ISSN: 2278-4632
Vol-11 Issue-02, February 2021

A Survey on Security Issues in IOT Environment

A.SANDHYA RANI

Associate Professor
sandhyarani1203@gmail.com

PALASAMUDRAM HIMABINDU

Assistant Professor
himubindu5808@gmail.com

V.L.PADMA LATHA

Assistant Professor
vlpadmalatha@gmail.com

Abstract:

Internet of Things (IoT) comprises of a substantial number of associated objects that are speaking with one another. As IOT does not require any human to machine cooperation, it is by all accounts one of the biggest influxes of upheaval according to the examination going on, thus security is required. With the end goal to help believed correspondence between IoT objects, viable validation techniques ought to be connected between the imparting substances. The brisk improvement of IOT has inferred with the difficulties as far as security of things. This survey paper focus on the general security issues and attacks in cloud IOT model with respect to different existing authentication schemes and provides some suggestions to overcome the drawbacks in the existing schemes.

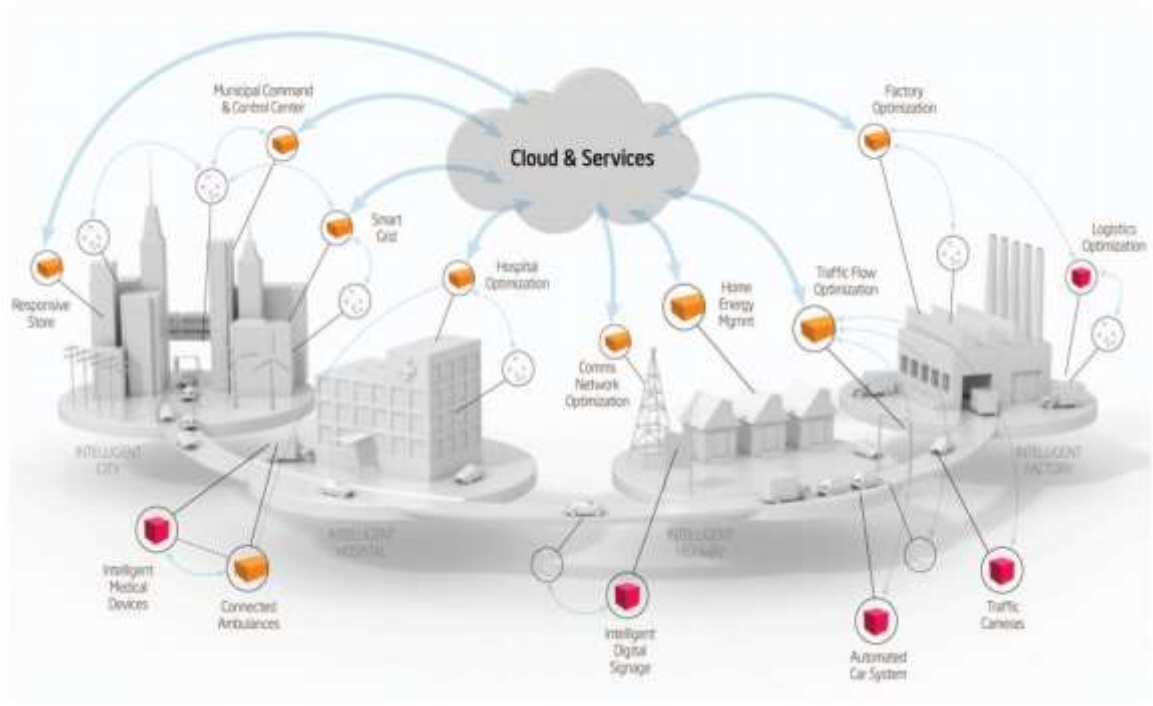
Keywords: Internet of Things; authentication; cloud computing; security attacks.

1. Introduction

In early days the word web is utilized to express the innovation of interfacing PCs everywhere throughout the globe utilizing wired or remote connections. From that point forward the web has been adequately utilized for documents sharing, web perusing, web based business, web based life, and so forth. Be that as it may, ongoing advancement and organization of brilliant innovations have raised the requirement for articles to be pervasively associated together. Thus, this requires the requirement for more modern advancements to help new machine-to-machine (M2M) correspondence. With the end goal to develop toward another universe of associated objects, the Internet of Things (IoT) has been presented as the eventual fate of the web.

Confirmation is the way toward perceiving clients and gadgets in a system and constraining induction to approved people and non-controlled gadgets. This procedure really depends on username and secret word and don't work with unattended gadgets. Verification can be of one-way confirmation and common validation. In an IoT situation, the protest confirms the server and the other way around. Here, the server is overseeing security testaments given by the IoT gadgets. In this way, just genuine clients and servers can take an interest in the data exchange.

ISSN: 2278-4632
Vol-11 Issue-02, February 2021



As shown in fig.1,cloud administrations can work crosswise over extensive variety of frameworks and handle a colossal measure of information, it has been considered as a vital part of IoT.The approach of distributed computing has gone about as an impetus for the advancement and arrangement of adaptable Internet-of-Things plans of action and applications. In this way, IoT and cloud are currently a day's two firmly associated future web advances, which go as one in non-minor IoT arrangements. Distributed computing and IoT guarantee an imaginative change in outlook which will permit interconnecting a few sensors, shrewd gadgets to assemble and share information for perception and understanding. This developing merger offers an extensive variety of potential applications that can enhance an incredible nature.

In this Study, we break down the dangers that may happen in multi-server IoT condition systems amid the correspondence procedure.

In Section 2, we depict the security dangers that may happen in a multi-server IoT condition in distributed computing. In Section 3, we provide the review of some secured authentication protocolsin multi-server IoT environments. In Section 4, wedescribe the attacks possible in those protocols and provide the suggestions to overcome the possibility of attacks in the explained protocols. Finally, our conclusions are listed in Section 5.

2. Security Threats

Cloud-IoT-based situations confront a similar arrangement of dangers like any ordinary system. In any case, because of the enormous measure of information that is being put away on the cloud servers, the cloud specialist organizations turn into a simple and appealing focus for the assailants. A few dangers/assaults that begin from various substances with their foe models are:

(a) Eavesdropping assault: This assault alludes to unlawful block attempt of a correspondence between two elements. Such assaults can happen when the cloud specialist organization gets to the information put away on the server to straighten something up. These assaults are threatening since they are hard to distinguish and the clients unwittingly putting away delicate information, for example, passwords, on the server.

(b) Integrity assault: An information trustworthiness assault happens when an aggressor endeavors to degenerate or control information without authorizations of the proprietor. The assault is generally completed by means of malware program that erases or adjusts substance of a shrewd gadget.

(c) Denial assault: In this assault, one of the imparting parties denies either all or some piece of the transmission assignments.

(d) Denial of service assault: This assault happens when a cloud server is overwhelmed by vast number of administration demands which it can't deal with. It can make the server crash and authentic clients are denied from administration.

(e) Cloud server compromise assault: This assault happens when an assailant picks up control of the server after system arrangement. An aggressor can interface with a server and can totally control it for getting the data or controlling that server and its further correspondence.

(f) Replay assault: This assault happens when the malignant substance sees the progressing correspondence that happens between the two gatherings. The vindictive element gathers the verified data, e.g. shared session key and after those attempts to contact the collector later on with that key. The aggressor just replays the listened in message.

(g) Impersonation assault: In this assault, the aggressor attempts to mimic a lawful substance and endeavors to speak with the other element as a genuine element.

(h) Stolen verifier assault: In such assaults, the assailant is fruitful in taking fundamental data from server either from the present or already effective sessions. The aggressor can utilize the stolen data to access the information put away on the server.

(i) Insider assault: Such assaults happen when the assailant is a believed element having approved induction to the framework and furthermore has all comprehension of the basic design. Such assaults are conveyed with an aim to complete a cheat, burglary of mystery data or of protected innovation.

(j) Man-in-the-middle assault: Such assaults happen when the assailant can subtly transmit and furthermore change the correspondence occurring between two elements who think they are speaking with one another.

3. Review of Existing Protocols

i) Xue et.al. Scheme:

This segment quickly a survey the Xue et al. conspire which includes three kinds of element, for example, client Ui, specialist organization server Sj and control server (CS). The CS basically gives enlistment system to all Ui and Sj. The Sj gives set of administrations to all the clients on interest.

Registration Phase

The Ui choices desired identity IDi, password Pi, a random number b and calculates Ai = h(b||Pi) and submits registration message (IDi, Ai, bi) to the CS . Now the CS first takes two random numbers x, yi and calculates PIDi =h(IDi || b), Bi = h(PIDi || x) and forwards Bi to the user securely. After receiving Bi, the Ui calculates Ci = h(IDi || Ai), Di = Bi$\oplus$(PIDi || Ai) and embeds (Ci, Di, b, h(·)) in the smart card.

During the specialist organization server enrollment, the Sj decisions identity SIDj, a random number d and sends (SIDj, d) to the CS. Subsequent to getting it, the CS computes PSIDj = h(SIDj|| d), BSj = h(PSIDj|| y) and sends BSj to Sj safely. At last, the Sj records mystery parameter (BSj, d) into his/her memory.

Login Phase

The Ui punches the smart card into the card reader and provides IDi and Pi. At that point, the card reader ascertains Ai* = h(b || Pi), Ci* = h(Di || Ai) and checks the condition (Ci*? = Ci). On the off chance that (Ci*== Ci), the card reader acknowledges the Ui as an authenticity client; generally, rejects the association.

Authentication and Key agreement Phase

This stage describes shared confirmation and in addition key understanding among the Ui, Sj and the CS. All

activities performed in this stage are given underneath.

Stage 1: User Ui creates a current timestamp TSi, a random number Ni1 and figures (Bi, Fi, CIDi, Gi, Pij) as pursues:

$$Bi = Di \oplus Ci$$
$$Fi = Bi \oplus Ni1$$
$$CIDi = IDi \oplus h(Bi \,||\, Ni1 \,||\, TS\ i||\ ”00”)$$
$$Gi = b \oplus h(Bi \,||\, Ni1 \,||\, TS\ i||\ ”11”)$$
$$Pi\ j = h(Bi \oplus h(Ni1 \,||SIDj||PIDi||TSi))$$

Where "00" is a 2 bit two fold "0" and "11" are 2 bit binary "1". At that point, Ui forwards (Fi, Pij,CIDi, PIDi,Gi, TSi) to Sj freely.

Stage 2: After getting messages from Ui, Sj first checks the time interim condition (TSj − TS i<ΔT), where TS j, ΔT is the Sj's present timestamp and expected time interim during message transmission separately. In the event that the condition isn't false, Sj proceeds; generally, stops this session. At that point, the Sj produces a random number Ni2 and figures the accompanying activities:

$$Ji = BSj \oplus Ni2$$
$$Ki = h(Ni2 \,||BSj||\ Pij||TSi)$$
$$Li = SIDj \oplus h(BSj||\ Ni2 \,||TSi||\ ”00”)$$
$$Mi = d \oplus h(BSj||\ Ni2 \,||TSi||\ ”11”)$$

The Sj at that point sends (Fi, Pij,CIDi,Gi, PIDi, TSi, Ji, Ki, Li, Mi, PSIDj) to the CS openly.

Stage 3: After getting messages from Sj, CS first checks the condition (TScs − TS i<ΔT), where TScsis the current timestamp of the CS. Stops the association if the condition is false; something else, the CS plays out the accompanying activities:

$$BSj = h(PSIDj||\ y)$$
$$Ni2 = Ji \oplus BS\ j$$
$$Ki = h(Ni2 \,||BSj||Pij||TSi)$$

The CS checks the condition (Ki* ? = Ki). If (Ki* == Ki), it further calculates:

$$Bi = h(PIDi||\ x)$$
$$Ni1 = Bi \oplus Fi$$
$$IDi = CIDi \oplus h(Bi \,||\, Ni1 \,||\, TS\ i||\ ”00”)$$
$$S\ IDj = Li \oplus h(BSj||\ Ni2 \,||TSi||\ ”11”)$$
$$Pi\ j = h(Bi \oplus h(Ni1 \,||SIDj||PIDi||TSi))$$

Then, the CS checks the condition whether (Pij*? = Pij) or not. If (Pij* ,Pij), stops this session; generally, computes the accompanying tasks:

$$b = Gi \oplus h(Bi \,||\, Ni1 \,||TSi||\ ”11”)$$
$$d = Mi \oplus h(BSj||\ Ni2 \,||TSi||\ ”00”)$$
$$PIDi* = h(IDi||\ b)$$
$$PSIDj* = h(SIDj||\ d)$$

The CS checks whether (PIDi*= PIDi) and (PSIDj* = PSIDj) are right or not. In the event that these condition isn't false, the CS takes a random number Ni3 and calculates the accompanying tasks:

$$Pi = Ni1 \oplus Ni3 \oplus h(SIDj||\ Ni2 \,||BSj)$$
$$Qi = h(Ni1 \oplus Ni3)$$
$$Ri = Ni2 \oplus Ni3 \oplus h(IDi \,||\, Ni1 \,||\, Bi)$$
$$Vi = h(Ni2 \oplus Ni3)$$

Then, the CS sends (Pi, Qi, Ri, Vi) to the Sj.

Stage 4: On the receipt of answer message from CS , the Sj computes the accompanying tasks:

$$Ni1 \oplus Ni3 = Pi \oplus h(SIDj||\ Ni2 \,||BSj)$$
$$Qi = h(Ni1 \oplus Ni3).$$

ISSN: 2278-4632
Vol-11 Issue-02, February 2021

At that point, the Sj confirms whether (Qi* ? = Qi). In the event that (Qi* == Qi), it infers that the CS and Ui are real and sends answer messages (Ri, Vi) to the client Ui.

Stage 5: On the receipt of answer message from Sj, the Ui calculates,

$$Ni2 \oplus Ni3 = Ri \oplus h(IDi||Ni1||Bi)$$
$$Vi^* = h(Ni2 \oplus Ni3)$$

At that point, the Ui checks the condition (Vi* ? = Vi). On the off chance that (Vi* == Vi), the Ui affirms that CS and S j are credible. Finally,the Ui, Sj and CS concur upon a typical mystery key S K = h((Ni1 Ni2 Ni3) ||TSi).

ii) Parwinder et.al. Scheme:

Registration Phase

Medical Pofessional	Cloud Server
Submits ID_{MP}, PW_{MP},B_{MP},	
$<ID_{MP}, PW_{MP},B_{MP}>$ →	
	Generates random Y_{MP}, Computes, BIO_{MP},=h(B_{MP}) T_{MP}=H(ID_{MP}||PW_{MP}||BIO_{MP}||⊕H(X) R_{MP}= H(ID_{MP}||PW_{MP}||BIO_{MP}||⊕H(Y_{MP}) S_{MP}=$Y_{MP} \oplus ID_{MP} \oplus PW_{MP} \oplus BIO_{MP}$
$<T_{MP}, R_{MP},S_{MP}>$ ←	
Stores T_{MP}, R_{MP},S_{MP} into smart card	
	Computes, D_{MP} = H(H(ID_{MP}||Y_{MP}) ⊕ X) Stores, D_{MP} , Y_{MP} ⊕ X, ID_{MP} ⊕ H(X||Y_{MP}) into memory

Login Phase

Medical Pofessional	Cloud Server knows X (Private Key)
Enters ID'_{MP}, PW'_{MP},MP,B'_{MP} BIO'_{MP}=h(B'_{MP}) Generates random, a Computes, ECCpoint: A = a x G C = a x P_{cs} Y'_{MP} = $S_{MP} \oplus ID'_{MP} \oplus PW'_{MP}$ ⊕MP,BIO'_{MP}	

ISSN: 2278-4632
Vol-11 Issue-02, February 2021

R'_{MP}= H($ID'_{MP} \oplus PW'_{MP} \oplus BIO'_{MP}$) ⊕H($Y'_{MP}$)
Checks if R'_{MP}?=R_{MP}
Computes,
H(X) = S_{MP} ⊕ H(ID_{MP}||PW_{MP}||BIO_{MP})
MID = H(ID_{MP}||Y_{MP} ⊕H(X))
Z_{MP} = H(ID_{MP}||H(X)||Y_{MP})
EncryptsA using Z_{MP} i.e. Ez_{MP}(A)
Computes β=H(Z_{MP} || T_1)

<ID_{MP}, MID,Ez_{MP}(A),β,T_1>

On insecure channel

Authentication and Key agreement Phase

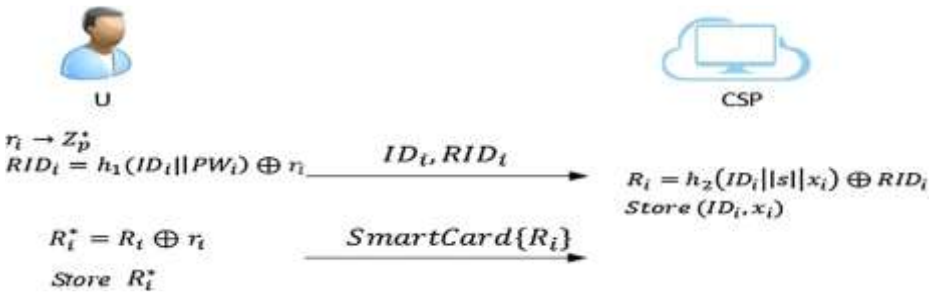
Cloud Server knows X (Private Key)	Medical Pofessional
Checks if ($T_1 - T_{curr}$)<=ΔT? If no, the login process is terminated Otherwise, computes: D'$_{MP}$= H(MID ⊕ H(X) ⊕ X) Checks if D'$_{MP}$ = D$_{MP}$? If fails, the process is terminated Otherwise, computes Z'_{MP} = H(ID_{MP} || H(X) || Y_{MP} β'= H(Z'_{MP}|| T_1) *Checks if* β'=β ? Decrypts A using Z'_{MP}, i.e., Dz$_{MP}$ {Ez_{MP}(A)} to extract A Computes: C=A x X$_{cs}$,L = H(A || T_2) Generates random u Y^{cs} = H(c||u||Z'_{MP}|| T_2) < Y$_{cs}$,u,L, T_2>	
Computes session key S$_k$= H(H(X) || Z'_{MP} ||c||u)	If(T_2 - T_{curr})<= ΔT? If fails, rejects the message otherwise, computes L` = L? If fails, process terminates

ISSN: 2278-4632
Vol-11 Issue-02, February 2021

	$Y'^{cs} = H(c\|\|u\|\|Z_{MP}\|\| T_2)$ If $Y'^{cs} = Y^{cs}$? If fails, rejects the message Otherwise, computes **Session key**
Session key is computed as :$S_k = H(H(X)\|\|Z_{MP}\|\|c\|\|u)$	

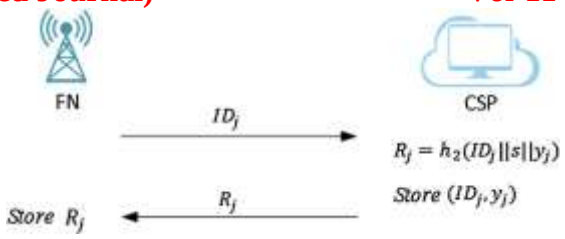
iii) Jia et.al. Scheme:

User registration phase

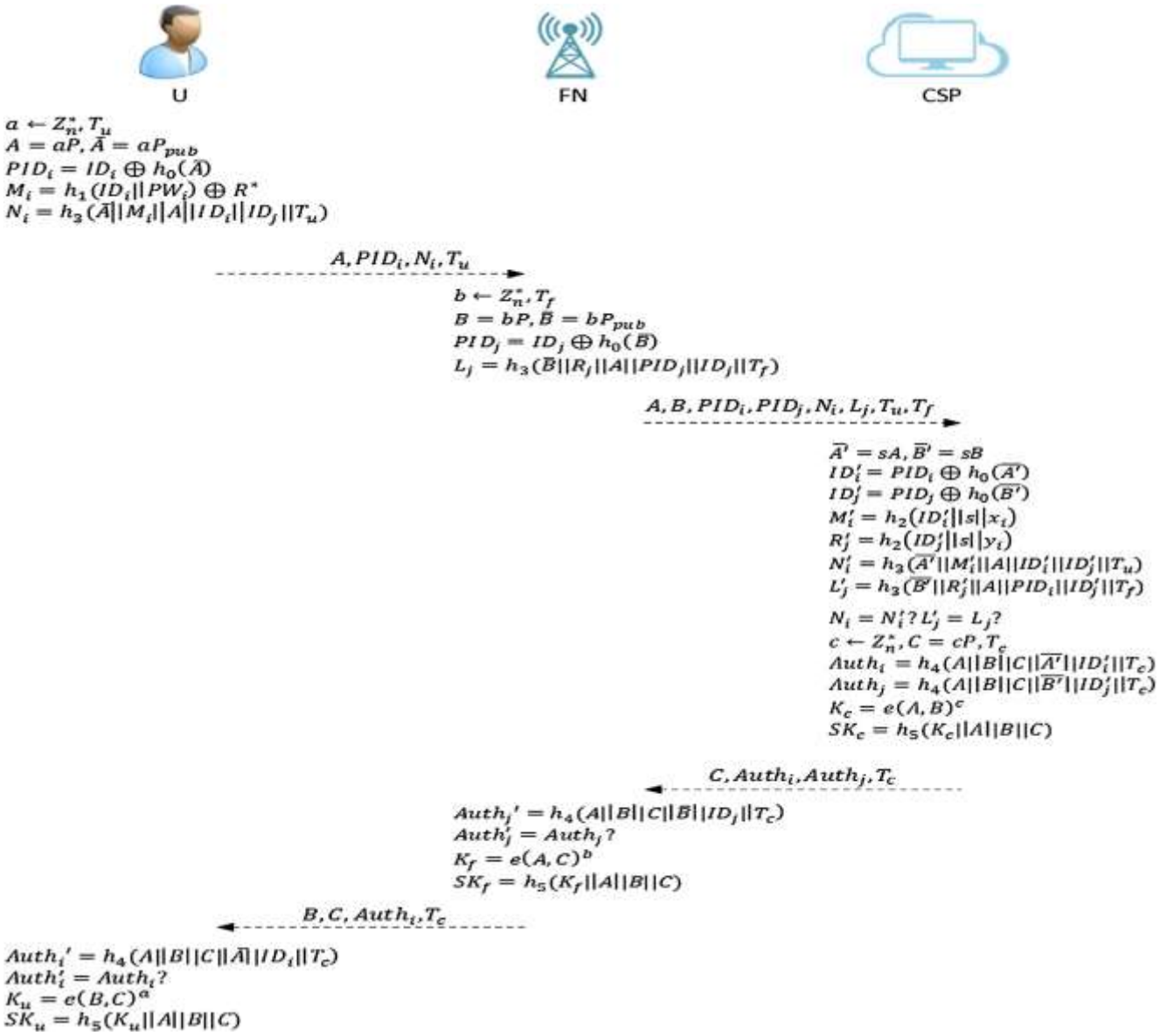


Fog registration phase

ISSN: 2278-4632
Vol-11 Issue-02, February 2021



Authentication and Key agreement Phase



From the complete writing survey of existing systems, it is clear that there are some significant assaults and difficulties in Authentication in IoT condition.

Some of thesecurity challenges highlighted are:

- Mutual authentication
- Integrity
- Confidentiality
- Availability

3. Cryptanalysis of Existing Schemes

i) Xue et.al. Scheme:

In Xue et. al. scheme, the registration phase itself suffers from some attacks. Some of the attacks that are possible in this existing scheme are:

a) Password Guessing assault:

In the registration phase, the user is sending the message <IDi, Ai, b>. As per the above message an intruder (legitimate user) can easily find the password P_i because he/she gets the registration message, so he knows the value of A_i.

By the expression $A_i = h(b||P_i)$, an adversary can get the password as he knows the two values A_i, and the random value can be guessed using the dictionary in n chances.

b) User Impersonation assault:

As adversary knows the id and password, he can easily change the password in password replace phase. So he can impersonate as a legal user and can send the illegal messages in the communication channel.

c) Server Impersonation assault:

In the scheme, as per the above attacks the legitimate user knows the values A_i, b(gets through the dictionary) through that he can attain the value of PID which in turn leads to leakage of B_i, C_i, D_i .

By the above values an adversary can behave as a server also.

d) Mutual Authentication:

In Xue et. al. scheme, mutual authentication is not possible because an adversary can impersonate the user as well as server which leads for an unreliable communication.

Suggestion:

If we replace the hash function with encryption while sending the important messages in the scheme, we can more securely send the messages between the user and the cloud server which leads to reliable communication.

ii) Parwinder et.al. Scheme:

a) Insider assault:

As the communication in this scheme is done through a public channel, a legal adversary can easily involve in the process and can get the details of the entire system as he/she retrieve the important data i.e., credentials which provides way to achieve the messages between user and server .The above process leads to the insider attack.

b) Availability:

In Parwinder et al. scheme, the messages are transmitted between user and server using timestamps T_1, T_2, T_{curr}. Sometimes this may lead to the unavailability of the values to both user and server that leads to incomplete message formation.

Suggestion:

In Parwinder et. al. scheme, authors are using encryption, hash and also XOR operations for secured message transfer which leads to high computational and communication cost. So it is better to use the required authentication operation in apt situation i.e., use the operation if needed.

iii) Jia et.al. Scheme:

a) Stolen verifier assault:

In Jia et. al. scheme, the registration message <IDi, RIDi> send from user to server can easily theft by adversary as $RIDi= h(IDi||Pw_i) \oplus r$, where r is random number. If adversary is a legal user then he'll get the values in the message, so that he can retrieve Pw from the above equation which is a vital data in the scheme leads to stolen verifier attack.

ISSN: 2278-4632
Vol-11 Issue-02, February 2021

b) Denial of service assault:

This scheme contains a flood of messages between user and server. Sometimes server can't handle the overflow of service requests. This may lead to server crash and legal user is unable to fulfil the service. This in turn leads to denial of service attack.

c) Impersonationassault:

In the scheme, the adversary gets the identity and password (ID, Pw) of a legal user. So he replaces the credentials with his own and can behave as a legal user and can transmit the illegal messages.

Suggestion:

In order to overcome the above attacks in the Jia et. al. scheme, the user has to use the three-way authentication i.e., password, digital certificate and biometric etc. in the communication to achieve an authenticated communication.

Conclusion

This paper shows the outline of validation in cloud IoT condition and its exploration challenges. Wide assortments of literary works were displayed. Present investigation was looked into to comprehend the issues and issues in the security of IoT situations. As indicated by the above displayed writing study, it is distinguished that security in IoT is a noteworthy issue when it turns into a reality. Along these lines, IoT security framework must be intended for upgrading the verification and approval to convey better security benefit. On the off chance that the confirmation system is more grounded and settled, it will avert numerous security dangers and issues like listening in, pantomime and replay assault, shared verification, integrity etc. In addition, the validation systems ought to be quick and light weighted without trading off security. The proposed investigation gives the itemized rendition of assaults exists in the current plans and furthermore the proposals to conquer the conceivable assaults. The proposed study gives us an exhorted approach to structure a confirmation conspire which is free from all the previously mentioned assaults and security issues.

References

[1] K. Xue, P. Hong, C. Ma."A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture" Journal of Computer and System Sciences 80 (2014) 195-206.
[2] Xiaoying Jia, Debiao He, Neeraj Kumar, Kim-Kwang, Raymond Choo. "Authenticated key agreement scheme for fog-driven IoT healthcare system". Journal of Wireless Networks, Springer Nature 2018.
[3] Parwinder Kaur Dhillon, Sheetal Kalra. "Multi-factor user authentication scheme for IoT-based healthcare services", Journal of Reliable Intelligent Environments, Springer 2018.
[4] Ruhul Amin, Neeraj Kumar, G.P. Biswas, R. Iqbal, Victor Chang. "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment", Future Generation Computer Systems (2016).
[5] Aakanksha Tewari, B. B. Gupta. "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags", Journal of Supercomput (2016).
[6] Won-il Bae, Jin Kwak. "Smart card-based secure authentication protocol in multi-server IoT environment", Multimed Tools Appl (2017).
[7] Ruhul Amin, Neeraj Kumar, G.P. Biswas, R. Iqbal, Victor Chang. "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment". Future Generation Computer Systems (2016).
[8] T. Xiang, K. Wong, X. Liao "Cryptanalysis of a password authentication scheme over insecure networks" Journal of Computer and System Sciences" 74 (5) (2008) 657 - 661.
[9] L. Lamport "Password authentication with insecure communication", communication of the ACM, Vol. 24, No. 11, PP. 770-772, 1981.
[10] X.Li, W.Qiu, D.Zheng, K.Chen, J.Li "Anonymity enhancement on robust and efficient password authenticated key agreement using smartcards", IEEE Transactions on Industrial Electronics 57(2)(2010)793-800.
[11] J. Yashaswini, "A Review on IoT Security Issues and Countermeasures", ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY (2017)
[12] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., &Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. Information Sciences, 258, 371–386.
[13] Xiao, Z., & Xiao, Y. (2013). Security and Privacy in Cloud Computing. IEEE Communications Surveys Tutorials, 15(2), 843–859.
[14] Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. In 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 1, pp. 647–651).

[15]Tan Z (2014) A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. J MedSyst 38(3):1–9

