ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

USER AUTHENTICATION IN INTERNET OF THINGS: A SURVEY

S. Jagadeesh, Riaz Shaik, Gandharba Swain[*], K. Rahul
Department of Computer Science and Engineering, K L University, Vaddeswaram-522502, Guntur, India.
Email: siripurapujagadeesh2@gmail.com

Received on: 18.10.2016 *Accepted on: 11.11.2016*

Abstract

With the development of IoT, the number of devices connected in it becomes very large in number. The existing authentication models are becoming vulnerable to many new attacks. A number of security principles should be provided for attaining the secured IoT implementation. IoT development in the coming future depends upon how we deal with the security problems and how we solve them. User authentication plays a crucial role, since the data or information should not be taken by faulty hands. Many researchers have addressed many security concerns regarding user authentication by providing related counter measures. This paper presents an overview of various proposed counter measures for user authentication and the advanced ways for providing security in IoT.

1. Introduction

IoT is a recent innovation which is pulling numerous fields for interconnection of things. Thing can be sensor nodes, Radio Frequency Identifiers (RFID tags), actuators, and many others. These things can associate with each other. All those would be interconnected in Internet. In the early years WSNs began as straight forward examination ventures financed by the military (Defense Advanced Research Projects Agency) [22]. A small view of IoT is as shown in Fig.1. Authentication is nothing but checking whether a user is legitimate or not by ensuring the trust worthiness [2]. For maintaining faith in IoT message transfers and by confirming the aims for information protection, appropriate measures must be implemented for user validation and server validation [2]. The whole idea of IoT stand firm because of the Wireless Sensor Networks (WSNs). These systems assume a basic part and are being utilized as a part of IoT. In olden days there used to be just homogeneous WSNs, with equivalent sensor nodes (containing sensors with same computational capacities and so on) as of the advancements accessible at that time. But with the development of technologies these sensor networks along with infrastructure are also revolutionized with new means of usage and working procedures. Homogeneous WSNs are sup-planted with heterogeneous WSNs. These heterogeneous WSNs can work with unequal sensor nodes and sensors with more computational power. These heterogeneous WSNs comprises of various, minimal effort sensor nodes which are having low computational capacities and a sink node with more computational abilities, called as Gate Way Nodes (GWN) [21]. These GWNs are more secured and have more computational capacities contrasted with the ordinary sensor nodes. The central station in WSN handles each and every sensor node by using CPU and storage allocated to it [1].

Since, these nodes are having more computational capacities than that of the regular sensors nodes, these are utilized for validating the client and with the end goal of correspondence of clients with the sensor or terminal nodes. In the earlier days the sensor or terminal nodes are not used to straightforwardly speak with clients or themselves, the base stations used as middle person between the client and the node. These base stations are also used for collecting and checking the information from each and every terminal node, also for sending commands from end user to terminal nodes and providing authentication schemes, etc., [3]. But with the progression of the infrastructure from infrastructure based networks to ad hoc networks, now they are able to interact with any device, which are having internet connectivity. A terminal node has less computational abilities, yet the client (host) will have higher computational capacities. Along these lines, it is not exactly hard for attacker with its computational abilities to assault or trade off the security of the system. In this way, the clients who wants to access any sensor in a network, must be approved, if client is legitimate, then he can send summons to the nodes or recover data from the nodes.

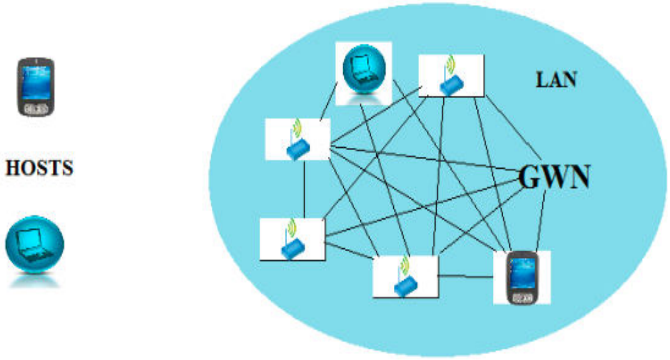

Fig.1. The IoT overall structure.

Sensors recognize the changes in the environment around it and change the information to computerized structure (binary form) and they will forward it to the concerned host or other sensor or passage node. Utilizing analog to digital converter the data or information is changed over and went on to the WSN. But with the introduction of new types of devices into the IoT, new security problems are arising, which are needed to be addressed. Also the existing security schemes are becoming more vulnerable. Because of this the existing security is under attack. That is why there is a need for new authentication security schemes. There are basically five authentications models for WSNs. They are as shown in Figs.2-6.

In Model-1, shown in Fig.2, the end user contacts the gate way node first and requests required data, then the gate way node fetches the data from the terminal nodes and forwards it to the end user. Here the end user can also be a terminal node. Many researchers believed that this model is the best secure model than compared to other models, because the end user will not directly interact with the sensor node. Everything that passes to both parties will be validated by the GWN in the middle.

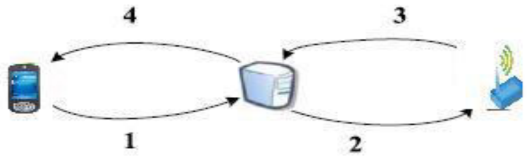

Fig. 2 Model-1

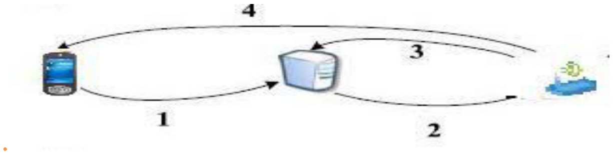

Fig.3 Model-2

In Model-2, shown in Fig.3, the end user firstly contacts the gate way node for the required information or data, then the gate way node validates that users details and sends the same details to its corresponding sensor node. If details are legitimate, then that sensor node will forward the data to the end user and also a reply to the gate way node. Here the end user can also be another sensor node.

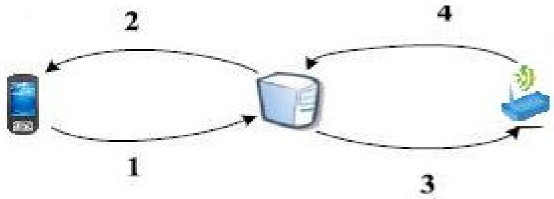

Fig 4 Model-3

In Model-3, shown in Fig.4, the end user communicates with the gate way node. There is no direct interaction between the terminal node and the end user. The gate way node only fetches the information and forwards the data from user to terminal node and terminal nodes to end user.

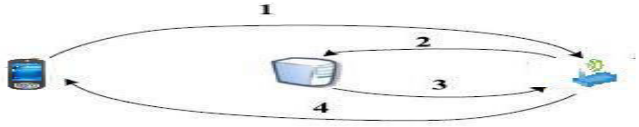

Fig.5 Model-4

In Model-4, shown in Fig.5, the end user directly contacts with sensor node, from which it requires the data or information. Then the sensor node forwards the user data to the gate way node, to authenticate the user. After successful authentication, the sensor node forwards the data to end user. This scheme is for direct interaction of client and terminal nodes, without using gate way nodes. Here also the end users can be sensor nodes. This scheme was used in [3].

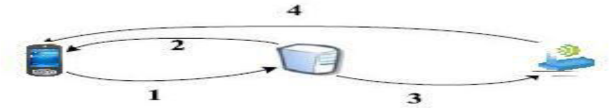

Fig.6 Model-5

In Model-5, shown in Fig.6, the user contacts the gate way node for required information, then the gate way node authenticates the user and gives a reply to the user, also transfers the message, consisting of user data to its concerned terminal node. Then that terminal node forwards the data to that user.

2. Security of IOT

This module discusses about the security issues in IoT. The security issues plays an important role in IoT. There are mainly three layers where we need to provide security, (i) Application layer, (ii) Network layer, and (iii) Sensor layer as shown in Fig.7. As per Wen [5], the following three points are notable. Initially, terminal nodes can interact with all other nodes, by connecting to internet. Secondly the identification of any device in IoT is automatic. The third is intelligent operating, these would portray toward automation, self-feedback, intelligence maintenance etc. The security in IoT implies more on safe data collection from the sensors, secured transmission over network and secured authentication.

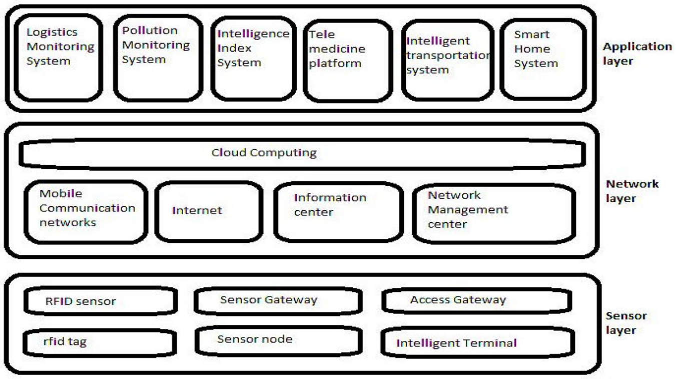

Fig.7 Security framework of IOT proposed by Wen [5].

The sensor layer deals with an important role in IoT, in which the sensors are sensed. The Network layer deals with the transmission of data from node to node or user (in same network or different network). Since, this sensor layer plays an important role in the IoT, security need to be provided at the sensor layer. Some common issues at the sensor layer are, wireless link signals may be weak, node exposal, limited computational and storage capacities.

Generally terminal nodes will interact among themselves and also the end user using WSNs [23]. And the regular sensor nodes are having low computational capacities, so they may not be having enough capacity to handle it. At the same time, other signals also may result the wireless signals. Some of the sensor nodes that we use in IoT may be available straight outside world. For example, RFID tags are not only available to even attackers. By using that the attacker may gain possibility to attack.

The IoT sensors do not have much computational capacities and storage capacities, because of the low power consumption. There are some security technologies, provided by different means of operations. Some of them are discussed here. Those are encryption mechanism, access control and authentication schemes. The encryption mechanism is required for the purpose of security. Even if the attacker captures the cipher text, attacker cannot be able to gain the plain text. So, the data to be transferred is encrypted before transmission and then forwarded it in to the network. And the encryption mechanism must be very light weighed because of resource-constraint nature of the sensor nodes. The access control scheme means the authorized users or nodes are only given access. The authentication schemes deals with the security provision. The user must be authenticated before given access to the data.

3. Problem Statement

IoT deals with a lot of confidential data and security related data. Any data that a user can know and can control, that cannot be leaked into faulty hands. User authentication plays a vital role in this scenario because of that sensitive data IoT is dealing with. So, a secured two-way validation among terminal nodes, users and the GWNs must be done. Various researchers proposed a number of authentication schemes, for user authentication. But, since new devices are entering into IoT, new security challenges are arising which should be addressed and resolved. The existing schemes are not fully providing authentication. This paves the way for new authentication schemes, which provides more security features. Users need to be authenticated, because any attacker claims to be user and gain access to the data. The nodes need to be authorized because any attacker may dynamically add a sensor node, claiming to be legitimate. So, to overcome that problem, senor nodes are also to be authorized. This paper also discusses various existing authentication schemes, the vulnerabilities and corresponding counter measures.

4. Existing Authentication Models

Das [18] planned two-factor user validation technique in WSNs. It comprises of 2 phases, (i) registration phase, and (ii) authentication phase. The authentication phase itself includes two other stages namely, login stage and verification stage. But Nyang & Lee [19] proved that this technique is weak in providing security for some attacks like offline password guessing attack, terminal node compromising attack, and is not protecting the messages that are received at clients from the terminal nodes. Also Nyang & Lee planned their improved two-factor validation protocol for WSNs. Khan & Alghathbar [20] shown that, Das's technique was weak against some more attacks also, than that of the Nyang & Lee. The practical explanation for more attacks like password updating by any user is not possible, also not providing mutual validation among the gateway node and terminal nodes, and is becoming unguarded for gateway bypass attack and insider attacks [20]. In this paper they did not provide an improvement for that scheme. But they provided the patches using their own algorithms, for the attacks they did find. They have provided the comparison table for the security analysis between those three versions. They have proved that their scheme was more secure and robust.

Xu et al. [6] proposed a paper that mainly considered about the client validation that confirms that no system resources are being accessed by illegitimate clients, in a faulty way. This paper also proves that the schemes proposed by Lee et al. [7] and Lee & Chiu [8] are having vulnerabilities. Lee et al. technique was becoming unguarded for offline password guessing attack [6]. Then they improved the scheme along with countermeasures for the above attack. In Lee & Chiu scheme, as shown in Fig.8, there are three stages such as, registration phase, login phase and authentication phase.

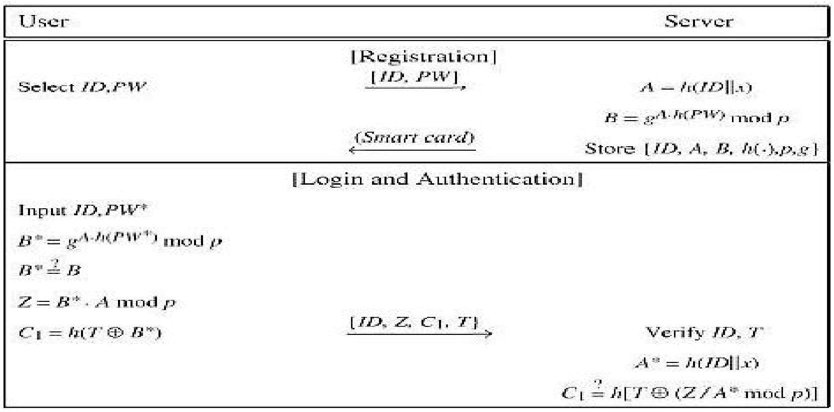
User
Server
[Registration]
Select ID, PW
$[ID, PW]$
$A - h(ID||x)$
$B = g^{A \cdot h(PW)} \bmod p$
$(Smart\ card)$
Store $\{ID, A, B, h(\cdot), p, g\}$
[Login and Authentication]
Input ID, PW^*
$B^* = g^{A \cdot h(PW^*)} \bmod p$
$B^* \overset{?}{=} B$
$Z = B^* \cdot A \bmod p$
$C_1 = h(T \oplus B^*)$
$\{ID, Z, C_1, T\}$
Verify ID, T
$A^* = h(ID||x)$
$C_1 \overset{?}{=} h[T \oplus (Z / A^* \bmod p)]$

Fig.8 Lee-chiu authentication scheme.

But, Xu et al. [6] proved that Lee & Chiu's technique was becoming unguarded for imitation attack, using some stolen smart card and also not supporting mutual validation. In Lee et al technique, shown in Fig.9, there are three stages such as, registration stage, login stage and authentication stage. But, Xu et al. proved that Lee et al. technique was becoming unguarded for offline password guessing attack. So Xu et al. [6] proposed an improved scheme, in which the errors are cleared and the performance was improved. This is shown in Fig.9. This paper talks about the enhanced improved validation technique using smart cards and Diffie and Helman asymmetric user authentication schemes [10], which provided mutual authentication. Then later Xu et al. [6] proposed an improved version and also removed the above raised errors. That scheme also consists of the same three stages as those of above. This is shown in Fig.10. But the problem with this scheme was its memory overhead [3], since every node needed to save all people in public keys of different nodes and clients furthermore defenseless against inside and mimic assaults. So, Song [11] proposed an advanced validation method using smart cards, by removing the above raised flaws.

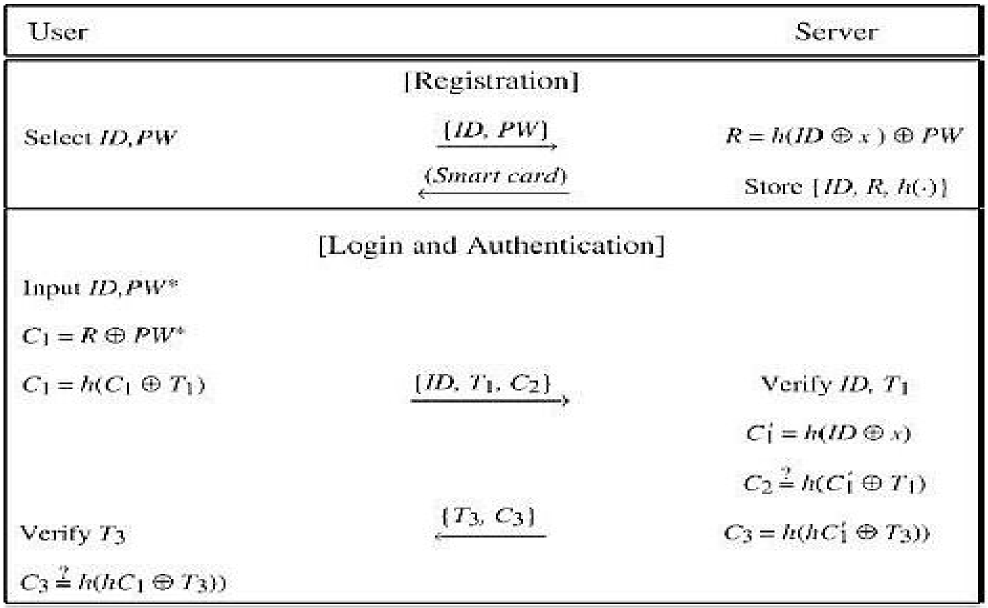
User
Server
[Registration]
Select ID, PW
$\{ID, PW\}$
$R = h(ID \oplus x) \oplus PW$
$(Smart\ card)$
Store $\{ID, R, h(\cdot)\}$
[Login and Authentication]
Input ID, PW^*
$C_1 = R \oplus PW^*$
$C_1 = h(C_1 \oplus T_1)$
$\{ID, T_1, C_2\}$
Verify ID, T_1
$C_1' = h(ID \oplus x)$
$C_2 \overset{?}{=} h(C_1' \oplus T_1)$
$\{T_3, C_3\}$
Verify T_3
$C_3 = h(hC_1' \oplus T_3))$
$C_3 \overset{?}{=} h(hC_1 \oplus T_3))$

Fig.9 Lee–Kim–Yoo authentication scheme.

Zhao et. al [4] proposed a two-way validation mechanism between platform and terminal nodes by making use of Elliptic Curve Cryptography(ECC), Secure Hash Algorithm(SHA), and feature extraction. This methodology makes use of Elliptic Curve Digital Signature Algorithm and SHA1 to calculate message digest in personal computer. SHA1 is more opted, because of its low cost of time compared to that of ECC [4]. The secure hashing algorithm converts the data into unreadable and not understandable form, but as per [9] the SHA and MD5 are no longer secured i.e. they have vulnerabilities. So, hashing is combined to feature extraction. Since feature extraction is irreversible, is used to confirm protection and this one is more suitable in IoT because it is light weight technique. The feature extraction was mixed with hashing, in order to prevent collision assaults [4]. The plan concentrates on authentication process when a specific terminal node is attempting to send information to platform and not doing the inverse. Although the scheme will improve the security, apart from theory there is no practical proof provided for it [4]. But as an advantage it reduces the size of data to be transmitted. This proposed mutual authentication scheme consists of three stages, (i) initialization stage, (ii) CA verification stage, and (iii) mutual authentication stage. In the period of initialization, some credentials are pre-circulated to both the terminal nodes and platform.

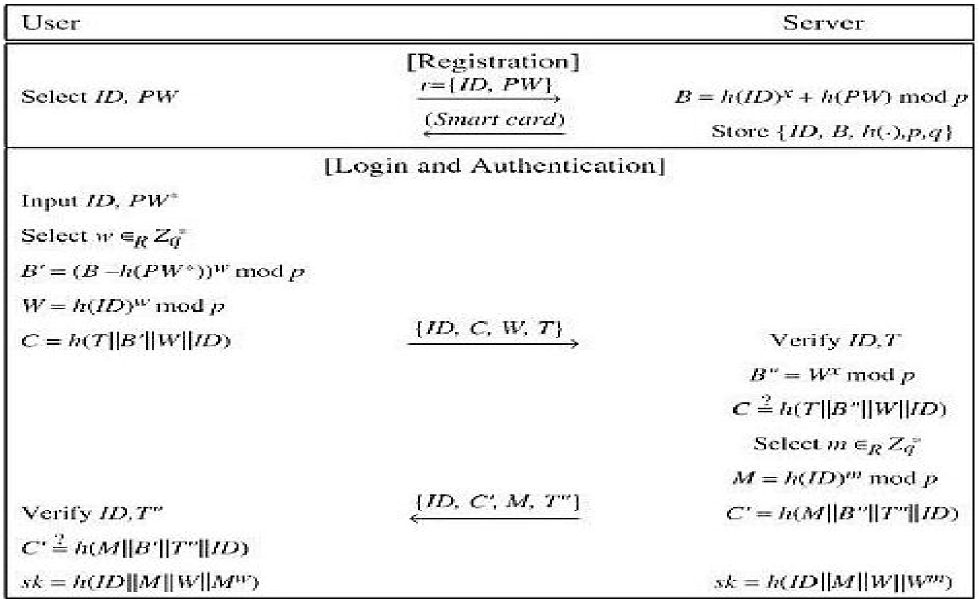
User
Server
[Registration]
Select ID, PW
$r=\{ID, PW\}$
$B = h(ID)^x + h(PW) \bmod p$
(Smart card)
Store $\{ID, B, h(\cdot), p, q\}$
[Login and Authentication]
Input ID, PW^*
Select $w \in_R Z_q^*$
$B' = (B - h(PW^*))^w \bmod p$
$W = h(ID)^w \bmod p$
$C = h(T \| B' \| W \| ID)$
$\{ID, C, W, T\}$
Verify ID, T
$B'' = W^x \bmod p$
$C \overset{?}{=} h(T \| B'' \| W \| ID)$
Select $m \in_R Z_q^*$
$M = h(ID)^m \bmod p$
Verify ID, T''
$\{ID, C', M, T''\}$
$C' = h(M \| B'' \| T'' \| ID)$
$C' \overset{?}{=} h(M \| B' \| T'' \| ID)$
$sk = h(ID \| M \| W \| M^w)$
$sk = h(ID \| M \| W \| W^m)$

Fig.10. Xu-Zhu-Feng authentication scheme.

In Fig.11 shown that the information at sensor nodes includes identifier, account, pre-circulated matrix password card, public key, second public key and private key, residual private key, arbitrary number and other required data [4]. In second stage, CA focus can be utilized safely to confirm the authentications of both the base station and the terminal nodes. The testament confirmation technique is the same as the current model. In authentication stage, an asymmetric authentication scheme is used. Because of the complex structure and higher processing capabilities than the terminal nodes, it will be difficult for the attacker to claim his/her self as the legitimate base station or platform [4]. Wen [5] proposed an authentication method between the sensor nodes in the sensor layer using unique identifiers. This paper portrays the entire structure of Internet or IoT security in each of the following 3 layers. They are sensor layer, system layer and application layer in each and every thing in Internet. This method makes use of time stamp and a dynamic variable cipher security certificate and is very light weight encryption or decryption technique with the help of timestamps [5]. These time stamp values are used for starting a session or to cancel the session. And the methodology used is “One Time One Cipher”. Both the correspondence gatherings will have a pre-shared key grid.

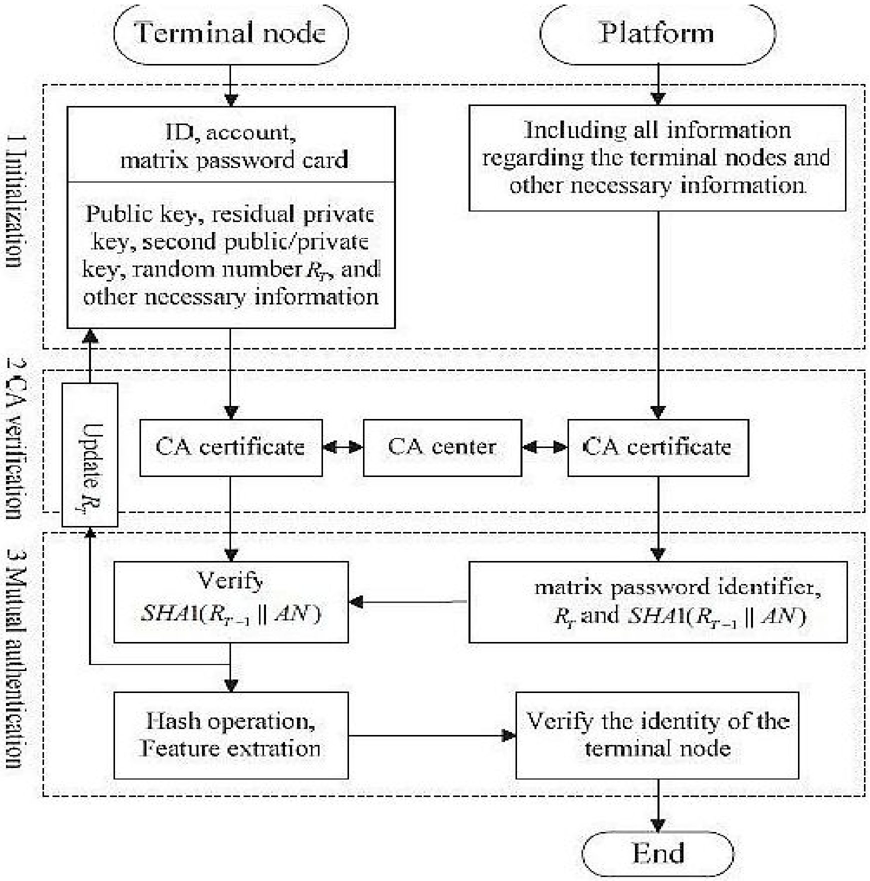
Terminal node
Platform
1 Initialization
ID, account, matrix password card
Public key, residual private key, second public/private key, random number R_T, and other necessary information
Including all information regarding the terminal nodes and other necessary information
2 CA verification
Update R_T
CA certificate
CA center
CA certificate
3 Mutual authentication
Verify $SHA1(R_{T-1} \| AN)$
matrix password identifier, R_T and $SHA1(R_{T-1} \| AN)$
Hash operation, Feature extration
Verify the identity of the terminal node
End

Fig.11. Authentication model proposed by Zhao et al.

Along these lines, both the correspondence gatherings won't exchange the keys, yet they will exchange the key directions from that pre-shared key matrix. Since, that lattice is not known, the assault is impractical, even the attackers catch the key directions being exchanged. The aggregate security of the correspondence relies upon the key network. The directions must be variable, so that more security will be achieved. Since the whole security of this plan relies upon the pre-shared key framework, its establishment must be done safely. The direction values must be extremely arbitrary, its reiteration might come about aggressor phishing and catching the key-grid values. Since the whole security of this plan relies upon the pre-shared key network, its establishment must be done safely [5].

Xue et al. [14] proposed one temporal-credential-based two-way validation and key agreement technique for WSNs. This scheme makes use of password based authentication. With secret key validation assistance, GWN can provide a worldly certification to every client and terminal node. Transient accreditation or certification can be safely secured and set away clearly in the customer’s smart card. Its temporal credential is related to its identity and must privately store in its storage medium [14]. Furthermore, using GWN, a lightweight key agreement technique is proposed to embed into the proposed protocol, because it only needs basic hash computations and XOR operations. This light weight is more suitable and attractive in IoT. This proposed technique is having three stages, (i) registration stage, (ii) login stage, and (iii) authentication and key agreement stage [14]. By making use of the hashed secret credentials and the proposed algorithms, all the stages are carried out. As per the security analysis results of the paper, this scheme provides mutual authentication, key agreement, masquerade attacks and spring back occurrence of insider attacks, password protection, password updating, identity protection, spring back occurrence of stolen smart card attacks, springing back occurrence of GWN bypassing attacks, springing back occurrence of replay attacks. But this scheme was vulnerable to stolen verifier attack and insider attacks, off-line password guessing, smart card lost problem and many logged-in users' attacks [15, 16]. Even it is vulnerable, it provides low communication cost, computation cost and storage cost. Then both [15, 16] provided their improved versions of this scheme. Also, this paper suggests some other usage style of GWNs that will lead to an improved version.

Das et al. [12] proposed one dynamic password-based user authentication scheme for hierarchical WSNs. This plan utilizes direct collaboration of terminal nodes with the client, without the base station. It utilizes the acclaimed Dolev–Yao threat model [17] , wherein two imparting parties (nodes) communicate through an insecure channel. In this threat model, the channel is insecure and the end-points (users, cluster heads, sensor nodes) cannot in general be trustworthy. Generally, the sensor nodes are modest, constrained abilities and nonspecific remote devices. Sensor node is prepared with limited memory size, processing capability, battery power, and short in radio transmission range [12]. The hierarchical structure of the WSNs is shown below in Fig.12. By the utilization of dynamic node addition stage, there is no compelling reason to overhaul put away data in the client's smart card for getting to continuous real-time information from the new group or cluster heads. The proposed scheme consists of seven stages. They are pre-deployment stage, post-deployment stage, registration stage, login stage, authentication stage, password change stage and dynamic node addition stage [12]. In this the dynamic node addition consists of two cases, (i) addition of sensor node, and (ii) addition of cluster nodes. For all the stages to complete, there are proposed algorithms in [17]. The proposed technique allows the user to authenticate at both base station and cluster heads inside the WSN [17]. After authentication is successful, the cluster head and user will be able to establish one secret session key between them, from which user wants to access real-time data in the target field. Later using this session key, the user can communicate with the cluster head for real-time data inside WSN. As per the security analysis results, this scheme was resistant to stolen-verifier attack, password guessing attack, replay attack, many logged-in users with the same login-id attack, denial-of-service assault, password change assault, springing back occurrence against nodes capturing assault, smart card breach assault, privileged-insider assault, masquerade assault. But later Turkanovic & Holbl [13] shown the faults in this scheme and proved it is infeasible for implementation.

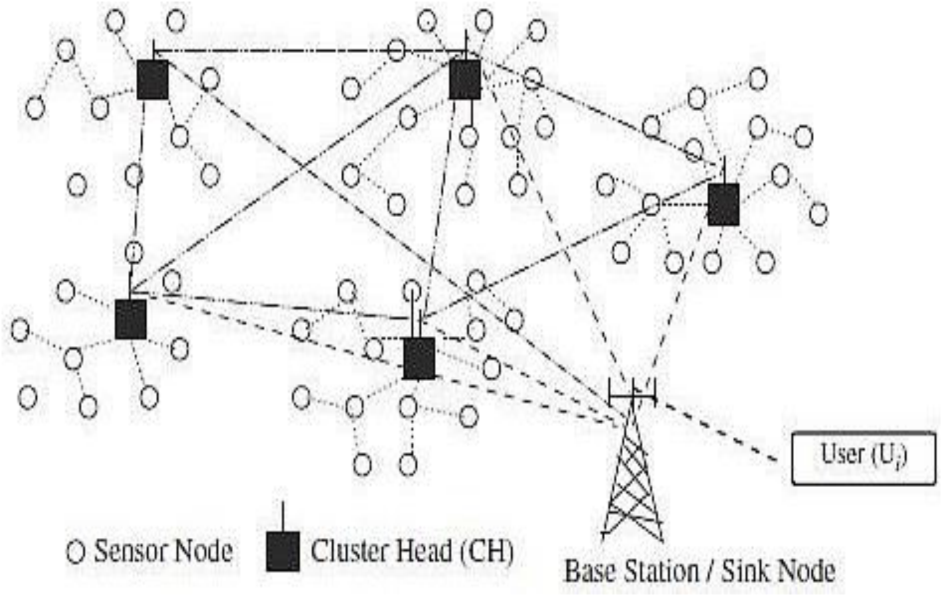

Fig.12. The Hierarchical structure of WSNs.

Turkanovic & Holbl [13] proposed an improved dynamic password-based user validation technique for hierarchical WSNs. This paper clearly states the flaws and reasons why Das et al.'s technique cannot be implemented in reality. Das et al.'s technique contains seven stages, which include pre-deployment stage, post-deployment stage, registration stage, login stage, authentication stage, password change stage and dynamic node addition stage [12]. In Das et al.'s scheme authentication process was done at two different phases where there are no sufficient parameters. This flaw is linked with the registration phase, login phase, authentication phase and password change phase. Now, this paper corrected only the above mentioned four stages and proposed flaw less scheme, leaving pre-deployment stage, post-deployment stage and dynamic node addition stage unchanged. It also reduced the number of hash functions [13]. Thus, this provided security from the well- known attacks. But still vulnerable to some other attacks.

Turkanovic and Hölbl [16] proposed a two-sided validation technique among sensor nodes, users and the base stations or gate way nodes using smart cards. This is a light weight authentication strategy, which is more alluring in IoT, due to its resource-constraint nature. The proposed plan empowers a remote client to safely arrange a session key with a general terminal node, utilizing a lightweight key understanding convention [3]. This scheme makes use of basic hashing and XOR operations. This entire technique consists of five stages i.e. pre-deployment stage, registration stage, login stage, authentication stage, and the dynamic node addition stage. This is a mutual authentication scheme initiated by user, when tried to communicate with a particular terminal node. In this method the user's data is pre-stored in the local database. Now if any user wants to login into the sensor the gate way node checks the user data in the smart card. The register stage will have two types of stages, they are node registration stage and user registration stage. Authentication stage will be carried out by GWN, but the user directly won't communicate with it. They both communicate with sensor as mediator. Dynamic node addition stage enables a remote addition of node to the network. But, this method can be used by attacker to gain information, so more security need to be provided. This scheme is resistant to many popular attacks.

5. Comparison

The comparative view of the security features and performance, of the above mentioned security schemes was tabulated in Table 1. In this table S stands for 'yes' and N stands for 'no'.

Table-1: Comparison based on security features.

Security Feature & Performance	[2]	[3]	[4]	[9]	[10]	[1]	[12]	[11]
Mutual authentication	S	S	S	S	S	S	S	S
Key agreement	S	S	S	S	S	S	S	S
Password change	N	--	S	S	S	S	S	S
Dynamic node addition	--	--	--	--	S	S	--	S
User anonymity	--	--	--	--	--	S	S	N

Not only based on the security features and performance, but also the times for calculating hash functions are even best in some schemes provided above. Also the computational and storage consumption analysis and the communication analysis for some of the above mentioned methods were mentioned below. The comparison in computation and communication costs is shown in Table 2. Where the acronym Th means time for Hash Function and TE/D means symmetric key Encryption/Decryption.

Table-2: Comparison based on computation cost.

Authentication schemes	User	Sensor node	GWN	Communication cost
[1]	7 Th	5 Th	7 Th	4 Messages
[10]	5 Th + 1 TE/D	--	2 Th + 1 TE/D	4 Messages
[11]	1 Th + 2 TE/D	3 Th + 2 TE/D	4 Th + 4 TE/D	4 Messages
[12]	7 Th	6 Th	13 Th	6 Messages

6. Future Scope

The future of IoT depends basically on the security. No illegitimate client or node ought to access sensors. Many researchers proposed numerous authentication plans. The assortment of sensors in the IoT are expanding quickly, which paves the way for new authentication plans, because of emerging vulnerabilities in the current authentication plans. By accomplishing the security, IoT can be utilized as a part of numerous fields like military, social insurance, smart home, etc. Addressing and resolving these security flaws is the best way for future realization of IoT.

7. Conclusion

This paper in depth discusses various authentication schemes that are proposed by the researchers. Some of these are as yet having numerous vulnerabilities; there are a few plans where the expense and framework support will be high and in addition the security moreover. But, due to the resource constraint nature of the terminal nodes, these schemes are not being adapted, even they provide good resistance from the well-known security issues. Hence, light-weight validation schemes are required, to have the best fit for this scenario.

References

1. G. Usha Devi, E. Vishnu Balan, M. K. Priyan, C. Gokulnath, Mutual authentication scheme for IoT applications, Indian Journal of Science and Technology, 2015, 8(26), DOI: 10.17485/ijst/2015/v8i26/80996.
2. K. A. Rafidha Rehiman, S. Veni, A secure authentication infrastructure for IoT enabled smart mobile devices – an initial prototype, Indian Journal of Science and Technology, 2016, 9(9), DOI: 10.17485/ijst/2016/v9i9/86791.
3. M. Turkanovic, B. Brumen, 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, 2014, 20, pp. 96–112.

4. G. Zhao, X. Si, J. Wang, X. Long, T. Hu, A novel mutual authentication scheme for Internet of Things, Proceedings of International Conference on Modelling, Identification and Control, 2011, pp. 563-566.

5. Q. Wen, X. Dong, R. Zhang, Application of dynamic variable cipher security certificate in internet of things, Proceedings of International Conference on Cloud Computing and Intelligent Systems, 2012, pp.1062-1066.

6. J. Xu, W.T. Zhu, D.G. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces, 2009, 31, pp.723–728.

7. S.W. Lee, H.S. Kim, K.Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces, 2005, 27 (2), pp.181–183.

8. N.Y. Lee, Y.C. Chiu, Improved remote authentication scheme with smart card, Computer Standards & Interfaces, 2005, 27 (2), pp.177–180.

9. X. Wang, H. Yu, How to break MD5 and other Hash functions, proceedings of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2005, pp.19-35.

10. W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 1976, IT-22, pp.644-654.

11. R. Song, Advanced smart card based password authentication protocol, Computer Standards & Interfaces, 2010, 32, pp.321–325.

12. A. Das, P. Sharma, S. Chatterjee, J.K. Sing, A dynamic password–based user authentication scheme for hierarchical wireless sensor networks, Journal of Network and Computer Applications, 2012, 35(5), pp.1646-1656.

13. M. Turkanovic, M. Hölbl, An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks, Elektronika Ir Elektrotechnika, 2013, 19(6), pp.109–116.

14. K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Networks and Computer Applications, 2012, 36(1), pp.316–323.

15. C.T. Li, C.Y. Weng, C.C. Lee, An advanced temporal credential based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors, 2013, 13, pp.9589–9603.

16. M. Turkanovic , M. Hölbl, Notes on a temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Wireless Personal Communications. 2014, 77(2), pp 907–922.

17. D. Dolev, A. Yao. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2), pp.198–208.

18. M. L. Das, Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communication, 2009, 8(3), 1086-1090.

19. D.H. Nyang, M.K. Lee, Improvement of Das's two-factor authentication protocol in wireless sensor networks, 2009, https://eprint.iacr.org/2009/631.pdf.

20. M.K. Khan, K. Alghathbar, Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks, 2010, 10(3), pp.2450-2459.

21. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks, 2002, 38(4), pp.393–422.

22. K. Romer, F. Mattern, The design space of wireless sensor networks, IEEE Wireless Communications, 2004, 11(6), pp.54–61.

23. Y. Baocai, Y. Huirong, F. Pengbin, G. Liheng, L. Mingli, A Framework and QoS based web services discovery, Proceedings of IEEE International Conference on Software Engineering and Service Sciences, 2010, DOI: 10.1109/ICSESS.2010.5552261.