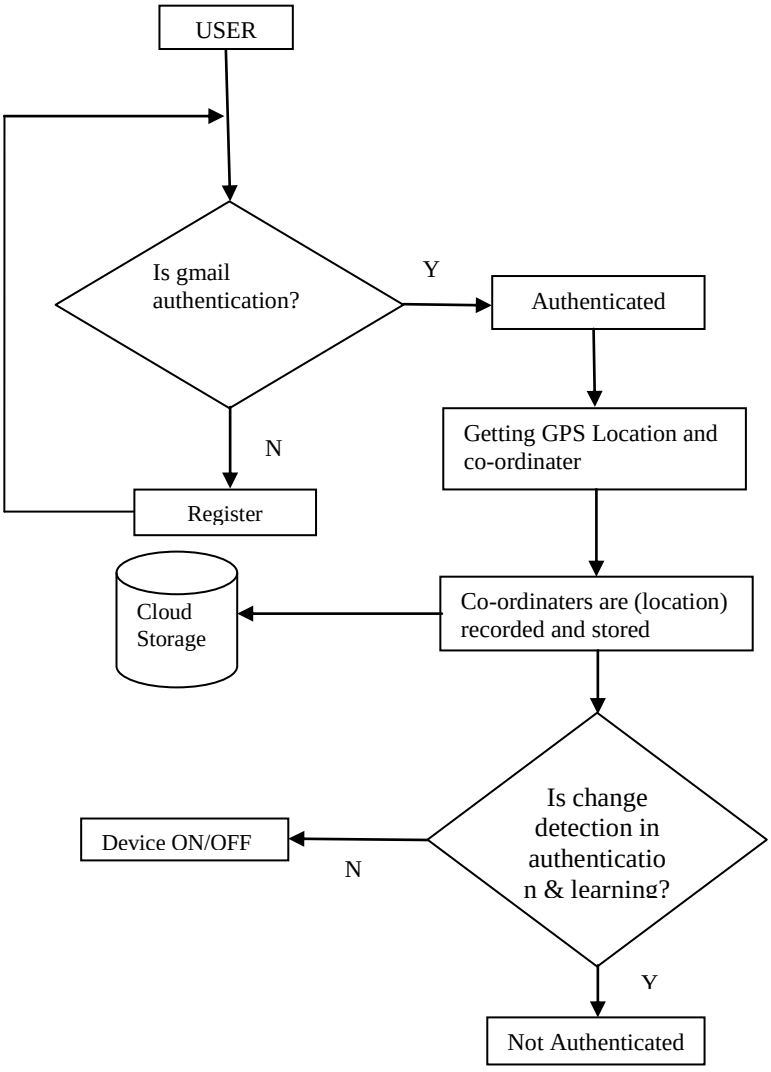


Figure 3.1: Architecture of Proposed System.

## IV. SIMULATION RESULTS

### 4.1 Results & Evaluation

The system was evaluated using a variety of metrics such as performance, security level calculation. The following Table 5.1 shows the results of performance evaluations determining the overhead on the request-level for these authentication parameters.
In existing system there was partial IoT concepts was used with local database. In the proposed method we are using complete IoT with cloud security engine (Google Plus). Than second we are using Google gps service for area wise authentication for authorized user. If existing user wants to operate its IoT devices from various gps locations in case he

has to register with fingerprint authentication. If the user gps location list avail in cloud, than he can easily use its IoT devices otherwise user has to authenticate using fingerprint.

Table 4.1: Comparison of used credentials for authentication.

| Used Credentials | Existing | Proposed |
|---|---|---|
| GPS | NO | YES |
| User Name/ Password | YES | YES (Gmail) |
| Database | LOCAL | CLOUD |

Table 4.2: Comparison of used credential time for authentication.

| Used Credentials | Existing Time | Proposed Time |
|---|---|---|
| User Name/ Password | 98 ms | 10 ms |
| Location | 90 ms | 70 ms |
| Location with User Name/ Password | 98 ms | 80 ms |

## V. CONCLUSION AND FUTURE WORK

S In this thesis we presented a cloud enabled smart-home IoT security framework which employs the user smart authentication factor. In our architecture, the smart-phone is a central element used to facilitate each device authentication to a cloud service. In the first part of the thesis we described a generic GPS and Gmail authentication framework which aims to provide authentication of an IoT device to a cloud service in a user-friendly manner.

### 5.1 Future work

In our future work we intend to adapt the privacy-preserving scheme to a smart city scenario by implementing the described model with hybrid machine learning model. This security solution will be adequate for embedded devices which are not designed for user interaction. In a smart city, a central device like a gateway could authenticate through devices (or other mechanism) to a cloud service, and then transfer the cryptographic material to each device from the network, thus mitigating privacy related security attacks. We will also adapt the authentication and authorization methods to an open-source cloud platform like Kaa IoT, thus permitting IoT devices to attach to user account in a privacy-preserving manner.

## REFERENCES

[1]. T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in Proceedings of the 14th ACM Workshop on Hot Topics in Networks. ACM, 2015, p. 5.
[2]. D. Harkins, "Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks," in Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications, ser. SENSORCOMM '08, 2008, pp. 839–844.
[3]. Shamir A. Identity-based cryptosystems and signature schemes Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 2014: 47-53.
[4]. T. Borgohain, U. Kumar and S. Sanyal, "Survey of Security and Privacy Issues of Internet of Things, "Department of Instrumentation Engineering, Assam Engineering College, Cornel University Library, 2015. pp 1-7. https://arxiv.org/abs/1501.02211.
[5]. J. Kouns, "Bring Your Own Internet of Things BYO-IoT" 2015 RSA Conference, pp 4-5.
[6]. J. Holdowsky, M. Mahto, M. E. Raynor and M. Cotteleer, "Inside the Internet of Things.
[7]. T. Kambies, M.E. Raynor, D.M. Pankratz and G. Wadekar, "Closing the digital divide: IoT in retail's transformative potential: The Internet of Things in the retail industry", 2016.
[8]. O. Vermesan and P. Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems," 2013.
[9]. Bourke, "CSCE 477/877", 2015 Cryptography and Computer Security Department of Computer Science & Engineering University of Nebraska—Lincoln, NE 68588, 2015, pp 5-138.
[10]. P. Trüb," π trillion digits of π", 2016 Project, DECTRIS Ltd. 5400 Baden Switzerland, 2016.
[11]. D. D. Moskovitch, "An Overview of the State of the Art for Practical Quantum Key Distribution", Vol. 4, 2015.
[12]. G. Patidar, N. Agrawal and S. Tarmakar, "A block based Encryption Model to improve Avalanche Effect for data Security", International Journal of Scientific and Research Publications, Vol: 3, 2013.
[13]. D. D. Moskovich. "An Overview of the State of the Art for Practical Quantum Key Distribution", Vol. 4, 2015.
[14]. S. Ramanujam and M. Karuppiah, "Designing an algorithm with high Avalanche Effect," 2011 IJCSNS International Journal of Computer Science and Network Security, vol. 11, No.1, 2011, pp 106-111.
[15]. K. Shujaat, I. M. Sohail, K. K. Ahmed and E. Mansoor "Security Analysis of Secure Force Algorithm for Wireless Sensor Networks performance evaluation of 64, 128 and 192 bit secure force algorithm architecture" 2014 Asian Journal of Engineering, Sciences & Technology, Vol. 4 Issue 2, 2014, p46-52.
[16]. A. A. Maaita and H. A. Alsewadi, "A Multi-Threaded Symmetric Block Encryption Scheme Implementing PRNG for DES and AES Systems," 2017 International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017 pp 76-82.
[17]. C. P. Dewangan and S. Agrawal, "A Novel Approach to Improve Avalanche Effect of AES Algorithm," 2012 International Journal of Advanced Research in Computer Engineering & Technology Vol. 1, 2012, pp 248-252.
[18]. A.J. Paul, A. Saju and R. Lekshimi, "Data based Transposition to Enhance Data Avalanche and Differential Data Propagation in Advanced Encryption Standard," International Journal of Computer Applications (0975 – 8887), vol. 67– No.12, 2013.