IJAMML 13:1 (2020) 5-23 September and December 2020
ISSN: 2394-2258
Available at http://scientificadvances.co.in
DOI: http://dx.doi.org/10.18642/ijamml_7100122152

ROBUST DATA SECURITY FRAMEWORK FOR IoT NETWORK USING INTEGRATED TECHNIQUES

Fadele Ayotunde Alaba[a], Abayomi Jegede[b] and Christopher Ifeanyi Eke[c]

[a]Department of Computer Science, Federal College of Education, Zaria, Nigeria

[b]Department of Computer Science, University of Jos, Nigeria

[c]Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

---

Abstract

The Internet of Things (IoT) expects to improve human lives with the rapid development of resource-constrained devices and with the increased connectivity of physical embedded devices that make use of current Internet infrastructure to communicate. The major challenging in such an interconnected world of resource-constrained devices and sensors are security and privacy features. IoT is demand new approaches to security like a secure lightweight authentication technique, scalable approaches to continuous monitoring and threat mitigation, and new ways of detecting and blocking active threats. This paper presents the proposed security framework for IoT network. A detail understanding of the

*Corresponding author.
E-mail address: ayotundefadele@yahoo.com (Fadele Ayotunde Alaba).

2020 Mathematics Subject Classification: 68, 91.
Submitted by Jianqiang Gao.
Received August 15, 2020

existing solutions leads to the development of security framework for IoT network. The framework was developed using cost effective design approach. Two components are used in developing the protocol. The components are Capability Design (mainly a ticket, token or key that provides authorization to access a device) and Advanced Encryption Standard (AES)-Galois Counter Mode (GCM) (a-security protocol for constrained IoT devices). AES-GCM is an encryption process that is based on authentication and well suitable IoT.

Keywords: IoT, security, framework, authentication, encryption, decryption.

---

1. Introduction

The presence around us of a variety of object (e.g., RFID tags, sensors, actuator, mobile phones etc.), which through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach a common goal (Atzori et al. [2]). The potential applications span several fields, such as like healthcare, industrial automation, smart homes, smart grid, and smart city (Fadele et al. [6]).

One of the problems with IoT network is that more connection of things will create more chances for malicious attacks and hijacking of the networking communication channel due to the presence of inadequate security. Hence, there is a need for a robust authentication framework that will coordinate and control how devices can be accessed by authentic users (Gu et al. [7]). Authentication is a verification process of a device identity to ensure the authenticity of the device. Authentication process are granted to devices that possesses access control. With the nature and threats imposed on IoT network, there is a need to introduce secure identity and access control on devices (Srinivas et al. [25]).

Devices like sensor node or RFID do not have access control function and exchange information freely with each other. For instance, RFID communication between a tag and reader can easily lead to security issue, where an attacker can access the tag and obtain the result through eavesdropping (Qiu and Ma [27]). Therefore, there is a need to establish an authentication and authorization scheme among devices in order to attain the security goals for IoT network. Authentication includes

confirmation between routing peers of connected IoT devices prior to exchanging the route information (known as peer authentication), and guaranteeing that the source of the route data is from the connected peer devices (known as data origin authentication). This helps to enhance the primary element in IoT vision, which is M2M communication (Perera et al. [21]). The motivation behind the authentication protocol is to provide access to authentic IoT users. In the IoT application domain, authentication allows the integration of different IoT devices and its deployment in various smart environments, such as smart cities. A smart environment can merge different services provided by different multiple shareholders and scales to support numerous users in a dependable and distributed way. With the presence of different and complex attacks, the capability to notice potential attacks and to mitigate the impact of malicious attacks becomes a critical issue. However, researches on developing an authentication framework for IoT devices are few. Moreover, the existing security framework focus primarily on how to speed up the elementary security functions for IoT devices (basic security properties for embedded devices). Recently, Guan et al. [8] suggested an approach known as, "an Anonymous and Privacy Preserving data Aggregation (APPA) scheme", meant for Fog networking authentication in IoT domain. This approach (APPA) is device-oriented that is flexible, efficient and can independently manage and secure communications between IoT devices. For instant communication in fog-enhanced IoT computing domain, APPA is the most preferred scheme due to its features listed above. However, APPA is only effective and implemented in fog-IoT. Nevertheless, the proposed scheme should be broadened and actualized in other IoT applications for instance intelligent city, e-health, intelligent grid, intelligent home among others.

Likewise, an access authentication capacity-aware security system referred to as AccessAuth was developed by Tao et al. [5] specifically for merged IoT-enabled Vehicle-to-Grid (V2G) networks. Moreover, "AccessAuth", a lightweight protocol with conditional confidentiality in V2G networks also has the ability to reduce the probability of dropping and blocking packets in a session thus enabling access requests in V2G network application domain.

In this paper, we propose a novel authentication security framework for IoT network. A detail understanding of the existing solutions leads to the development of security framework for IoT network using Advanced Encryption Standard (AES)-Galois Counter Mode (GCM).

The main contributions of this paper are summarized as follows:

- Proposal of a novel authentication security framework for IoT network.
- The integration of AES-GCM technique to provide authentication and encryption for resource constrained devices with minimum latency, low operational overhead and efficient low cost implementation.
- The use of capability as a second line of defense for access control and random number generator.

2. Existing Authentication Schemes for IoT

This section explores existing authentication schemes in IoT. Many security authentication framework employing a variety of defense techniques have been developed to address authentication challenges in IoT domain. Caraguay et al. [26] propose a security protocol for bulk data transfer among "things" and a framework for enhancing security, trust and privacy for embedded system infrastructure. The proposed solution uses lightweight symmetric encryption (for data) and asymmetric encryption (for key exchange) in Trivial File Transfer Protocol (TFTP). Jararweh et al. [12] propose a comprehensive software defined based framework model (SDIoT) to simplify IoT management process. It provides a vital solution for the challenges in the traditional IoT framework to forward, store, and secure the produced data from the IoT objects. SDIoT system framework allows using the cloud resources in an efficient way by creating slices/slivers and letting the data flow in a transparent way. However, there is no experimental framework for SDIoT to test different forms and types of IoT topologies. Sicari et al. [24] analyze available solutions for security, privacy, and trust in IoT heterogeneous environment. This study discusses the existing solutions in detail, but ignores the privacy policies in managing the adaptability and

heterogeneous setting of IoT. Chakrabarty et al. [4] propose a secure IoT framework for smart cities to address the vulnerabilities in traditional IoT systems. The four basic IoT architectural blocks for secure smart cities are black network, trusted SDN controller, unified registry, and key management system. Moosavi et al. [19] propose a secure and efficient authentication and authorization framework for IoT-based health-care systems. It uses a distributed smart e-health gateways framework to handle computation, communication overhead, authentication and authorization. Moreover, Randhawa et al. [22] suggested an energy efficient multi-domain technique that employs "chaining message authentication code (CCM)" mode for OSCoAP in the mac-domain security suite of IoT components. The implementation of CCM guarantees memory efficiency, thus, saving more energy by up to 10 times, while improving battery life by 30%; and 37% faster than the implementation of CMM software for OSCoAP. In addition, OSCoAP is capable of alleviating IoT devices threats in which CoAP proxies are involved. This is due to the fact that proxies are usually exposed spots, as it is at the proxy that the underlying Datagram Transport Layer Security (DTLS) terminates. Nevertheless, this recommended technique only handles the security related issues in the application domain. Therefore, there is a need to extend this approach to both network and physical domains of IoT.

Similarly, Mavropoulos et al. [18] proposed an approach called "Apparatus" which is used for analyzing security issues in IoT systems. It utilized the class-based scheme of the modelling language and an organized strategy for shift between various models. This technique helps to find out the challenges imposed on IoT system models manually. The manual procedure for finding the security vulnerability in IoT models consumes more time and is not efficient enough for resource-constrained devices with limited energy. In this case, it is fundamental to introduce more automated and semi-computerized procedures for creating models thereby reducing security concerns in the IoT network.

Yigit et al. [9] developed a cost-aware security approach by means of compact attack graphs techniques to help in ensuring the security of IoT gadgets. In this technique, the compact attack graphs are centered on greedy algorithm, which is applicable to far-reaching graphs with an enormous quantity of IoT nodes. Moreover, in conjunction with network hardening, the suggested technique also has the ability to measure the level of security of the entire network in systematically thereby indicating the degree of exposure of the IoT network. Using Shamir's secret sharing scheme, a secure and scalable storage system for data collection in IoT was proposed by Jiang et al. [16], to reduce key management complexities related with the old-fashioned cryptographic algorithms while offering dependability feature at the data level. Moreover, with Shamir's mystery sharing plan, information adaptability can be accomplished despite the fact that the quantity of structures applied in storage systems may produce computational overheads that incite potential bottlenecks. In addition, Li et al. [17] proposed public verifiable privacy-preserving aggregation and its application in the IoT using public verifier that enables an untrusted aggregation node to perform the aggregation over data from source nodes without revealing the data, while the correctness of the aggregation result can be checked by a public verifier. This approach is secured under the co-CDH assumption, but needs to improve its robustness and also provides an efficient way to carry out drop-outs of data owners.

However, the effect of attack trails with regard to confidentiality, availability as well as integrity of IoT components cannot be ascertained in this technique.

Figure 1 provides the classification of existing authentication schemes for IoT.

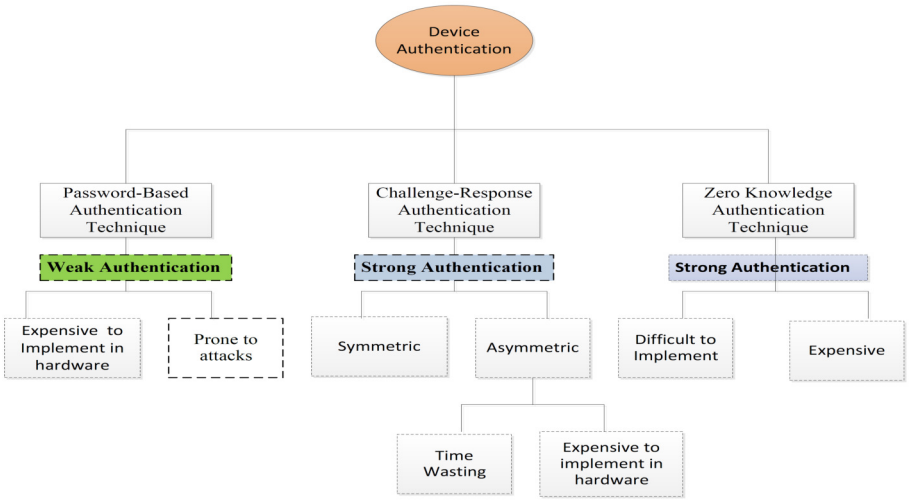

Figure 1. Classification of existing authentication schemes for IoT.

Generally, the existing authentication schemes are classified into three (Gu et al. [7]), as shown in Figure 1:

(1) Password-Based Authentication Technique (Weak Authentication): The Password-Based authentication technique provides weak authentication and is prone to attacks.

(2) Challenge-Response Authentication Technique (Strong Authentication): The Challenge-Response authentication is a technique that is broadly used because of its cryptographic features, such as symmetric and asymmetric, offer a strong level of authentication. The major drawback of asymmetric authentication is time consuming and its implementation in hardware is expensive.

(3) Zero Knowledge Authentication Technique: This technique involves "robust" mathematical problems. The mathematical nature of this technique makes it implementation very difficult and costly (Kim [14]).

The challenges imposed on the present authentication techniques discussed make IoT channels communication technologies prone to different threats and attacks such as authenticity of devices, eavesdrops, MitM, data confidentiality among connected devices, data integrity and freshness.

3. Proposed Authentication and Encryption Scheme for IoT Framework

Lightweight cryptographic encryption is the latest concept (Sankaran [23]) commonly used for securing embedded IoT devices. It helps to provide both authentication and data encryption that can easily be deployed as a security scheme for embedded device. In this research, we use Advanced Encryption Standard (AES)-Galois Counter Mode (GCM) technique for the authentication and encryption process in the IoT.

Capability is a ticket, key or token that provides authorization to access a device. Its implementation is in the form of a data structure, composed-of identifier, a random number and access rights. On IoT devices, a single name is used as an identifier. A standard capability structure that is made up of the following attributes: Device, Rights and Random. All these attributes are represented as a single ticket for capacity. Device identifier is a name or identity of a device. Access rights are sets of access information that describes device capability. Thus, capability is denoted as;

$$Capability = (ID_n, R_n, RNG). \quad (1)$$

From Equation (1), ID_n represents sets of device identifier, R_n represents set of access rights, and RNG represents the random number generator.

The GCM is a security protocol for constrained IoT devices. It is a strong security model for message authentication and confidentiality against attacks introduced by Bellare et al. [3]. GCM uses block cipher

mode for operation that makes use of a universal hashing in a finite field Ghash Function (GF)(2^{128}) to provide message authentication encryption. In order to achieve low cost, high speed and minimum latency, GCM should be implemented in hardware. Also, to achieve a good performance, GCM is necessary for software implementation (Hori et al. [11]). It uses tools that is well-understood and supported by a theoretical basis. Its security depends on the security of the block cipher. It is a normal assumption in cryptographic designs and it also appears to be valid for AES. AES-GCM is the most recent authentication encryption algorithms suitable for hardware implementation. It provides both message confidentiality and authentication for embedded devices (Hori et al. [11]).

AES-GCM authenticated encryption operation has four inputs, each input in form of a string:

(1) A secret-key K, whose length is suitable for the basic cipher block.

(2) Initial Vector (IV) that can have any number of bits between 1 to 2^{64}. The major purpose of IV is to be a nonce, that is, for a constant value of key, every IV value needs to be unique.

(3) A plaintext P, which can have any number of bits between 0 and 2^{39} to 2^{56}.

(4) Additional Authenticated Data (AAD), which is denoted as A. "A" implies that data is authenticated but not encrypted. It can be any random number of bits between 0 to 2^{64}.

To provide strong security encryption and confidentiality, AES-GCM utilized the AES block cipher in counter-mode (i.e., a mode of operation that repeatedly apply a cipher's single-block operation securely to transform large amount of data that is larger than a block) to provide high-level security that is well-suitable for hardware implementation (Hinsenkamp et al. [10]). In this manner, the best security solution for embedded IoT devices is used in AES-GCM technique.

In addition, AES-GCM meets the necessary security requirements for resource-constrained devices. It improves the computational speed and storage capacity when implemented using hardware and software co-design approach (Anggorojati et al. [1]).

The proposed protocol makes use of capacity-based addressing in Anggorojati et al. [1], Jayasinghe et al. [13] and Sankaran, [23] in addition with AES-GCM to provide access control to the devices.

A. GCM notation

In this research, we adopts the recommended "block cipher modes of operation" notations by Hori et al. [11]. GCM have major functions, which are block cipher encryption and multiplication that is used over the field $\mathrm{GF}(2^{128})$ for providing robust authentication. The block cipher encryption is denoted as $E(K, A')$, where A is the encryption value and K is the key. The multiplication and addition of two elements (i.e., A' and B') is denoted as $A'B'$ and $A' \oplus B'$, respectively, given that $A', B' \in \mathrm{GF}(2^{128})$. The concatenation of two-bit strings X and Y is denoted as $X \| Y$. The function len() returns a 64-bit string containing the non-negative integer describing the number of bits in its argument, with the least significant bit on the right. The expression 0^l denotes a string of l zero bits. The function $\mathrm{MSB}_t(S)$ returns the bit string containing only the most significant (leftmost) t bits of S, and the symbol { } denotes the bit string with zero length.

B. Encryption

Plaintext consists of sequence bit strings between 0 to 128. Given that, x and y denotes a pair of unique positive integers such that the total number of bits in the plaintext is $(x-1)128 + y$, where $1 \leq y \leq 128$. The data blocks is denoted as J^*_n with the following bit sequence $J_1, J_2, \ldots, J_{n-1}, J^*_n$. Similarly, $C^*_n \in y$ represents the ciphertext with

bit strings sequence of $C_1, C_2, \ldots, C_{n-1}, C^*_n$. In addition, AAD "A" have the following bit of strings sequence of $A_1, A_2, \ldots, A_{m-1}, A^*_m$. In this case, the last string A^*_m is a partial block of length r. Both m and r are unique positive integers such that the total number of bits in A is $(m-1)128 + r$ and $1 \le r \le 128$. The GHASH function is defined as; $GHASH(H, A, C) = A'_{m+x+1}$. Therefore, we define the authentication encryption operational process using Equation (2) and Figure 2.

$$
\begin{aligned}
H &= E(K, 0^{128}), \\
B'_0 &= \begin{cases} IV \| 0^{31}1, & \text{if } len(IV) < 96, \\ GHASH(H, \{\}, IV) & \text{otherwise.} \end{cases} \\
B'_i &= incr(B_{i-1}) \qquad \text{for } i = 1, \ldots, n, \\
C_i &= P_i \oplus E(K, B'_i) \qquad \text{for } i = 1, \ldots, n-1, \\
C^*_n &= P^*_n \oplus MSB_y(E(K, B'_n)), \\
T &= MSB_t(GHASH(H, A', C) \oplus E(K, B'_0)).
\end{aligned}
\tag{2}
$$

An authenticated data encryption operational process for a situation when only a "single block of additional authenticated data" (i.e., Authenticate Data 1) and plaintext of two blocks (Kim et al. [15] and Pawar et al. [20]) is provided in Figure 2. E_K denotes the block cipher encryption using the key K, Mul_H denotes multiplication in $\text{GF}(2^{128})$ by the hash key H, and *incr* denotes the counter increment function.

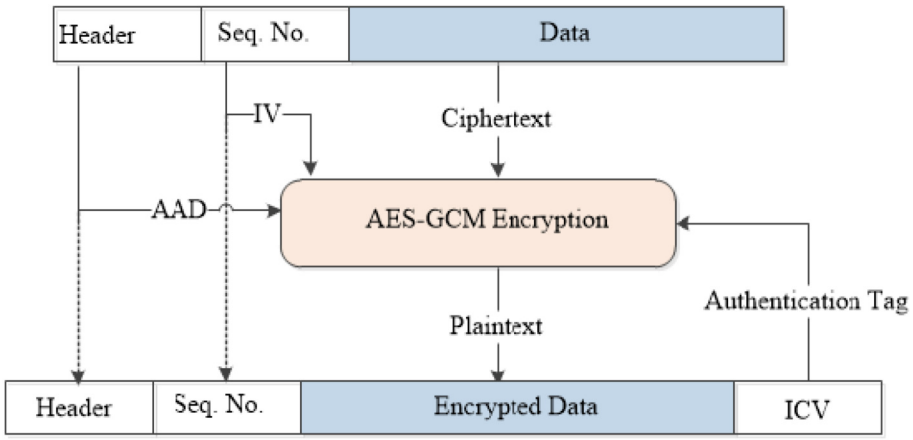

Figure 2. AES-GCM encryption and authentication process for IoT devices.

C. Decryption

The authenticated data decryption operational process is related to the operational process of data encryption, but with the order of the hash step and encrypt step reversed. Thus, we define the authentication decryption operational process using Equation (3) and Figure 3.

$$
\begin{aligned}
&H = E(K, 0^{128}),\\
&B_0' = \begin{cases} IV \| 0^{31}1, & \text{if } len(IV) < 96,\\ GHASH(H, \{\}, IV) & \text{otherwise.} \end{cases}\\
&B_i' = incr(B_{i-1}) \qquad \text{for } i = 1, \ldots, n,\\
&P_i = C_i \oplus E(K, B_i') \qquad \text{for } i = 1, \ldots, n,\\
&P_n^* = C_n^* \oplus MSB_y(E(K, B_n')),\\
&T' = MSB_t(GHASH(H, A', C) \oplus E(K, B_0')).
\end{aligned}
\tag{3}
$$

The tag T' that is computed by the decryption operation is compared to the tag T associated with the ciphertext C. If the two tags match (in both length and value), then the ciphertext is returned. Otherwise, the special symbol **FAIL** is returned. Figure 3 shows the operational process of data decryption.

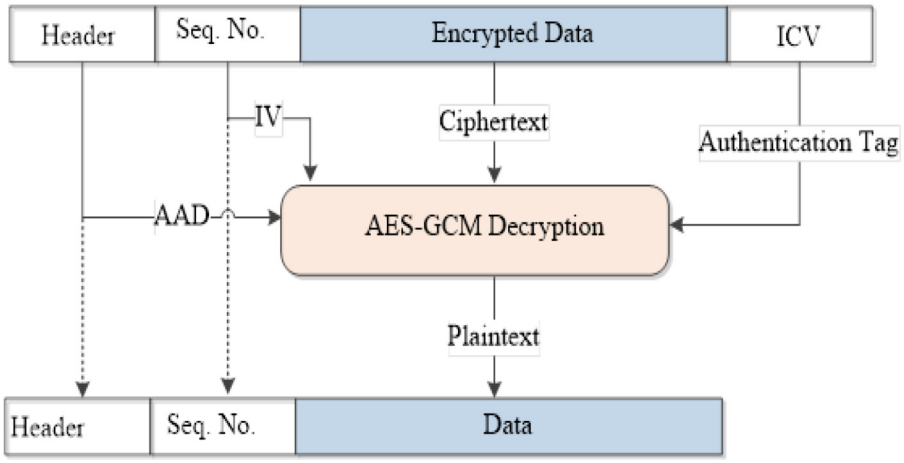

Figure 3. AES-GCM decryption and authentication process for IoT devices.

Figures 2 and 3 elucidates how fields of the security encapsulation map onto the inputs and outputs of the authenticated encryption and decryption mode. In some situations, it may be desirable to have the same AES-GCM key used for encryption by more than one device. In this case, coordination is needed to ensure the uniqueness of the IV values. A simple way in which this requirement can be met is to include a device-specific value in the IV, such as a network address. The AES-GCM employs multiplication operation bit vectors (Zhou et al. [10] and Hori et al. [11]) in order to simplify the specification of the nodes. However, a detail multiplication operator is provided below.

Multiplication for AES-GCM $(\mathbf{GF}(\mathbf{2}^{\mathbf{128}}))$

The multiplication operation is defined as an operation on bit vectors in order to simplify the specification. Each element is a vector of 128 bits. The i-th bit of an element K is denoted as K_i. The leftmost bit is K_0, and the rightmost bit is K_{127}. The multiplication operation uses the special element $R = 11100001 \| 0^{120}$, and is defined in Algorithm 1 presented in Table 1.

Table 1. Multiplication for AES-GCM

Algorithm 1. GF(2^{128}) Multiplication

Required

D ∈ GF(2^{128}); D ← 0, R ← K

(1) **Input**: K, L

(2) **Output**: D, R

(3) **While** $0 \leq i \leq 127$ Do

(4) **If** $B_i = 1$ **Then**

(5) D ← D ⊕ R

(6) **Else if**

(7) **If** $R_{127} = 0$ **Then**

(8) R ← rightshift(R)

(9) **Else**

(10) R ← rightshift(R) ⊕ L

(11) **End if**

(12) **End**

Note: The function rightshift() moves the bits of its argument one bit to the right.

To prevent adversaries from IoT network, AES-GCM pre-processed packets before transmission but the packets remain unencrypted. Thus, adversaries cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. AES-GCM serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.

4. Using AES-GCM

This section discussed the important of using AES-GCM protocol for securing IoT devices. During encryption, the data fields authenticated and encrypted. The encrypted data is conveyed together with a header and a sequence of number. The authentication of header is done by incorporating AAD in it, while IV is included in the sequence of number. In addition, Integrity Check Value (ICV) field is included alongside the encrypted data and authentication tag. It should be noted that, during the encryption process, there is no need to reduce/mitigate the plaintext, since there is no specific length for an input. The plaintext is the output that is provided during authentication decryption process. However, in a situation when the authentication check failed, the decryption process instead of plaintext will return FAIL. The decapsulation will terminated and the plaintext will be discarded.

Working process of the proposed protocol

The working processing of trust computation different layers is based on fuzzy weighted digraph. It consists of a set $(X_1, X_2, \ldots, X_n)$ of n interconnected nodes representing variable of communicating nodes of the modelled system for IoT network such as inputs, outputs, states, events, and signed weighted arcs which describe the causal relationships between these nodes and interconnect them. However, the value of each node is computed from the influence of other nodes to the specified node, by applying the calculation rule in Equation (4)

$$Y_i^{(t+1)} = V(Y_i^{(t)} + \sum\nolimits_{j=1J\neq i}^{n} Y_j^{(t)} * W_{ji}), \tag{4}$$

where $Y_i^{(t+1)}$ is the value of communicating nodes X_i at time step $t+1$; $Y_i^{(t)}$ is the value of communicating nodes X_i at time step t and W_{ji} is the edge weight that interconnects the layers together. It is a given

value on the interval $[-1, 1]$ to indicate three possible types of relationship among the layers. V is the threshold or activation function for converting the output of each computation to the range $[0, 1]$ or $[-1, 1]$.

5. Conclusion

In this research, a protocol known as "capability-based authentication and access control protocol" is proposed IoT devices. AES-GCM is then used to encrypt the data in order to provide strong encryption and authentication for the IoT devices. Also, in this paper, a challenge-response type of protocol that improves computation overhead of IoT devices is proposed. To achieve sound security solutions for IoT devices involve the introduction of security mechanisms on these devices right from the development stage. It is essential to consider the security requirements during the design process of embedded IoT devices in order to detect the vulnerabilities of the devices right from the development stage. When the sources of the vulnerabilities is known, then a defense mechanisms should be embedded inside the devices during the design stage. Therefore, AES-GCM protocol and capabilities was introduced for embedded IoT devices. It provides efficient authentication and encryption standard for embedded IoT devices implemented at low cost. Also uses capability as a second line of defense for access control to provide right values for authenticated. Finally, the utilization of hash function $\boldsymbol{h()}$, random number $\boldsymbol{R_n}$ and secret value $\boldsymbol{K}$ provide efficient security in both static and dynamic IoT network.

References

[1] B. Anggorojati, P. N. Mahalle, N. R. Prasad and R. Prasad, Capability-based access control delegation model on the federated IoT network, In: IEEE 15th International Symposium on Wireless Personal Multimedia Communications (2012), 604-608.

[2] L. Atzori, A. Iera and G Morabito, The internet of things: A survey, Computer Networks 54(15) (2010), 2787-2805.

DOI: https://doi.org/10.1016/j.comnet.2010.05.010

[3] M. Bellare, J. Kilian and P. Rogaway, The security of the cipher block chaining message authentication code, Journal of Computer and System Sciences 61(3) (2000), 362-399.

DOI: https://doi.org/10.1006/jcss.1999.1694

[4] S. Chakrabarty and D. W. Engels, A secure IoT architecture for smart cities, IEEE Annual Consumer Communications & Networking Conference, 2016.

DOI: https://doi.org/10.1109/CCNC.2016.7444889

[5] M. Tao, K. Ota, M. Dong and Z. Qian, AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks, Journal of Parallel and Distributed Computing 118(1) (2018), 107-117.

DOI: https://doi.org/10.1016/j.jpdc.2017.09.004

[6] Fadele A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, Internet of things security: A survey, Journal of Network and Computer Applications 88 (2017), 10-28.

DOI: https://doi.org/10.1016/j.jnca.2017.04.002

[7] Z. Gu, G. Han, H. Zeng and Q. Zhao, Security-aware mapping and scheduling with hardware co-processors for flexray-based distributed embedded systems, IEEE Transactions on Parallel and Distributed Systems 27(10) (2016), 3044-3057.

DOI: https://doi.org/10.1109/TPDS.2016.2520949

[8] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma and J. Hu, APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT, Journal of Network and Computer Applications 125 (2019), 82-92.

DOI: https://doi.org/10.1016/j.jnca.2018.09.019

[9] B. Yigit, G. Gür, F. Alagöz and B. Tellenbach, Cost-aware securing of IoT systems using attack graphs, Ad Hoc Networks 86 (2019), 23-35.

DOI: https://doi.org/10.1016/j.adhoc.2018.10.024

[10] G. Zhou, H. Michalik and L. Hinsenkamp, Efficient and high-throughput implementations of AES-GCM on FPGAs, Proceedings of International Conference on Field Programmable Technology (2007), 185-192.

DOI: https://doi.org/10.1109/FPT.2007.4439248

[11] Y. Hori, A. Satoh, H. Sakane and K. Toda, Bitstream encryption and authentication using AES-GCM in dynamically reconfigurable systems, National Institute of Advanced Industrial Science and Technology (AIST), Advances in Information and Computer Security, Proceeding 53(12) (2012), 261-278.

DOI: https://doi.org/10.1007/978-3-540-89598-5_18

[12] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk and A. Rindos, SDIoT: A software defined based internet of things framework, Journal of Ambient Intelligence and Humanized Computing 6(4) (2015), 453-461.

DOI: https://doi.org/10.1007/s12652-015-0290-y

[13] D. Jayasinghe, R. Ragel, J. A. Ambrose, A. Ignjatovic and S. Parameswaran, Advanced modes in AES: Are they safe from power analysis based side channel attacks?, IEEE International Conference on Computer Design, 2014.

DOI: https://doi.org/10.1109/ICCD.2014.6974678

[14] J. Kim, Secure and efficient management architecture for the internet of things, SenSys '15: Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems (2015), 499-500.

DOI: https://doi.org/10.1145/2809695.2822522

[15] M. S. Kim, S. R. Kim, J. Kim and Y. Yoo, Design and implementation of MAC protocol for SmartGrid HAN environment, Proceedings - 11th IEEE International Conference on Computer and Information Technology (2011), 212-217.

DOI: https://doi.org/10.1109/CIT.2011.78

[16] H. Jiang, F. Shen, S. Chen, K.-C. Li and Y.-S. Jeong, A secure and scalable storage system for aggregate data in IoT, Future Generation Computer Systems 49 (2014), 133-141.

DOI: https://doi.org/10.1016/j.future.2014.11.009

[17] T. Li, C. Gao, L. Jiang, W. Pedrycz and J. Shen, Publicly verifiable privacy-preserving aggregation and its application in IoT, Journal of Network and Computer Applications 126 (2019), 39-44.

DOI: https://doi.org/10.1016/j.jnca.2018.09.018

[18] O. Mavropoulos, H. Mouratidis, A. Fish and E. Panaousis, Apparatus: A framework for security analysis in internet of things systems, Ad Hoc Networks 92 (2019); Article 101743.

DOI: https://doi.org/10.1016/j.adhoc.2018.08.013

[19] S. R. Moosavi, T. N. Gia, A. M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho and H. Tenhunen, SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Computer Science 52 (2015), 452-459.

DOI: https://doi.org/10.1016/j.procs.2015.05.013

[20] P. M. Pawar, R. H. Nielsen, N. R. Prasad, S. Ohmori and R. Prasad, Behavioural modelling of WSN MAC Layer Security Attacks: A sequential UML approach, Journal of Cyber Security and Mobility 1(1) (2012), 65-82.

[21] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE Communications Surveys and Tutorials 16(1) (2014), 414-454.

DOI: https://doi.org/10.1109/SURV.2013.042313.00197

[22] R. H. Randhawa, A. Hameed and A. N. Mian, Energy efficient cross-layer approach for object security of CoAP for IoT devices, Ad Hoc Networks 92 (2019); Article 101761.

DOI: https://doi.org/10.1016/j.adhoc.2018.09.006

[23] S. Sankaran, Lightweight security framework for IoTs using identity based cryptography, In 2016 International Conference on Advances in Computing, Communications and Informatics, Sept. 21-24, 2016, Jaipur, India (pp. 880-886).

DOI: https://doi.org/10.1109/ICACCI.2016.7732156

[24] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello and A. Coen-Porisini, A secure and quality-aware prototypical architecture for the internet of things, Information Systems 58 (2016), 43-55.

DOI: https://doi.org/10.1016/j.is.2016.02.003

[25] J. Srinivas, S. Mukhopadhyay and D. Mishra, Secure and efficient user authentication scheme for multi-gateway wireless sensor networks, Ad Hoc Networks 54 (2017), 147-169.

DOI: https://doi.org/10.1016/j.adhoc.2016.11.002

[26] A. L. V. Caraguay, A. B. Peral, L. I. B. López and L. J. G. Villalba, SDN: Evolution and opportunities in the development IoT applications, International Journal of Distributed Sensor Networks 10(5) (2014), 1-10.

https://doi.org/10.1155/2014/735142

[27] Yue Qiu and Maode Ma, A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN, IEEE Transactions on Industrial Informatics 12(6) (2016), 2074-2085.

DOI: https://doi.org/10.1109/TII.2016.2604681

■