Study of Security Threats and Challenges in Internet of Things Systems

Rohit Chawla [a], and Prof. N. K. Joshi[b]

[a,b] MIMT, Kota, India

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: The interpretability and secured communication are major challenge in internet of things. The embedding of wireless device has low energy and bandwidth. The low energy and bandwidth cannot effort computational overhead and compromised with security threats. Primary the conventional cryptography algorithm is applied for generation and sharing of key for mode of communication. The conventional cryptography algorithms have several bottleneck issues related to generation of key and distribution of key. The NIST models provides the secured communication channel in the environments of mobility. Lack of integrity, confidentiality and authorization process of data transmitted over the network of internet of things used the concept of key generation and allocation. The process of key generation and authentication provides the authorization and authentication of data over the internet of things. In this paper present the review of security threats of internet of things.

Keywords: IoTs, security, NIST, key generation, authentication, attacks

1. Introduction

The integration of technology born the concept of internet of things. The quick improvement of Internet-of-Thing (IoT) gadgets empowers the enormous combination of advancements from detecting innovation, correspondence innovation, information preparing, to distributed computing and artificial knowledge[1, 2, 3]. In this situation, sensors in the recognition layer gather information from nature and do quick handling. At that point, this information is transmitted through the system layers over the Internet to the cloud. In the cloud, information is additionally prepared by various applications[4], for instance, huge information applications or information mining applications to settle on choices or potentially to advise clients, and so forth[5, 6, 7, 8]. In any case, IoT gadgets and information transmitted through multilayer systems may contain private information or discharge information; while the Internet condition uncovered security issues, for example, individual protection, digital assaults and sorted out violations[9, 10, 11]. This raises the worries about the security and protection of the IoTs[12, 13, 14]. The answer for security and protection issues is to incorporate security highlights, for example, gadget identification, gadget/client verification and information encryption[15, 16, 17]. These security capacities are regularly considering the cryptographic calculations, including open key cryptography and symmetric cryptography, which involve handling force and increment power and vitality utilization[18, 19]. The present issues on security of the IoTs might be comprehended by utilizing the current accessible cryptographic natives[20]. Gadgets and conventions with appropriate utilization of identification, verification and information encryption will diminish the danger of uncovering emit or individual information to aggressors. Interestingly, symmetric cryptography including square figure and stream figure is adjusted to information encryption as a result of its quick activities[21, 22, 23]. Between two kinds of symmetric cryptography calculations, stream figures are fit for producing the encoded information stream quick, however they are restricted to just stream information encryption[24, 25, 26]. Then again, piece figures can be configured for various security capacities utilizing the task modes to be utilized as a stream figure, a square figure, or a component for validation[27, 28, 29]. It is more flexible for applications to utilize piece figures for various security purposes. Among piece figure calculations, AES is an all-around examined calculation which is generally utilized as a part of the present guidelines for IoT as well as for different applications, for example, arrange conventions, information encryption, and capacity encryption etc[30]. As of late, there has been the development of new square figure calculations that are lightweight as far as equipment or programming usage and memory impressions, yet they concoct diminished security levels. The respectability and privacy of information rely upon the security arrangement of system layers[31, 32, 33]. The rest of paper discuss as in section-II discuss the issue and challenge of IoTs. In section III discuss system model of cloud based IoTs. In section IV discuss the research goals of security and finally discuss the conclusion and future work in section V.

2. Issue and Challenges

The open communication models of internet of things faced a issue of security threats. The security threats of internet of things basically focus on three layers application layer, network layer and mac layer. The issue and challenges of security describe in format of tables.

Et al.	Author	DESCRIPTION	ISSUES AND CHALLENGES

[1]	Jun Zhou, Zhenfu Cao, Xiaolei Dong and Athanasios V. Vasilakos	1. Internet of Things 2. Network Architecture of Cloud-Based IoT 3. Security and Privacy Requirements for Cloud-based IoT 4. Secure Packet Forwarding in Cloud-Based IoT 5. Privacy-Preserving Authentication in Cloud-Based IoT	• How to design new efficient privacy-preserving solutions for next generation mobile technologies with IoT–cloud convergence is a crucial issue of great concern. • The first problem is fine-grained cipher-text access control in cloud-based IoT.
[2]	Prem Prakash Jayaraman, Xuechao Yang, Ali Yavari, Dimitrios Georgakopoulos and Xun Yi	1. Integrated privacy protection scheme for end-to-end security 2. Privacy preserving IoT architecture	• The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for matching attributes. User keys are issued by some trusted party. • We tackle the IoT privacy preservation problem.
[3]	Engin Leloglu	1. IoT Scope and Architecture 2. Security of IoT	Data security is another issue on these layers. There are various precautions taken by security system on IoT such as: • Safe programming and anti-virus software testing against malicious code injections and service loopholes, • Verification of data and developing temporary cache against malicious operations, • Session inspection mechanism to stop attacks of hijacking and redo sessions, • Boundary inspection, data encryption mechanism and resource access control to avoid leakage of privacy.
[4]	Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe	1. Survey of the Evolution of IoT Architectures 2. General Security Analysis of IoT Systems 3. Mobility-First-Based IoT Architecture 4. IoT Middleware Security 5. Delegation-Based Key Provisioning Protocol	• This paper addresses this issue by introducing a unified IoT framework based on the Mobility-First future Internet architecture that explicitly focuses on supporting security for the IoT.
[5]	Behrouz Pourghebleh and Nima Jafari Navimipour	1. Related terminologies and basic concepts 2. Research methodology	• The important issue of the tree-based mechanism is the building of an energy efficient data aggregation tree.

		3. Data aggregation mechanisms in IoT	• security is an essential issue for data aggregation process and it needs further examination. • The accuracy of the results is improved through the battery leakage issue in this mechanism.
[6]	Soumya Ranjan Moharana, Vijay Kumar Jha, Anurag Satpathy, ourav Kanti Addya, Ashok Kumar Turuk and Banshidhar Majhi	1. Preliminaries 2. Proposed Architecture 3. Simulation Results and Discussion	• The most important shortcoming of IoT cloud networks which needs immediate addressing is the issue of IoT nodes when used within a virtual network of a cloud system. • The issue here is the use of same access strategy across all devices making it to share a common password across all other devices within a network. • we addressed the issue of secure key-distribution in IoT cloud networks thereby reducing the infection between the user-groups within a IoT cloud network as well as managing the traffic for communication among the user-groups and IoT nodes present inside them.
[7]	Bilal Javed, Mian Waseem Iqbal and Haider Abbas	1. Applications of IoT 2. Future Prospects of IoT 3. Security Challenges 4. Design Considerations for IoT	• Embedded security becomes a key issue in IoT devices which are constrained in terms of processing, power, memory and bandwidth. • Intentional interference of GNSS signals, including jamming and spoofing, is discussed with a view on the legal challenges it presents. Legal issues are dis-cussed on a supra-national level, that is, in the framework of the European Union (EU). • Privacy of users' location information in LBS is an issue of increasing importance as more and more of peoples' sensitive location information gets recorded and stored into LBS.
[8]	Liang Chen, Sarang Thombre, Kimmo Jã, Rvinen, Elena Simona Lohan, Anette Alã Savikko, Helena Leppã Koski, M. Zahidul H. Bhuiyan1, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Pã„Ivi Korpisaari and Heidi Kuusniemi	1. Robustness and security of GNSS-based solutions for localization in IoT 2. Security of non-GNSS solutions for localization 3. Cryptographic techniques for secure and privacy-preserving positioning in IoT 4. Legal dimensions of location data privacy 5. Technical and legal requirements and recommendations for trusted localization solutions in IoT	• The key management problem in the defined access structure. • Scheme is secure against possible known attacks under the hardness assumption of factorization of RSA modulus N = pq and hardness of solving computational Diffie-Hellman problem (CDHP) • Under the hardness of solving the integer factorization problem, our scheme is secure against an adversary

[9]	Vanga Odelu, Ashok Kumar Das, Muhammad Khurram Khan, Kim-Kwang Raymond Choo and Minho Jo	1. Mathematical preliminaries and definitions 2. Key management in defined access structure 3. Proposed CP-ABE-CSKC scheme 4. Security analysis	• Feasible solutions for the problem of establishing a session key between a client and a server in the context of the Internet of Things were surveyed. • The Decision Diffie-Hellman (DDH) problem is easy but the Computational Diffie-Hellman (CDH) problem is hard. • The protocol uses a sequence of games under the decisional Diffie-Hellman (ECDDH) problem in order to proof that the protocol provides secure and perfect forward secrecy authentication.
[10]	Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang and Lei Shu	1. Surveys Articles for the IoT 2. Threat Models 3. Countermeasures and Formal Security Verification Techniques 4. Taxonomy and Comparison of Authentication Protocols for the IoT 5. Open Issues	• This special issue is intended to collect recent research outcomes that address key issues and topics related to self- organizing and smart protocols for heterogeneous ad hoc networks in the IoT.
[11]	Tie Qiu	1. Internet of Things 2. Self-organizing 3. Smart protocols	• IoT security concerns under the security triad perspective and explores the current privacy issues of IoT systems under different points of view. • The major security issue with NFC is that for some cases it is not encrypted, i.e. to maintain backward compatibility with RFID.
[12]	Diego Mendez, Ioannis Papapanagiotou and Baijian Yang	1. Structure of IoT systems 2. Vulnerable landscape 3. Enabling technologies and protocols 4. Confidentiality, integrity, availability and privacy concerns for IoT systems 5. IoT security challenges and some solutions	• Data confidentiality as a “fundamental issue” for IoT solutions, “particularly relevant in the business context”.
[13]	Martin Henze, Benedikt Wolters, Roman Matzutt, Torsten Zimmermann and Klaus They hrle	1. Controlling IoT networks 2. D-CAM design 3. Security discussion 4. Evaluation 5. Confidentiality	• This problem is addressed, who realize fine-grained access control for commands sent to an IoT device.
[14]	Prosanta Gope, Ruhul Amin, S.K. Hafizul Islam, Neeraj Kumar and Vinod Kumar Bhalla	1. RFID-based distributed IoT system architecture 2. Proposed lightweight anonymous	• To address these issues, lots of anonymous RFID-based authentication schemes have been designed using lightweight cryptographic tools, e.g., the hash function and symmetric key encryption.

		authentication scheme 3. Functionality and security analysis	
[15]	Namje Park and Namhi Kang	1. Review of Secure IoT Environment 2. Proposed Security Scheme 3. Service Flow of IoT Service Middleware Platform	• They are found to be insecure to un-traceability problem, forgery attacks, de-synchronization or DoS attacks. • pseudo-identity, one-time-alias identity and track sequence number are used to resolve the problem of strong anonymity, which includes the anonymity and un-traceability of RFID-tag. • This problem is avoided in the proposed scheme thanks to the distributed nature of the used other protocol. Finally, the proposal is also resistant to identity theft because node access is controlled by a strong protocol.
[16]	Hafsa Tahir, Ayesha Kanthey r and M. Junaid	1. Key technologies involved in internet of things 2. Applications of IoT 3. Wireless technology security issues	• Each sensor connected to a device in the IoT environment must write complicated and burdensome program code for data collection. To solve this problem, a new method is proposed, for design of a reconfigurable smart sensor interface in IoT environment for industrial WSN. • It is evident from scientific research that a great number of individuals connected via social network deliver more precise results to complex problems than an individual working on the same problem. • Scenario of the existing Internet, many protocols and tools are available to meet many of the security problems, but applicability of existing tools in the field of IoT are limited due to restrictions on the IoT hardware nodes and wireless sensor networks.
[17]	Antonio L. Maia Neto, Artur L. F. Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille, Antonio A. F. Loureiro, Diego F. Aranha, Harsh Kupwade Patil and Leonardo B. Oliveira	1. Authentication of things 2. Development 3. Evaluation	• This is the well-known key escrow problem of identity-based systems; and the main challenge for the wide adoption of IBC. • It has also shed some light on many long-standing open problems allowing quite a few of them to be solved elegantly.
[18]	Hokeun Kim, Armin Wasicek, Benjamin Mehne and Edward A. Lee	1. IOT security requirements 2. Security measures in the field 3. Proposed approach	• The architecture provides security guarantees while addressing IoT-related issues including resource constraints. • the authentication flows cannot address some of the IoT-related security and scalability issues.
[19]	Mustafa Abdullah Azzawi, Rosilah Hassan and Khairul Azmi Abu Bakar	1. Internet of things for healthcare 2. Proposed authentication mechanism	• Data protection is a critical issue for networks devices. In the field of IoT, security plays a vital role where malicious attack or interference with IoT devices can cause a threat to human life especially with critical IoT applications.

[20]	Xin Huang, Paul Craig, Hangyu Lin and Zheng Yan	1. IoT and security requirements 2. SecIoT Framework 3. Authentication	• Attempts to address this problem through the development of a prototype security framework with robust and transparent security protection. • The problem with having more things interconnected and accessible in a 5G IoT network is that there are more data available with more sensors and more opportunities for malicious attacks where the network can be hijacked, or sensitive personal data can be leaked because of inadequate security protection.
[21]	Kai Fan, Yuanyuan Gong, Chen Liang, Hui Li and Yintang Yang	1. Lightweight radio frequency identification mutual authentication protocol with cache in the reader 2. LRMAPC protocol proof 3. LRMAPC evaluation 4. ULRMAPC protocol	• The LRMAPC can address all the security and privacy problems discussed previously, and thus it achieves stronger security.
[22]	Lukas Malina, Jan Hajny, Radek Fujdiak and Jiri Hosek	1. Security and privacy in IoT 2. Cryptographic primitives and schemes on various devices 3. Perspective of privacy-preserving techniques in internet of things	• Many authentications and cryptographic schemes are based on hash functions. The use of such schemes that are performing many hash functions or hashing the large data structures (several kB) can be difficult and problematic in the IoT infrastructure that employs constrained devices. • A small RAM memory is usually problematic for some security schemes that are implemented on those devices.
[23]	Mohammed Riyadh Abdmeziem, Djamel Tandjaoui and Imed Romdhani	1. E-health applications in the context of Internet of Things 2. Network scenario 3. Reducing the overhead of MIKEY-Ticket	• Classical countermeasures are not suitable to the constrained environment of IoT due to several factors such as power and computation limitations, weak reliability of wireless links and the scalability issue. • To overcome this issue, we have introduced the use of nonce in the different exchanged messages.
[24]	Constantinos Kolias, Angelos Stavrou, Jeffrey Voas, Irena Bojanova and Richard Kuhn	1. Leakage of Personal Identifiable Information 2. Personalized Light Switch System 3. Risks with the Personalized Lights 4. Beaconing of Unique Identifiers	• practical assurance approaches addressing this resource problem have been developed: distributed frameworks allowing geographically separated parties to cooperate on testing, they are becoming available, providing a full complement of shared testing resources to reduce cost and testing time.

		5. Hiding the Identity 6. Leakage of Sensitive User Information 7. Remote Watering System 8. Points of Failure of the Watering System 9. Lack of encrypted communications 10. Plugging the Leaks 11. Unauthorized Execution of Functions 12. Automatic Control of Devices	
[25]	Jerker Delsing, Jens Eliasson, Jan van Deventer, Hasan Derhamy and Pal Varga	1. Local clouds for automation	• The problems discussed are often related to low level technologies e.g. protocols (CoAP, 6LowPAN), or various IoT cloud concepts e.g. Cumulosity, ThingWorx, Xively, Azure, Websphere. • Automation is a key driver, the technology discussions to a very large extent is addressing computer science problems with little or no reference to the automation requirements.
[26]	Er. Kritika, Dr. Harjit Pal Singh, Er. Narinder Pal Singh and Er. Mamta	1. Key Generation Time 2. Key Transmission and Verification Time 3. Data Transmission Time 4. Entropy 5. Probability of Key Connectivity 6. Probability of Key Exposure 7. Probability of Key Selection 8. Memory Usage	• Given the study on security and privacy within the web of Things: Current standing and open problems. As IoT systems are going to be present and pervasive, variety of security and privacy problems can arise. Credible, economical, economical and effective security and privacy for IoT area unit needed to make sure precise and correct confidentiality, integrity, authentication, and access management, among others.
[27]	Gourinath Banda, Chaitanya Krishna Bommakanti and Harsh Mohan	1. Protocol 2. Communication media 3. Security 4. Message structures	• They are not concerned about any potential hardware specific problems of Things, they experimented with simulated models of Things instead of real hardware.
[28]	Shahid Raza, Ludwig Seitz, Denis Sitenkov and Goran Selander	1. S3K for datagram TLS	• Key management is one of the hardest problems in cyber security. • It is even more challenging in the internet-connected IoT considering that most things are resource constrained (limited storage, processing, and bandwidth).

			• The problem comes from the DTLS protocol specification. The DTLS state machine is initialized on the Resource Server right after the Client-Hello message with valid cookie is received.
[29]	Pawani Porambage, An Braeken, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila	1. Network architecture and preliminaries 2. Proxy based key establishment protocol 3. Security analysis	• The lowest energy consumption at the initiator node in the proxy-based solution is highly acceptable for the devices with limited battery life.
[30]	Ning Huansheng and Liu Hong	1. The cyber-physical-social-thinking space 2. The science and technology framework for the IoT 3. The cyber-physical science 4. The technology framework	• To solve practical problems during human education activities based on the principle of "people-oriented values". • The local and indoor localization technologies (e.g., RFID, and Wi-Fi) are subsequently applied to address such problem. • Quantum computer adopts the full complexity of a many-particle quantum wave function to solve a computational problem, and it is engineered to control the coherent quantum mechanical waves with an advantage of inherent parallelism
[31]	Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha	1. IoT security overview 2. Taxonomy of security protocols for the IoT 3. Asymmetric key schemes 4. Symmetric key pre-distribution schemes	• To deploy security solutions to this problem, devices are required not only to use cryptographic algorithms to perform encryption. • Rabin's scheme is very similar to the RSA algorithm, which is also based upon the hardness of the factorization problem. • ZKP relies on some hard-mathematical problems, such as the factorization of integers or the discrete logarithm problem (DLP).
[32]	S. Sicari, A. Rizzardi, L.A. Grieco and A. Coen-Porisini	1. IoT security requirements: authentication, confidentiality and access control 2. Privacy in IoT 3. Trust in IoT 4. Enforcement in IoT 5. Secure middleware's in IoT 6. Mobile security in IoT	• partially address afforested questions because they specifically target the problem of lightweight cyphering in pervasive environments. • A problem common to ACLs (Access Control Lists), RBAC and ABAC is that in these systems it is hard to enforce the principle of least privilege access. • A main problem with many approaches towards trust definition is that they do not lend themselves to the establishment of metrics and evaluation methodologies. • The problem is that there are more and more collaborations and communications among these domains, therefore a cross-domain policy enforcement becomes an essential component.
[33]	Antonio Puliafito, Antonio Celesti, Massimo Villari and Maria Fazio	1. Single and Multicloud Scenarios for IoT 2. Towards Secure Self-Identification of IoT Devices	• One of the main problems in deploying IoT devices is the self-configuration of such devices that is necessary to interconnect them over the Cloud. • They examined problems in applying the DTLS protocol to IoT, which comprises constrained devices and constrained networks.

		3. An IoT Cloud-Based Architecture 4. Registration Strategies of IoT Devices Joining the Cloud	
[34]	Tuhin Borgohain, Uday Kumar and Sugata Sanyal	1. Introduction to OS for the IoT environment 2. OS’es	• The paper introduces the various aspects of the operating systems designed for the IoT environment where resource constraint poses a huge problem for the operation of the general OS designed for the various computing devices.
[35]	Rinju Ravindran, Jerrin Yomas and Jubin Sebastian E	1. Basic IoT architecture 2. Protocols in IoT 3. Security issues and measures	• It has been designed in such a way that it overcomes the problems of HTTP such as high computation complexity, low data rate and high energy consumption. • Specific authentication cohesive mechanism, the end-to-end authentication and key agreement mechanism, PKI (Public Key Infrastructure), WPKI for wireless, Security routing, Intrusion detection, etc. are used to tackle the security problems in the network layer.
[36]	Sabrina Sicari, Cinzia Cappiello, Francesco De Pellegrini, Daniele Miorandi and Alberto Coen-Porisini	1. IoT: Security and data quality needs 2. System architecture 3. Application case study	• They have showed that data quality problems are frequent, and they should be solved or at least users should be aware of the poor quality of the used data sources. • One of the problems faced by managers of retailing stores, indeed, is that they have no direct access to knowledge on the behaviour of users within their store.
[37]	Ms. R. Sujitha, Mr. N. Vijaya Raghavan, Ms. K. S. Suganya and Prof. A. Devipriya	1. Problem design 2. IoT architecture 3. Security of IoT architecture 4. Security of perception layer 5. Applications of IoT	• The security problems of IoT system technologies are grid sensor attacks, network content security, unauthorized login, and intrusions. • IoT faces other security problems such as information tracking over the internet, secure electronic systems, and data integrity of things.
[38]	Jun Wu, Mianxiong Dong, Kaoru Ota, Jianhua Li and Bei Pei	1. Cross-domain secure access scheme	• SIoT has been studied widely. [4] focused on the problem of understanding how the information provided by members of the SIoT must be processed to build a reliable system on the basis of the behaviour of the objects. • fine-grained cross domain security access control is one of the core problems.
[39]	Depeng Li, Srinivas Sampalli, Zeyar Aung, John Williams and Abel Sanchez	1. SAR system with confidentiality service 2. Security analysis	• different protocols can be used to solve the IP mobility problem within the aeronautical environment is surveyed.
[40]	Qi Jing Athanasios V, Vasilakos Jiafu Wan, Jingtwei Lu and Dechao Qiu	1. Security architecture of IoT 2. Security issues analysis of IoT 3. Security issues comparison between IoT and	• If IoT cannot have a good solution for security issues, it will largely restrict its development. Thus, above all the problems of IoT, security problem is particularly important. • Security architecture, divide IoT into layers, and sub layers, and we will extract major technical supports of each sub layer, propose security architecture to the problems of these technologies.

		traditional network 4. Open security issues of IoT	
[41]	Zheng Yan, Peng Zhang and Athanasios V. Vasilakos	1. Trust properties and objectives of trust management 2. Trust management in IoT 3. A research model	• Secure multi-party computation (SMC) deals with the problem of secure computation among participants who are not trusted with each other, particularly with the preference of privacy preserving computational geometry. • The problems of SMC are specifically different in different scenarios. • Secure data statistics is a specific SMC problem, particularly on database query privacy preservation.

3. System Model of Cloud Based IoTs

The success story of internet of things depends on the cloud network. The cloud network provides the facility of data access and data analysis[34, 35].

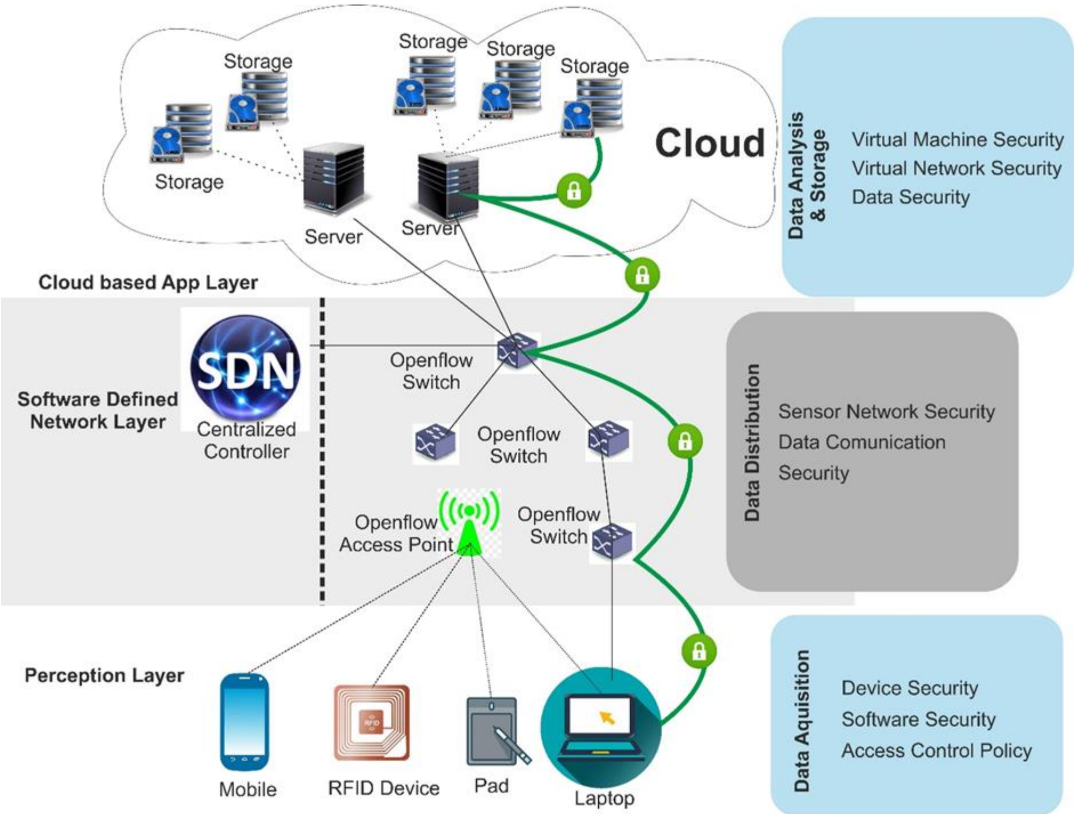

Figure 1 shows that the process integration of IoTs devices with cloud-based network.

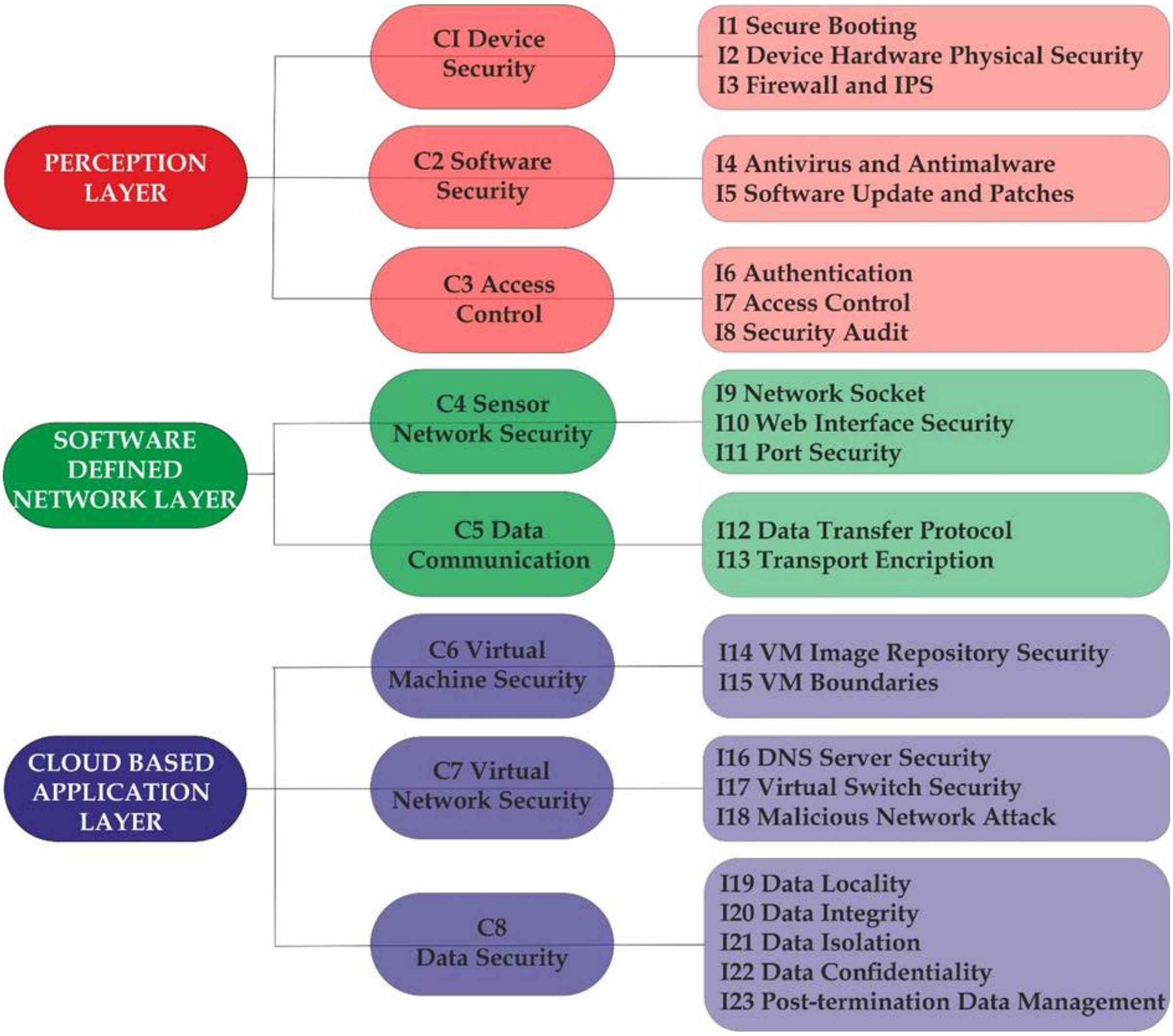
PERCEPTION LAYER
CI Device Security
I1 Secure Booting
I2 Device Hardware Physical Security
I3 Firewall and IPS
C2 Software Security
I4 Antivirus and Antimalware
I5 Software Update and Patches
C3 Access Control
I6 Authentication
I7 Access Control
I8 Security Audit
SOFTWARE DEFINED NETWORK LAYER
C4 Sensor Network Security
I9 Network Socket
I10 Web Interface Security
I11 Port Security
C5 Data Communication
I12 Data Transfer Protocol
I13 Transport Encription
CLOUD BASED APPLICATION LAYER
C6 Virtual Machine Security
I14 VM Image Repository Security
I15 VM Boundaries
C7 Virtual Network Security
I16 DNS Server Security
I17 Virtual Switch Security
I18 Malicious Network Attack
C8 Data Security
I19 Data Locality
I20 Data Integrity
I21 Data Isolation
I22 Data Confidentiality
I23 Post-termination Data Management

Figure :2 Data-security-oriented security assessment index framework

4. Research Issue

S. No.	RESEARCH GOALS	RESEARCH RESULT
01	Lightweight protocols	6LoWPAN, uIP, RPL, NanoIP, TSMP
02	Energy efficiency	Device protocol stack focused solutions: EnOcean, LoRa, SigFox, Ingenu, Weightless, DECT ULE, BLE, IEEE 802.11ah (WiFi HaLow), IEEE 802.11af (White-WiFi), IEEE 802.11ba (WUR),
03	Cognition	Bio-inspired Algorithms, Artificial Intelligence, Machine Learning
04	Security	Light weight cryptographic algorithms such as CLEFIA, PRESENT, ENOCORO, TRIVIUM
05	Identification, addressing and discovery	EPC, uCode, IPv6, URIs, mDSN, UPnP, Hypercat
06	Data	Concepts conclude big data analytics, cloud computing, fog computing, Protocols include MQTT, CoAP, AMQP, DSS, URI
07	Connectivity	D2D networks such as IEEE 802.11 family, Bluetooth, Zigbee, Z-ware. NB-IoT, Sigfox, Others include LTE-advanced, D2D in LTE, ICN, SDN, NFV, CCN
08	Miniaturized devices	SoC, Smart dust, Nanotechnology, NoC

5. Conclusion & Future Scope

Security is big challenge in internet of things scenario. For the prevention of threats in scenario of internet of things used various security models. The cryptography play an important role in security concern in internet of things. The cryptography provides public and private cryptography algorithms for the generation of key for the process of authentication and authorization. The security threats is big barrier of reachability of internet of things. The IOT's based communication used collaborate and hybrid stack of protocol open stack protocol faced various challenges of security, data privacy and user authentication. Now need to provide better security protocol stack for the prevention of security and authentication of data.

References

5. *Jun Zhou, Zhenfu Cao, Xiaolei Dong and Athanasios V. Vasilakos "Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions", IEEE, 2017, Pp 26-33.*
6. *Prem Prakash Jayaraman, Xuechao Yang, Ali Yavari, Dimitrios Georgakopoulos and Xun Yi "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation", Future Generation Computer Systems, 2017, Pp 1-10.*
7. *Engin Leloglu "A Review of Security Concerns in Internet of Things", Journal of Computer and Communications, 2017, Pp 121-136.*
8. *Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang and Wade Trappe "A Security Framework for the Internet of Things in the Future Internet Architecture", Future Internet, 2017, Pp 1-28.*
9. *Behrouz Pourghebleh and Nima Jafari Navimipour "Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research", Journal of Network and Computer Applications, 2017, Pp 23-34.*
10. *Soumya Ranjan Moharana, Vijay Kumar Jha, Anurag Satpathy, ourav Kanti Addya, Ashok Kumar Turuk and Banshidhar Majhi "Secure Key-distribution in IoT Cloud Networks", IEEE, 2017, Pp 197-202.*
11. *Bilal Javed, Mian Waseem Iqbal and Haider Abbas "Internet of Things (IoT) Design Considerations for Developers and Manufacturers", IEEE, 2017, Pp 1-7.*
12. *Liang Chen, Sarang Thombre, Kimmo Jã, Rvinen, Elena Simona Lohan, Anette Alã Savikko, Helena Leppã Koski, M. Zahidul H. Bhuiyan1, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, Jenna Lindqvist, Laura Ruotsalainen, Pã,,Ivi Korpisaari and Heidi Kuusniemi "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey", IEEE, 2017, Pp 8956-8977.*
13. *Vanga Odelu, Ashok Kumar Das, Muhammad Khurram Khan, Kim-Kwang Raymond Choo and Minho Jo "Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts", IEEE, 2017, Pp 3273-3283.*
14. *Mohamed Amine Ferrag, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang and Lei Shu "Authentication Protocols for Internet of Things: A Comprehensive Survey", Hindawi, 2017, Pp 1-42.*
15. *Tie Qiu "Self-organizing and smart protocols for heterogeneous ad hoc networks in the Internet of Things", Ad Hoc Networks, 2017, Pp 1-2.*
16. *Diego Mendez, Ioannis Papapanagiotou and Baijian Yang "Internet of Things: Survey on Security and Privacy", arXiv, 2017, Pp 1-16.*
17. *Martin Henze, Benedikt Wolters, Roman Matzutt, Torsten Zimmermann and Klaus Wehrle "Distributed Configuration, Authorization and Management in the Cloud-based Internet of Things", IEEE, 2017, Pp 1-8.*
18. *Prosanta Gope, Ruhul Amin, S.K. Hafizul Islam, Neeraj Kumar and Vinod Kumar Bhalla "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment", Future Generation Computer Systems, 2017, Pp 1-10.*
19. *Namje Park and Namhi Kang "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Sensors, 2016, Pp 1-12.*
20. *Hafsa Tahir, Ayesha Kanwer and M. Junaid "Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation", International Journal Of Multidisciplinary Sciences And Engineering, 2016, Pp 14-22.*
21. *Antonio L. Maia Neto, Artur L. F. Souza, Italo Cunha, Michele Nogueira, Ivan Oliveira Nunes, Leonardo Cotta, Nicolas Gentille, Antonio A. F. Loureiro, Diego F. Aranha, Harsh Kupwade Patil and Leonardo B. Oliveira "AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle", ACM, 2016, Pp 1-15.*
22. *Hokeun Kim, Armin Wasicek, Benjamin Mehne and Edward A. Lee "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities", IEEE, 2016, Pp 1-9.*
23. *Mustafa Abdullah Azzawi, Rosilah Hassan and Khairul Azmi Abu Bakar "A Review on Internet of Things (IoT) in Healthcare", International Journal of Applied Engineering Research, 2016, Pp 10216-10221.*
24. *Xin Huang, Paul Craig, Hangyu Lin and Zheng Yan "SecIoT: a security framework for the Internet of Things", Security and Communication Networks, 2015, Pp 3083-3094.*
25. *Kai Fan, Yuanyuan Gong, Chen Liang, Hui Li and Yintang Yang "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G", security and communication networks, 2015, Pp 3095-3104.*
26. *Lukas Malina, Jan Hajny, Radek Fujdiak and Jiri Hosek "On perspective of security and privacy-preserving solutions in the internet of things", Computer Networks, 2016, Pp 83-95.*
27. *Mohammed Riyadh Abdmeziem, Djamel Tandjaoui and Imed Romdhani "Lightweighted and Energy-Aware MIKEY-Ticket For E-Health Applications in the Context of Internet of Things", HAL, 2017, Pp 1-22.*
28. *Constantinos Kolias, Angelos Stavrou, Jeffrey Voas, Irena Bojanova and Richard Kuhn "Learning Internet of Things Security Hands-on", IEEE, 2016, Pp 1-17.*

29. *Jerker Delsing, Jens Eliasson, Jan van Deventer, Hasan Derhamy and Pal Varga "Enabling IoT automation using local clouds", IEEE, 2016, Pp 1-6.*
30. *Er. Kritika, Dr. Harjit Pal Singh, Er. Narinder Pal Singh and Er. Mamta "Multivariate Authentication and Encryption Scheme for Data Privacy in IoT Healthcare Monitoring", Imperial Journal of Interdisciplinary Research, 2016, Pp 543-550.*
31. *Gourinath Banda, Chaitanya Krishna Bommakanti and Harsh Mohan "One IoT: an IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible", J Reliable Intell. Environ. 2016, Pp 131-144.*
32. *Shahid Raza, Ludwig Seitz, Denis Sitenkov and Goran Selander "S3K: Scalable Security with Symmetric Keys -DTLS Key Establishment for the Internet of Things", arXiv, 2016, Pp 1-11.*
33. *Pawani Porambage, An Braeken, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila "Proxy-based End-to-End Key Establishment Protocol for the Internet of Things", ICCW, 2015, Pp 1-6.*
34. *Ning Huansheng and Liu Hong "Cyber-physical-social-thinking space-based science and technology framework for the Internet of Things", Science China, 2015, Pp 1-19.*
35. *Kim Thuat Nguyen, Maryline Laurent and Nouha Oualha "Survey on secure communication protocols for the Internet of Things", Ad Hoc Networks, 2015, Pp 17-31.*
36. *S. Sicari, A. Rizzardi, L.A. Grieco and A. Coen-Porisini "Security, privacy and trust in Internet of Things: The road ahead", Computer Networks, 2015, Pp 146-164.*
37. *Antonio Puliafito, Antonio Celesti, Massimo Villari and Maria Fazio "Towards the Integration between IoT and Cloud Computing: An Approach for the Secure Self-Configuration of Embedded Devices", Hindawi Publishing Corporation, 2015, Pp 1-9.*
38. *Tuhin Borgohain, Uday Kumar and Sugata Sanyal "Survey of Operating Systems for the IoT Environment", arXiv, 2015, Pp 1-5.*
39. *Rinju Ravindran, Jerrin Yomas and Jubin Sebastian E "IoT: A Review On Security Issues And Measures", Engineering Science and Technology: An International Journal, 2015, Pp 348-351.*