International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Securing Communication in IoT Ecosystem Using Cryptographic Algorithms

Anshul Jain, Tanya Singh

Abstract: ***Internet of Things (IoTs) is defined as an ever-growing network, which comprises of numerous physical objects with a specific IP address along with wireless internet communication, which enables the process of information sharing between two objects. Due to the frequent transfer and exchange of high confidential data between two devices through internet, there arise some susceptible attacks in IoT such as denial of service, eavesdropping attack and so on. A high-level authentication protocol and cryptographic techniques are required to resolve the issue of vulnerable attack and data loss. The current study presents a review of various IoT models and applications. Furthermore, the concerns related to security with respect to data sharing and numerous attacks have been featured in this paper. In order to avoid and minimize these attacks, numerous security measures and cryptographic algorithms have been developed by different authors. The study on several existing protocols has been carried out in this research along with the study on authentication algorithm developed by the authors. The result section contrasts a brief idea about the key requirements for the data security and authentication for the future aspects along with necessity of memory and power utilization. Additionally, some examination has been carried out briefing the future directions in which additionally work would be possible on the development of lightweight cryptography protocols.***

Keywords: ***IoT, Cryptography, Authentication, Energy consumption, Data security, lightweight cryptography protocols.***

I. INTRODUCTION

In recent times, the digitized data computing will be captured and differentiated through numerous smart application devices. The key example during the deployment is found to be Internet of Things (IoT) [1]. IoT is defined as a collection of distinct objects in which the interaction through numerous devices and data communication with other medium can be achieved through the wireless or wired communication medium. IoT can be stated as a real time communication medium which comprises of numerous sensors to provide communication amongst the network and the ability for the users to share and access information and take the required action based on the prerequisites. With the improvement of wireless sensor communication devices has led to new inventions in the field of IoT. Some of the applications of IoT are discussed below [2].

Digitized home automation framework, where the electronic things can be controlled in houses through portable telephones and workstations, in this way making a framework that empowers a brilliant smart home. It additionally gives the access of distinguishing crises; control of energy utilization inside the house, and so forth like:

- Smart vehicle transportation system where the traffic monitoring can be effectively achieved through monitoring, control the rate of traffic jams, and traffic violations observed can be effectively reported to the respective authorities.
- In environmental parameters measurement and control through forecast of cataclysmic events and detailing basic temperature changes, by steady checking of condition utilizing sensors. Observing Ecological contamination like estimating level of dangerous gases in air, substance of lethal material in water.
- In medical services where facilities from the health care can be given like remote checking of patients, steady observing of wellbeing parameters and exercises, bolster for autonomous living, checking medicines consumed by the patient and so on.
- In security applications, observing and mentoring, tracking of individuals, objects and creatures, examining spaces and betrayed regions, upkeep and maintenance of foundation and gear, alarming, alerting frameworks and numerous more offices have end up conceivable with IoTs [3].

A. IoT's Architecture

The nature of the deployed IoT infrastructure is usually heterogeneous. The elements, insight, intelligence and versatility of IoT has made it a prerequisite for future innovation yet in addition, it has made the IoT defenceless and unsafe with respect to security factors. The unique stages of IoT, which can be accessed easily has made it even more troublesome for the security analysts to discover far reaching answers and solutions for the present challenges in security. Hence, the significance of, comprehension of the establishment and the parts of IoT ends up important.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Tanya Singh, Dy. Director, Department of IT & Engineering, Banasthali University, India.

Anshul Jain, Technical Manager, Department of Network Technology and Management, Amity University, Uttar Pradesh, India.

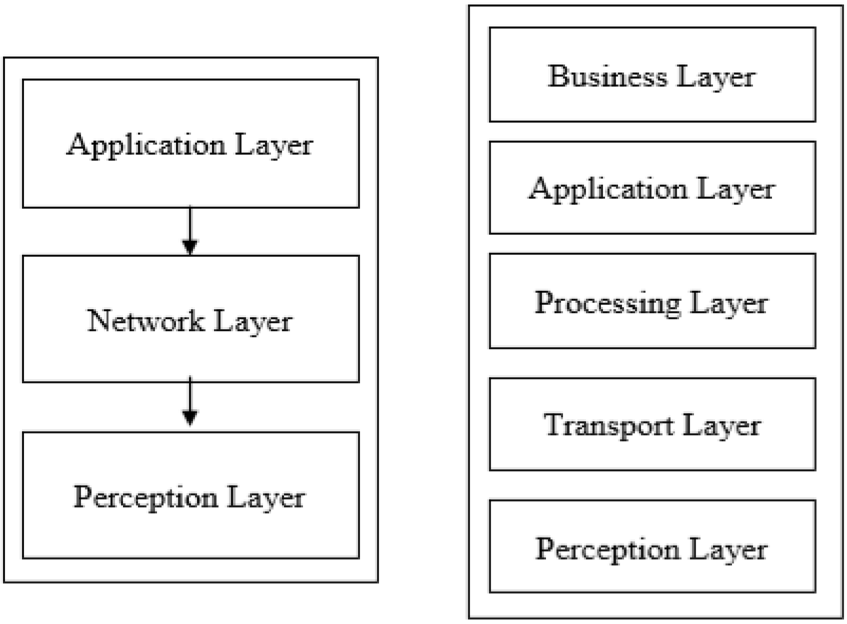

Fig. 1. Typical three layer and five-layer structure of IoT

he Authors in [4] examine the fundamental models of IoT which comprise of three layers viz. the physical, network and the application layers. The individual objects of the IoT are distinguished by the physical layer and it will also accumulate the data related to each object in the IoT region. This layer mainly comprises of cameras, RFID tags, sensors etc which are helpful in the process of gathering information. The network layer, also referred to as the centre of IoT will help in transmitting the data assembled by the physical layer. This layer mainly comprises of equipment and products of the system which mainly concentrates on the administration and data focus. The main objective of the application layer, which is the final layer is to act as a scaffold among the social and mechanical requirements of IoT. This design consisting of three layers gives the basic level data but does not completely classify the definite affiliation and structure of the IoT.

The author [5] has depicted an architecture model for IoT comprising of four layers with an assurance that it is the most suitable model. The four layers involved in this model are perception, accessing network in heterogeneous format, data management and the smart administration layers. The exchange of data among the digital and the physical world is found to be easier through this approach. The physical and the data perception layer are similar to each other. Network Access Layer whose nature is heterogeneous Approaches Web all around through an extensive variety of wireless medium, predominantly Wi-Fi, Zigbee, GSM, Bluetooth, WCDMA, WiMAX and Satellite. Information Management layer oversees information traveling every way. There are numerous data centre communities for cloud figuring, servers of directory management, which help during the process of data storage. The best layer called as Intelligent Service Layer gives astute administrations to the IoT clients covering zones like horticulture, home computerization, transportation, environmental monitoring and so on.

With the further advancement in technology, five-layer architecture has been developed with business, application, processing, network and perception layers. The characterisation of the applications of IoT is achieved by the business layer while the focus of the application layer is to decide the type of application which can be used by IoT. It will additionally make these applications simpler and more secure. The information assembled by the previous layers will be taken care of by the processing layer. This procedure has two fundamental highlights; data analysis and storage of the same in the database. Crafted by this layer is extreme as it manages huge amount of information. In this way, it utilizes a few strategies, for example, database programming, distributed computing, pervasive figuring, and smart processing in handling of information and its capacity. The network layer will help in the transmission of the information forward and backward among the perception and processing layers. It utilizes innovations like infrared communication, Wi-Fi and Bluetooth. This layer takes care of individual process in the framework by utilizing IPV6. The accumulation of data from the IoT framework and conversion of this information to signs is achieved by the perception layer. It utilizes advanced technology devices such as GPRS and RFID for the data accumulation process. The design ought to be skilled to give support to the application, quality of administration, security and information administration, and dependability, be flexible to numerous types of attacks and have optimized and upgraded execution.

The deployment of IoT comprises of numerous innovations with different properties for particular applications. Those innovations additionally raise some issues related to security which must be rectified depending on their abilities and restrictions observed with individual.

In this paper, review on the security protocols will be addressed along with numerous communication protocols such as ZigBee, Wi-Fi will be ascertained.

Its design methodology along with the design parameters and issues observed during the deployment along with authentication protocols will be explained in the following sections.

II. LITERATURE REVIEW

The IoT offers interconnectivity network between both human-to-machine and machine-to-machine correspondences. Soon, every device is probably going to be digitized with connectivity through IoT and its interface through Internet. This capability is beneficial for various spaces in our everyday life from building machinery, deployment of smart cities and observing the scheme of all the gadgets. Higher the number of IoT gadget implementations higher will be the threats faced by the framework of the data. A significant number of IoT equipment's are powerless against various security attacks like replay attacks, denial of services due to the constrained resource property and lack of numerous protection methods which will provide assistance to this type of attacks. This sort of attacks prompts sensors to consume more battery and leads to poor detection of applications. In more genuine cases, data spill from such little gadgets can open private, sensitive and critical information to the outside world, infiltrating the policy of confidentiality. In this segment, we right off the bat present the basic security properties for the IoT. At that point, we outline the difficulties to be tended to in the IoT.

The main aim of deployment of IoT is to enable the latest technologies of next generation devices, naming a few like smart wireless sensor networks (WSNs), development of smart cities through digitization, IoT based smart homes and mobile health monitoring devices. The implementation of these devices requires an authentication solution with high end security to prevent the confidential information from exposure or other means of critical actuating activities through peer transmission and secure information transmission between the IoT hubs and servers. Notwithstanding, the current IP-based IoT structure and natives are not completely composed with the confinement of asset obliged IoT gadgets, (for example, energy utilization, calculation of assets, correspondence ranges, RAM, FLASH, and so forth.). Subsequently, more lightweight security arrangements are important to guarantee the security at the situation of constrained resource IoT devices.

During the development of IoT environment, several limitations will be observed at the end nodes of IoT, which comprises of several aspects and few of them are as follows:

- Processing speed of the system resource, Its processor, RAM and the CPU.
- Storage space considered for the design process.
- Processing capacity of the communication network.
- Requirement of user interface, its additional embedded systems and display unit.
- Energy consumption of WSN environment.

Similar to that of the existing IP systems, in the distinctive situations of IoT, the cryptographic protocols in IoT are used to confirm to the principle security objectives for communication of network between individual nodes and the framework itself. The fundamental security objectives in IoT are as follows:

Data confidentiality: The data transmitted is revealed only to approved and the authenticated clients, nodes, specified devices and administrations. The privacy is about the controlling of numerous devices, accessing any required data. The private information, keys and security certifications must be very much shielded from unapproved and unauthenticated entities.

Data integrity: In the design and development of IoT based systems, the integrity requirements will depend on the type of particular application like e-healthcare systems which will be restricted with the integration device constraints compared to the application of smart city.

Authorization of the concerned data and its authentication: The integration amongst numerous IoT devices will give rise to the limitation of authentication due to the process of access control and the characteristics of IoT systems.

Availability of resource: The framework should continuously serve its need and remains uninterruptedly accessible for authentic elements. The IoT frameworks are required to be powerful and robust to give administrations such that it can be accessed at any time.

III. METHODOLOGY

The process of IoT can be realized through numerous communication protocols and the deployment of the same are done based on designed IoT architecture layers. The main function of perception layer is to determine and track the correct objects for data transmission. Several technologies have been deployed to achieve the same and some of them are RFID based devices, WSNs and bar code determination. The next layer in WSNs are network layer in which several standard protocols are deployed to evaluate the process of routing, and determination of effective path for data transmission to ensure safe and secure data transmission. Some of these protocols will be explained in the following section as follows:

1. Protocols

A. *IEEE 802.15.4*:

IEEE 802.15.4 is a data communication protocol which is developed for the application of MAC layer and physical layer in wireless personal area networks [6], [7]. The objective of this protocol is to concentrate more on the deployment of low-rate wireless personal area networks (LRWPANs), enabling low rate associations of all things which use less energy in individual region, transmitting at a low rate and ease [8]. The stack of this protocol is designed based on Open System Interconnection (OSI) show, where each layer just executes parts of transmission capacities, also a lower level layers can administer the upper layers. IEEE 802.15.4 aids the groups with bandwidth range of 868/915M and 2.4Ghz, and the rate of transmitting information on these groups can accomplish as high as 20 kbps, 40 kbps, and 250 kbps, separately [40].

This protocol is a premise for some remote correspondence advancements and conventions, for example, Zigbee [9], Wireless HART [10], and so on. In real time scenario, IEEE 802.15.4-based WSNs work in the region of different remote systems that are considering various advances. Such arrangements confront the test of interfering with different communications because of having these advanced technologies, like 802.15.4, in the unlicensed Modern, Scientific, and Medical (ISM) band at 2.4 GHz. Models of these innovations incorporate 802.15.1 (Bluetooth) and 802.11 (WLAN). The interference process takes place during the overlapping of the 2.4 GHz wireless communication devices in particular frequencies, time, and space. This obstruction will seriously influence execution of the existing clustered networks. Furthermore, there is a requirement of relieving the impact of interference experienced by the system during the process of data communication. There have been numerous works that concentrates and defines the issue of interference from the viewpoint of the 802.15.4 PHY layer [11]- [14]. From the 802.15.4 MAC viewpoint, we can feature a few key commitments as well. Jung et al. in [15] introduced an interference intercession plan to determine the concurrence of ZigBee and WLAN systems. The author has mainly concentrated on some scenarios where a network of ZigBee network is gathered with a few WLAN systems in such a way that the previous can't discover a channel free of interference to initiate its interchanges. To determine this circumstance, the author has presented an interference mediator (IM) that employs ZigBee and WLAN modules to organize the interference amongst the systems.

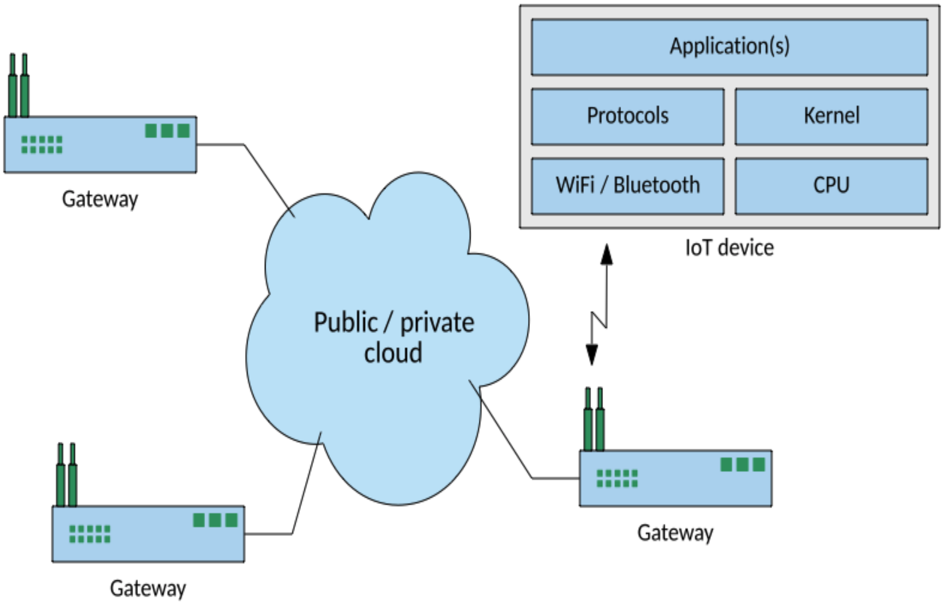

Fig. 2. The IoT ecosystem

Source: https://developer.ibm.com/articles/se-iot-security/

B. Wi-Fi

With the advancement and development of wireless devices and SoC innovation, numerous sorts of Wi-Fi remote sensor SoC chips are being created for low power applications. Another type of Wireless Sensor Network(WSN) which go with it, named Wi-Fi based WSN, came into reality [16-18]. Wi-Fi based WSN comprises of low power utilization nodes deployed for the identification zone, sink hubs and system that directors work by the strategies for self-association. WSN based on Wi-Fi is the mixture of mesh network in Wi-Fi and WSN has the advantages of both the technologies. The rate of power utilization in the utilization of wireless sensor nodes is low to the point that one AA battery is sufficient for a period of 5 to 10 years [19].

C. ZigBee

The process of Zigbee protocol is designed based on communication on short term basis with the rate of energy consumption kept at very low value. Five layers of physical, MAC, transmission, organisation and application layers were included in the design of this protocol [20]. The points of interest of Zigbee systems is due to the advantages of low energy consumption, ease of deployment, cost of deployment is very less, low data rate, complexity of the system is less along with high reliability and data security. Zigbee system can provide assistance to numerous topologies, which includes tree, star and work [21].

D. Z-Wave

Z-wave is a transient remote correspondence communication system with numerous advantages such as reduced implementation cost, low energy utilization, and high rate of reliability. The primary goal of Z-wave is to give solid and efficient transmission amongst control unit and at least one end-devices. It is suitable for the systems with less data transmission. It is seen that an approximate amount of around 232 nodes (slaves) can be incorporated into an organised network of Z-wave, and the controller with a routing capacity will control all the slaves [22], [23]. Z-wave arrange underpins the dynamic steering innovation, and each slave stores a course list in its memory, or, in other words the controller [24].

Albeit both of Z-wave and Zigbee provide assistance to the wireless communication devices of short ranges with minimal effort and low energy utilization, there are a few contrasts between them. The primary contrast among Zigbee and Z-wave is the band of frequency range of the physical layer. The frequency band for the physical layer in ZigBee is 2.4GHz and that for Z-wave is within 1GHz. The Zigbee system has the ability to aid up to 65000 slaves while the Z-wave can just aid 232 slaves [23].

In correlation with Zigbee design, the implementation of Z-wave is simpler and efficient.

Furthermore, numerous protocols have been introduced to enhance the rate of communication along with effective transmissions.

2. Design Methodology

In designing an efficient protocol for IoT systems, several key terms and concepts has to be considered and ascertained to make the design more effective. The key terms that should be considered will be explained in brief as follows,

A. Confidential [25]

Deployment of confidential parameter can guarantee that the information is just accessible to approved clients all through the procedure, furthermore, can't be interfered or eavesdropped by non-approved clients. In IoT, privacy is a vital security rule, since an expansive number of estimation devices (RFID, sensors, and so forth.) will be coordinated in IoT.

B. Data integrity [26]

The process of data integrity can guarantee that the information can't be altered by proposed or un-planned obstruction will be obtained during the process of information transformation in communication systems and at last providing the exact information for legitimate users. Integrity is essential in IoT, supposing that the applications of IoT get false information or altered information, wrong activity status can be evaluated furthermore, wrong input directions can be made, which could additionally disturb the task of IoT applications. To accomplish high rate of integrity, upgraded secure information trustworthiness components (false information separating plans, and so forth.) ought to be produced and connected.

C. Data Recognition and Authentication [27]

Recognition can guarantee that the devices with third party software's or non-authorized devices can't be associated with IoT, and the data authentication can guarantee that the information conveyed in systems are real, and applications that which demand the information are authentic also. In IoT, distinguishing and confirming every datum and question is troublesome, in light of the fact that an extensive number of various articles include an IoT. In this way, outlining effective systems to manage the verification of articles is basic in IoT.

D. Communication privacy [28-29]

The privacy can guarantee that the genuine user will control the information, and no one else can access or process the information. Not at all like secrecy, which means to scramble the information without being listened in and meddled by non-approved clients, security guarantees that the client can just have some particular controls dependent on got information and can't surmise other profitable data from the gotten information. Security is considered as one of vital security standards because of an extensive number of devices, administrations, and individuals having a similar network of communication in IoT.

E. Trust [30]

It can guarantee the previously mentioned security along with the key objectives of the privacy that is to be accomplished amid the communications among various articles, diverse layers of IoT and unique applications. The targets of trust in an IoT can be separated as trust amongst each layer of IoT, trust among the devices, and trust among numerous applications and devices. The protection and security can be upheld with trust. Trust administration frameworks ought to be intended to actualize these trust goals in IoT.

3. Security issues

The service layer in SoA-based IoT is built up by means of extricating the usefulness of information benefits in the layers of the application and system. Along these lines, challenges of security in the administration layer can be credited to issues in the system and the application layers. In this section, the numerous challenges of security in various layers are ascertained. Figure 3. illustrates a simple architecture of an IoT. It includes wireless devices inside and outside the firewall which are connected to the IoT platform. Then, the application will use data from these devices to perform the functions. Hence the applications, systems and the development tools that make up the system have to be secured.

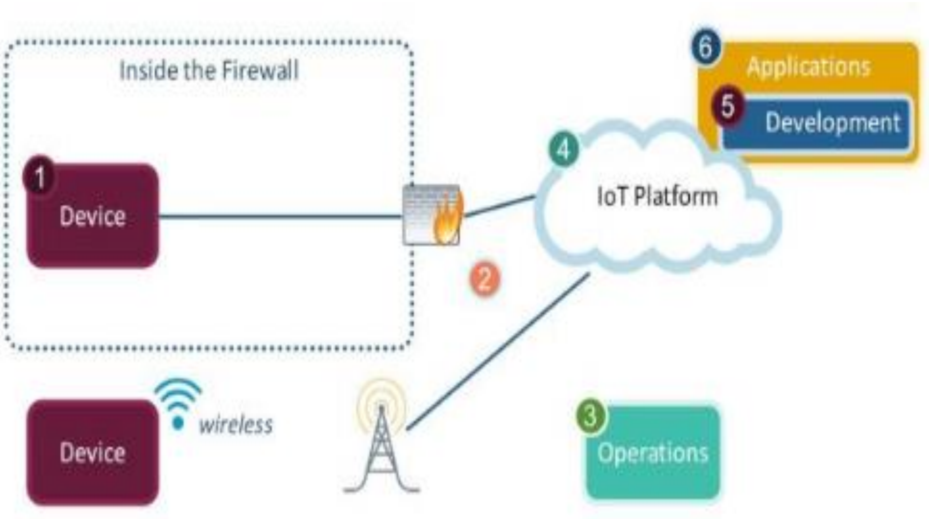

Fig. 3. Architecture of IoT security

Source: https://www.engineering.com/IOT/ArticleID/12554/IoT-Security-How-to-Protect Connected-Devices-and-the-IoT-Ecosystem.aspx

A. Node Capture Attacks

During this process, the foe can catch and control the node or device in IoT by physical supplanting of the complete node or alteration with a similar equipment of the device. When the node is imperilled by the node catch attack, the critical data (assemble correspondence key, radio key, coordinating key, and so forth.) can be presented to the opponent. The opponent can likewise duplicate the vital data related with the caught node to a malignant node, and after that, the malignant node acts as an authority to associate with the framework of the IoT This assault is meant as the node replication assault. A node catch assault can cause a genuine effect on the system. To safeguard against this attack of node capture, viable plans to screen and distinguish malevolent nodes should be considered [31].

B. Eavesdropping and Interference

Since, the vast majority of devices in IoT will impart data by means of wireless systems, the data loss or vulnerability attack takes place in the way that data conveyed in wireless links can be of eavesdropped through the non-approved clients. Calculations and key administration plans are needed for the management of secure encryption and eavesdropping. The opponent can likewise send commotion information or flag to meddle with the data conveyed in wireless networks. To guarantee the exactness and on time delivery of information, several efficient noise filtering techniques should be deployed for filtering the noise parameter in the data and re-establish the unique information [32].

C. Sinkhole Attacks

In WSNs based IoT systems, the sinkhole attack is mainly caused due to a traded off devices or node claims excellent abilities of energy, its computation, and communication, to such an extent that all the more neighbouring devices or nodes will choose the traded off device or node as the sending node in information directing procedure due to the engaging capacities. By doing this, the traded off device or node can build the measure of information and got previously delivered in the IoT framework. A sinkhole attack not exclusively can break the classification of conveyed information, however likewise can be a principal advance to dispatch extra attacks (DoS assault, and so on.). To shield against the sinkhole attack, methods, for example, secured routing protocols need to be considered and connected [33].

4. Cryptographic Algorithms

The devices deployed in IoT based systems, for example, RFID, cards with smarter technology, sensors nodes have a significant role to play in the system. The battery and memory of the worked devices is restricted by these devices. T The calculations of standard cryptography, (for example, AES) give great security yet their execution isn't worthy on these devices due to the huge memory prerequisites to store s-boxes, expansive square and key sizes. For determining these issues, NIST prescribed leaning toward lightweight calculations which gives security of the same level and their execution is likewise worthy on these gadgets [34]. The figure 4 illustrates the trade-offs between security, performance and cost. For lower cost small key and serialised structure is used. In case of high throughput, the number of rounds is less, and the rounds are more if the security is high.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

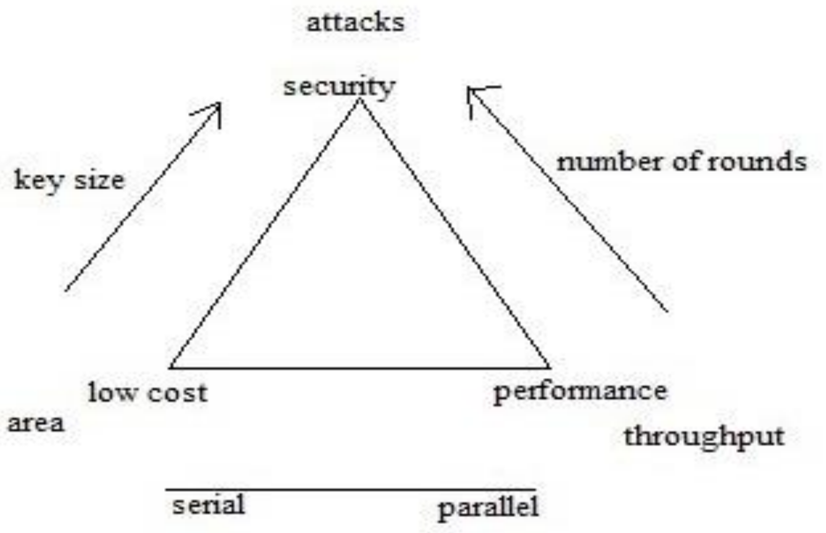

Fig. 4. Trade-off between the performance, cost and security for cryptography

A. AES

A low power link-based security algorithm for providing authentication at the layer security stage in IoT is developed by author [35]. At the initial stage, the author has carried out a survey on numerous security aspects and its performance evaluation at the link layer of IEEE 802.15.4 standards in IoT devices. The advanced encryption standards (AES) has been deployed in order to develop a symmetric block cipher which will be further utilized to develop, encrypt and decrypt the data by using similar keys. In specific, AES-128 based block cipher technique is used for the implementation of CCM and the symmetric keys are set at the range of 128 bits.

The overall authentication process is divided into two stages namely forward transmission where the data is authenticated at the transmitter stage and backward transmission where data is decrypted from receiver stage. Experimentation of the developed system is carried out using UNIX based platform and the results obtained shows that substantial savings are achieved in terms of the memory with an approximate range of up to six times along with reduction in the delay compared to other software counterparts. It is also seen that the hardware layer security links does not comprise with any significant impact in enhancing the network lifetime of the system [36].

B. ECC

Elliptic Curve Cryptography is an asymmetric key cryptography which depends on the elliptic curves. It was discovered in the late 1980s by Miller and Koblitz. It was found that ECC is suitable for smaller devices since it required lesser parameters for encrypting and decrypting when compared to Rivest Shamir Adleman (RSA) technique [42]. It was also observed that ECC was slow in the process of encryption and efficient in case of decryption.

C. PRESENT

An ultra-light weight block cipher titled PRESENT has been developed by author [37] to overcome the limitation of AES. In this research, both security aspects along with the efficiency of hardware systems is given high importance during the design and implementation of the cipher protocol. The architecture of present comprises with 31 rounds with the structure similar to that of the SP network. The generic block length is of 64 bits and is of the range of 80 to 128 bits. During the design of the developed protocol, add round key has been applied to the current data selection state followed by the deployment of S box layer which is of 4-bit range and permutation layer for data transmission. The generated key schedule will be of the length of 80 to 128 bits. The developed protocol is modelled using VHDL based platform and the results obtained from the study shows that better security is achieved with the developed ultralight weight cipher with the block size of 64 bit and size of authentic key is of 80 bit [38], [39].

D. SIMON

The family of SIMON block ciphers was mainly designed to provide security for a constrained device in which the design simplicity is a crucial factor [45]. The author discussed the algorithm and the design consideration for the SIMON block ciphers. The non-linear function of SIMON is composed of a bitwise AND operator and two rotations, which required minimal amount of hardware. the computations are also easily done. The round functions used are simple hence the algorithms can be realised easily, and it is well suited in case of constrained platforms.

E. CAMELLIA

Camellia is a block cipher which was developed together by Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation in 2000. The security level and processing abilities of Camellia can be compared to the advanced encryption standard. The author described the high speed and compact hardware architectures of 128 block ciphers CAMELLIA and AES [44]. This protocol is highly resistant to Brute force attacks on key generations and has better security when compared to AES.

F. TWINE

Twine is a lightweight highly efficient block cipher which supports 80 and 128-bit keys. It can be used for hardware which are extremely small, and it also provides a significant performance for embedded software. TWINE is of two types based on the bit keys it supports TWINE-80 AND TWINE-128. Both these algorithms have 36 rounds and block size of 64 bits. The number of iterations for both the key functions is 36.

G. HIGHT

A new block cipher namely HIGHT for the application of low source devices is developed by author [40]. In this research, the author has developed a new block cipher namely HIGHT which is of the key length of 128 bits and provides reduced resource hardware implementation which is suitable for the high technology object detection methods such as RFID. In encryption process, the key schedule comprises with the development of whitening key generation which is of the size of 8 key bytes, sub key generation in which 128 sub keys have been used for the single computation. In transformation process, the initial key is converted into the round function format and final transformation is of SWAP process. The decryption process is similar to that of the canonical form of encryption process. The result obtained from the analysis shows that better high-end security is achieved from the developed protocol.

H. RECTANGLE

A bit slice security light weight protocol namely RECTANGLE for the application in multiple framework is developed by author [41]. The key principle during the development is to develop an authentication protocol which is of both light weight and faster implementation by deploying bit slice techniques. A range of sixteen 4*4 S boxes has been used for the substitution layer structure and three rotations for a permutation layer. The deployment of this protocol both high range of accessibility in both the hardware as well as software environment which provides flexibility in different application scenarios. The deployment of this protocol has many advantages such as hardware friendly, reduced number of gates with high throughput and energy efficiency and high processing speed. The author has developed RECTANGLE protocol with an encryption speed ranged from 3.9 cycles per byte and from the study on findings show that the developed protocol provides high security range to numerous security attacks. Due to the advancement in internet and faster range of data transfer, there is a huge requirement of efficient and effective security protocol which can cope up with that range of data transmission with high end security.

I. RSA

Rivest Shami Adleman (RSA) is treated as the first practical and real life asymmetric cryptosystem. Hence its security depends on the integer factorisation problem (IFP) [42].

An efficient public key-based cryptography technique namely Rivest Shami Adleman (RSA) is implemented and developed by author. The practical and theoretical examination of its security determined that RSA is effective in case of encryption but slow in case of decryption.

IV. COMPARATIVE ANALYSIS

A comparative table is developed as shown in Table 1 based on the survey done on different cryptographic algorithms. The main goal is to transfer the given data in a highly authenticated format. Some key terms have been captured from the analysis and deployed in the table as shown below,

Table 1. Comparative analysis of various existing protocols

Algorithms	AES [35]	ECC [42]	PRESENT [37]	SIMO [45]	CAMELLI [44]	TWINE [43]	HIGH [40]	RECTANGLE [41]	RSA [42]
Type	Light weight	Light weight	Ultra-light weight	SPN based structure	SPN based structure	FN based structure	Ultra-light weight	SPN based structure	Light weight
Key Length in Bits	128	163-571	80-128	128	128	80-128	128	128	1024-15360
Block Size in bits	128	-	64	128	128	36	64	64	-
Area in GE	2400	-	1030	1317	6511	1866	3048	1787	-
Power Consumption in uW	2.48	-	1.54	1.32	1.54	1.30	5.48	1.78	-

Scalability in uM	0.13	-	0.18	0.13	-	0.09	0.25	0.13	
Throughput evaluated at 100kHz in Kbps	56.6	-	12.40	178.0	290.10		188.2	246	-
Possible Attacks	Boomerang, fraud key generation	Edge channel attacks	Internal attacks, differential cryptanalytics, edge channel attacks	Differential attack reduced	Timing delay attack, differential attack	Off break attacks, saturation attack	Biclique cryptanalysis, Differential attack	Slide based attacks, cryptanalytics	Middle timing attack, factoring attack
Summary	Provides assistance to larger values of key sizes. Processing speed is faster	High processing speed and less memory requirement	High energy efficiency	Provides support to high key size, efficient software performance	High resistance to brute force attack on key generation. Good security compared to AES	Suitable for small sized hardware, performance is highly efficient	Advanced security parameters along with better RFID tagging	Easy implementation through bit slice technology	High end security can be achieved

V. RESULTS AND DISCUSSION

Throughout the survey and analysis on different authentication protocols, several key concepts have been depicted which will be useful in analysis and development of security algorithm in future. The key aspects are as follows:

- In IoT, information validation and security are major concern, hence the quantities of systems introduce hybrid schemes for encryption and validation calculations are made (for example, hybrid model of AES and RSA system). However, this results in an increase in the requirement of memory. The encryption protocols work in the CCM mode (where both security and verification are provided) to resolve this issue.
- In the deployment of lightweight protocol, it gives similar security level as in regular security algorithm with the quantity of rounds being expanded. The vast quantity of rounds corrupts the execution. Along these lines, the future research course is to develop a lightweight protocol, which gives quick confusion and diffusion with reduced number of rounds.
- The protocols such as RSA and ECC is a mathematical demonstration dependent on discrete logarithm and measured math. This type of modelling incorporates vast number of augmentation activity. In this way, is used to evaluate the traditional process of Vedic Multiplier, (for example, UT and NDD Vedas) in place of regular multiplier for quick reaction.

VI. CONCLUSION

The IoT has been quickly discovering its way through our cutting-edge life and is intended to enhance the nature of life by associating us with various miniaturized devices with numerous approaches, applications and innovations. The IoT is to develop a situation of finish automation, robotization by replacing the traditional manual systems. In spite of the fact that several researches have been carried out in the field of IoT, yet at the same time there is something else entirely to investigate. The rising consideration of enterprises and governments in this innovation has prompted a far-reaching look into and brought about numerous effective ventures. A portion of the issues in IoTs like the general engineering, security and protection concerns have drawn tons of consideration, while others concern like accessibility, dependability and execution of the keen gadgets still require more thought. In this paper we have examined about the diverse designs, security, protection issues and lightweight arrangements that can be considered to overcome the limitations of security and authentication aspects in IoT.

REFERENCES

1. K. Zhao and L. Ge, “A Survey on the Internet of Things Security,” in Ninth International Conference, on Computational Intelligence and Security, Dec. 2013, pp. 663-667.

2. R. Khan et al., “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” in 10th International Conference on Frontiers of Information Technology, Dec. 2012, pp. 257-260.
3. Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.
4. E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” in Computer Communications, 54, pp.1-31.
5. O. Said and M. Masud, “Towards Internet of Things: Survey and Future Vision,” in International Journal of Computer Networks, 2013, vol. 5(1), pp.1–17.
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
7. Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In Internet Technology and Applications (iTAP), 2011 International Conference on (pp. 1-4). IEEE.
8. LAN/MAN Standards Committee. (2002). IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture (En línea). New York-NY-USA. The Institute of Electrical and Electronics Engineers Inc.
9. Kluge, W., Poegel, F., Roller, H., Lange, M., Ferchland, T., Dathe, L., & Eggert, D. (2006, February). A fully integrated 2.4 GHz IEEE 802.15. 4 compliant transceiver for ZigBee applications. In Solid-State Circuits Conference, 2006. ISSCC 2006. Digest of Technical Papers. IEEE International (pp. 1470-1479). IEEE.
10. Kim, A. N., Hekland, F., Petersen, S., & Doyle, P. (2008, September). When HART goes wireless: Understanding and implementing the WirelessHART standard. In Emerging Technologies and Factory Automation, 2008. ETFA 2008. IEEE International Conference on (pp. 899-907). IEEE.
11. Shin, S. Y., Park, H. S., & Kwon, W. H. (2007). Mutual interference analysis of IEEE 802.15. 4 and IEEE 802.11 b. Computer networks, 51(12), 3338-3353.
12. Won, C., Youn, J., Ali, H., Sharif, H., & Deogun, J. (2005, September). Adaptive radio channel allocation for supporting coexistence of 802.15. 4 and 802.11 b. In IEEE Vehicular Technology Conference (Vol. 62, No. 4, p. 2522). IEEE; 1999.
13. Pollin, S., Ergen, M., Timmers, M., Dejonghe, A., Van der Perre, L., Catthoor, F., ... & Bahai, A. (2006, June). Distributed cognitive coexistence of 802.15. 4 with 802.11. In Crowncom(pp. 1-5).
14. Shuaib, K., Boulmalf, M., Sallabi, F., & Lakas, A. A. L. A. (2006, April). Co-existence of Zigbee and WLAN, a performance study. In Wireless Telecommunications Symposium, 2006. WTS'06 (pp. 1-6). IEEE.
15. Jung, B. H., Chong, J. W., Jung, C. Y., Kim, S. M., & Sung, D. K. (2008, September). Interference mediation for coexistence of WLAN and ZigBee networks. In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on (pp. 1-5). IEEE.
16. Lei Yuan, Xiong construction, Zhao Xiaohui. “Wi-Fi-based wireless sensor network design and research”. Modern electronic technology, Nov.2009, vol.18, pp.192-197
17. Huang Jianqi, “Wi-Fi in the application of wireless sensor networks”, China New Telecommunications, 2008, vol.15
18. Shao Yuefeng, “Using Wi-Fi technology to build wireless sensor networks”, Electronic system design, Http://www.icembed.com/info28618.htm, July.2008
19. Wu line, “How to use the latest micro-power wireless SoC chip WiFi sensor network design”, Electronics world, http://www.eepw.com.cn /article/87545.htm, Aug.2008
20. J. Tan and S. G. M. Koo. A survey of technologies in internet of things. In Proc. of 2014 IEEE International Conference on Distributed Computing in Sensor Systems, May 2014.
21. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and zigbee standards. Computer Communications, 30(7):1655–1695, May 2007.
22. H. B. Pandya and T. A. Champaneria. Internet of things: Survey and case studies. In Proc. on 2015 International Conference on Electrical and Electronics, Signals, Communication and Optimization (EESCO), January 2015.
23. J. Tan and S. G. M. Koo. A survey of technologies in internet of things. In Proc. of 2014 IEEE International Conference on Distribute Computing in Sensor Systems, May 2014.
24. C. Gomez and J. Paradells. Wireless home automation networks: A survey of architectures and technologies. IEEE Communications Magazine, 48(6):92–101, June 2010.
25. S. Capkun, L. Buttyan, and J. P. Hubaux. Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing, 2(1):52–64, January 2003
26. X. Yang, J. Lin, W. Yu, P. M. Moulema, X. Fu, and W. Zhao. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. IEEE Transactions on Computers, 64(1):4–18, January 2015.
27. M. C. Chuang and J. F. Lee. Team: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Systems Journal, 8(3):749–758, September 2014.
28. X. Yang, X. Ren, J. Lin, and W. Yu. On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems. IEEE Transactions on Parallel and Distributed Systems, PP(99):1–1, January 2016
29. L. Zhang, Z. Cai, and X. Wang. Fakemask: A novel privacy preserving approach for smartphones. IEEE Transactions on Network and Service Management, 13(2):335–348, 2016.
30. I. Andrea, C. Chrysostomou, and G. Hadjichristofi. Internet of things: Security vulnerabilities and challenges. In Proc. of 2015 IEEE Symposium on Computers and Communication (ISCC), July 2015.
31. M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani. Node capture attack in wireless sensor network: A survey. In Proc. of 2012 IEEE International Conference on Computational Intelligence Computing Research (ICCIC), December 2012
32. J. R. Mohammed. A new simple adaptive noise cancellation scheme based on ale and nlms filter. In Proc. of Fifth Annual Conference on Communication Networks and Services Research (CNSR), May 2007.
33. G. Kalnoor and J. Agarkhed. Qos based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. In Proc. of 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), March 2016.
34. T. Eisenbarth et al., “A Survey of Lightweight-Cryptography Implementations,” in IEEE Design & Test of Computers, 2007, vol. 24(6), pp. 522-533.
35. Altolini, D., Lakkundi, V., Bui, N., Tapparello, C., & Rossi, M. (2013, July). Low power link layer security for IoT: Implementation and performance analysis. In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International (pp. 919-925). IEEE.
36. S.Aruna Sankaralingam, G.Usha, Ankita Acharya (2018). A HYBRID CRYPTOGRAPHIC ALGORITHM BASED ON AES AND SHA 1 IN RFID, International Journal of Pure and Applied Mathematics, Volume 118 No. 11, 835-840
37. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, September). PRESENT: An ultra-lightweight block cipher. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 450-466). Springer, Berlin, Heidelberg.
38. Z’aba, M. R., Jamil, N., Rusli, M. E., Jamaludin, M. Z., & Yasir, A. A. M. (2014). I-PRESENTTM: An Involutive Lightweight Block Cipher. Journal of Information Security, 5(03), 114.
39. Yap, H., Khoo, K., Poschmann, A., & Henricksen, M. (2011, December). EPCBC-a block cipher suitable for electronic product code encryption. In International Conference on Cryptology and Network Security (pp. 76-97). Springer, Berlin, Heidelberg.
40. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., ... & Kim, H. (2006, October). HIGHT: A new block cipher suitable for low-resource device. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 46-59). Springer, Berlin, Heidelberg.
41. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. Science China Information Sciences, 58(12), 1-15.

42. Mahto, D., Khan, D. A., & Yadav, D. K. (2016, June). Security Analysis of Elliptic Curve Cryptography and RSA. In Proceedings of the World Congress on Engineering WCE (Vol. 1).
43. P. Kumarkushwaha et al., "A Survey on Lightweight Block Ciphers," in International Journal of Computer Applications, 2014, vol. 96(17), pp. 1-7.
44. A. Satoh and S. Morioka, "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," in Lecture Notes in Computer Science Information Security, Springer, 2003, pp. 252-266.
45. R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers," in Proceedings of the 52nd Annual Design Automation Conference, 2015, pp.1-6.

AUTHORS PROFILE

Tanya Singh received the bachelor's degree in Electronics from M.I.T., Dr. Babasaheb Ambedkar University, India. Master's in information technology from School of Information Technology, Guru Gobind Singh Indraprastha University, New Delhi, India. Ph.D. in IT & Engineering from Banasthali University, India. Prof. (Dr.) Tanya Singh is currently working as Dy. Director (Academics), Amity University, Uttar Pradesh, India. With wide experience of over 20 years in the field of Teaching, Research, Planning and Development in Education and Operational role outs, she has emerged as Technical Evangelist for Networking, Cyber Security. Her aim is teaching and learning new technologies, assist and develop the knowledge amongst students, instructors by encouraging critical thinking, implementation and ability to convert technological ideas into innovation. She has more than 35 research papers in reputed journals with Thompson ISI, Scopus etc.

Anshul Jain received his M.Sc. in Network Technology and Management from Amity University, Uttar Pradesh, India. Currently, he is pursuing Ph. D. from Amity Institute of Information Technology, Amity University, U.P., India. He has a wide work experience of over 12 years in different multinational organizations in the field of Information security, integration, maintaining and troubleshooting Telecom softwares, IoT, RF, MFS (Mobile Financial Services), VAS (VMS/SMSC/Prepaid Recharge/Mobile Money), VoIP (IP based call center), Linux, UNIX, Solaris, SS7, VoIP servers. His research areas are Security in Information Technology on Internet of Things using innovative and latest technologies like blockchain and Artificial Intelligence. Currently he is working as a Technical Manager in amdocs.