ANALYZING SECURITY STRATEGIES IN THE INTERNET OF THINGS

SeyyedKeyvan Mousavi[1], Arash Tabe[2], Kaveh Shaker[3], Payam Hatamzadeh[4]

[1]Department of Computer, Urmia Branch, Islamic Azad University, Urmia, Iran
[2]Computer Engineering Student, Department of Computer, Tabriz University Campuses, Tabriz, Iran
[3]Computer Engineering Department, Mizan Higher Education Institute, Tabriz, Iran
[4]Faculty of Engineering, Department of Computer Engineering, University of Isfahan, Isfahan, Iran

ABSTRACT

The Internet of Things (IoT) is a technology based on a network of physical objects, devices, vehicles, buildings, and more which are comprised of such systems as electronics, software, and sensors. This type of internet connects physical devices through RFID labels, sensors, and smart objects. The IoT is faced with many challenges including data security, privacy maintenance, data quality and trust, which requires mechanisms such as integrity, authentication, access control and confidentiality. First, this paper examines the security aspects of IoT, then it investigates the security infrastructure provided for this kind of internet. Studies have shown that most of the infrastructures make use of cryptographic algorithms, authentication techniques, and data-hashing. According to the findings, authentication and encryption factors are very effective in increasing the security of IoT equipment. If authentication works correctly only authorized users can access the Internet space, the data, and the sensors. The key is used to encrypt and decrypt data. The Internet of Things and its security challenges are examined in this study. According to the literature, various algorithms such as RSA and elliptic curve encryption have been used to encrypt data in security infrastructure.

KEYWORDS

Internet of Things, Security, Authentication, Encryption

1. INTRODUCTION

One of the greatest challenges facing the IoT is the security issues associated with it. Security issues are crucial at institutionalized organizations where Internet access devices are assigned to control sending and receiving sensitive data; therefore, it is imperative that the institutionalized organizations pay attention to the security issues related to IoT functions prior to conducting any operation. Security must be concentrated on controlling access and authentication. Validation makes it easy for users to access hardware devices (such as sensors), and these solutions can be useful in protecting data against damages and misuse [1].

With the increase of the number of equipment connected to the Internet in Internet-based applications, the probability of security vulnerabilities increases. Poor-security equipment can be

the starting point for cybercrime attacks, as it allows hackers to restrict system performance by reprogramming these equipment. They could also be used to steal user data. An important solution to increase the security is data encryption and decryption. In this study, security architectures on the IoT are examined, and methods of preventing intrusion are proposed to enhance security.

The term "Internet of Things" was first used by Kevin Ashton in 1999 and was first introduced to the world by the MIT Institute Publisher and described a world where everything, including non-living objects, could have their own digital identity and could allow computers to organize and manage them [1]. The IoT is not a unique technology. Rather, it is a set of empowering and idea generation technologies. One aspect of empowerment is to minimize electronic components and reduce their charges.

The IoT is a new technology in the world of information and communication technology that is capable of sending and receiving data through communication networks [1]. Simply put, the IoT refers to the association of various objects and their communication with each other via the Internet. The IoT technology has a great role in developing and upgrading smart systems. The IoT architecture consists of five main layers. Each layer has its own tasks and functions which provides services for its higher or lower levels in the meantime.

Perception Layer: This layer is similar to the physical layer of Open System Interconnection (OSI) consisting of various sensors (e.g., RFID, ZigBee, Infrared radiation, etc.), environmental devices and elements [1]. This layer is generally related to public management of sensor devices, that is, the identification and accumulation of specific information obtained by each sensor device. The data collected can be from the type of position, wind speed, vibration, humidity information, and so on. This information is transmitted to the central data processing system through the network layer due to its reliable communications.

Network Layer: This layer includes the following applications [1]: controlling access and transfer origin and authentication management. It also transfers information to the central data processing system securely. For this reason, it is responsible for data transference from the layer of perception to the higher layer.

The Middleware Layer: when the devices are connected and interconnected, the data is saved and retrieved by this layer [2].

Application Layer: This layer is inclusive of applications for the IoT and is responsible for managing them based on the information processed in the middleware layer [1]. IoT applications can be smart mail, smart health, smart shipping, and more.

Business Layer: The functions of this layer cover all service administrations and the IoT applications [1]. This layer can create charts, business models, workflow diagrams, executive reports, and so on. These actions will be based on the information received from the lower layer and their processing.

Despite all the advantages of the Internet of things, they are subject to unauthorized access and being hacked because of the fact that objects such as computers and smartphones are connected to the Internet [3]. Due to the large number of people who are connected to the set of IoT, they will

have widespread harm at the time of hacking. Security is the most important issue on the IoT. The security must be so intensive that the security of the data can be ensured on the Internet space. Security ought to be provided in order to prevent the invaders from infiltrating the IoT network. Ensuring service security is a very important factor in building trust among users and using this platform. Users must be confident that the IoT, its applications, and equipment that are connected to it are sufficiently safe to conduct online activities against threats [4]. If users do not make sure that their equipment and information are reasonably safe from disruption and abuse, this distrust will reduce the use of IoT-based applications.

In this paper, IoT and its security architectures are discussed with respect to data encryption and decryption; having investigated the architectures, the best solutions are selected as the safe architecture and the required recommendations are given.

2. REVIEW OF LITERATURE

A model based on the authentication and encryption of data is proposed for the IoT architecture [5]. In the proposed model, users are supposed to use a special ID to enter the IoT environment and use the key to decrypt the data. Data encryption is performed on sensors using the AES algorithm. In this regard, confidentiality, integrity, and authentication are made available simultaneously. The AES algorithm is considered to belong to a category of high-security algorithms in a sense that most of the organizations use this algorithm for encryption purposes. AES encrypts the data in 128-bit blocks and can use 128, 192, 256-bit keys. The algorithm is considered to of symmetric algorithms type; in other words, a single key is used by coder and decoder to encrypt and decrypt data.

A model is proposed on the basis of RC4 encryption and Biometric to have access to data in IoT [6]. On the IoT, data transfer must be done without any vulnerabilities; therefore, encryption plays a major role in data protection. Data security depends on various access control mechanisms and is controlled by encryption and decryption. One of the most important symmetric cryptographic algorithms is called RC4 stream encryption algorithm; the advantages of this algorithm are fast encryption and decryption, less resource utilization, ease of understanding and implementation, low spatial and temporal complexity compared to other algorithms. In this architecture, fingerprinting is used to access data. In the first step, fingerprint users are authenticated, and then the key is used for decryption to access the content of the data.
The IoT requires mechanisms such as access control, confidentiality, integrity, authentication, and availability. Researchers have used the Blowfish algorithm to provide data security [7]. Blowfish symmetric cryptographic algorithm is one of the most common encryption methods. This algorithm uses a public-key in the range of 32 - 448 bits. The results have shown that Blowfish algorithm is faster in data encryption and decryption than AES and DES algorithms.
Network security, data, and sensor devices are regarded as the important topic in IoT. Researchers have studied the validation and controlling access to data on the IoT by using the RSA encryption algorithm [8]. The RSA algorithm uses two keys for encryption: the private key and the public key. The data is encrypted on the central server of the IoT and decrypted by users based on the private key. The results have indicated that the RSA algorithm is faster than the AES and SHA-1 algorithms.

The IoT tries to integrate and connect electronic devices in the real world through Internet. Despite the numerous advantages and benefits of the IoT, it also has some challenges for which

major strategies need to be taken. A security model is proposed for data encryption based on the combination of RSA and AES algorithms [9]. In this model, the data are initially encrypted by RSA then by AES algorithms.

An AES algorithm based model [10] is proposed for the encryption of IoT data. In the proposed model, the key length for encryption and decryption is 400 bits. The data sent by the sensor to the users is encrypted in the data format and must be decrypted by the key that are owned only by authorized users.

The midgar platform [11] is proposed to encrypt text messages that are exchanged between sensor nodes. On the midgar platform, the cryptographic key is first specified. In the second step, the hash operation is performed to change the original text. In the third step, digital signing takes place over the text for further security; and finally the original text is converted to the encrypted state by the public key. The hash function receives a long string as the input and displays a string with constant length in the output. The resulting hash is a representation of the entire content of the text or input string and can be considered as a kind of "digital fingerprint" for that text. Hash functions are used to check the authenticity of messages and digital signature of texts in a wide range of applications such as Authentication and Verification. Symmetric algorithms such as DES, 3DES, AES, Blowfish and IDEA are used for encryption and decryption. The length of the encryption key is 56 -256. IDEA algorithm is the longest key. Also, the MD5, SHA-1, SHA-2 and SHA-3 algorithms are used for hash operation.

RSA and DES algorithms are proposed for encryption and decryption of IoT data [12]. The cryptographic operation was initially performed by RSA and then by DES algorithms. Every message sent to users through objects is initially encrypted by the server. The RSA encryption has large-sized keys, and the larger the number (for example, 2048 and 4096) the algorithm works more slowly because of the large numbers and more complexity. That is why, it is utilized only in the initial stage. The RSA key with 2048 bits is used for authenticating or signing purposes and ensures that only can the primary receiver access the information sent or encrypted.

Elliptic Curve Cryptographic Security Signing Plan is proposed for the security of data on the IoT [13]. Elliptic curve cryptography is an encryption method in the form of public key based on an algebraic structure of elliptic curves designed on finite fields. The elliptical curve encryption needs a smaller key compared to the other encryption. The main advantage of elliptical curve encryption is smaller size of the key, which means reducing the storage and transmission of data. That is to say, an elliptic curve system can have the same level of security as an RSA-based system with large modules and long key length.

In [14], a strong encryption method has been proposed based on Elliptic Curve algorithm for RFID tags. Encryption-related operations are carried out in Back-End section. There are storage devices, servers, hardware, communicational equipment and platforms that provide IoT services on the internet. Back-End is normally managed and controlled by a company or system manager, and given each user the required services, certificates, traffic, protocol organization and definition, and etc. are provided. The objective of the proposed model is ensuring authentication, encryption, and confidentiality. Data is hashed for security maintenance.

Researchers [15] have studied IoT based on such factors as access control and authentication. EEC algorithm is used data encryption. Users are supposed to pass security codes to have access

to data and devices and the Internet environment accordingly. In the application layer, users` passwords are evaluated and they can get connected to the Internet space if the passwords are correct.

Cipher text-Policy Attribute-Based Encryption (CP-ABE) model [16] is one of the strong models for data encryption. The users code their data and save it in the coded data set for confidentiality. In CP-ABE model, users first log in to the system and ought to use a key to have access to the data so that data could be encrypted. Managing the users is also controlled by the dataset manager.

3. SECURITY OF THE INTERNET OF THINGS

IoT is faced with many challenges including data security, privacy sustenance, data quality, and trust. Therefore, such mechanisms as cohesion, authentication, access control, and confidentiality should be included in this technology. Increasing distribution of services which have been made feasible through the IoT creates many challenges with regards to data security and quality. In addition to data security and quality, confidentiality has a prominent role in the IoT space. Since security, confidentiality, and data protection are of crucial prominence, IoT suppliers should consider the three important criteria such as data protection, content correctness, and trustworthiness of information sources [17]. First, all the data should be encrypted, controlled, protected, stored, transferred and made available for secure access by their owners. Second, data originality and comprehensiveness should be considered with regards to ordering users` privacy protection in the process of data and integration; third, accessing and sharing data should be carried out through digital signing and issuing certificate processes in order to prevent non-permissible changes in the content of sensitive data [18].

3.1. COMPARISON OF SECURITY INFRASTRUCTURE IN THE IOT

With the ascending growth of applications on the IoT, various architectures have been created for the IoT,the purpose of which is to ensure security and control IoT hardware. To this end, investigating and comparing IoT architectures is a necessity, and IoT developers can choose the best architecture to block intrusion. A comparison of security infrastructures is demonstrated in Table (1). Security infrastructures have been compared based on encryption factors, encryption algorithms, authentication, access control, hashing, and confidentiality.

Table 1: Comparing Security Infrastructures in the IoT

Refs	Encryption	encryption algorithm	Authentication	Access control	Data hashing	Confidentiality
[5]	Y	AES	Y	N	N	Y
[6]	Y	RC4	Y	N	N	N
[7]	Y	Blowfish	N	N	N	N
[8]	Y	RSA	N	N	N	N
[9]	Y	RSA+AES	N	N	N	N
[10]	Y	AES	N	N	N	Y
[11]	Y	MD5, SHA-1	Y	N	Y	Y
[12]	Y	RSA, DES	Y	N	N	Y
[13]	Y	ECC	N	N	N	Y
[14]	Y	ECC	Y	Y	N	Y
[15]	Y	ECC	Y	Y	N	N
[16]	Y	ABE	Y	N	N	Y

Encryption: one of the methods of enhancing security on the IoT is encryption. When encryption is used a set of keys is created and the data will be handed to the user only if s/he has the key. According to table (3-1), it is obvious that RSA and ECC (Elliptic Curve Cryptography) algorithms are more applicable in encryption. Elliptic Curve Cryptography is a public key encryption method.

Authentication: generally, the aim of authentication is to allow authorized users and disallow unauthorized ones into the IoT environment. As a matter of fact, this process identifies, confirms the identity of, and allows the users into the system which in turn is composed of two phases, i.e., identification and authentication [19]. Identification phase is responsible for identifying the user. This identity is usually defined in the form of username for the system, so the system identifies the users using it. Authentication is the process of confirming user identity. In fact, when the user is identified by the system in the first phase, his/her identity is confirmed based on the documents provided in the authentication phase. This phase checks the user identity documents with what exists in the system. These identity documents can be passwords or any other pre-provided document which are called authentication factors. In order to initiate the processes of authentication, certificate issuing, and responding, the users should give an identity to the identification system on the IoT. In the authentication phase, a code is sent to the user`s cell phone for final confirmation and user identification [20]. If the user can correctly enter the password, s/he can log in to the IoT space and have access to the data.

Confidentiality: the data is valuable only on condition of being correct and this alludes to the issue of maintaining and ensuring data preciseness and cohesion on the IoT. Users` information should be protected against unauthorized access, illegal functions, accidental damages, destruction, and deficiencies [21]. IoT network and its infrastructure ought to be protected through security strategies including security software, intrusion detection data set, and other protectionary technologies against unauthorized access.

Hashing data: hashing data is considered to be one of the most crucial topics in IoT. Sometimes, it is required to store information in a safe way that could not be intruded. In this case, data can be hashed using MD5 algorithm [11] and stored on the IoT servers. Hashing is a method of data coding with fixed length which carries out the act of encryption in one way, and data scrambling is carried out in the best way possible. Therefore, it is impossible to decrypt data without key [22].

3.2. ENCRYPTING DATA ON THE IOT ENVIRONMENT

Data sequence diagram on the IoT environment is shown in Figure (1). The actual user can encrypt data using the special key. This causes the data to be saved in the encrypted form and decrypted only using the actual user's special key. Hence, if an intruder aims to enter the IoT system, s/he will be faced with encrypted data and cannot consequently have access to them.

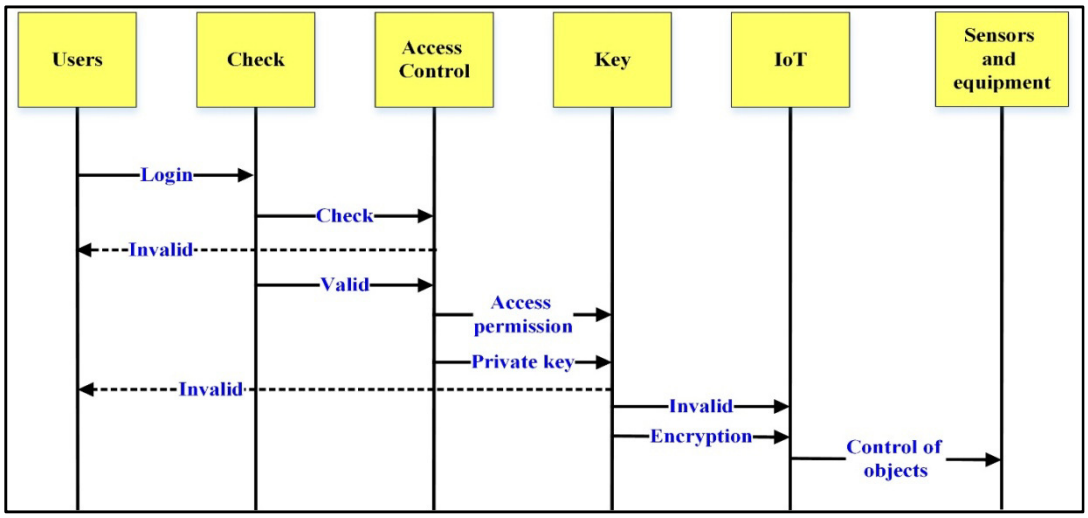

Figure 1: Sequence Diagram of Data Encryption Operation with Key

The chart of users' log in to the IoT space is shown in Figure (2). Diagram shown in Figure (2) is used in the majority of security infrastructures for users' log in to the IoT space. Diagram is the activity of a flowchart which is used for illustrating the controlling stream from one activity to the other. According to the activity diagram of Figure (2), first the log in page is shown to the users. Then, the users enter their username and password. Validation is performed in two modes in the system section i.e., valid and invalid modes. If the password is in the valid mode, users can log in to the system and connect to the IoT server.

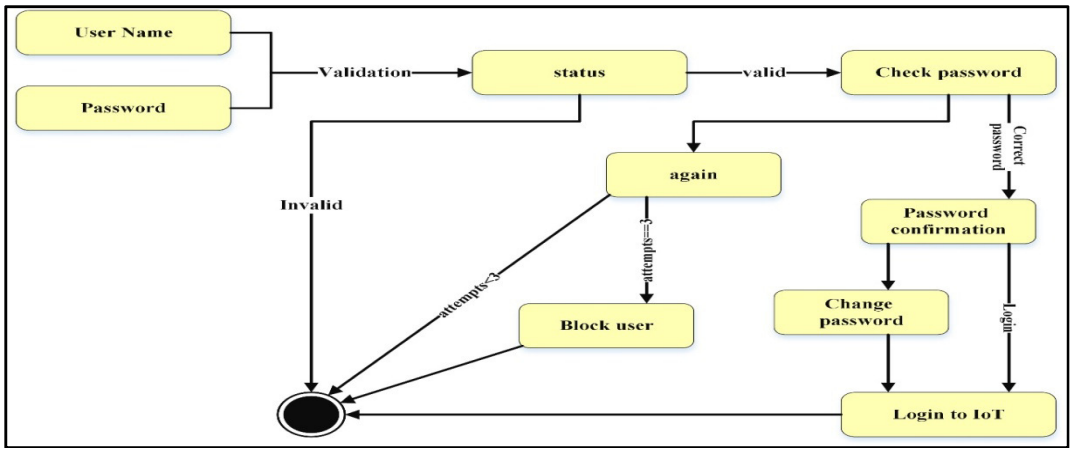

Figure 2: Activity Diagram of Users' Log in to the IoT Environment

3.3. Reasons For Security Infrastructures In The IoT

Security infrastructures should include hardware and software to resist intruders and bad ware. Security infrastructures should manage attacks and security incidents in a central sense, control them intelligently, analyze and prevent threats that are likely to occur in the IoT space [23].

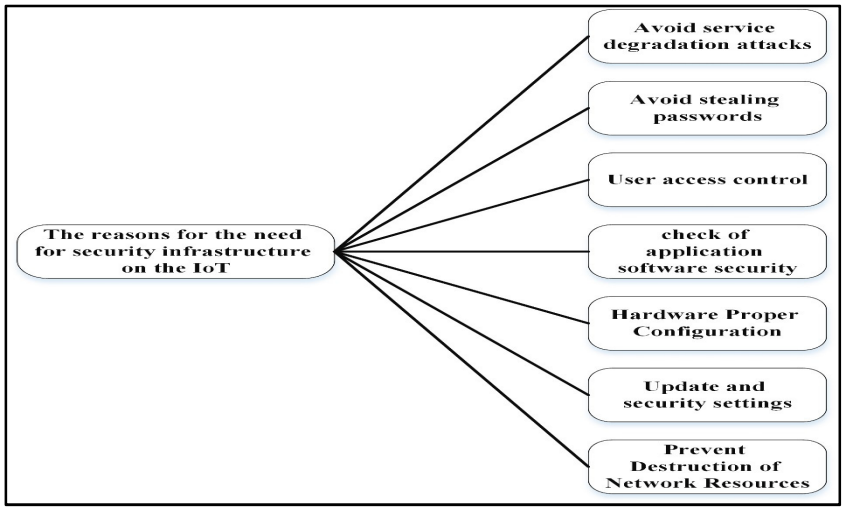

Figure 3: Reasons for Security Infrastructures in the IoT Space

3.4. Objectives Of Security Infrastructures

In short, the following can be summarized as the most important security infrastructure goals [24, 25]:

- Minimizing attacking risks to the IoT servers
- Minimizing the costs of decentralized security management
- Identifying known and unknown attacks and investigating the threats

- Decreasing the required sources for managing security risks
- Preventing intrusion into the vulnerable databases in the IoT
- Taking appropriate precautions to authenticate and confirm the users
- Use of suitable security tools: key encryption

If security infrastructures are properly managed and configured, they will act as a smart security agent and reduce the risk of attacking data and prevent attacks.

3.5. REASONS FOR SERVER VULNERABILITIES IN THE IOT

Default Server Settings: without changing default server settings, it is likely that users know username and passwords and have the permission to apply certain commands on the servers.
Invalid Configuration of Operating Systems and Networks: Some configurations, such as allowing specific users to execute some commands on a server, may be problematic.

Bugs in The Operating System: bugs are discovered over the server operating systems and software, then they are reported and resolved by security developers. Bugs may be detected by hackers before being fixed and be exploited and manipulated.

4. DISCUSSION

1) In order to reduce the security threats on the IoT, complex and robust authentication methods must be designed and implemented; in order to make a secure relation on the IoT devices, many security solutions and protocols have been implemented, including [26, 27]:

- Public-key infrastructure to ensure security between internet-connected devices
- Implementing Secure Sockets Layer protocol on the IoT to prevent network communications encryption
- Storage on the basis of data encryption
- Using security software in the application layer
- Valid configuration of routers

What is evident is that security strategies are also required for embedded devices that are connected to the internet. It is also necessary to protect these devices against attacks such as eavesdropping, blocking disrupted service, and network traffic manipulation.

2) One of the main concerns of the IoT is the danger of information loss which occurs in the process of unauthorized access to the information. The solutions recommended for this threat are as follow:

- Implementing strong access controlling
- Encrypting and protecting data cohesion while transference and reception
- Protecting data in both levels of storage and retrieval

Internet of Things consists of a wide range of services. Hence, reducing threats, protecting privacy, detecting probable damages, and presenting effective strategies are helpful in preventing penetration.

3) In the Internet of Things, ensuring the accuracy and speed of IoT servers' performance, services, and network equipment is highly important. The most important factor in the Internet of Things is supervision and monitoring which should be done by the network experts periodically. The most important items in monitoring the IoT equipment are: prevention of penetration, increase of service performance, regulation of servers, and network equipment.

4) It is imperative that weak and vulnerable points should be detected and dealt with before penetration in order to increase the security of Internet of Things. The following should be taken into consideration to increase the security of IoT equipment.

- Ensuring accuracy of equipment configuration
- Ensuring the update of the IoT systems and sensors
- Ensuring the security of devices against the latest vulnerabilities
- Finding the weak points before the attackers can take advantage

Ensuring security for the users in the Internet of Things is not simple. The fundamental and elementary functions of the IoT is based on data transference and the information between billions and thousands of billions objects connected to the Internet. One of the open and unsolved issues regarding the security of the IoT which has not been attended to in the standards is the distribution of keys between the tools.

5) One of the most important operations in the Internet of Things is hardware configuration. Lack of hardware security on the IoT allows intruders to configure in their intended manner by gaining access to the equipment. In this way, any kind of penetration or information robbery or any other kind of damage to the IoT can be done by the intruder. Hardware Security is more and more trustworthy than software security. It is possible to embed locking systems on hardware; with this solution, it is possible for the servers to include hardware locking. Hardware locking with strong internal encryption algorithms is very resistant to the attacks. An advanced hardware lock has a non-volatile internal memory and can include encryption keys.

6) Security infrastructures should have the capability to resist bad ware in order to protect the security of IoT data. Bad ware is a set of programs and software that are created with the aim of disrupting and destructing IoT servers and misuses the systems by penetration into the IoT systems through information distribution and copying. Operating system and the software installed on the IoT servers should be updated in order to resist the bad ware. That is because, a number of the program problems that may cause misuse of IoT system is solved by each updating and this improves the security of IoT space.

7) With the increase of attacks in different layers of IoT, using unified threat-management system (UTM) is a suitable method of preventing penetration by offering various security capabilities. The UTM system manages several layers of software and hardware by placing a piece. Using this system, we can evaluate and configure all the security strategies. Some of the major capabilities that UTM system provides include: firewall, penetration prevention antivirus, bandwidth management, controlling applications and concentrated reporting. UTM system is an appropriate strategy for ensuring the environmental security of the small, medium, and large networks. Blocking virus penetration, bad ware, preventing attacks and penetration are some of the characteristics of these devices.

8) Security is considered to be highly important in the application layer of the IoT in a sense that it is known as one of the highest security layers in the IoT space. Most of the attacks are done through this layer and can cause breakdown, robbery, and data distortion. The majority of operating systems, applications, and other products that work on the IoT can create a safe and certain environment for the users if run according to the manufacturers` standards. But, the main problem occurs in the field of practical software security when different users set out to design and implement practical software commensurate with their needs. Therefore, security precautions should be regarded in designing applications.

5. CONCLUSION AND FUTURE WORKS

The Internet of Things is a network of physical objects, devices, vehicles, buildings, and more that are embedded in systems which consist of electronics, software, sensors, and network connection. Encryption and authentication are two important factors to increase security in the Internet of Things. Authentication requires suitable infrastructures to prevent the penetration of intruders into the IoT space. The ultimate goal of security is ensuring confidentiality, cohesion, and data origin. The three criteria of security in devices, in communications and security management should be attended to in security architectures and frameworks. In this paper, IoT security infrastructures were studied to enhance security and prevent intrusion. Using encryption algorithms, we can store the information saved on the IoT servers in an encrypted manner and prevent unauthorized people from accessing them. In the majority of security infrastructures, AES, RSA, and ECC algorithms are used for data encryption. A combination of encryption algorithms can be used in the future research to increase security on the IoT. Penetration detection systems can also be used to prevent attacks. These systems can detect penetration based on network traffic and inform the actual user. In future works, we will propose encryption techniques such as DES, RSA, and MD5 in order to encrypt data frames to take in consideration the security issues.

REFERENCES

[1] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey, Journal of Network and Computer Applications, Vol. 88, pp. 10-28, 2017.

[2] M.A. Razzaque, M.M. Jevric, A. Palade, S. Clarke, Middleware for Internet of Things: A Survey, IEEE Internet of Things Journal, Vol. 3, Issue: 1, pp. 70-95, 2016.

[3] M.Ammar, G. Russello, B. Crispo, Internet of Things: A survey on the security of IoT frameworks, Journal of Information Security and Applications, Vol. 38, pp. 8-27, 2018.

[4] K.Sha, W. Wei, T.A. Yang, Z. Wang, W. Shi, On security challenges and open issues in Internet of Things, Future Generation Computer Systems, In press, corrected proof, Available online 7 February 2018.

[5] F.Li, J. Hong, A.A. Omala, Efficient certificateless access control for industrial Internet of Things, Future Generation Computer Systems, Vol. 76, pp. 285-292, 2017.

[6] C.Xie, and S.T. Deng, Research and Application of Security and Privacy in Industrial Internet of Things Based on Fingerprint Encryption, ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 102-110, 2017.

[7] M.Suresh, M. Neema, Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things, Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology, Procedia Technology, Vol. 25, pp. 248-255, 2016.

[8] T.Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, DTLS based security and two-way authentication for the Internet of Things, Ad Hoc Networks, Vol. 11, Issue 8, pp. 2710-2723, 2013.

[9] A.Darwish, M.M. El-Gendy and A.E. Hassanien, A New Hybrid Cryptosystem for Internet of Things Applications, Multimedia Forensics and Security, pp. 365-380, 2017.

[10] Ritambhara, A. Gupta, M. Jaiswal, An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT), International Conference on Computing, Communication and Automation (ICCCA), pp. 422 - 427, 2017.

[11] G.S.Arias, C.G. Garcia, and B.C. Pelayo G-Bustelo, Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things, Future Generation Computer Systems, Vol. 74, pp. 444-466, 2017.

[12] I.Hussain, M.C. Negi; N. Pandey, A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer, International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), pp. 464-470, 2017.

[13] X.Jia, D. He, Q. Liu, K.K.R. Choo, An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment, Ad Hoc Networks, Vol. 71, pp. 78-87, 2018.

[14] M.L.Das, Strong Security and Privacy of RFID System for Internet of Things Infrastructure, International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2013: Security, Privacy, and Applied Cryptography Engineering, pp. 56-69, 2013.

[15] S.Sasirekha, S. Swamynathan, S. Suganya, An ECC-Based Algorithm to Handle Secure Communication Between Heterogeneous IoT Devices, Advances in Electronics, Communication and Computing, pp. 351-362, 2017.

[16] S.Perez, D. Rotondi, D. Pedone, L. Straniero, M.J. Nunez, F. Gigante, Towards the CP-ABE Application for Privacy-Preserving Secure Data Sharing in IoT Contexts, International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2017: Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 917-926, 2017.

[17] M.Beltran, Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things, Computers & Security, Vol. 77, pp. 595-611, 2018

[18] K.H. Wang, C.M. Chen, W. Fang, T.Y. Wu, A secure authentication scheme for Internet of Things, Pervasive and Mobile Computing, Vol. 42, pp. 15-26, 2017.

[19] M.S. Farash, M. Turkanovic, S. Kumari, M. Holbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks, Vol. 36, Part 1, pp. 152-176, 2016.

[20] Z. Mahmood, A. Ullah, H. Ning, Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things, IEEE, Vol. 6, pp. 29460-29473, 2018.

[21] R.H. Weber, Internet of things: Privacy issues revisited, Computer Law & Security Review, Vol. 31, Issue 5, pp. 618-627, 2015.

[22] B.V. Sundaram, M. Ramnath, M. Prasanth, J.V. Sundaram, Encryption and hash based security in Internet of Things, 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), IEEE, pp. 1-6, 2015.

[23] S.Yoon, J. Kim, Remote security management server for IoT devices, International Conference on Information and Communication Technology Convergence (ICTC), IEEE, pp. 1162-1164, 2017.

[24] S.Sridhar, S. Smys, Intelligent security framework for iot devices cryptography based end-to-end security architecture, International Conference on Inventive Systems and Control (ICISC), pp. 1-5, 2017.

[25] X.Lu, Q. Li, Z. Qu, P. Hui, Privacy Information Security Classification Study in Internet of Things, International Conference on Identification, Information and Knowledge in the Internet of Things, pp. 162-165, 2014.

[26] S.C. Arseni, S. Halunga, O. Fratu, A. Vulpe, G. Suciu, Analysis of the security solutions implemented in current Internet of Things platforms, Conference Grid, Cloud & High Performance Computing in Science (ROLCG), pp. 1-4, 2015.

[27] S.Raza, L.Seitz, D. Sitenkov, G. Selander, S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things, IEEE Transactions on Automation Science and Engineering, Vol. 13, Issue: 3, pp. 1270-1280, 2016.