A Middleware Approach for Authenticate user on IoT Devices Accessibility

Ms. Nidhi Dandotiya[1], Dr. Pallavi Khatri[2]
[1,2]Department of Computer Science And Application, ITM University, Gwalior
*** Corresponding author's Email:nidhi.birthare28@gmail.com**

Abstract:

As per current networking style large number of heterogeneous or homogeneous devices are connected over the internet. This proposed middle ware approach is helpful to stop all existing attacks to improve security aspects while getting connected with the IOT devices to maintain secure concurrent connectivity. Hashing plus encryption/decryption SHA 256, Device IP, ID and SDK are the main helpful component parameters to set a secure connectivity with all respective IOT devices. Efficiency also gets improved to simulate data movement performance among the devices.

Keywords: Hashing,IoT security, authentication, IoT Devices, authorization

DOINumber:10.14704/nq.2022.20.11.NQ66796 **NeuroQuantology2022;20(11):8029-8040**

1.Introduction

The network is the back bone connectivity among the various IOT devices those has actuators and sensors as well as embedded and distributed to establish secureconnection capabilities to make their task flow efficiently with significant influence on day-to-day life. As a result, in the coming years, cities population increasing timely so smart connectivity among the peoples and all facilities are the basic need of coming years to achieve effective living style the Internet of Things (IoT) is one of the most promising technologies for satisfying modern society's growing demands for standardization and modernization. The IoT is a network that connects several communication devices and allows them to communicate data without human intervention [1]. In the field of IoT, a lot of work has been done. The fundamental idea behind IoT deployment is to make network accessible to anybody, everywhere, at any time. The IoT communication protocols provide optimum security for the information that is transferred among linked IOT devices. This is the huge concern of the researchers, who are looking for a way to make data flow between devices safer and more authentic. The Internet of Things is expected to have 75 billion connected devices by 2025 [2]. In recent years, there has been a lot of research and development on the Internet of Things (IoT). Smart home appliances, smart road traffic management, smart security, and smart weather prediction systems are examples of IoT use cases. The Internet of Things (IoT) network is more intricate and expansive, encompassing RFID systems, sensor gadgets, and smart mobile phones, among other things. The layered architecture of IoT system designed with three layer and five-layer architecture as discussed in [3] and [4]. The layered architecture of IoT system is shown in figure 1.1

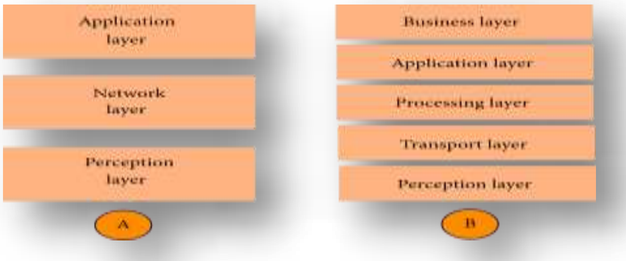


Figure 1.1: Layered Architecture of IoT

The identification of a specific object in this interconnected network of "smart objects" is a fundamental hurdle that affects all other operations of the system, including governance, confidentiality of data, access control, general design, and so on. The whole IoT system, from manufacturers to consumers, still faces several security concerns as in [5] our approach is to provide end to end secure connectivity with efficient data transmission among the devices:

- Insufficiency of Compliance on the part of IoT Manufacturers,
- Lack of User Knowledge and Awareness,
- IoT Security issues in Device Update Management,
- A scarcity of Physical Hardening

Its applications include smart city and industrial deployments. smart home, automation, healthcare, emergency response and transportation, [1]. The IoT network connectevery digital device to the internet thereby opening new and diverse area for applications and services.

Each device connected to internet and transmitting data over network is prone to adversarial attack. The Attack vectors in IoT are yet to be secured completely and are thus vulnerable to variety of cyber-attacks.For ensuring the long-term survival of the IoT all vulnerabilities must be addressed. There are numerous security challenges like object identification and locating device in IoT network, Authorization and Access control of IoT devices, authentication and identity management of IoT devices, detecting software and backdoor vulnerabilities, developing lightweight cryptosystem and security protocols, ensuring data privacy and integrity, finding efficient solutions for massive heterogeneous data in IoT [1][2][3][4][5][6].

The Internet of Things ecosystem should be capable of networking a large number of diverse items. As a result, layered architecture must be flexible and adaptable. Every layer in the IoT is characterised by the functions and applications that it employs. In the IoT, there are differing viewpoints on the no. of levels. [4][5] Offered a three-layered architecture, as seen in figure 1, which was taken into account for this investigation.

All 3 layer of IoT architecture are vulnerable to varied kinds of attacks like Denial of Service (DoS), Man-in-the-Middle (MITM), Eavesdropping/sniffing, Routing attacks that are being identified by the researches in the past [6] [7] [8] [9] [10] [11].IoT devices have been popular in a variety of fields, including E-Commerce, E-Health, E-Home, and E-Trafficking.
This research proposes an authentication scheme for IoT networks that will prevent many security threats like MITM, XSS and etc. Rest of paper is organised in five sections where section two summarises the work done in past as literature survey, section three discusses the proposed methodology; section four describes the security offered by proposed scheme and is concluded in section five.

2 Literature Survey

Rising use of IoT devices in reality, they may be, and in some instances already are, targets of malicious attacks aimed at compromising their security and privacy. [17] [18] [19]. The most prevalent security risks to IoT devices, as well as top hurdles to tackling safety in smart devices, must also be examined **[20] [21]**. The authentication of heterogeneous network devices is one of the security problems. These gadgets' uniqueness has made it impossible to implement typical security measures developed over the years for IoT applications.However, various lightweight solutions for IoT applications have been offered, but they are inefficient. [22]There are several privacy-preserving authentication techniques for RFID systems [23], and a multi-factor user authentication and key agreement mechanism [24] is presented that is suited to IoT contexts and has a tolerable computational time. Various authentication schemes have been planned by various researchers, including remote user authentication schemes [22], multifactor authentication outlines [25], secure authentication and addressing (SCSAA) schemes [26], behavioural-based authentication procedure [27], and device authentication based on certificates [28]. There was a broad range of literature was presented. Each research was examined to determine the concerns and issues related to IoT security [29] [30] [31].

Table 2.1: Existing Gaps (previous develop mechanism drawback)

Challenges Addressed	Proposed Scheme	Method	Tools
Authentication Protocols relying on RFID are vulnerable to leaks.	Utilizing RFID tags to minimize authentication disclosure attacks	Using the RFID tag AES method to build a 128-bit secret key for encrypting messages	N/A
Due to a growth in the number of devices, it is becoming increasingly tough to carry out an authentication procedure.	Local user authentication scheme uses lightweight technique that is based on NFC technology	three steps constructed on Bluetooth or ZigBee. to authenticate messages, a hash function (such as Chaskey) is used.	-NFC Technology
Pre-defined keys and passwords aren't practical in an IoT network.	Token-based user authentication for IoTdevices is lightweight.	Authentication can be made even more secure by utilising authentication tokens.	N/A
Io devices cannot currently use the current authentication protocols since they are not globally applicable.	Scheme for hardware serialization-based authentication	An integrated microchip generates a unique identifier for each device.	Maxim DS24II
Single-channel authentication is used by MQTT, making it vulnerable.	IoT devices with limited resources can be authenticated using architectural tokens.	For resource-constrained IoT devices, a MQTT broker and server are necessary.	N/A
Weak encryption and slow encryption in IoT	Authentication in the IOT must be robust and secure.	securing and encrypting data with AES and ECC	N/A
In an IoT world, traditional authentication methods are ineffective.An app usage-based behavioural profiling model	An app usage-based behavioural profiling model	Utilize machine learning to discover patterns in the data provided by the user.	PANDA
In an IoT setting, traditional authentication approaches aren't practical enough.	Convenient and light-weight gait authentication system based on subconscious activities	machine learning is used to find trends and authenticate persons by extracting features from the user's phone	Motorola G4 Plus
Cryptographic credentials cannot be loaded into IoT devices that are too small.	Two methods of implementing authentication have emerged. LISA and LISAT	VLC provided by multitouch displays to configure sensor devices. The signals conveyed are detected using a photodiode BPW34 and a 1M resistor.	GSM Module, Arduino Pro Mini, Android Smartphone

Table 2.2: Types of Attacks

Attacks	S0	S1	S2	S3	S4	S5	S6	S7	BW	PW
Impersonation attack	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**
Off-line guessing attack	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**

Masquerade attack	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**
Forward secrecy attack	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**1**	**1**	**1**
MITM attack	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
DOS attack	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Password change attack	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**1**
Anonymity and untraceable Attack	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**1**
Message forgery attack	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**
Replay attack	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**
Device compromise attack	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**
Cross scripting attack	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**

Table 2.3:

References and proposed methodology annotations		
S0	:	[6, 34, 35]
S1	:	[55, 36, 52]
S2	:	[31, 37]
S3	:	[1, 4]
S4	:	[38, 42, 43]
S5	:	[30, 39, 40]
S6	:	[44]
S7	:	[53, 54]
BW	:	Base Work
PW	:	Proposed Work

According to the above-mentioned literature review, security in IoT would be a serious problem once it becomes a reality, as it has been identified as such. IoT security systems must be created to enhance authentication and authorization in order to provide better security services. Many security threats, including as eavesdropping, impersonation, MITM, Dos, and replay attacks, can be prevented if the authentication process is robust and well-established. Furthermore, the authentication systems should be light and rapid without sacrificing security.

3 Proposed Scheme

There are variety of methods explored and proposed by researchers in past to secure the device and algorithms/techniques are proposed to partially detect the attacks in IoT and to prevent the exploitation of IoT devices. The research work in the past has been done for developing schemes for authentication for devices in IoT networks. In similar context,highest work has been done on the physical layer and cloud.

There are lots of attacks that can be done on all the layers of IoT as explained in section 2 and still there is a need for a robust authentication model that can improve the security of IoT network from these attacks. From literature survey, it has been observed that the existing schemes failed to authenticate the devices in case when some new type of attack is launched like cross scripting attack to effect end to end secure connectivity.

This work proposes a generic strategic implemented idea which can be applicable on any kind of device authentication like biometric driven authentication for network layer or application layer that defeats majority of attacks done on this layer of IoT protocol stack. This work proposed a middleware strategic one-time and end to end authentication to establish secure connectivity among the devices with the users for secure data transmission. Thisproposed long-time end to end secure pip lined connectivity to perform data transmission over the network.

Middleware is basically place where devices, user authentication and checksum security logic written because user and device will first hit middleware logic then after crossing the middleware next step will take place for further execution like sync or another task which we would like to perform.

The scheme is divided in to 3 phases that will ensure the security of IoT network.

Phase 1: User Registration

This is the first phase where user is required to register himself with the server with personal credentials. Registration credentials taken in to consideration by proposed system are used identity, password (of user choice as per password policy), and biometric identity of user. The user makes a registration request to the server with these credentials and registration process start as shown in fig. Fig 3.1

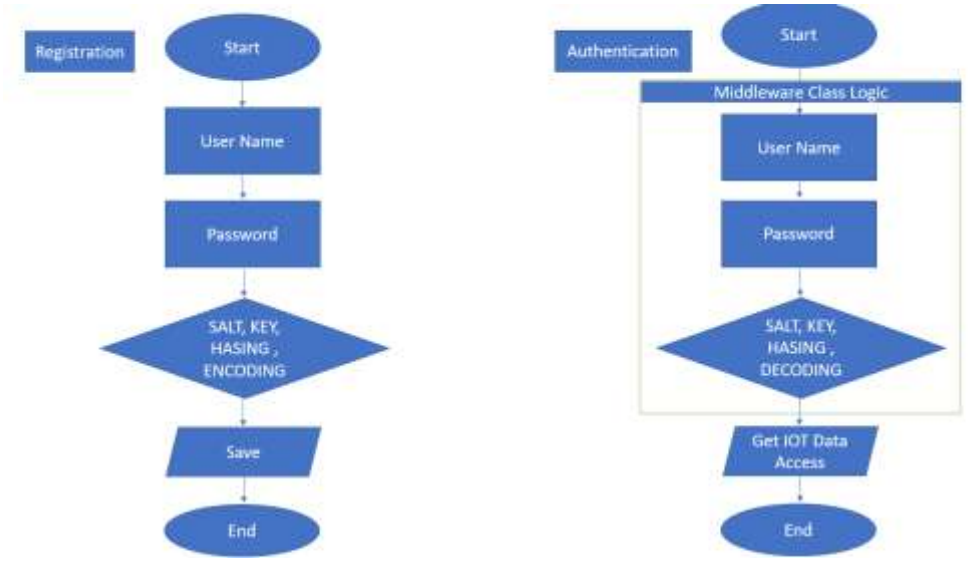


Figure 3.1: User Registration and Middleware pip lined Authentication

Algorithm_User_Registration (User End):

Step 1: Input user identity$\boldsymbol{ID_i}$, User Name UN, Password $\boldsymbol{PWD_i}$ and Biometric $\boldsymbol{BIO_i}$.
Step 2: Input a Random Number $\boldsymbol{R_i}$.(Salt)
Step 3: Compute 3 Hash values using hashing algorithm with $\boldsymbol{R_i}$ (salt) and each input from user.

Step 4: Compute Masked identities $\boldsymbol{MID_i}$, $\boldsymbol{MBIO_i}$ and $\boldsymbol{MPWD_i}$ as given in equations 1,2, and 3.

$\boldsymbol{MIDi = h(Ri \,||\, IDi)}$ **--------(1)**
$\boldsymbol{MBIOi = h(Ri||BIOi)}$**---------(2)**
$\boldsymbol{MPWDi = h(Ri||PWDi)}$**--------(3)**

```
salt = os.urandom(32) # A new salt for this user
key = hashlib.pbkdf2_hmac('sha256', PWDi.encode('utf-8'), salt, 100000)
users[username] = {
   'salt': salt,
   'key': key
}
```

A channel is used to transfer the messages $\boldsymbol{MID_i}$,$\boldsymbol{MBIO_i}$, $\boldsymbol{MPWD_i}$, $\boldsymbol{Ts}$ to the server where $\boldsymbol{Ts}$ is the senders timestamp.

Phase 2: Device Registration

After successful login user can add and register all devices in the home network. The flow of registering a device as shownin fig.3.2

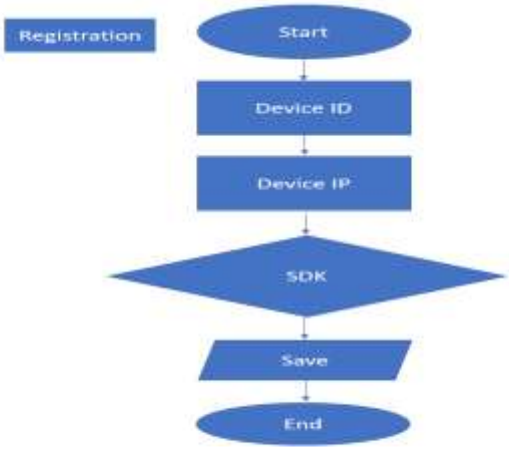


Figure 3.2: Registration of a Device

Algorithm_Device_Registration (User End):

Step 1: User Logins using **UID$_i$**generated in Phase 1 of User Registration
Step 2: Input **Device_ID**, **DeviceIP I** and generate a random number **N$_i$**.
Step 3: Compute Hash values using hashing algorithm with **N$_i$** as given in equation 5.

$ID_D = h(Device\_ID\|R)$**--------------(5)**

A channel is used to transfer **ID$_D$, MBIO$_i$, Device_Type ,Ts** to the server where **Ts** is the sender timestamp.

Phase 3: Login Authentication Phase

In this phase middleware logic has been proposed and applied in the form of authentication pipelined programmatic process to authenticate user with respect to available IOT Devices for their data manipulation and observation

Once the registration of user and device is done user needs to login to access home network with the registered device. User uses UIDi and MID$_D$ which is unique for every user and device. The login procedure is shown in fig 3.3

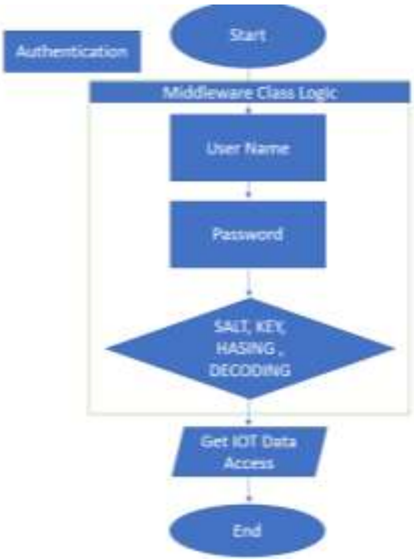


Figure 3.3: Login Authentication

This phase, the login request submits to server by user. To initiate a session following steps are used for user login

Step 1: The user inserts User Id UIDi, password PWDi to identify a user.
Step 2: User application sendUIDiand masked password MPWDi and time stamp Tj to the server.
Step 3: The future server verifies the time stamp (T2-T1) ≤ ΔT if the timestamp is verified then precede otherwise terminate the process. After that server match UID' that sends to the user and UID that is stored in the server user table. If both are matched then processed otherwise discard the login. After verify timestamp and user id server compute

$A = h(UID_j \| N_j \| T_j$**-------(7)**
here UIDj is user id and Nj is random number and Tj is time stamp or
$B = h(MPWD_j \| A \| N_j$ ---------**(8)**
here MPWDj is masked password A that compute before and Nj is random number and then B(OTP) send to user via secure channel.
Step4: User receives B(OTP) and Enter in the application. And now B' send to the server.
Step 5: Server Verify B'=B and Timestamp if both are ok then proceed otherwise discard the login process.
Step 6: Proposed algorithm and middleware logic will work here to process IoT device and user authentication.

Time taken by user registration, IOT Device Mapping and user login has depicted in below table 3.1,After crossing the middleware pipeline all available IOT can be connect and data processing and analysing can be gone through on the same respective IOT devices, as demo image dataanalysedand analytic response shown in figure 3.6 and 3.7 respectably.

Table 3.1 :

Phases		Execution Time second
1	user registration	1.08
2	IOT Device Mapping	1.04
3	User Login	0.06
4	Verification	1.05
5.	IOT image data analysing	18.75

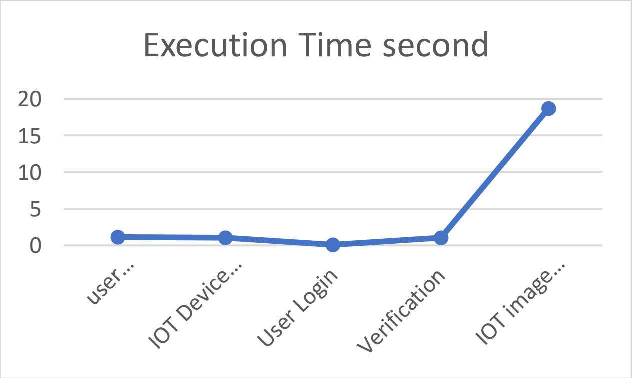


Figure 3.5: Execution Time of all phases

Table 3.2 represent device to device performance, table 3.3 performance of proposed MW strategy Table 3.4 with figure 3.6 represent the performance comparison and

Table 3.2

Method	Encrypt MS	Decrypt MS	Ciphertext Bits	Mutual Auth.(MS)
LMA	29	2	272	1401
Opt. MW.	15	1	136	1050

Table 3.3

Scheme	Encrypt	Decrypt
LMA	(wd + w − d − 1)A + 1S	dA + dM
Opt. MW	wda+1s	A+M

Table 3.4 :

Scheme	Time in Second	
	Security level bits (80)	Security level bits (112)
RSA	23.5	175.56
ECC	6.16	16.6
LMA	1.401	1.96
Our Opt. MW Auth.	1.01	1.1

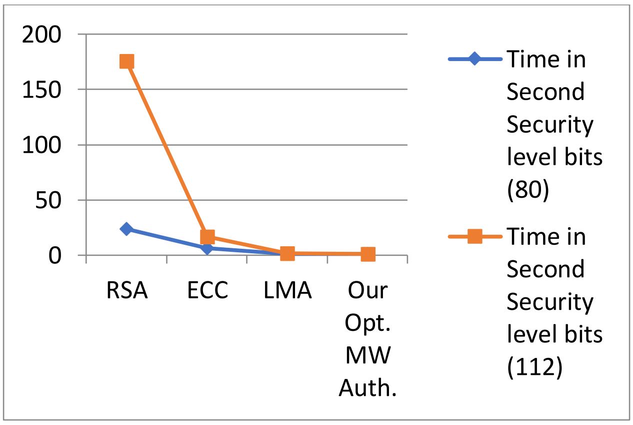
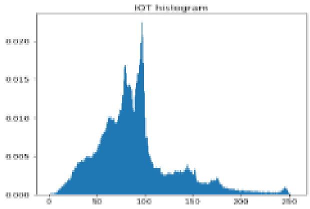
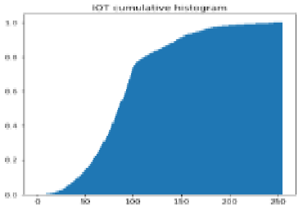


Figure 3.6: Performance comparison with ECC , RSA and LMA





1. As IOT device get connected through network, proposed model starts their functioning to get connected with the device or manual efforts would also be putted to make device in network connectivity range.

2. After above step our proposed model will verify device and device user on the basis of told parameter UID, PWD, Device IP, Device ID, SDK (Every device gets connected by their own SDK

which is shown as SDK 1 to SDK N)section after device verification.

3. N number of IOT Device and user authentication can be perform by above of proposed middleware architecture with steps execution

4. Evaluation Metrics–

Evaluation matrixes that will be used to evaluate the performance of the proposed scheme are

4.1 Average Response time -Average response time is basically a device response over the time stamp of device authentication where user connection gets reduced because number of layers get reduces by single middle ware architecture.

4.2 Energy consumption -Energy consumption in every phase has also get reduced because all phase like Separate device id authentication or separate device IP authentication or respective SDK verification and authentication layer architecture replace by single middle ware architecture.

4.3 Security Achieved - This authentication scheme provide authentication, password protection and is resistance to several attack. The analysis confirm that the proposed scheme is resistant against all the major attack-

a. User Impersonation attack – to become trusted user consider attacker A send illegal login request to home server. The opponent compute identiesIDattacker, PWD and present time stamp. Because the opponent does not have user id UID that why this request fails and if suppose adversary also have UID than at the time of login server send OTP to registered device. The attacker don’t have this device so this attack not possible.

b. Device Impersonation attack- This attack is also not possible because user can access device after successful login as user impersonation attack is not possible that why this scheme is also safe from this attack.

c. Replay Attack - Accept that the attacker interrupted the conveyed message <UIDj, MPWDj, Tj> either during login phase and with the login request message attacker starts a new session <UIDj’, MPWDj’, Tj’>. Then the process will terminate because the proposed scheme verify the timestamp during every transmission.

d. MIM Attack – Accept that the attacker interrupts the conveyed message <UIDj, MPWDj, Tj> during the login phase and <B> the attacker can modifies the login request message during the authentication <UIDj’, MPWDj’, Tj’> the attacker can only login in the home network but at the time of sending request to IoT device attacker need MID$_D$ the probability of knowing thid MID is very low.

e. DoS attack – The user is secure against DoS attack in this proposed scheme. This is possible because the user obtains an acknowledgment or denial message from the node that lets them know that the response message was genuine by inserting received OTP. Also, the use of timestamps in the schema mitigates all important demands accordingly. The planned outline is resistant to DoS attacks.

f. **Password change attack security**- An attacker cannot alter a user's password by impersonating a valid user's personal biometric data. Change the password even if the attacker logs in to the smart device. An outdated password is required. Even the attacker may get access to the smart device and retrieve the confidential data it contains. From the available data, it is still difficult to deduce the PWD password and BIO biometric information. As a result, the proposal is secure against password change attacks.

g. XSS Attack- XSS is a web vulnerability that allows an attacker to inject harmful code into a link that would otherwise be innocuous. When you click the link, the innocent request as well as the malicious script is sent to the genuine website. The website responds to the original request with the attacker's script, which, since it originates from a trusted source, is run by the local web browser. A successful XSS attack causes no user notifications and may consequence in online account takeover, session theft, browser remote control, or redirection to malicious sites. However, the influence does not stop there. Although certain anti-XSS methods have been included in some add-ons and web browsers, they do not deliver total protection against this sort of vulnerability. Patching XSS

vulnerabilities is ultimately a work for web developers who create websites & online apps. XSS is still popular, despite the fact that it has been available for a decade.IoT gadgets NAS, routers, DVR systems, IP cameras, and smart home hubs are just a handful of the linked devices that might be vulnerable to XSS issues. Installing the most recent firmware version is frequently a solid security standard in the IoT sector.

4.4 Cost of Communication: According to the literature, the number of communications during authentication varies and depends on protocols used. In addition, establishing communication will necessitate several stages and a predetermined number of messages. At least four messages were involved in the authentication process, such as those sent from sensors to central nodes to create a secure communication channel between sensors and the user or the central node[30,41,42,43,44,45].To make matters more complicated, the number of communication channels varies and the information conveyed by each channel differs. As a result, communication costs must be considered, since different standards have different threshold values. IEEE 802.15.4, for example, has a maximum of 127 bytes for its networking protocol. IEEE 802.15.6, on the other hand, has a maximum frame length of 255 bytes.

4.5 Cost of Computation: Protocols within the IoT also play a role in computation. Computing large amounts of data or information from IoT networks is not possible due to the computational limitations of the vast majority of network devices. As a result, IoT network authentication protocols are being designed to be as light as possible by protocol architects. As a result, researchers have used the principles of hash, XOR, and concatenation [33,46] to safeguard messages travelling across networks. ECC-based and Fuzzy extractors are also used to authenticate the identity of IoT devices in IoT network.

4.6 Cost of Storage/Memory: To implement IoT authentication, protocols use a variety of different types of schemes. A smart card is a common approach. Various types of data can be stored on a smart card, including sensor data, login credentials, and details about the gateway node itself[47,48]. The cost of storage/memory is a significant performance metric used by various protocols in order to achieve authentication, among others.

5 Conclusions –

When it comes to reality, IoT security is a huge concern. As a result, IoT security systems must be created to improve authentication in order to provide better security services. Many security concerns, such as eavesdropping, impersonation, MITM and Dos, replay attack, and so on, may be avoided if the authentication method is solid and well-established. Furthermore, without jeopardising security, authentication techniques should be quick and light..In this paper, we propose an authentication model

which enhances security of the internet of things network from attacks. The proposed scheme takes into account the middleware architecture. Pre-Initiative with the user and the device before reaching or failing to cross the proposed middleware logic. This work secures an IOT device with an unauthorized user. in this research, we provide the first three-step of the proposed scheme and also provide the different aspects in which our scheme gets evaluated. In Future use plan of this research is to generate all phase of this scheme and implement it.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. (Yadav et al. 2018), “IoT: Challenges and Issues in Indian Perspective”, IEEE,3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU),2018
2. (Goyal et al. 2020), “Internet of Things: Applications, security, and privacy: A survey”, Materials Today: Proceedings 34 Elsevier, May 2020
3. (Rachit et al. 2021), “Security trends in Internet of Things: a survey”, SN Applied Sciences volume 3, Article number: 121 (2021)
4. (Tabassum et al. 2019),” Security Issues and Challenges in IoT”, International Conference on Computer and Information Sciences (ICCIS), 2019
5. (Zamfir et al. 2016),”A Security Analysis on Standard IoT Protocols”, IEEE International Conference on Applied and Theoretical Electricity (ICATE),2016
6. (Frustaci, et al. 2018),”Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”, IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 4, AUGUST 2018
7. (Airehrour et al. 2016), “Securing RPL routing protocol from blackhole attacks using a trust-based mechanism”. 26th International Telecommunication Networks and Applications Conference (ITNAC), Dunedin, New Zealand, 7–9 December 2016.
8. (Glissa, G. et al. 2016), “A Secure Routing Protocol Based on RPL for Internet of Things.”

IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016.

9. Mukherjee, A. “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints”. Proc. IEEE, 103, 1747–1761, 2015
10. (Gurung, et al. 2017), “Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET”. Wirel. Netw., 25, 1–14,2017
11. (Xiaopeng, G. et al. 2007), “A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”. IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007), Liaoning, China, 18–21 September 2007.
12. (Meghdadi, M. et al. 2011),” A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks”. IETE Tech. Rev. 2011, 28, 89.
13. (Diaz, A. et al. 2016), “Simulation of Attacks for Security in Wireless Sensor Network.” Sensors 2016, 16, 1932.
14. (Pathan, A. et al. 2006), “Security in wireless sensor networks: Issues and challenges”. 8th International Conference Advanced Communication Technology, Phoenix Park, Korea, 20–22 February 2006.
15. (Sharma, S. et al. 2016), “A defensive timestamp approach to detect and mitigate the Sybil attack in vanet”.2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016.
16. (Hari, P.B. et al. 2016), “Security issues in Wireless Sensor Networks: Current research and challenges”. International Conference on Advances in Computing, Communication, &Automation (ICACCA) (Spring), Dehradun, India, 8–9 April 2016.
17. (TejasviAlladi, et al. 2020), “Consumer IoT: Security Vulnerability Case Studies and Solutions”, Published by the IEEE Consumer Electronics Society, 2020
18. (Reylonet al. 2021) , “IoT: Security Attacks and Countermeasures, Second International Conference on Smart Energy and Communication” , pp 229-238, 05 January 2021(Springer)
19. (Sokolov et al. 2020”, the XIII International Scientific Conference on Architecture and Construction 2020 pp 47-56, (Springer)
20. (Yash Shah et al. 2020), “A survey on Classification of Cyber-attacks on IoT and IIoT devices”, 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),2020
21. (Sadhukhan, et al. 2021), “A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography”.The Journal of Supercomputing volume 77, pages1114–1151(2021)
22. (ManikLal Das et al. 2020), “Secure and Privacy Preserving RFID Authentication Scheme for Internet of Things Applications”, Wireless Personal Communications volume 110, pages339–353 (2020)
23. (Mohammad Nikravan et al. 2019),” A Multi factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things”, Springer Science+Business Media, LLC, part of Springer Nature 2019
24. (Fan Wu et al. 2021), “A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion” , IEEE Systems Journal (Volume: 15, Issue: 1, March 2021)
25. (Pankaj Kumar et al. 2020),” A secure authentication scheme for IoT application in smart home”, Springer Science+Business Media, LLC, part of Springer Nature 2020
26. (YosefAshibani et al. 2021),”Design and evaluation of a user authentication model for IoT networks based on app event patterns”, Cluster Computing volume 24, pages837–850(2021)
27. (Dilip Kumar Sharma et al. 2020), “Multiple Degree Authentication in Sensible Homes based on IoT Device Vulnerability”, International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC) 2020.
28. (Krishna PriyaGurumanapalli et al. 2020), “A Survey on Secured Authentication Schemes over IoT Devices”, International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 3854–3862
29. (Omphulusa Lucia et al.2019),” Device Authentication Schemes in IoT: A Review”, International Multidisciplinary Information Technology and Engineering Conference (IMITEC),2019
30. (R. Shantha et al.2016), “Authentication in IoT Environment: A Survey”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 10, October 2016 ISSN: 2277 128X,2016

31. Azmoodeh A, Dehghantanha A, Choo K-KR (2019) Big data and internet of things security and forensics: challenges and opportunities, pp 1–4
32. Tsai J-L, Lo N-W (2015) A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst J 9(3):805–815
33. Jiang Q, Ma J, Wei F (2016) On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst J 12(2):2039–2042
34. Hussain MM, Beg MS (2019) Using vehicles as fog infrastructures for transportation cyber-physical systems (t-cps): fog computing for vehicular networks. Int J SoftwSciComputIntell 11:47–69
35. 3. Cisco (2013) How many things are currently connected to the internet of things. Forbes
36. Kalra S, Sood SK (2015) Advanced password-based authentication scheme for wireless sensor networks. J InfSecurAppl 20:37–46
37. Tewari A, Gupta B (2020) Security, privacy and trust of different layers in internet-of-things (iots) framework. Future GenerComputSyst 108:909–920
38. He D, Zeadally S, Kumar N, Lee J-H (2016) Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 11(4):2590–2601
39. Sharma G, Kalra S (2018) A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-iot applications. J InfSecurAppl 42:95–106
40. Gope P, Hwang T (2016) A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans Ind Electron 63(11):7124–7132
41. Stergiou C, Psannis KE, Gupta BB, Ishibashi Y (2018) Security, privacy & efficiency of sustainable cloud computing for big data &iot. Sustain Comput: InfSyst 19:174–184
42. Bai TDP, Rabara SA (2015) Design and development of integrated, secured and intelligent architecture for internet of things and cloud computing. In: 2015 3rd International conference on future internet of things and cloud. IEEE, pp 817–822
43. Agrawal M, Zhou J, Chang D (2019) A survey on lightweight authenticated encryption and challenges for securing industrial iot. Peer-to-Peer Netw. Appl. In: Security and privacy trends in the industrial internet of things. Springer, pp 71–94
44. Carpenter B, Jiang S (2014) Significance of ipv6 interface identifiers. IETF RFC
45. Rasti MR (2012) Doing business without ssn, ein, and charge card numbers. US Patent 8,281,145 21. Siddiqui AU, Singh MHK (2015) Aadhar management system. IITM J Manag IT 6(1):40–43
46. Rao M, Newe T, Grout I (2014) Secure hash algorithm-3 (sha-3) implementation on xilinxfpgas, suitable for iot applications. In: 8th International conference on sensing technology (ICST 2014), Liverpool John Moores University, Liverpool, United Kingdom, 2nd–4th September
47. Johnson D, Perkins C, Arkko J et al (2004) Mobility support in ipv6
48. Han Y-H, Hwang S-H (2006) Care-of address provisioning for efficient ipv6 mobility support. ComputCommun 29(9):1422– 1432
49. Quittek J, Zseby T, Claise B, Zander S (2004) Requirements for ip flow information export (ipfix). Technical report, RFC 3917 (informational)
50. Shah JL, Parvez J (2015) Optimizing security and address configuration in ipv6 slaac. ProcediaComputSci 54:177–185
51. Hinden R, Deering S (2006) Ip version 6 addressing architecture. IETF RFC
52. Hinden R, Haberman B (2005) Unique local IPv6 unicast addresses. IETF RFC 4193
53. Gont F et al (2014) A method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration (slaac). IETF RFC 7217
54. 31. Narten T, Draves R, Krishnan S (2001) Privacy extensions for stateless address autoconfiguration in ipv6. Technical report 32. Wang X, Qian H (2015) Dynamic and hierarchical ipv6 address configuration for a mobile ad hoc network. Int J CommunSyst 28(1):127–146
55. (Jing et al. 2014), “Security of the Internet of Things: perspectives and challenges”, Springer Science+Business Media New York 2014
56. Rwan Mahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges, and Prospective Measures, The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)
57. Dr.KahkashanTabassum, Dr Ahmed Ibrahim, Dr Sahar A. El_Rahman, Security Issues and Challenges in IoT, 2019 International Conference on Computer and Information Sciences(ICCIS)