Review on Challenges in IoT Device Security Approaches

Tejal Irkhede
Kalinga University, Raipur
tejal.irkhede@gmail.com

Sanjay Kumar
Kalinga University, Raipur
Sanjay.kumar@kalingauniversity.as.in

Article Info
Page Number: 9056 - 9067
Publication Issue:
Vol 71 No. 4 (2022)

Article History
***Article Received**: 15 September 2022*
***Revised**: 25 October 2022*
***Accepted**: 14 November 2022*
***Publication**: 21 December 2022*

Abstract

Almost every industries is working on different traditional or modern automation using remote controlling and the monitoring system. With the rapid growth in internet connectivity, the reach of this remote control or monitoring system enhanced globally. Internet mainly designed to provide connectivity between computational machines or the computers and worked on specially designed hardware and network firmware. On other hand, industrial automation or electronic appliances never designed to be a part of the internet or large network. Latest compact computers, microcontrollers, or the System on Chip (SOC) devices are enabling interconnectivity between electronics system using communication module. IoT devices are growing rapidly and count of devices deployment is in highest progression. Due to lacking of low resourced hardware and firmware IoT device facing problems to enable high level of security and no standardization of security models for IoT devices. This paper is primarily focus on existing security models and the enhancement expected in the field. It also suggest the possible solution for standardization of individual device identity and authorization

Keywords: SOC, IoT

1. INTRODUCTION

Internet of Things is simply an interaction between the physical and digital worlds where the digital world interacts with the physical world through sensors and actuators. Internet of Things (IoT) is the technology where privacy and security is very important concern due to the numerousnatures of devices, large scale appliances, and its exposure in the working area or the environment. According to [1], there is drastic growth in number of IoT devices like in 2020; the numbers of devices are 8.74 billion with an increase of 31% which can rise up to 33% till 2021. Instead, in comparison, the applications of IoT devices are changing the various fields from smaller to larger scales like from smart Grid to smart City. Though, various cyber-attacks and security threats are surrounded by IoT devices due to large popularity. According to HP analysis, various common IoT devices experience atleast average of 20% exposures per device. Serious security solutions are therefore required in IoT because of such type of trend. Due to this, computational processing, low power and limited memory problems are seen in IoT devices [2]. Delicate and Simple structure of IoT makes it more susceptible to the threats related to security of IoT. IoT system is composed of three components such as a sensing unit having large number of sensors, mobile terminals and actuators to detect the physical environments [3].

Nevertheless, IoT devices undergo from other various security issues and challenges which are addressed by various approaches by different authors. Strong security is the need of IoT due to the rapid growth in IoT devices and various cyber attacks [4]. By 2030 [5], as per predication the number of IoT devices will increase up to 25 billion and can be pervasive and ubiquitous in nature. In last few years, the numbers of devices are rapidly increasing;so the security has become a serious issue and has grasped attention of various authors. IoT deals with the peer to peer communication between every device [6], so every individual device needs security.In IoT, the trust model is expected to provide data integrity as well as confidentiality for making end-to-end communication which is possible through an authentication mechanism. Moreover, to avoid improper usage of data, the privacy model requires defining access policies and mechanisms for encrypting and decrypting data. The security aspect incorporates three layers corresponding to the services, communication, and application. To grab attention in this regard, to cope with the security various reviews have adviseddifferent mechanisms to overcome problems and challenges in Internet of Things.

Bhandari and Gupta [7] implemented a logical review based upon systematic analysis of fault in IoT. Mohammadi *et al.* [8] accomplished systematic approach for security analysis of IoT and performed SLR and given trust based techniques for IoT reference. Aly *et al.* [9] analyzed the security issues based upon different layers which are affecting to IoT systematically. Fazal *et al.* [10] performed the security by categorizing challenges at three different levels such as cloud server of IoT, hardware and network through systematic approach. Macedo *et al.* [11] performed SLR to explore and analyze

Table 1: Research Questions

Research Questions		Goals
RQ1	What are the challenges in IoT implementation and deployment?	To find out the reasons which restricting IoT device to implement in real world.
RQ2	What are the communications protocols available for IoT?	Finding out existing available IoT communication protocols and its pros and cons.
RQ3	What is the encryption techniques involved in messaging security?	Exploring the feasibility of different encryption methodologies in IoT with its features
RQ4	Is Blockchain technology can be used to secure IoT implementation?	To find out the possible role of Blockchain application in IoT deployment.

the security based upon four security levels such as authentication, trust, and access control and data protection. Martínez *et al.* [12] identifiedattacks, threats, challenges related to security of IoT. Witti and Konstantas [13] explainedsystematic mapping study with the help of the existing security and privacy issues in IoT. Similarly, Sultan *et al.* [14] elaborated and provided the solution by using block chain technology for the security issues in IoT.

2. BACKGROUND

In IoT threats are enormouslyvaried and difficult. By 2025, most of the attacks will be cyber attacks and will be IoT-based over businesses as predicted by Gartner. However, now a days market is prioritizing the price and security then solely depend on the design which is built. Similarly, user awareness and educational promotions are considered. Therefore, IoT devices are explored with highrate of frequency and their misuse continues to quicken and worsen. Consumer IoT devices evaluations presented in [15,16] for the security and privacy which shows that maximum devices show some form of exposure, while some devices have a better security stand than others. IoT devices are used in multiple sectors and industries, like Consumer applications where IoT consumer products include smartphones, smart watches and smart homes, which control everything from air conditioning to door locks, all from a single device. In Business applications where businesses use a wide range of IoT devices, including smart security cameras, trackers for vehicles, ships and goods, as well as sensors that capture data about industrial machinery. And Governmental applications where governmental IoT applications include devices used to track wildlife, monitor traffic congestion and issue natural disaster alerts. Although large scale attacks affect big harms, but small scale attacks can be even more unsafe since they often go ignoredor undetected for relatively a long time. Hence, it is substantial to toughen cyber security by recognizing what needs to be secured and developing alternative solutions that can help distinct devices to overcome physical limitations in IoT.

IoT devices are now commonplace in the medical industry, with examples including pacemakers, heart monitors and defibrillators. While convenient (e.g., a doctor can fine-tune a patient's pacemaker remotely), these devices are also vulnerable to security threats.An improperly secured device can be exploited to interfere with a patient's medical care. It's an exceedingly rare occurrence, albeit one to be considered when developing a strategy for securing IoT devices. It is really important to note that IoT security is not only a technical issue but the legislator have identified its importance for citizens, businesses and the whole society by supporting and pushing the definition of proper safety, security and privacy measures and practices to fight security threats. User awareness and education regarding the purchase and use of IoT devices is the another important issue to be addressed in the framework of IoT security. Although the use of default authorizations associated with IoT devices represents one of the biggest security weaknesses, many users are not aware of this vulnerability and leave these passwords unbothered.

Security in IoT has also been broadly analyzed in the collected works. Research and Study efforts under different viewpoints for different challenges are given. Numerousreviewsintended at appraising and reviewing these efforts have been published in recent years. More specifically, Aly et al. [17] presented a methodical literature review aimed at providing procedures for researchers and practitioners interested in acceptingand understanding security issues and also focused on the IoT reference models layers. Ammar et al. [18] discussedindustrial and customer applications which are developed to adopt security of IoT frameworks and also compares the architectures of the frameworks for discussing the approaches which aredeveloped for confirming security and privacy. Mosenia and Jha [19] outlined the possible alternatives against the attacks which can analyze the vulnerabilities disturbing the edge side layer of IoT (i.e., edge node, communication and edge computing). Neshenko et al. [20] based on ordering and grouping multi-dimensional classificationis given for IoT exposures. Zhou et al. [21] suggestedcharacterization for IoT devices which are uniquely designed for some set of features and network subsystems. Also discussed the probabledangers and vulnerabilities associated with each feature as well as solutions and prospects to deal the threats. So, it is worth mentioning that most of the reviews on IoT security emphasis on specific feature of the IoT environment, such as networking organizations, deployment environments.

3. CHALLENGES & AVAILABILITY

Internet of Things devices makes their security a high priority and is crucial for the future wellbeing of the internet ecosystem. And these devices enable themselves to collect and exchange data.IoT interconnects various things on the networks to carry out resource sharing, analysis and management across heterogeneous network.In IoT, major concerns are security and privacy which leads to various IoT restrictions. To overcome such limitations IoT schemes needs to be expandable in a way that billions of devices or things can span. Therefore, a newmanagingstandardneed to be entreated.

Internet is base of IoT and there are enough and stable security implemented in terms of network security protocol. All these protocols are designed and implemented keeping computer or central processing unit based system. These systems are having sufficient processing resources like operating system, multithreading or applications, kernels, drivers, sufficient RAM or the storage devices. This much of resources supports different network protocols like TCP or UDP which already having stable and secure communication. On other hand IoT devices designed with electronics component in mail consideration. Adding computational power to the electronics appliances may lead to high price and other deployment issues. IoT devices and the network has limited processing resource in terms of bandwidth, memory, clock pulse, hence it needs lightweight yet efficient security architecture. In order to either we need to design new stack of electronics communication devices or existing network security architectures need to re-design keeping low processing power and low resources issues in considerations. Different manufacturing companies are developing the electronics communication modules which may embedded in to real-world application in order to make device IoT compatible. Primarily IoT devices fall it to wired, wireless, or mobile type connection method. Again these connection methods having different categorized applications and the user likely,

A. Industrial application: These type of applications required stable and high speed connectivity where Broadband, Ethernet, Fiber optics, leased line, or any direct wired internet lines are considered as connection media

B. Domestic application: In this scenario, multiple devices may work in same area, home or small office space. These type of devices are mobile devices with limited roaming area. Wi-Fi based internet access would be the best choice for such a devices
C. Mobile application: Any other device having no fixed roaming area and need connectivity while moving at different distanced location mobile data services like GSM, GPRS, 2G, 3G are used. These networks provide mobile connectivity with high-speed internet connectivity on the go.

For mobile or wireless connectivity application on electronics side, SOC (System on Chip) module like GSM (SIM900, SIM808, SIMCOM), Wi-Fi (ESP, NRF), or Bluetooth (HC-01, HC-05) are available for IoT device manufacturer. Due to the high increase in IoT deployment mobile service provider come up with the IoT special SIM cards which may having dedicated identification number schemes and may have custom service plans to suits the application. This advancement and the availability of resources may help in real-world IoT deployments but it costs.

4. COMMUNICATION PROTOCOLS

In order to successful and secure communication in dynamic public network, system has to gone through multiple stages and the processes. These stages may include 1) Service discovery 2) Connection establishment 3) Authentication 4)Session maintenance 5) Message transfer. Since IoT infrastructure is low resource and considered for instant communication with minimum packet drop, it required new set of communication protocol rather than available low level and application level communication protocols like TCP, UDP, FTP, or the HTTP. As a part of research we categorized Available IoT communication Protocols primarily

4.1 Application Layer Protocols

The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health. An essential component of the IoT environment is communication protocols of the application layer as they are responsible for the communications among IoT devices and cloud substructure which deals with messaging and service discovery. Specifically, discovery refers to detecting devices and services being offered while, messaging refers data sharing and exchanges among devices. The seven standard protocols which are analyzed with their features are, messaging protocols likewise MQTT, CoAP, AMQP, DDS and XMPP (these are five protocols) and service discovery protocols likewise mDNS and SSDP (these are two protocols) summarized in Table 1.

IoT protocols are a crucial part of the IoT technology stack without them; hardware would be rendered useless as the IoT protocols enable it to exchange data in a structured and meaningful way. Protocols vary in various aspects such as transport protocols and architectural models as well as interaction models. Few protocols are built on fully distributed architectures, while others use centralizedor client/server architectures.

Message Queuing Telemetry Transport is a lightweight publication/subscription type (pub/sub) messaging protocol. Designed for battery-powered devices, MQTT's architecture is simple and lightweight, providing low power consumption for devices. According to this model message exchanges are implemented in general.

Also, Constrained Application Protocol (CoAP) was designed to translate the HTTP model so that it could be used in restrictive device and network environments. CoAP relies on the User Datagram Protocol (UDP) for establishing secure communication between endpoints. Apart from transferring IoT data, CoAP controls Datagram Transport Layer Security (DTLS) for the secure exchange of messages in the transport layer. Specifically, messaging protocols are based on TCP whereas service discovery protocols are based on UDP. MQTT and CoAP are mostly suitable for data collection like Sensor updates in controlled environments. On contrary, address specific service requirements are fulfilled by AMQP, DDS and XMPP protocols for mainly business messaging, instant messaging and online presence detection and real-time exchanges, mDNS and SSDP are the protocols of choice for IoT environments where service discovery is impoertant. Moreover, choice of the application protocol depends on nature of the IoT systems requirements.

4.2 Messaging Protocols

Messaging protocols are discussed here which are used in IoT environments. Specifically, MQTT and CoAP considered in detail because of wide acceptance in these protocols, while AMQP, DDS and XMPP are briefly covered as they find applications in IoT, even though they are not seen as a typical IoT solution.

4.2.1 MQTT

Probably the most widely adopted standard in the Industrial Internet of Things now a day is Message Queuing Telemetry Transport which is a lightweight publication/subscription type (pub/sub) messaging protocol. Message Queue Telemetry Transport (MQTT) protocol is an open standard messaging protocol.MQTT is based on subscriber, publisher and broker model. Within the model, the publisher's task is to collect the data and send information to subscribers via the mediation layer which is the broker. The role of the broker, on the other hand, is to ensure security by validating the permission of publishers and subscribers. When a client wants to send data to the broker, this is known as a "publish." When a client wants to receive data from the broker, it will "subscribe" to a topic or topics. When a client subscribes to a certain topic, it will receive all messages published on that topic going forward. Along with the message itself, the publisher also sends a QoS (Quality of Service) level. This level defines the guarantee of delivery for the message.

4.2.2 CoAP

Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the IoT. It is intended to support simple, constrained devices to join the IoT even if there is low bandwidth and low availability of constrained networks. It is generally used for machine-to-machine (M2M) applications such as smart energy and building automation. Even though HTTP protocol shares many characteristics with CoAP, it has been specifically designed for constrained devices with limited storage space, energy, processing power and transmission capabilities. As already deliberated, Datagram Transport Layer Security (DTLS) protocol is supported by CoAP, and security is guaranteed bya UDP execution of the TLS protocol. COAP uses UDP as the underlying network protocol. COAP is basically a client-server IoT protocol where the client makes a request and the server sends back a response as it happens in HTTP. The methods used by COAP are the same used by HTTP. DTLS binding for the CoAP protocol is defined in terms of four security modes that differ in key negotiation mechanisms and authentication and range from no security to certificate-based security. The protocol is designed for reliability in low bandwidth and high congestion through its low power consumption and low network overhead. In a network with a lot of congestion or limited connectivity, CoAP can continue to work where TCP based protocols such as MQTT fail to exchange information and communicate effectively.Apparently, CoAP environments compromised because of inappropriate security services which lead to attack.

4.2.3 AMQP

Advanced Message Queuing Protocol (AMQP) is an open protocol used as IoT protocol which consists of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables supporter programs to talk to the broker and participate with the AMQP model. Through orientation to security, AMQP for ensuring integrity and confidentiality of communication supports the Simple Authentication and Security Layer (SASL)

Table 2: Describes the summarization of the characteristics of well-known IoT application layer protocols. The bullets presentsthebasic features of the protocols, and the circles to supported additional features of the protocols.

Protocol	Functions		Architecture		Interaction		Transport	
	Messaging	Discovery	Central	DeCen.	Pub/Sub	Req/Res	TCP	UDP
MQTT	●		●		●		●	
CoAP	●	○	●		○	●	○	●
AMQP	●		●		●	○	●	
DDS	●	○		●	●	○	●	●
XMPP	●	○	●		●	●	●	
mDNS		●		●		●		●
SSDP		●	●			●		●

Framework for client authentication and TLS. In AMQP these security services are usually permitted by default unlike MQTT and CoAP, which can reduce the risk of security. However, agreeing to the NVD database, extensive variability of vulnerabilities revealed in the past few years in products and services which are based on AMQP,

4.2.3 AMQP

Advanced Message Queuing Protocol (AMQP) is an open protocol used as IoT protocol which consists of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables supporter programs to talk to the broker and participate with the AMQP model. Throughorientation to

security, AMQP for ensuring integrity and confidentiality of communication supports the Simple Authentication and Security Layer (SASL) framework for client authentication and TLS. In AMQP these security services are usually permitted by default unlike MQTT and CoAP, which can reduce the risk of security. However, agreeing to the NVD database, extensivevariability of vulnerabilities revealed in the past few years in products and services which are based on AMQP,

4.2.4 DDS

DDS stands for Data Distribution Service. It enables scalable, real-time, reliable, excessive-overall performance and interoperable statistics change via submit-subscribe technique. It is an IoT protocol developed for M2M (Machine to Machine) Communication by OMG (Object Management Group) and enables data exchange via publish-subscribe methodology. DDS makes use of brokerless architecture unlike MQTT and CoAP protocols. It uses multicasting to bring high quality QoS to the applications. DDS protocol can be deployed from low footprint devices to cloud.

4.2.5 XMPP

Extensible Messaging and Presence Protocol (XMPP) used for Networked Device Communication. Advantage of XMPP is that it offers good security, since private XMPP servers can be isolated from the public Intranet, for example on a company Intranet, and strong SASL and TLS security is built into the core XMPP specifications. The XMPP protocol uses a distributed client-server architecture where clients do not talk directly to one another, but there is no central server either. By supporting SASL for the authentication process and the TLS, the XMPP protocol provides robust security services for confirming data confidentiality and integrity. But, the protocol is not secure due to absence of encryption support.

4.3 Service Discovery Protocols

In IOT architecture Service Discovery layer has a prominent role. It is the service discovery or service management layer which differentiates an IOT network with that of typical internet network. The IOT devices need to connect and communicate with web or cloud based services and applications for IOT implementation. Here, the service discovery protocols specifically mDNS and SSDP are discussed.

4.3.1 mDNS

Multicast Domain Name System (mDNS) is a DNS like service discovery protocol. It is used to resolve host names to IP addresses in a local network without using any unicast DNS server. Without any additional infrastructure it can be used or DNS server in the network. The protocol operates on IP multicast UDP packets through which a node in the local network enquires the names of all other nodes. This protocol, combined with DNS-based Service Discovery (DNS-SD), offers the flexibility required by environments where it is necessary to automatically integrate new devices. It does not provide any built-in security service unlike messaging protocols. Due to this, protocol is exposed to security attacks. Modern improvements are done in DNS security, such as DNSSEC and DNS over TLS, but these are very complex to use.

4.3.2 SSDP

Simple Service Discovery Protocol (SSDP) is widely used for service discovery. Simple service discovery protocol allows clients to passively discover published network devices and services in a residential or small office environment with minimal manual configuration. More and more IOT devices are using SSDP, which is an HTTP like protocol that uses NOTIFY and M-SEARCH methods. It uses multicast addressing over UDP port 1900.Universal plug and play is a set of protocols that enables discovery of networked devices. Relating to security, the SSDP protocol is very weak like mDSN because it does not offer any integral mechanism. Therefore, security risks of various types can affect SSDP supported devices.

5. SECURITY METHODS

Design criteria for cryptographic algorithms which are used are having extremely low resource devices which are different from that of the commonly used ones. Hence, there is a requirement of lightweight cryptography algorithms to be developed that have extremely low requirements. Although no strict criteria are defined for lightweight cryptography algorithms, the features usually include any one or more of the following,

- Low application cost;
- Low computational power of microprocessors or microcontrollers;
- Minimum size required for hardware implementation;

There is a trade-off between security, costs and performance i.e. in cryptographic algorithms, the key length is correlated with security and cost tradeoff, while the number of rounds in encryption provides a security, performance trade-off and hardware architecture. Usually two of these goals are kept in mind while designing the lightweight algorithms, as it is difficult to optimize all the three design goals. As a part of the research study following are the best-suited encryption and cryptographic algorithms may use in IoT security implementation with low resourced devices and application.

DESL & DESXL: The lightweight version of classical DES algorithm is DESL and A lightweight version of the DESX algorithm is DESXL where both uses a single S-box (substation block) instead of 8 S-boxes. There is only a single S-box so, memory is saved and the S-box makes them resistant to most of the common cryptanalytic attacks.

CURUPIRA: To qualify this algorithm as the lightweight algorithm, which is based on the “Wide Trail” strategy by Joan Daemen, it has the following features:

- The number of rounds is determined based on the key length;
- The data block size is 96 bits and is represented as 3 X 4-byte array. The key lengths can be 96, 144 or 192 bits;
- The 8 X 8-bit S-box is implemented as two 4 X 4-bit S-boxes which reduces the space required to store the S-boxes

KATAN & KTANTAN*:* These ciphers are from a family of hardware oriented six block ciphers, which are divided into 3 KATAN ciphers: KATAN32, KATAN48, and KATAN64 and 3 KTANTAN ciphers: KTANTAN32, KTANTAN48 and KTANTAN64. The number in the algorithm’s name represents the block size of the algorithm in bits. Both uses 80-bit key size. The difference is that KTANTAN is more compact in hardware where the key is burnt into the target device and cannot be changed. So KTANTAN ciphers are small block ciphers when compared to KATAN and is used in devices which are initialized with one key. The resource requirements for Katan & Ktantan algorithm are low due to the following features,:

- They process small blocks of data which are from 32 to 64 bits;
- They use the shift registers and feedback functions which are easy to implement in hardware and provides required nonlinearity. The size of the internal state is equivalent to the block size of the algorithm.

PRESENT:has obtained the ISO/IEC standard for lightweight cryptography and is one of the leanest lightweight algorithms. It is based on the transformation layers of Serpent and DES that has been analyzed in detailed, especially on security and hardware efficiency. As it is the leanest algorithm, it has the following features to consider,

- It performs 31 rounds on 64-bit data block
- It uses very less gate count and less memory.
- The most compact hardware implementation of PRESENT needs 1570 (GE) and is therefore competitive with today's leading compact stream
- It allows to use 80 or 128-bit keys.

Hummingbird: Itis a hybrid algorithm of both stream and block ciphers. It encrypts,

- 16-bit blocks of data
- Has 80-bit internal state and
- Uses a 256-bit key
- Simple logic and arithmetic operations.

Because it uses a small block size, it has minimum response time and power consumption requirements and is suitable for RFID tags or wireless sensors without any modification of the current standard.

LED: It isLight Encryption Device and a symmetric block cipher that is lightweight and can be implemented in hardware efficiently. A use case of LED is the secure storage and transmission of RFID tags. It uses a block size of 64 bits and the key length is 64 bit (LED-64) or 128 bit(LED-128). Even key length between 64 bit and 128 bit is possible in which case the remaining bits will be padded with the prefix of the key. It can be used for software implementation.

TEA: It is Tiny Encryption Algorithm (TEA) developed with an objective to be used on low performing small computers. TEA is a block cipher and based on a high performance but mathematically simple encryption algorithm which are variants of a Feistel Cipher.

- TEA is a round based encryption method. 32 Tea cycles are recommended. But the number of the used rounds are variable.
- TEA encrypts 64 bit blocks which are divided into 32 bit blocks.Uses a 128-bit length key.

- TEA developed based on the assumption that security can be enhanced by increasing the number of iterations.

SEA: It is Scalable Encryption Algorithm, and has the following features,

- Small code size,
- Low memory,
- Limited instruction set. And

Due to use of 3-bit S-box, SEAis the most compact cipher which is based on Feistel structure. Scalable Encryption Algorithm is recommended for small encryption routines.

6. CONCLUSION

Redesigning the IoT communication architecture to provide feasible Authentication, Identification and communication over fixed, dynamic or ad-hoc network. Is most demanding requirement. We are proposing the Decentralizing the IoT service provider server deployment for load balancing and fail safe situation management using block chain. This idea may help IoT device service provider to create standard infrastructure which provide registration, authorization, authentication and message transfer.

7. REFERENCES

[1]. A. Dean and M. O. Agyeman, ``A study of the advances in IoT security,"in *Proc. 2nd Int. Symp. Comput. Sci. Intell. Control*, 2018, p. 15.

[2]. C.-T. Li, C.-C. Lee, C.-Y. Weng, and C.-M. Chen, ``Towards secureauthenticating of cache in the reader for RFID-based IoT systems," *Peer-Peer Netw. Appl.*, vol. 11, no. 1, pp. 198_208, Jan. 2018.

[3]. C.-T. Li, T.-Y.Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficientuser authentication and user anonymity scheme with provably securityfor IoT-based medical care system," *Sensors*, vol. 17, no. 7, p. 1482,Jun. 2017.

[4]. R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, ``An overview:Security issue in IoT network," in *Proc. 2nd Int. Conf. IoT Social, Mobile,Anal. Cloud (I-SMAC),* Aug. 2018, pp. 104_107.

[5]. J. Ahamed and A. V. Rajan, ``Internet of Things (IoT): Applicationsystems and security vulnerabilities," in *Proc. 5th Int. Conf. Electron.Devices, Syst. Appl. (ICEDSA),* Dec. 2016, pp. 1_5.

[6]. E. Buenrostro, D. Cyrus, T. Le, and V. Emamian, "Security of IoT devices,"*J. Cyber Secur. Technol.*, vol. 2, no. 1, pp. 1_13, 2018.

[7]. V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Saha_, "Trustbasedrecommendation systems in Internet of Things: A systematic literature review,"*Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 21,Dec. 2019.

[8]. G. P. Bhandari and R. Gupta, ``A systematic literature review in faultanalysis for IoT," *Int. J. Web Sci.*, vol. 3, no. 2, pp. 130_147, 2019.

[9]. K. Fazal, H. Shehzad, A. Tasneem, A. Dawood, and Z. Ahmed, ``A systematicliterature review on the security challenges of Internet of Thingsand their classification," *Int. J. Technol. Res.*, vol. 5, no. 2, pp. 40_48,2017.

[10]. M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, ``Enforcingsecurity in Internet of Things frameworks: A systematic literaturereview," *Internet Things*, vol. 6, Jun. 2019, Art. no. 100050.

[11]. E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello,F. M. G. Franca, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes,``On the security aspects of Internet of Things: A systematic literaturereview," *J. Commun. Netw.*, vol. 21, no. 5, pp. 444_457, Oct. 2019.

[12]. J. Martínez, J. Mejía, and M. Muñoz, ``Security analysis of the Internet ofThings: A systematic literature review," in *Proc. Int. Conf. Softw. ProcessImprovement (CIMPS)*, Oct. 2016, pp. 1_6.

[13]. M. Witti and D. Konstantas, ``IOT and security-privacy concerns: A systematicmapping study," *Int. J. Netw. Secur. Appl.*, vol. 10, no. 6,pp. 25_33, Nov. 2018.

[14]. A. Sultan, M. S. Arshad Malik, and A. Mushtaq, ``Internet of Things securityissues and their solutions with blockchain technology characteristics:Asystematic literature review," *Amer. J. Comput. Sci. Inf. Technol.*, vol. 6,no. 3, p. 27, 2018.

[15]. S.-R. Oh and Y.-G. Kim, ``Security requirements analysis for the IoT," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Feb. 2017, pp. 1_6.

[16]. Loi, F.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In Proceedings of the Workshop on Internet of Things Security and Privacy (IoTS&P), Dallas, TX, USA, 3 November 2017.

[17]. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380.

[18]. Aly, M.; Khomh, F.; Haoues, M.; Quintero, A.; Yacout, S. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. Internet Things 2019, 6, 100050.

[19]. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf. Secur. Appl. 2018, 38, 8–27.

[20]. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733.

[21]. Zhou,W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet Things J. 2019, 6, 1606–1616.

[22]. Susha Surendran, Amira Nassef, Babak D. Beheshti. "A survey of cryptographic algorithms for IoT devices" , 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018

[23]. MD Azharul Islam, Sanjay K. Madria, "A Permissioned Blockchain based Access ControlSystem for IOT", 2019 IEEE International Conference on Blockchain (Blockchain), DOI 10.1109/Blockchain.2019.00071