 ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

An Investigation of Security Concerns inside the Internet of Things (IoT) Ecosystem

[1]Putta Kishore Kumar, [2]Palem Naresh Kumar, [3]Uday kumar, [4]Bhavani Buthukuri

[1,2,3]Assistant Professor, Department of CSE, Narsimha Reddy Engineering College, Secunderabad, Telangana
[4]Associate Professor, Department of CSE, Narsimha Reddy Engineering College, Secunderabad, Telangana

Abstract:

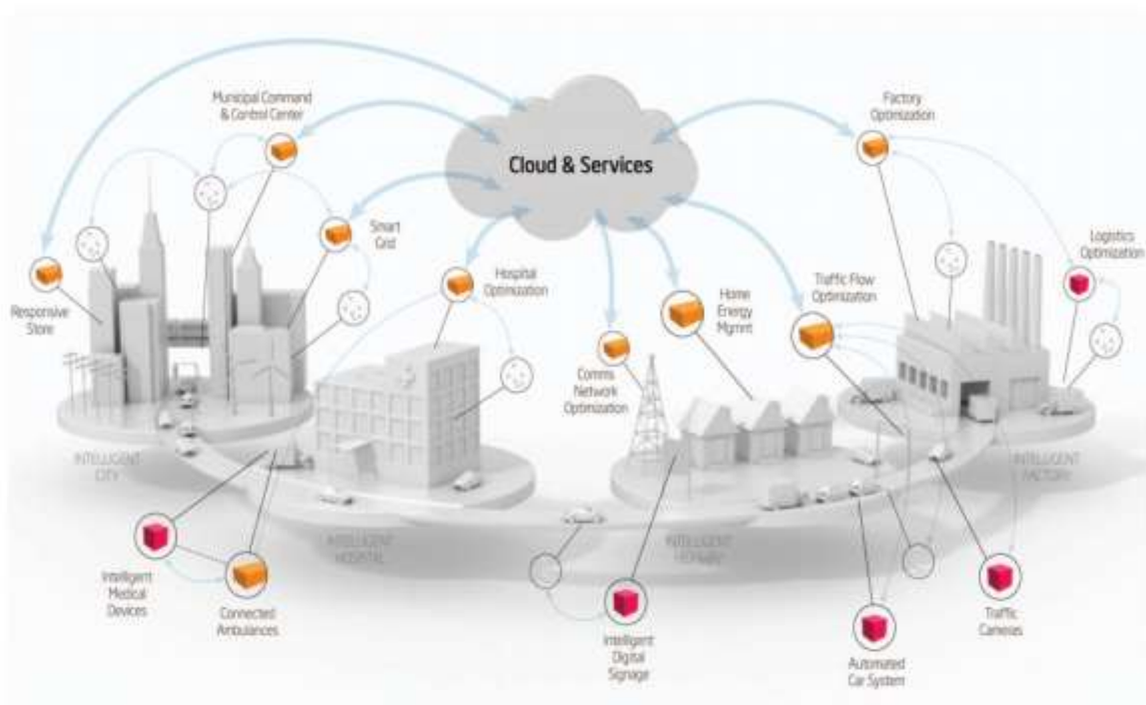
The Internet of Things (IoT) encompasses a significant multitude of interconnected entities engaged in communication with each other. According to ongoing research, the Internet of Things (IoT) is considered to be a significant disruptive force since it operates independently of human-machine collaboration. Consequently, ensuring security measures is imperative in light of this development. In order to facilitate reliable communication among Internet of Things (IoT) devices, it is necessary to provide effective authentication methods between the communicating entities. The rapid development of the Internet of Things (IoT) has raised concerns over the security of connected devices. This survey study examines the overall security concerns and assaults in the cloud Internet of Things (IoT) concept, specifically in relation to various authentication systems that are already in use. Additionally, it offers recommendations to address the limitations found in these existing schemes.

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

1. Introduction

During the first stages, the term "web" was used to denote the technological advancement of connecting computers throughout the world via wired or wireless connections. Since that juncture, the internet has been effectively used for the purposes of document sharing, online browsing, e-commerce, social media, and other related activities. However, the continuous progress and integration of innovative technologies have increased the need for goods to be extensively interconnected. Therefore, there is a need for further technological improvements to provide enhanced machine-to-machine (M2M) communication. The Internet of Things (IoT) has been introduced as the future of the internet, aiming to advance towards a new realm of interconnected entities.

The process of confirmation involves the identification of users and devices inside a network, as well as the restriction of access to authorized individuals and non-compliant devices. The efficacy of this process is contingent upon the use of a specific login and secret word, rendering it incompatible with unattended devices. Verification may include both unidirectional confirmation and mutual validation. In the context of the Internet of Things (IoT), the verification process establishes the mutual authentication between the server and the protest. In this context, the server is responsible for monitoring the security protocols provided by the Internet of Things (IoT) devices. In this manner, only authenticated clients and servers are able to participate in the process of data exchange.



As seen in Figure 1, cloud services have the capability to operate across a diverse range of systems and manage a significant volume of data. Consequently, they have been recognized as a crucial component within the Internet of Things (IoT) architecture.The use of distributed computing has served as a catalyst for the development and implementation of flexible Internet-of-Things business models and applications. Currently, the Internet of Things (IoT) and cloud computing are two closely interconnected future technologies in the field of web development, particularly in the context of IoT solutions. Distributed computing and the Internet of Things (IoT) provide a transformative paradigm shift that enables the interconnection of several sensors and intelligent devices to gather and exchange data for the purpose of visualization and comprehension. This emerging convergence has a wide range of possible applications that have the capacity to significantly improve quality.

This study aims to analyze the potential risks that may arise in multi-server Internet of Things (IoT) environments throughout the communication process.

In Section 2, we illustrate the potential security risks that might arise in a distributed computing environment with several servers in the context of the Internet of Things (IoT). In this section, we provide a comprehensive analysis of several safe authentication techniques used in multi-server Internet of Things (IoT) systems. In Section 4, the attacks that may occur in the aforementioned protocols are outlined, along with proposed strategies to mitigate the risk of such assaults. The findings are presented in Section 5.

2. Security Threats

Cloud-IoT-based scenarios encounter a comparable array of risks akin to those encountered by conventional networks. Due to the substantial volume of data stored on cloud servers, cloud service providers become susceptible and enticing targets for potential attackers. Several hazards and attacks arise from diverse chemicals, each with their own adversary models.

(a) Eavesdropping assault refers to the illicit interception of communication between two entities. Instances of such attacks may occur when the cloud service provider accesses the data stored on the server for administrative purposes. These attacks

ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

pose a significant concern because to their elusive nature, as well as the inadvertent disclosure of sensitive information, such as passwords, by clients who save them on the server.

(a) Integrity assault: An instance of information trustworthiness assault occurs when an assailant deliberately seeks to compromise or manipulate data without the owner's consent. The attack is often executed via the use of a malware software that deletes or modifies the content of an intelligent device.

(c) Denial of service attack: In this kind of attack, one of the communicating parties refuses to fulfill all or a portion of the transmission obligations.

The denial of service attack occurs when a cloud server becomes inundated with a large volume of administrative requests that exceed its capacity to handle. The occurrence of a server crash might result in the denial of access to administrative privileges for authenticated clients.

The cloud server compromise attack refers to the unauthorized acquisition of control over a server by an attacker subsequent to the system configuration process. An attacker has the capability to establish a connection with a server, enabling them to gain complete control over it. This control may be used to access data or manipulate the server and its subsequent communication.

The phenomenon of replay attack occurs when a malicious entity intercepts and observes the ongoing communication between two parties. The spiteful entity collects authenticated information, such as a shared session key, and then attempts to establish communication with the recipient using such key at a later time. The perpetrator just rebroadcast the intercepted communication.

Impersonation attack refers to a kind of aggression when the perpetrator seeks to imitate a legitimate entity or substance, with the intention of engaging in communication with another entity while seeming to be real.

In instances of stolen verifier attack, the perpetrator successfully acquires essential information from a server, either via ongoing or previously established connections. The perpetrator has the ability to use the pilfered data in order to get access to the information stored on the server.

(i) Insider assault refers to incidents in which the perpetrator is a trusted individual who has been granted authorized access to the system and has comprehensive knowledge of its underlying architecture. These attacks are perpetrated with the intention of carrying out fraudulent activities, such as theft of confidential information or intellectual property.

A man-in-the-middle attack occurs when an attacker is able to covertly intercept and manipulate the communication taking place between two entities who believe they are engaged in direct communication with one other.

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

ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

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:

$$Bi = h(PIDi||\, x)$$
$$Ni1 = Bi \oplus Fi$$

ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

IDi = CIDi⊕h(Bi || Ni1 || TS i|| ”00”)

S IDj = Li ⊕h(BSj|| Ni2 ||TSi|| ”11”)

Pi j = h(Bi ⊕ 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 ⊕h(Bi || Ni1 ||TSi|| ”11”)

d = Mi ⊕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 ⊕ Ni3 ⊕h(SIDj|| Ni2 ||BSj)

Qi = h(Ni1 ⊕ Ni3)

Ri = Ni2 ⊕ Ni3 ⊕h(IDi || Ni1 || Bi)

Vi = h(Ni2 ⊕ 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 ⊕ Ni3 = Pi ⊕h(SIDj|| Ni2 ||BSj)

Qi = h(Ni1 ⊕ Ni3).

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 ⊕ Ni3 = Ri ⊕ h(IDi||Ni1||Bi)

Vi* = h(Ni2 ⊕ 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}, $<ID_{MP}, PW_{MP},B_{MP}> \longrightarrow$	

Generates random Y_{MP},
Computes,
BIO_{MP},=h(B_{MP})
T_{MP}=H($ID_{MP}||PW_{MP}||BIO_{MP}||\oplus$H(X)
R_{MP}= H($ID_{MP}||PW_{MP}||BIO_{MP}||\oplus$H($Y_{MP}$)
$S_{MP}=Y_{MP} \oplus ID_{MP} \oplus PW_{MP} \oplus BIO_{MP}$

$<T_{MP}, R_{MP}, S_{MP}>$ $\longleftarrow$

Stores T_{MP}, R_{MP},S_{MP} into smart card
Computes,
D_{MP} = H(H($ID_{MP}||Y_{MP}$) $\oplus$ X)
Stores,
D_{MP} , $Y_{MP} \oplus$ X, $ID_{MP} \oplus$ 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}
$Y'_{MP} = S_{MP} \oplus ID'_{MP} \oplus PW'_{MP} \oplus$MP,$BIO'_{MP}$
R'_{MP}= H($ID'_{MP} \oplus PW'_{MP} \oplus BIO'_{MP}$) $\oplus$H(Y'_{MP})
Checks if R'_{MP}?=R_{MP}
Computes,
H(X) = $S_{MP} \oplus$ H($ID_{MP}||PW_{MP}||BIO_{MP}$)
MID = H($ID_{MP}||Y_{MP} \oplus$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,$T_1>$ $\longrightarrow$
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

ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

Otherwise, computes:
$D'_{MP} = H(MID \oplus H(X) \oplus X)$
Checks if $D'_{MP} = D_{MP}$?
If fails, the process is terminated
Otherwise, computes
$Z'_{MP} = H(ID_{MP} \| H(X) \| Y_{MP}$
$\beta' = H(Z'_{MP} \| T_1)$
Checks if $\beta' = \beta$?
Decrypts A using Z'_{MP}, i.e.,
$Dz_{MP}\{Ez_{MP}(A)\}$ to extract A
Computes:
$C = A \times X_{cs}, L = H(A \| T_2)$
Generates random u
$Y^{cs} = H(c\|u\|Z'_{MP}\| T_2)$

$< Y_{cs}, u, L, T_2 > \longrightarrow$

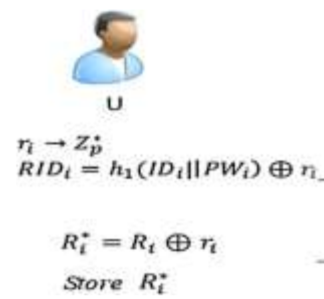
If($T_2 - T_{curr}) <= \Delta T$?
If fails, rejects the message
otherwise, computes
$L^{`} = L$?
If fails, process terminates
$Y^{`cs} = H(c\|u\|Z_{MP}\| T_2)$
If $Y^{`cs} = Y^{cs}$?
If fails, rejects the message
Otherwise, computes
Session key

Computes session key
$S_k = H(H(X) \| Z'_{MP} \|c\|u)$

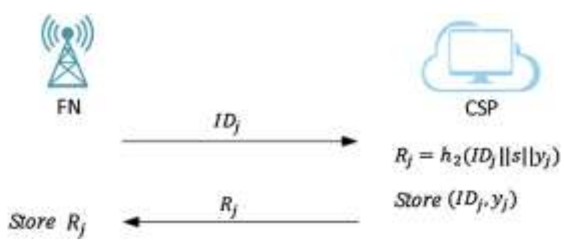
Session key is computed as : $S_k = H(H(X)\|Z_{MP}\|c\|u)$

iii) Jia et.al. Scheme:

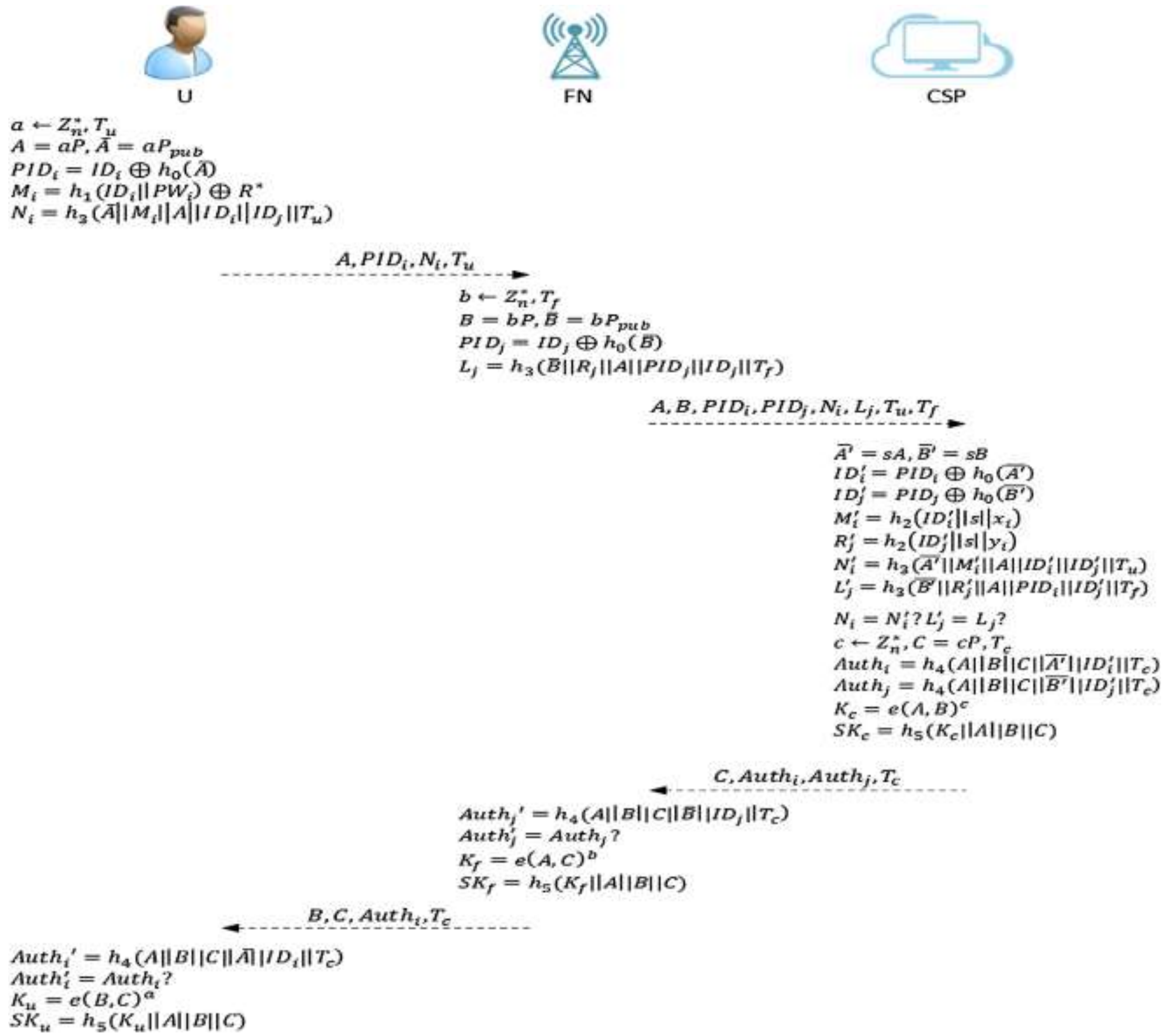
User registration phase



Fog registration phase



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.

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:

ISSN: 2278-4632
Vol-12 Issue-01 No.01 January 2022

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 article presents an overview of the validation process in cloud-based Internet of Things (IoT) environments, as well as the associated research issues. A diverse array of literary works were shown. The current study was conducted to get a comprehensive understanding of the challenges and concerns related to the security of Internet of Things (IoT) environments. As shown by the aforementioned written research, it is evident that security in the Internet of Things (IoT) is a significant concern as it becomes a tangible reality. In this context, it is essential to design an Internet of Things (IoT) security architecture that aims to enhance authentication and authorization processes in order to provide improved security benefits. In the event that the authentication system is enhanced and fortified, it will effectively mitigate various security risks and challenges, such as eavesdropping, impersonation and replay attacks, mutual authentication, and data integrity concerns. Furthermore, it is essential that the validation systems exhibit both expeditiousness and a minimal resource burden, while maintaining a high level of security. The present study presents a detailed analysis of the existing patterns of attacks and provides recommendations for mitigating potential attacks. The suggested research presents a recommended methodology for designing a verification scheme that is resilient to the aforementioned attacks and security concerns.

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