Maytham Azhar
Ferdowsi University of Mashhad, Iran
meysam.sadeghi1985@gmail.com

Amin H. Seno
Ferdowsi University of Mashhad, Iran
hosseini@um.ac.ir

Received on: 17/10/2018
Accepted on: 27/02/2019
Published online: 25/05/2019

A Group Authentication Protocol on Multilayer Structure for Privacy-Preserving IoT Environment

Abstract- *In the Internet of Things (IoT) systems, large amounts of data are accumulated from anywhere at any time, which may attack individuals' privacy, especially when systems are utilized in medical and everyday environments. With the promise of IoT's proactive systems, the integration of smart things into standard Internet creates several security challenges, because most Internet technologies, communication protocols and sensors are not designed to support IoT. Recent research studies have shown that launching security / privacy attacks against IoT active systems, in particular, Wearable Medical Sensor (WMS) systems, may lead to catastrophic situations and life-threatening conditions. Therefore, security threats and privacy concerns in the IoT area should be actively studied. This causes us in this paper to create a privacy authentication protocol for IoT end-devices on a four-layer structure that does not have the ability to accurately identify the device of request's sender so that some attacks can be minimized. We used the Blakley Sharing scheme to design a key generation and distribution system for secure communications between edge devices and end devices and examined the security properties of the protocol for the five common attacks in the IoT. The results of the experiments show that the proposed authentication protocol by the Blakley method is more efficient with increasing number of instructions in both fog structures and in a without fog structure, which shows a higher flexibility of the Blakley method than the Schemer because of the increasing number of instructions indicating increasing the number of nodes in the network. The proposed method has better performance.*

Keywords- *Internet of Things, (IoT), Security, Privacy, Authentication, Blakley Sharing scheme.*

How to cite this article: M. Azhar, S.A. Hosseini Seno, "A Group Authentication Protocol on Multilayer Structure for Privacy-Preserving IoT Environment," Engineering and Technology Journal, Vol. 37, Part A, No. 05, pp. 172-180, 2019.

1. Introduction

The Internet of things is one of the newest technologies in the present era. But its functional domains have not yet been thoroughly analyzed. After the application of the Internet of things has become widespread, the issue of security and confidentiality has attracted an IoT of attention and has become a controversial topic in this domain [1]. Protecting the Internet of things is complex and difficult. IoT requires confidentiality, integrity, authentication and access control precisely. The current Internet is being constantly attacked due to technical, legal and human problems. IoT is a future innovation in the field of wireless technology. This event will create hundreds of new security challenges that need to be explored in detail [2].

In [3] accountability, privacy, security, performance, and removal demands, which are dynamic for the authentication framework of the Internet of things end-devices by a weaker identity, are presented. According to research findings, this is the first paper for creating the protocol of authentication in a functional scenario. The authors of this paper used the secret sharing scheme of Shamir to design a system for creating, distributing a key to secure communication among end devices and edge devices. But in Shamir secret sharing scheme [4], heavy computing costs are needed to create n share and secret retrieval. As a solution to this problem and to reduce time and more security as well, a new group authentication method has been replaced.

In other words, in this paper, we have tried to create a privacy authentication protocol for IoT end devices on a four-layer structure that at the same time is able to authenticate the sender to avoid unwanted requests. In addition, because the cloud is not reliable, it should not be aware of the critical characteristics of the applicant identity. Unauthorized user disclosure of these critical attributes may cause some attacks on the device. This structure is an efficient attitude to achieving five aims: productivity, security, privacy, dynamic removal, responsiveness. In this protocol, the Blakley sharing scheme for designing the key creating, distributing system used for secure communications among edge - devices, end -devices.

http://dx.doi.org/10.30684/etj.37.5A4
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Regarding authentication, the approach outlined in the [5], uses the common packaging mechanism, smart business security protocol of IoT application, smart security services application protocol. This combines the multiple operating systems (multi-platform) by, authentication, signature, and encryption for improving the capabilities of IoT applications by creating secure communication between various things.

In [6], the first two-way authentication security model, fully implemented for the IoT, was defined in order to the existence standards of the Internet, especially the protocol for the datagram transferring layer security (DTLS) that is placed among the transfer layer, the plan. This scheme is in order to the RSA, planned for the IPV6 in personal domain networks with low-power (6LoWPANs). An authentication protocol for IoT is provided in paper [5], which uses the XOR encryption method for anti-counterfeiting and privacy protection for dealing with the IoT limited end devices.

Beginning with the WSN texture, user authentication, and key agreement design for heterogeneous wireless sensor networks are presented in [7]. This empowers the remote user to safely negotiate a call key by a sensor node utilizing a lean key agreement protocol. In this way, this guarantees the mutual authentication among users, gateway nodes, sensor nodes, although GWN will never be encountered by this user. Because of applying this design in architectures with limited resources, it only uses simple scrambling, XOR computing, like it noted in [8].

In [9], the authors have argued that most of the KMS protocols are not appropriate for IoT. Indeed, the key tank framework has an incomplete connection problem; the mathematical framework uses the spread of knowledge for optimizing the data structures construction, but this method is not be applied in IoT because user, server nodes are commonly placed in various physical situations; KMS compounding protocol has the problem of connection and scalability/ authentication.

In [3], writers provide the new authentication protocol to the end devices of the Internet of things by poorer individuality that is able to reach the optimal trade-off among the security, privacy. The protocol incorporates the accepted small set sign structure, Shamir's secret sharing scheme as the forcible attitude for reaching five aims: privacy protection, security, proficiency, responsibility, active omission.

The goal in this paper is to design a system for creating and distributing key for secure communications between edge devices and end devices and reducing time utilization using the Blackmail Sharing Schema in the authentication protocol.

The rest of the paper is organized as follows: In Section 2, Comparison of Shamir's and Blakley's Schemes is described. Section 3 is described as the proposed approach. Section 4 is the Security analysis of the proposed method. The evaluation of the proposed approach is presented in Section 5. Finally, Section 6 concludes the paper.

2. Comparison of Shamir's and Blakley's Schemes

The sole difference among the Blakley's, Shamir's schemes is a procedure for selecting S hyperplanes. Shamir offered polynomial attitude for producing matrix. It intends vector of the coefficient to each hyperplane must be in shape of $(1, x, x^2, x^3, ..., x^{S-1})$. Such scheme benefit is that just x demands worth to be stored to the storage-forcible answer. On the other hand, Blakley's scheme produces a vector of coefficient casually.

Main secret sharing schemes were utilized for the gap, cover secret data. So, the execution did not take into account, flowing case amounts were utilized. Although, as secret sharing's aim alterations, Galois field $GF(2^n)$ is utilized on the regular base for increasing execution, prevent accuracy issue caused by flowing case amounts. Below these situations, Shamir's secret sharing scheme is yet broadly utilized; however, this is no longer secure below GF. Shamir's, Blakley's schemes comparisons are given under according to flexibility, security, a complication of storage, a complication of time. Whole below argument is GF-based (2^8).

1) **Flexibility**: firstly, compared to the reasonable amount ground, Galois Fields (2^8) is the much more susceptible for cruel compulsion rush. Below the reasonable amount ground, Shamir's scheme can give the unlimited various coefficient vectors amount; however, below the Galois Fields (2^8), just there are 256 selections. It means this is not possible for the client to gap his secret in more than 256 parts. On the other hand, Blakley's scheme has around 2^{8T} selections to its coefficient vectors that are large enough to the share amount S while T is not too short.

2) **Security**: however, the secret sharing behaves like the "un-keyed" attitude, this indeed connected "key" matrix that is an aforementioned coefficient matrix, to "cipher-text," Hence, the

coefficient matrix must be produced at the security procedure. Distinctly, Shamir's 256 feasible to the coefficient vector is not security enough, can be assumed easily.
Combined by not enough shares achieved with a competitor, not secure coefficient matrix secret would guide the more rapid secret detection.
3) **Time Complexity**: Matrix multiplication is the main work of secret sharing. However, these two schemes utilize various procedures for produce coefficient matrix; later works are mostly alike. So, their time complexity is in the same class.
4) **Space Complexity**: main secret sharing schemes need various coefficient matrices along the hybrid progressing blocks for obtaining the severely security high-level. Although, this, not suitable storage scheme should be left to the low-cost, optimal execution. Now, the coefficient matrix should not differ between the various blocks. Although, such simplification omits Shamir's scheme space complexity benefit. As the size of information raises, more and more blocks share similar coefficient matrix, create especial cost partially. All over, Blakley's scheme is more adaptable, scalable, security to the huge information progressing.

3. Proposed Method

In the following section, at first, describe the proposed method, and then define the proposed authentication protocol. Proposed method contains two parts:

The first part is changing the structure of the base paper, i.e. [3] and the second part is using the sharing scheme of Blakley to design a key creation and distribution system for secure communications between edge devices and end devices in the authentication protocols of the base paper protocol.

I. Changing the layer structure

In order for the proposed challenges, the proposed strategy is to change the structure of paper [3] and use the fog in the structure. The method presented in paper [3] will be applied to the proposed layer structure (Figure 1).

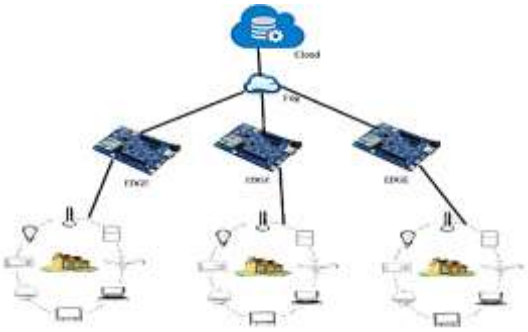

Figure 1: Layer structure

Part 1: First layer is things layer which utilized to control the physical world and collect data. The layer of things in Figure 2 is a smart hospital system in which there are some end devices like cameras, barometer sensors, body temperature control and ECG sensors.

Figure 2: Layer of things in Smart Hospital

Most of the end devices in a layer of things have resource constraints and have ram memory with 64 bytes, 2 kilobytes of memory space. So, many of the common security mechanisms, like algorithms based on asymmetric key encryption, are not appropriate because high resources require energy and computing power. In addition, also the issues of privacy are essential to the end devices in systems of IoT, in order to that the end-devices gather much private information, particularly while they are located in medical/daily living surroundings. Usually, higher privacy requests need a weaker identity because strong identity threatens individual privacy. However, having a strong identity is important to protect the security, particularly for authentication. So, choosing the right compromise between security and privacy is difficult.
Part 2: Second layer includes edge devices that connect the layers of end devices to the fog layer. Edge devices like routers, smartphones, and home servers help join the end devices to the cloud.
Part 3: this layer contains fog element that is an interface between the edge layer and the cloud layer. This layer required to take some vital real-time decisions and send the answer to the end devices. Because we have n group of the set of tools, that each set has a group key called K_{ei}, which is $(1< i < n)$. Also, this layer has the tasks assigned to the control center, and since it has the high processing power, it can perform these complicated calculations in the shortest time.
Part 4: in this layer, there is cloud computing, which due to its high processing and storage capability, will be used for large storage and heavy processing, and tasks with less processing

and storage requirements which require a real-time response will be responsible to fog.

II. Proposed authentication

The second part of the proposed method is to implement the Blakley sharing scheme to design a system for key creating and distributing for secure communication between end devices and authentication protocol devices of the base paper protocol.

The authentication protocol in [3] has six phases, and in the proposed method used the Blakley scheme for key distribution in the phase of registration, and the remaining phases of the protocol are similar to that paper. For details, readers are references to it.

1) Initialization Phase

Fog device generates a Group Public Key (gpk) for a specific edge device:

a. Fog selects a generator $g_2 \in G_2$ and computes $g_1=\psi(g_2)$.

b. Then, randomly chooses $\tau \in G_1$ and $c_1, c_2 \in Z_p^*$ and finds u, $v \in G_1$ such that: $u^{c_1} = v^{c_2}=\tau$.

c. In the following, Fog selects $\lambda \in Z_p^*$and sets $w=g_2^{\lambda}$.

And Fog performs these tasks:

a) Publishes gpk:

○ gpk = $(g_1, g_2, \tau, u, v, w)$ (1)

b) Sends λ to that edge device securely (e.g., through issuing a tamper-proof smart card or secure transmission protocol such as a wired transport layer security protocol)

c) Keeps Managed Private Key (mpk) for that edge device:

○ mpk = (c_1 , c_2) (2)

Edge device publishes $N = q_1, q_2$ where q_1 and q_2 are large cryptographic primes.

2) Registration phase

1. Each device forms the edge of a group. Each end device that wants to have a stable relationship with a specific edge device must register. The registration process is as follows:

2. The edge device initially selects a prime number p randomly, then chooses a group key K $\in Z_N$ and makes the point $Q = (x_0, y_0, z_0)$ based on it:

- x_0 is the same key as K.
- y_0 and z_0 are also two random numbers.

The edge device forms an equation of plane called c_i, where Q is located. This equation will be:

$c_i = z_0 - a_i x_0 - b_i y_0$ (3)

The edges of the device for each sensor i intended to be registered by placing a unique (a_i, b_i), forms a plane equation and provides a sensor in a secure way. The important point is that in all the equations of the designed planes, the Q point is common.

Then the edge device two of the equation of the other plane (in general, p-1 equation), based on Q, is generated and it broadcast in the environment and all the sensors receive it.

Each sensor, by receiving two equations of another plane and the X plane that it has, it can get the Q point, since Q is the point of intersection of these planes. Because in order to obtain a point in the 3D coordinate (plane), there needs to be a cross of only three equations of the plane. But in the n-dimensional general case, it is required that each sensor achieves (n-1) equation of n variable. In addition to its equation, it can extract the desired point. In the final step, the x_0 value at this point will be the value of the group key. Critical Instruction-Issuing, Authentication, Verification and Execution Phases are similar to [3].

In Tracing Phase Edge-device do the following:

1.It selects a p the prime number and allows x_0 to be secret. Selects the public key for the new group.

2.y_0 and z_0 randomly choose mod with the prime number, and $Q = (x_0, y_0, z_0)$ is a point in the three-dimensional space, and on the mod, the p is the prime number.

3.To each End, the device is given the equation of a plane to cross the Q point.

a_i and b_i on mod the prime number of p for each end device is selected and then calculated as follows:

$c_i \equiv z_0 - ai\ x_0 - bi\ y_0 \pmod p$ (4)

The plane is as follows

$z \equiv a_i x + b_i y + c_i \pmod p$ (5)

This is done for each End device.

The three pages will intersect at a point that should be Q. The two planes intersect at one line, so usually, there is no information about secret x_0, which is the corresponding key. The remaining end devices can use the three equations and the matrix of the equation to obtain the key. That is, the gpk can be retrieved. After that, the i-th End device cannot compute x_0. It also cannot get CI from other end devices.

4. Simulation Platform

The implementation of the proposed method is done with IFogSim [10]. This set of tools called IFogSim is an environment that is a development of the simulation environment CloudSim, which

allows processing in the side points of the network through a tool called fog devices.
In IFogsim simulation, to implement the scenarios, the network structure must first be designed in a coherent form, then considered scenarios designed in the form of an application, that each application containing a set of modules and communication edges between them. Each application is designed as a non-directional graph in which circles represent modules and lines representing the edges. After designing the application, the modules must be mapped to tools; it means that each module will run on which node.

I. Topologies

In order to implement the proposed algorithm and examine differences, two topologies for the network are considered. A matching with respect to the fog element on the edge of the network and the other without fog.

1) Topology without fog element

First topology: in this matching, a processing element called cloud is used (Figure 3). This element is placed in zero-level in matching because in the IFogsim simulator, there is a hierarchical structure for devices with different processing power. Also, in the first level, there are gateways that these elements are connected to the sensors and simulants of its group health system at the leaf level (second level).

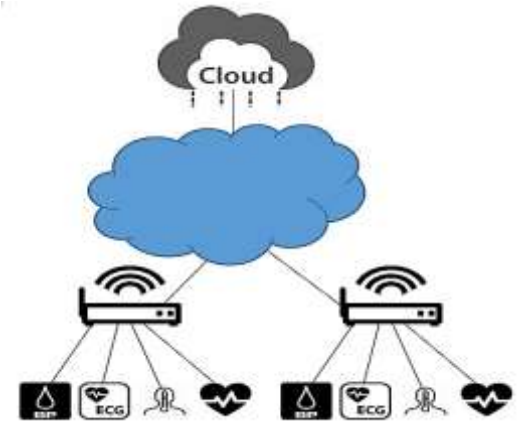

Figure 3: Topology with a cloud element

2) Topology with a cloud element

Second topology: it is similar to the first one, with the difference that the fog element is added between the cloud and the gateways at the edge of the network (Figure 4). In this alignment, a processing element called cloud is used, the element is aligned at the zero levels, the fog element is placed at the first level, which performs real-time and average power processing, and in the case of referring needs to the cloud. Also, in the second level, there are gateways that these elements are connected to the sensors and simulants of its group health system at the leaf level (third level).

Figure 4: Topology with fog element

II. Scenarios and related applications

1) Registration phase

For this phase, scenarios are considered that show the difference between the use of two Shamir and Blakley schemes for time complexity, security, and flexibility criteria. According to that, cloud and fog are not involved in this phase; scenarios are only considered by considering the differences in the type of used scheme. These scenarios are as below:

A. First scenario: using of Shamir secret sharing scheme

In this scenario, Shamir method is used to share the group key that has been produced at the gateway. Shamir scheme [11] is based on the Lagrange polynomial.
A patchwork is a confidential sharing scheme that divides the secret key vendor to each k partner or more than n persons can reconstruct the secret key, but if less than k partners share their shares, they are not able to reconstruct the secret key. To do this, the gateway divides the group key into n parts and broadcasts them, on the whole, the network. Then each sensor, only having the t part of this n part can extract the group key. In the used method, the considered values for variables n and t are respectively 5 and 3. That means each sensor with 3 parts of the total of 5 parts can get the group key.

B. Second scenario: using of Blakley secret sharing scheme

In this scenario, Blakley method was used to share the group key produced by the gateway. Blakley [12] is based on the visual geometry.
Blakley secret sharing scheme has the various attitude that is hyperplane geometry-based: for implementing the (t, n) threshold design, every n client is given the hyperplane equation in at dimensional storage over a limited ground like which every hyperplane goes via the sure case. The hyperplanes intersection case is secret. While t clients gathered, they are able to solve the equations system for finding the secret.
The described scenarios are four models that are considered in each model of all phases such as changing the structure of the base paper (presence or absence of fog), initialization and registration (by Shamir or Blakley), critical instruction phases, and authentication and tracking (by designed application) in Figure (5).

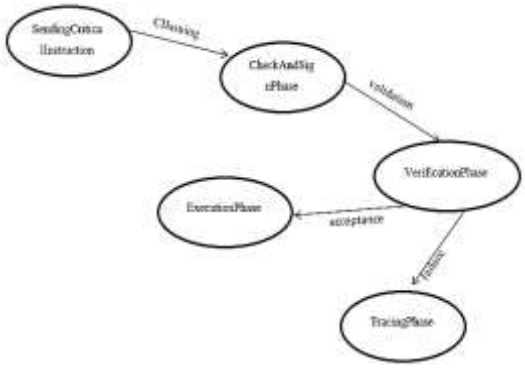

Figure 5: Modules designed in the application for scenarios in the authentication phase

2) Authentication phase
Four scenarios are considered in this section, because of the existence and absence of fog, as well as the use of secret sharing method re effective in evaluating the criteria.
o First scenario: in this case, the Shamir method is used in alignment which the fog element is used in it.
o Second scenario: in this case, the Shamir method is used in alignment which the fog element is not used in it.
o Third scenario: in this case, the Blakley method is used in alignment which the fog element is used in it.
o Forth scenario: in this case, the Blackley method is used in alignment which the fog element is not used in it.

A. Application related to the authentication phase scenarios

The designed modules in the application are shown in Figure (5), which are described below, and the mapping of each module to each node is shown in Table 1 for a fog mode and in Table 2 for a fog-without mode.

Table 1: Module mapping table to the node for fog-without topology

Module name	Device
Sending Critical Instruction	sensor
Check And Sign Phase	gateway
Verification Phase	cloud
Execution Phase	sensor
Tracing Phase	sensor

Table 2: Module mapping table to the node for fog topology

Module name	Device
Sending Critical Instruction	sensor
Check and sign Phase	gateway
Verification Phase	fog
Execution Phase	sensor
Tracing Phase	sensor

Sending Critical instruction module that is designed to provide a critical instruction will be applied in sensor beams.
Check and Sign Phase module which is implemented on the gateway, checks whether this critical instruction is sent from its own supported sensors and if the answer will be positive, it will sign it with its private key and send it to the next element (whether fog or cloud_ different based on the alignment).
Verification Phase module place on the cloud or fog, depending on the alignment and in this phase examines that whether the critical instruction has been encrypted by one of its gateways or not, this work is checked by the private key of the gateway.
Execution Phase module that is done on the actuators has the task of executing the critical instruction which has been approved.
Tracing Phase module will be done on the sensors and will be responsible for tracking resources related to the wrong critical instructions.

III. Evaluation of results

To evaluate the proposed strategy, the results are compared with the Wang method in [3]. The results we obtained include three charts. In Figure (6), the chart is about time cost comparison.

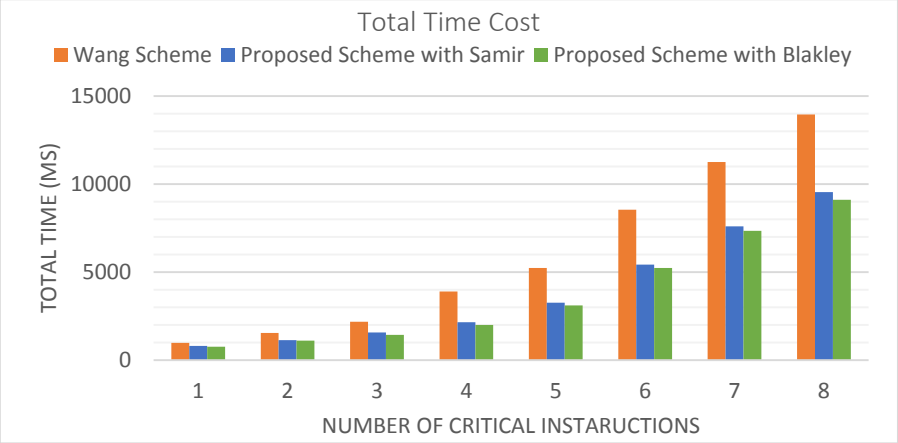

Figure 6: Comparison of the cost of the proposed scheme with the Wang scheme

As it can be seen, in the scenario where the proposed method was implemented using the Blakley scheme, it is better than Wang scheme in order to time and also better than the proposed scheme implemented with Shamir. For calculation of cost, formula (6) has been used:

$$Cost = CC + (CT\text{-}LUUT)*RPM*LU*TM \qquad (6)$$

That, CC is the current cost, CC shows the current time, LUUT is the last update time that has been used, RPM represents the rate in each MIPS, LU is the last usage, and TM is the total cost (memory allocation, bandwidth, processor).

At the beginning of the simulation, all costs are set and the initial cost is zero. After the simulation is performed, the updated values and the total simulation cost is derived based on the formula. The current system time value decreases from the amount of update time, then this amount is multiplied by the speed of receiving every one million instructions per second at any rate, and the results is added to the current simulator cost. This value is based on the non-negative number.
In Figures 7 and 8, related charts are for energy consumption comparison and usage of the network; energy consumption means the total energy used by the system.

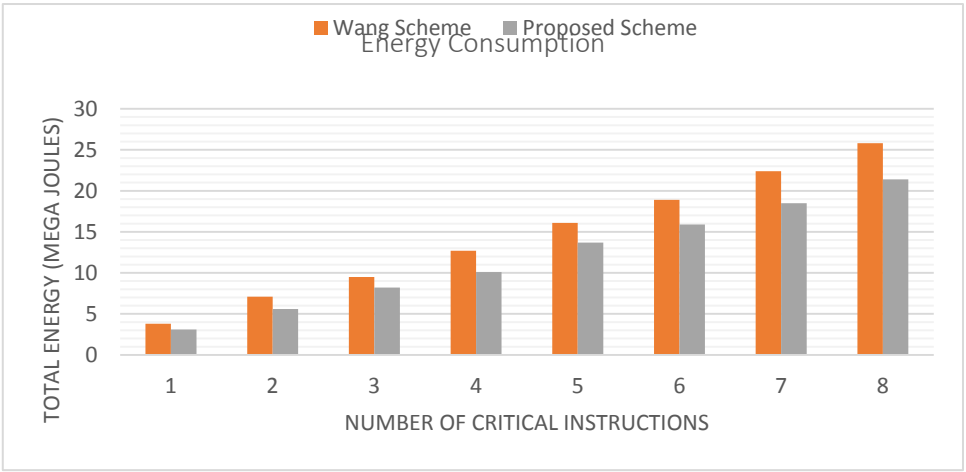

Figure 7: Comparison of the energy consumption the proposed scheme with the Wang scheme

This energy is used by each part of the network such as fog, sensor, and gateway and so on.
This using energy can be calculated by using formula (7).

$$Energy = CEC + (CT\text{-}LUUT)*HLU \qquad (7)$$

CEC is the current energy consumption. CT shows the current time. Also, LUUT shows the last updated time, HLU shows the last usage of the guest. The used energy is zero from the beginning of the simulation. After the performance of simulation for getting the used energy, the time of simulation, which is the difference between the current system time and the latest upgrade time, is multiplied at the last use of the host, and eventually added to the amount of current energy consumption.

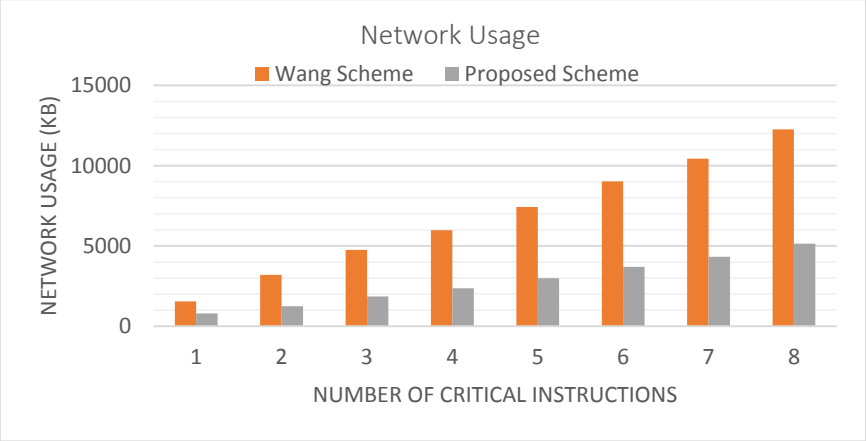

Figure 8 Comparison of the usage of a network of the proposed scheme with the Wang scheme

The following formula has been used to calculate the usage of the network.

$$Networkusage=(TL*TS)/MST \quad (8)$$

In formula (8), the values of TL and TS represent the total length and total size of the tuple. The maximum simulation time is shown with MST.

In this evaluation, we also compared the proposed method used in the Blakley scheme with the Wang scheme used by Shamir that again the proposed method with Blakley has been working better with the increasing number of instructions in both charts, which reflects the greater flexibility of Blakley method than Shamir method. Because with the increase in the number of instructions indicating an increase in the number of nodes in the network, the proposed method is performing better than Wang, and better results have been obtained. Also in the proposed method, for the routine, there is no need to use the cloud, so the amount of cloud utilization has reached to zero, but it can be used for the periodic review and knowledge generation of long-term information from the cloud in the proposed method.

5. Security analysis

An authentication protocol is planned to the end-devices by the poor identity in systems of Internet of things. In this section, assay protocol security features in the context of five normal attacks in systems of Internet of things.

I. Against Attacks to Edge-devices

Posing the edge-device for sending authenticated critical instruction, the attacker out of set must get temporary private key to. Although temporary private key to is produced with secret worth λ, that is saved in edge devices tamper-proof section. So, the outside attacker is not able to counterfeit the signature of an invalid set for fooling control center.

II. Attacks of Against Man in the Middle

A man in the middle attacker purposed for imitating proper person for fooling one side with utilizing data of another part. In edge device and end device connections, the divided symmetric key k is utilized for encrypting critical instruction CI, also long-term (LS) secret of the end device. This presented defense against attacks of man in the middle, while the attacker is not able to create the right zero-text with no k. In edge-device, also in control center connections, the set public key-based signature is utilized for authenticating the group's identity, also crucial instruction. This presented defense against attacks of man in the middle, while the attacker is not able to pension off the control center to adapt the counterfeited group public key.

III. Against Replay Attacks

When the attacker gets data connected among 2 sides, then he cut the connection and replays data malignity, that is known as a replay attack. In protocol utilized timestamp χ for avoiding connection replay attack among edge device and end device. When an attacker wants to reform χin end-devices zero-text to replay attack, so he should obtain symmetric encryption key k. Although, this is mostly not possible for assuming symmetric encryption key when secret sharing of Shamir is data-theoretically security.

IV. Against Attacks from Malignity End devices

When crucial instruction of malignity end device causes the severe results, then the whole following education of this must be constrained. This should be said; the malignity end-device must be interdicted of the group. In the protocol of proposed, map relationships among end-device

http://dx.doi.org/10.30684/etj.37.5A4
2412-0758/University of Technology-Iraq, Baghdad, Iraq

long-term secret keys and temporary private keys are saved in edge-device. However, the center of control is able to calculate temporary private key by utilizing operated private key; just an edge device is able to find the long-term secret key of the end device. Just edge-device is able to upgrade group key for blocking this end device.

V. Attacks on end devices

To impersonate authorized end device in a group to issue an incorrect CI, an external attacker must receive the current key of the k group. Nonetheless, since secret sharing of Blakley is a secure theory, for example, suppose two plane A and B are given $z = 2x + 3y + 13$ and $z = 5x + 3y + 1$ pages. A and B can reconstruct the secret without a third party ($2x + 3y + 13 = 5x + 3y + 1 \Rightarrow 3x = 12 \Rightarrow x_0 = 4$). But the other device cannot (y_0, z_0). X_0 cannot be restored. Therefore, an external attacker cannot reconstruct X_0. On the other hand, the internal attacker, which is a licensed end device, has no chance of obtaining long-term secrets x_0 of the other device.

6. Conclusion

During the authentication process, users may face serious threats related to their privacy, when they want to prove their identity. In fact, through a variety of authentication sessions, where a user is involved, a user can be identified or tracked. Therefore, maintaining anonymity and lack of location routing, are the important security requirements that should be considered in designing an authentication protocol for the internet of things environment. In this paper have attempted to make a privacy authentication protocol for the IoT end devices on a four-layer structure. In this work utilized sharing scheme of Blakley for designing the key creating, distributing system for secure communications among edge devices and end devices. Blakley scheme in terms of security and flexibility is better than Shamir scheme. Regarding the results obtained from the implementation of the proposed method, using the Blakley scheme, in terms of time cost, energy consumption and network utilization is much better than Wang scheme which uses the Shamir scheme, because in proposed method do not use the cloud, the cost is zero. Security analysis shows the amount of protocol power against attacks. Experimental results and performance analysis show that the proposed method has a better performance.

Reference

[1]. F. Xia, L.T. Yang, L. Wang and A. Vinel, "Internet of things," International Journal of Communication Systems Vol. 25, No. 9, pp. 1101-1102, 2012.

[2]. H. Kopetz, "Internet of things," In Real-time systems, PP. 307-323, 2011.

[3]. Z. Wang, "A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity," Future Generation Computer Systems, 2017.

[4]. J. Kurihara, S. Kiyomoto, K. Fukushima and T. Tanaka, "A new (k, n)-threshold secret sharing scheme and its extension," In International Conference on Information Security, PP. 455-470, 2008.

[5]. YL. Zhao, "Research on data security technology in internet of things," In Applied Mechanics and Materials, Vol. 433, N0. 1, pp.1752-1755, 2013.

[6]. T. Kothmayr, C. Schmitt, W. Hu, M. Brünig and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks Vol.11, N0. 8, pp.2710-2723, 2013.

[7]. M. Turkanović, B. Brumen and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," Ad Hoc Networks Vol.20, pp.96-112, 2014

[8]. JY. Lee, WC. Lin and YH. Huang, "A lightweight authentication protocol for internet of things," In Next-Generation Electronics (ISNE), 2014 International Symposium on, pp.1-2, 2014.

[9]. R. Roman, C. Alcaraz, J. Lopez and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," Computers & Electrical Engineering Vol.37, No. 2, pp.147-159, 2011.

[10]. H. Gupta, A. Vahid Dastjerdi, SK. Ghosh and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," Software: Practice and Experience Vol.47, No. 9, pp. 1275-1296, 2017.

[11]. A. Shamir, "How to share a secret," Communications of the ACM Vol. 22, No. 11, pp. 612-613, 1979.

[12]. GR. Blakley, "Safeguarding cryptographic keys," In Proceedings of the national computer conference, Vol. 48, pp. 313-317, 1979.