International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 2522–2538

Multifactor Authentication Methods: A Framework For Their Selection And Comparison

Tarun Dhar Diwan
Chhattisgarh Swami Vivekanand, Technical,University
Bhilai,Chhattisgarh, India.
tarunctech@gmail.com

Dr. Siddartha Choubey
Shri Shankaracharya Technical Campus,
Bhilai, Chhattisgarh, India.
sidd25876@gmail.com

Dr. H.S. Hota
Atal Bihari Vajpayee University
Bhilai, Chhattisgarh, India.
proffhota@gmail.com

Abstract

There are various techniques for users to authenticate themselves in software applications. Only minimal effort is required for many kinds of the attacks. In this paper, for mitigating attacks we propose different countermeasures based on the analysis of the possible attacks on the security. For protection against the various authentication attacks on a web applications different ways and methods are proposed in this paper. For variety of different attacks various different mechanisms of authentication is provided. It is an Easy compromising authentication using the method of traditional password authentications. It is very easy to hack through with various different attacks and therefore is not advised or recommendable. we suggest that, to assess the loopholes or weakness the framework of the MFA security should also support a panel of penetration testing. To calculate the risks and danger's external audits are mostly done by the developers in present scenario so as to analyses these external audits and act accordingly for a better planning. The MFA system should work on improving and providing user a secure environment.

Keywords: *security; Authentication; Counteraction; IoT; Vulnerabilities; Attacks; Threats.*

1. INTRODUCTION

The basic goal of multifactor authentication is, to protect the confidentiality, privacy, integrity, reliability, and availability of information on devices that manipulate and store the information. To maintain user accounts services and online transactions identifying one's identity is very useful [1]. To prevent theft of identity authentication is very important. The method of confirming the identity of a person to make sure that he is the same person as he is claiming to be this also comes under authentication. Efficient addressing of authentication is required as a valuable security aspect [2]. Easy compromising of different expect of security like confidentiality, authorization, non-repudiation, availability and auditing may be possible [3]. We have discussed in depth about the different authentication methods. On authentication aspect various attacks on security is the main focus of this paper Threats, Attacks and Vulnerabilities are three different things and it is very important to understand the difference between these three. Potential danger that may take place is called Threat [4]. For a future attack that is on its way it provides a signal for that attack. To an asset the incessant danger is represented by a Threat. Some of the Threats may not lead to damage and few of them may or may not be intentional too. room for an attacker is given by a

ISSN: 2233-7857 IJFGCN

Threat. To an asset that is unauthorized, preventing its access or gaining its access, misusing vulnerabilities and modification or destruction by any malicious activity is an Attack [5]. Attack in most cases does damage to assets and exploits vulnerabilities and is done quite intentionally. Any loopholes or weaknesses in systems that results to threats is called Vulnerability. If a hostile challenge is unable to be defeated [6]. A damage done to an asset attacker uses exploit as a weapon. Example of these situations is, "when antivirus is not updated continuously, system may be affected by some virus and cause damage to the server". Vulnerabilities is also absence of updating antivirus, the threats are caused by viruses and the one that leads to damage is called attack [7].

2.LITERATURE REVIEW

Taxonomy of Authentication overview methods, challenges, problem identification & suggestion.

In this paper, different authentication methods, challenges, problem and its countermeasure have been provided.

2.1 Internet of things (IoT) Device Authentication.

There are so many classifications of IoT devices that is required to be talked about in such small length paper but on the basis of security level they may vary in most of the cases [8]. Few of them uses proximity-based protocols like Radio Frequency Identification or RFDI, Bluetooth, Wi-Fi, Hardwire, GPS, 4G or 5G for connection.

Identification and prevention of weak security to uncertified devices for access when added along with IoT application for monitoring infrastructure and in IoT devices, a level of trust can be maintained through Digital Certificate that in other cases will be lacking behind [9].

Countermeasure: As easy as searching for any nearby device is connecting them, with the help of multi-factor authentication or by entering a short code for permission of recipient and authentication to different devices. Actually, there is no blockchain vs. PKI argument, but should be mention because of its importance [10]. Enhancement in PKI using block chain use of decentralized ledger and ensuring audit ability of digital cert management and irreversibility of any made changes. By digital cert provider perceiving as an initiative that is financially motivated PKI for the IoT cloud if no decentralization takes place [11]. to manage authentication is the prime concern.

2.2 An IoT System Actually Work.

IOT has much high value then just as a connected device, a dedicated and organized infrastructure is required ideally, that traditionally means to have four different stages through which path the data is reflected when it travels to final analysis from IOT devices [12]. In each of these four stages data processing can take place. These are the following stages-

a. Internet Gateways – Collection and conversion of Analog sensor to digital, then to the selected protocol it is streamed whether it is wired LAN, Wi-Fi or Internet. This permits the entire data to be moved for processing as real time analysis is data intensive [13]. For every IOT devices assume it as a preprocessed aggregation stage. The IOT hub is an example where data of device is sent to cloud.

b. The sensor or actuator – This can be understood using an example when a predetermined temperature is attained, performance of physical activity like opening and closing a valve by an actuator and to look after the temperature of water such data might be collected by a sensor [14].

c. The Data Center or Cloud – To the on-premise network the created report is sent and for left out data detailed analysis is possible. When there is Off-site occurrence of the data-intensive analysis and processing, the onsite lack of network bandwidth is not worried by the IT team [15].

d. Edge IT – Before the data is transferred to the data center additional analysis is executed by an intermediary stage. It ensures at data center that data bandwidth is not crossed and to decrease the traffic at the data center. An example of this is, only the data that is used to continue further action is required it doesn't need all data from all devices [16].

2.3 IOT Authentication Methods. The aim of IOT security is decided by two factors whether it needs SSO (single sign-on) for convenience or authentication is sufficient. To manage all devices using IOT, one might have specified needs for the quality of service that needs the use of an MQTT client. Message Queuing Telemetry Transport or MQTT is the protocol that is used by IOT devices possibly and is a messaging protocol [17].

ISSN: 2233-7857 IJFGCN

Countermeasure: For the security of IOT devices the IOT Authentication method is essential and there is various different way to do so. Dedicate IOT network may be assigned for some in which beneficial features are removed for the sack of security [18]. Integrating everything in such a way that security is kept in mind is also possible but one needs to be sure that the devices are made with security design.

2.4 Authentication and Machine Learning.

More than any of the intricate mechanisms and technology our brain is much highly complicated. For analysis and observation of human nature or behavior machines are getting highly advanced [19].

Countermeasure: For the betterment of other authentication process it can make a remarkable significance. Identification of actual owner of the device will be very hard especially if a situation of danger to erase or shut down itself arises [20]. As the present technology keeps on developing and this comes with an increased risk of getting hacked. There are different kinds of hackers and various methods to secure our data.

2.5 Passwords.

Password are one of the most well-known and widespread way of authentication. For a long duration password are used in our daily life's. As we need to create many different passwords not only one. Hence, password authentication becomes more and more complicated [21]. At least 26 different applications and websites are used by an average person on a daily bases that needs passwords. Websites and passwords become one of the favorite interest of programmers, in a data breach like the one that happened to 168 million users.

Countermeasure: In today's generation with the main focus of stealing data more and more malware programs are designed. using passwords that are long enough to provide reliable password and includes different letters, numbers characters, symbols and information's are used [22].

2.6. Two-Factor Authentication.

An additional security layer is allowed by various different services despite having the password by the help of Two-Factor authentication. It can perform the function like providing OTP to your mobile or code generator on your device [23]. Hackers try to hack Password and OTP, which is possible nowadays by producing similar code on external device.

Countermeasure: Nowadays creation of many malware (like trojan), sim swap attack technique to steal your smartphones database with all the passwords and OTP [24]. to avoid using SMS Messages for two-factor authentication there are number of authentication apps that provide similar service even though SMS message are vulnerable. best of all is to use non-SMS based MFA tools [25].

2.7. Captcha based Authentication.

The actual focus is to verify whether you are robot or not. There are few tasks that users have to perform that robots are unable to perform. In these tasks the users are provided with different images we know that robots are able to identify images with the help of source code, hence the robots will be unable to understand the messages that the images are providing [26].

There are different types of captcha as followed:

a. 3D super captchas - In this 3D super captchas user needs to identify an image but that image is provided in 3D.

b. "I'm not a robot" captchas - In this user is asked to check a box.

c. Marketing captchas - In this the user is asked to type a specific brand associated phrases or words [27].

d. Math captchas - In this user is asked to solve a very basic mathematics related task [28].

2.8. Biometric Authentication

Unique biological characteristics is used in the process of security in verification of a person whether the person being verified is the same person that he is trying to be or not. In database user's biometric details are captured and stored [29]. The biggest advantage or plus point of this is user doesn't need to remember it hence one can never lose it.

Biometric Authentication types

a. Face recognition - In this technology user's face scanned and recognized.

b. Iris recognition- Iris is the circular structure area that surrounds eyes pupil and its pattern is always unique and differs from person to person therefore, it is use in the process of authentication [30].

ISSN: 2233-7857 IJFGCN

c. Finger vein recognition- This is commonly used in wide range of devices and serves as the most common method of authentication.
d. Finger scanning- This is similar to ink and paper fingerprint method in the process of authentication. As a Touch ID these ways of authentication is also found [31].
e. Voice recognition- Speakers shape of mouth and throat created special characteristics and these are the key factor for this authentication process [32].

Countermeasure: One of the biggest problems of biometric data is that it is very hard to be used online. Remote analysis and checking of biometric data are very difficult. As some or the other devices like fingerprint scanner and cameras are used for analysis of biometric data and online it is not possible [33]. there is high possibility of biometric data to be theft and can be very dangerous, if these biometric data are not securely stored. cryptographically changing the biometric data is not possible. In simple words this means that the hashing this data is not possible [34]. The key point is that none of the biometric can be same.

2.9 Public and Private Key Authentication.

For asymmetric cryptography such type of authentication is a key feature. In systems like Bitcoin it is generally used but in the authentication system pairs of private and public key is very easily found [35]. on the device user's private data is saved and on the service servers the public one could be saved and uploaded. Hence, one will be successful to use same pair of keys for different services [36].

Countermeasure: Slow public key encryption and complete messages of a user can be read by the attacker if he gets the private keys of the user in public key cryptography private and public key can be generated using DSA, RSA and ECC algorithms. The messages confidentiality is given by this. It is also be useful for digital signatures [37].

2.10 The Bottom-Line Authentication

Password is considered as one of the best methods of authentication by most of the researchers considering all the above-mentioned information and all the method of authentication. it is really a hard challenge to recognize the last user without knowing the password and it is a time consuming and costly process [38]. Another huge problem is password resetting and also with the help of many server it is very easy to abuse it.

Countermeasure: There are millions of user accounts in the internet in such a situation also only few easy entry centers are need by a skilled hacker to crack the account and this can easily lead to an impactful loss [39]. With the help of Face recognition, Iris recognition, Finger vein recognition, voice recognition, Finger scanner, Identification card, etc. Efficiency and protection of passwords can be increased significantly [40]. For security of sites and administration of passwords the policies are required to be created by network administrator, and as a result to is very important for the user to understand such policies.

2.11. Conventional Password Authentication

It is very easy to hack through the methods of traditional password authentications; it is at a very high risk and therefore one should probably not use them. Spoofed login, keyloggers, phishing attacks and shoulder surfing attack is highly vulnerable [41]. The conventional password –

a. In between two successive key presses the time taken.
b. during a key press and release the time taken.

Countermeasure: No extra hardware is required, usage is easy, no specialized person needed, easy memorization and this scheme is very simple. It creates two mathematical related keys private key and public key using these private and public keys the messages might be encrypted or with the help of public and private key it can be decrypted too [1,5].

1.12 Keystroke Dynamics Authentication

The technique of authentication which uses the time difference between the key pressed and in the keyboard rhythmic typing by the users are the biometric solutions in keystroke dynamics. because of the user's different typing speed there is high occurrence of rejections. even the actual user's recognition is also very tricky [8,13].

ISSN: 2233-7857 IJFGCN

Countermeasure: Programming skill is alone satisfying and doesn't requires any additional hardware. spoofed login, keyloggers, phishing attacks and shoulder surfing attack are all prevented [23]. no access can be gained by the hackers even after knowing the password.

1.13 Click Pattern Authentication: -

Instead of text-based passwords a strong password is given by the click pattern. the varying symbol combination and various colors are contained in the click area. in this along with the click pattern there is maintenance of click rhythm of the user [16]. because of the user's varying mental levels, it may cause large number of rejections.

Countermeasure: Extra hardware is required and spoofed login, keyloggers, phishing attacks, shoulder surfing attack, etc. are prevented. even when the password is known it is difficult to hack through [19].

1.14 Graphical Authentication: -

Selection is need by the user for the displayed graphical object. With the help of touch pad, mouse or touch screen the object being selected is drawn [24]. Objects preprocessing runs by the system and transformed into hierarchical form. only if on the touch sensitive screen, a proper sketch is drawn by the user it is approved in the system authentication. How well is the sketch drawn by the user decide the processing time.

Countermeasure: - Additional features like call to mobile for OTP or SMS to mobile is needed. An OTP might be of a type random challenge-response. by the prover promotion of a nonce. By a list of passwords,a creation of an OTP is possible. Graphic based password is an option for a text-based password but is not included sufficiently by companies like finance and banking companies where they widely use text-based passwords [41].

1.15 Biometrics Authentication

A system of authentication in which recognition of face, speech, iris, fingerprint, signature verification, retina is use against original specimens for verification and it is image based [27].

Countermeasure: Hard to implement, costly, consumes time, can be compromised easily and is not a method that is matured completely. Unique and real signature can never be theft this is an important advantage of this method. Image classification is done only when the image is preprocessed [31].

1.16. Digital Signatures Authentication

The document integrity is proved by the mathematical way of Digital signatures. Whether the document is altered during transit can be confirmed by the recipient using this. The security aspects authentication, integrity and non-repudiation are provided. using the private key, the message might be encrypted by the sender and the recipient might be using public key to decrypt the message [35]. Only the specified recipient can decrypt the message and this is known by the sender that the information about the private key is only known to that particular person.

Countermeasure: The document which at first is hashed and with the use of the sender’s private key it is encrypted afterwards and then to the original document it is appended to a digital signature. On the other hand, using the public key the recipient decrypts the document hence he has the confirmed knowledge about the specific sender [14]. Then the recipient hashes the document and with the actual hash verifies it. Now the identification of the sender is done by the verifier or the recipient and consecutively gets assure about the modification done to the messages [11].

1.17 Authentication Panel

In place of clicking the same button for the password in this password scheme, user is supposed to click in the panel at the specific location on the words of Identification [32].

Countermeasure: By updating the not so strong component on the regular basis rectification of vulnerabilities can be done. dictionary, brute force and video recording attacks can be prevented.no additional hardware is required and it is faster [36].

Table 1. Attacks Comparative Analysis, Counter Action, Authentication Mechanism, advantages, impact.

ISSN: 2233-7857 IJFGCN

Attack	Counter Action	Authentication Mechanism	Advantages	Impact
Brute Force Attacks	Tarpitting	Biometric	Unique	Data gets changed
	IDS	Honeypot	Simplicity	Risk
	Test Human	CAPTCHA	Avoids bots	Difficult to read
Eavesdropping	Encryption	SSL	Secured Online	Costly
	Token-based CAS	Ruby CAS, SecurID	Single-Sign on	Less control over navigation control
	Authentication Protocols	Kerberos	Single-Sign on, mutual authentication	Migrating users to Kerberos database is difficult
Phishing Attacks	Mutual Authentication	Digital Certificates	Protects from Impostor	Vendor support, algorithm strength
	Avoid download from unreliable source	Digital Signatures	Non-repudiation, prevents imposter	Compatibility, cost
	Check for Padlock icon	HTTPS	Confidentiality	Performance
Session Hijacking	SSL with Cookie management	Shibboleth	ACL defined easily	change - restart web server
	Secure Protocol	Kerberos	Never sent across	Replay attack
	Encryption	Cryptography	Privacy & safe	Consumes time
Man-in-the Middle Attack	Encryption	SSL	Confidentiality	Performance
	Mutual Trust	CA – Certificates	Speed & Security	Expired & Cost
	Hashing	HMAC	No need of SSL	Inconsistent
Keylogger Attack	Virtual Keyboard	Microsoft OSK	save cost, space	slow typing
	OTP	SafeNet OTP	security	Spoofable
	Anti-logger	Zemana, Sandboxie	Avoid keyloggers	cost & maintenance
SQL Injection Attack	Update regularly	Proper Validation	Defines input	Time consuming
		Access Control strictly defined	Protects from Intruders	compromised if rights elevated
Shoulder surfing attacks	Confuse the attacker	Including wrong information	safe from social engg. Attack	Simple
Malicious Code Attack	Update regularly	Enable auto-update	Auto management	can be compromised
Replay Attacks	Dynamic unique data such as Time Stamp, OTP, Nonce	OTP/NONCE SSL	OTP - Two factor authentication	OTP - dependent on additional technology, spoofable
Dictionary Attack	Strong passwords	Hashed with SALT value	Makes guessing harder	Slow
Insider Attacks	Access Control, Monitoring	IDS	Monitors threats inside & outside	Differentiate friend & foe
Shoulder surfing attacks	Confuse the attacker	Including wrong information	safe from social Engineering Attack	Simple
Dictionary attacks	Multiple login attacks	Strong encrypted password	Privacy & safe	Confidentiality lose

ISSN: 2233-7857 IJFGCN

Before designing an authentication system different attacks and its countermeasures can be considered with the help of these surveys. On the basis of nature and type of applications the required method of authentication can be picked [40]. For online applications and offline applications solutions have been provided by us in this. We have also discussed advantages and disadvantages of these authentication methods implementations.

3.FRAMEWORK OF AUTHENTICATION LEVEL.

Critical components like storage of data, communication channels, processing devices and sensors are components of digital system in any MFA framework. These are at a very high risk of verity of attacks various at different levels, it might be a simple attempt of replay to adversary attack. To maintain and unable privacy hence security is a very important tool. So now we start with the attacks that are performed on itself by input devices. So that the processing and accessing sensitive personal data is done by the legitimate controllers only. Hence, the main risk to the MFA security is exposed to the community.

3.1 EOTP Authentication Algorithm

Step1: Transaction / Authentication process starts.
Step2: Firstly, user sent the request to the server for send the OTP.
Step3: Server receives the OTP request from the user.
Step4: Server Generates OTP (one-time password) using its algorithm which is in alpha-numeric form.
Step5: After OTP is generated, Appling DES Encryption Algorithm to the Generated OTP.
Step6: After Encryption is done, we will get Encrypted One Time Password.
Step7: After Encrypting the OTP, we will cover the Encrypted OTP with the Image.
Here covering The EOTP with the image is done as any other intruder or unauthorized user could not access the EOTP in the middle of the connection.
If intruder get the Image+EOTP which is transferred from server to the actual user than also the intruder can't get that EOTP. Because it will be seeming to be an ordinary image.)
Step8: User gets the EOTP+Image which will be automatically separated by Applying separation method.
Step9: After that EOTP will extracted by applying separation method.
Step10: After that decryption EOTP will be done.
Step11: After decryption is done user will get the OTP Generated by the server. User enters that OTP to the required OTP box.
Step12: After user submits the OTP server match that OTP with the OTP which is generated by the server.
Step13: If both the OTP is not equal then process will be stoped and exit.
Step14: If Both OTP is equal then Server will generate OTP Authentication success certificate.

ISSN: 2233-7857 IJFGCN

Fig.1. EOTP Authentication System.

3.2 Digital Signature Authentication Algorithm: -

Step1: Firstly, user inputs (plug-in) the data with the help of any drive.
Step2: After that the data is encoded in the hash code.
Step3: Then Encrypt the Hash Code with the sender's private key.
Step4: After that attach the Encrypted Hash Code on the OTP Authentication successful Certificate as a Digital Signature.

ISSN: 2233-7857 IJFGCN

Step5: Signing of certificate with Digital Signature is done.

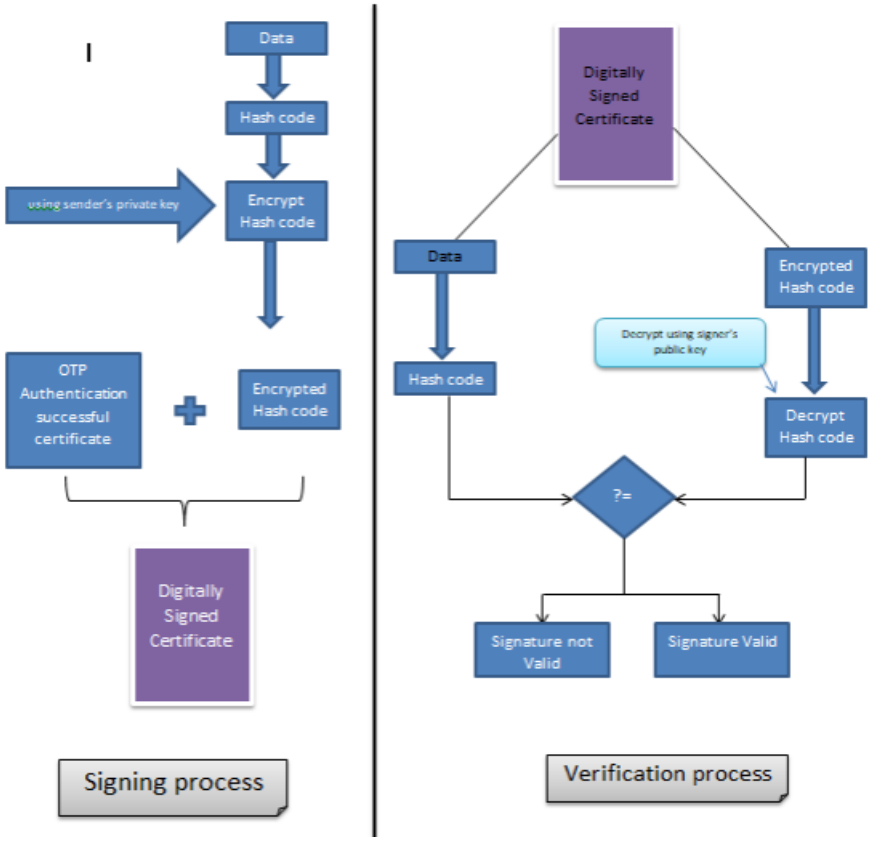


Fig.2. Digital Signature Authentication Algorithm

3.3 Digital Signature Authentication Algorithm: - Verification process:

Step1: when the server receives the Digitally Signed Certificate, it Automatically Separates the Encrypted Hash Code and Data.
Step2: Decrypt the Encrypted Hash Code.
Step3: Encode the separated Data in hash code.
Step4: Compare both the hash code.
Step5: if both the hash code is equal then the signature is valid.
Step6: if both the hash code is not equal then the signature is Invalid.

3.4 Multi-Function Authentication Algorithm

Step1: A certificate is generated and sent to the user after OTP Authentication is successful server.
Step2: User receives the certificate sent by the server.
Step3: User Attach the digital signature on the certificate received from the server.
Step4: Server checks the digital signature is Authentic or not.
Step5: If the digital signature is not Authentic the process will be stopped and exit.
Step6: If the digital signature is Authentic server will generate Thumb Impression Verification Portal.
Step7: User will get request to input the Thumb Impression.
Step8: User inputs His/her Thumb Impression.
Step9: Server verifies the Thumb Impression.
Step10: If the verification is failed then process will stop and exit.
Step11: If the biometric verification is successful server will show the Multi-Function Authentication successful message.

ISSN: 2233-7857 IJFGCN

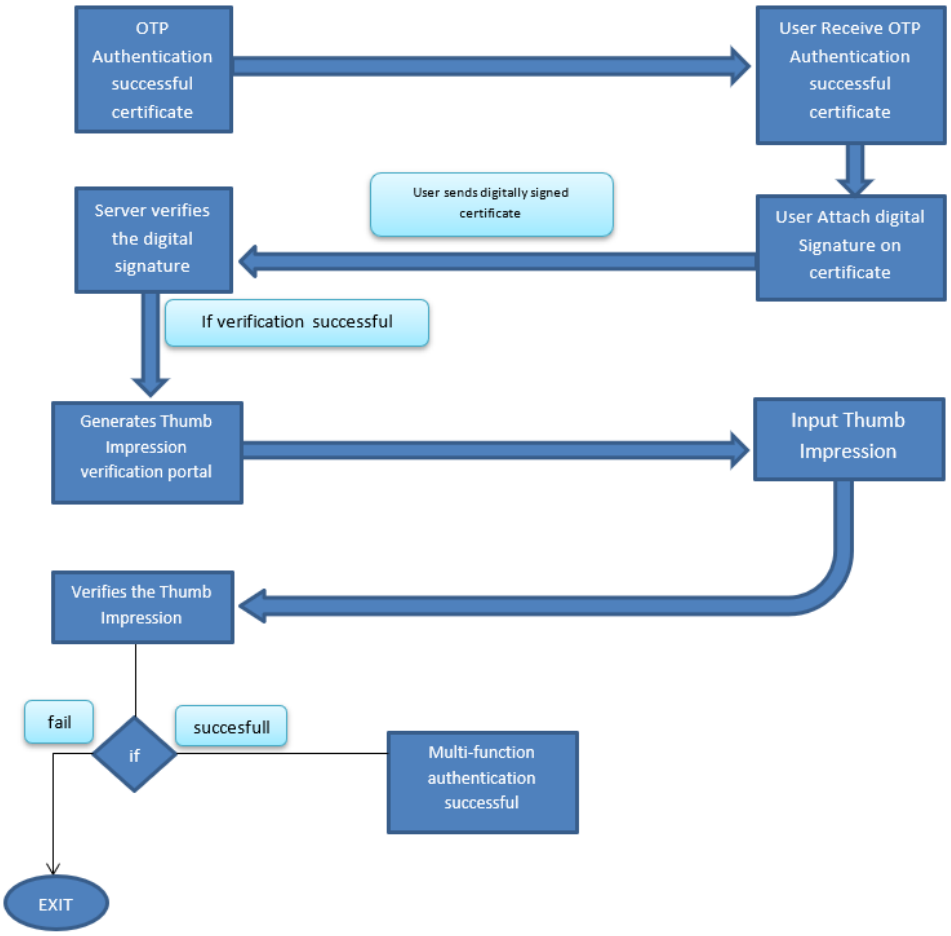


Fig.3.Multi-Function Authentication Algorithm:

MFA systems performance, count of vulnerabilities can also be increased by them and by an intruder that can also be exploited. At the duration of transmission between the storage/processing unit and sensor is the yet another sensitive,data,therisk.

4. EXPERIMENTATION, RESULT AND DISCUSSION

Authentication to maintain the security of this process is a key enabler. Covering hyper-connected world's various different areas like communication, online payments, access right management and many more. Beginning from the SFA or Single-Factor Authentication and through 2FA or Two-Factor Authentication,3FA or Three Factor Authentication. this help us to understand this journey and evolution to the MFA or Multi-Factor Authentication. By enabling user authentication to be friendly, fast and reliable while using server it is thought to incorporate human-to-everything interaction by MFA. To calculate the risk frequently external audits are conducted by the developers and for planning's that are most careful are on the basis of evaluation like this.

ISSN: 2233-7857 IJFGCN

ISSN: 2233-7857 IJFGCN

5. CASE STUDIES: Case studies based on existing applications with a hypothetical counterpart.

The case studies are split in three categories: (i) people who were realized by comparing the framework's recommendation against the implemented scheme or method on an existing application, (ii) those that were realized by comparing the framework's recommendation against the recommendations given experts for hypothetical applications, and (iii) people who were realized by comparing the framework's recommendation against the implemented scheme or method on an existing application and also against the advice given by experts for hypothetical applications with nearly an equivalent features because the existing ones. These case studies are presented in Tables 3-5, respectively, presenting the implemented scheme or method in the existing application, the framework's recommendation, the most recommended scheme or method by the experts, and

Authentication methods	**Choose Combination of Authentication Factor**	**Application Area**	**Usability**	**Authentication Security level**
Single Phase Authentication	Behavioral biometrics Text passwords Graphical passwords Palm print/fingerprints Face biometrics	Social Applications, Mobile device security application.	High	Very low
Two Phase Authentication	Behavioral biometrics +Graphical passwords Behavioral biometrics +OTP Palm print/fingerprints +Text passwords OTP +Graphical passwords behavioral biometrics +Text passwords Encrypted OTP +Text passwords	Banking, E-commerce, internet uses application.	Medium	Medium
Three Phase Authentication	Graphical passwords +behavioral biometrics +smart cards Text passwords +behavioral biometrics + encrypted OTP Graphical passwords +behavioral biometrics +OTP Graphical passwords +facial biometrics +OTP Text passwords+ behavioral biometrics +smart cards Text passwords + facial biometrics +smart cards Text passwords+ bio metrics +Digital Signature	Very Confidential platforms, application.	Low	high
Multiphase Authentication	Text passwords+ bio metrics +Digital Signature +encrypted OTP+ location-based factor +tokens Text passwords +behavioral biometrics + encrypted OTP + Digital Signature+ secret question+ smart cards Graphical passwords +behavioral biometrics + encrypted OTP+ key stroke+ SMS+ Security Tokens behavioral biometrics + numeric password +computer algorithm + pin number + physical object +- encrypted OTP Biometrics factor +- encrypted OTP+ numeric PIN +security token +inherent factors + Digital Signature	IoT Devices, Very Confidential platforms, application.	Very Low	Very high

therefore the acceptance rate of the framework's recommendation, as appropriate.

ISSN: 2233-7857 IJFGCN

Table 2. Combination of Authentication methods, Factor, Application Area, Usability, Authentication on Security level.

Table 3. Case studies based on Implemented scheme and Framework's recommendation.

ID	Implemented scheme or method	Framework's recommendation
1.	Three factor authentications (text passwords + smart cards)	Multiphase Authentication behavioral biometrics + numeric password +computer algorithm + pin number + physical object +- encrypted OTP
2.	Two factor authentications (Text passwords +OTP)	Three factor authentications (Text passwords+ bio metrics +Digital Signature)
3.	OTP (demanded by client)	encrypted OTP

Table 4. Case studies based on existing applications

ID	Experts' recommendation	Framework's recommendation	Acceptance rate of framework's recommendation
4.	Three factor authentication or Multiphase Authentication	Multiphase Authentication	100%
5.	Two factor authentications or Three factor authentications	Three factor authentications	70%

Table 5. Case studies based on hypothetical applications

ID	Implemented scheme or method	Experts' recommendation	Framework's recommendation	Acceptance rate of framework's recommendation
6	Multiphase factor authentication	Text passwords	Encrypted OTP	100%
7	Digital Signature +Text passwords	Three factor authentications	Multifactor factor authentication	70%

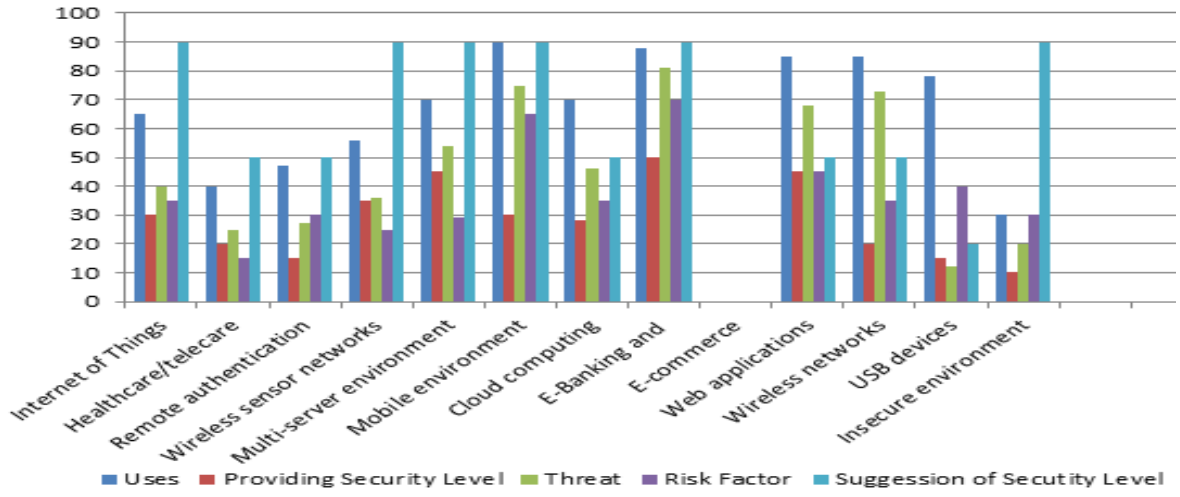
In general, the results of the case studies are favourable for the framework. it's important to say that, where discrepancies are observed, there was often a reasoning behind them. for instance, for case study 3 (existing application), the implemented scheme was demanded by the client and not selected by the software development team. On method, implemented and properly designed multifactor authentication are better for fraud determination and its reliability is also more. A panel of penetration testing should also be supported security framework of MFA to assess it. Hence for a more secure surrounding the MFA system should be the assess to the deliver.

Table 6. Providing Security Level Authentication, Factor, Uses, Application Area, Risk Factor, Suggestion of Security Level.

Application Area	**Uses**	**Providing Security Level**	**Threat**	**Risk Factor**	**Suggestion of Security Level**
Internet of Things	65	30	40	35	90
Healthcare/telecare	40	20	25	15	50
Remote authentication	47	15	27	30	50
Wireless sensor networks	56	35	36	25	90
Multi-server environment	70	45	54	29	90
Mobile environment	90	30	75	65	90
Cloud computing	70	28	46	35	50
E-Banking and E-commerce	88	50	81	70	90

ISSN: 2233-7857 IJFGCN

Web applications	85	45	68	45	50
Wireless networks	85	20	73	35	50
USB devices	78	15	12	40	20
Insecure environment	30	10	20	30	90



❖ Single level security =20, Two face authentication =50, Multifactor authentication =90

Fig 4. Result of different type application area, risk factor and suggestion of security level.

Multi-factor authentication inside an organization serves a very important role such as securing the users identity, securing access to corporate network and ensuring the user's identity that he is the same person as he claims to be, around mobile device and cloud application evolving business requirements, the requirement for reduction in cost, included with increasing threats, need completely new access control considerations, for an access management pie authentication is just one segment. Requesting and greeting applications access a framework provides the solution for the Access and Identity Management, assuring access event visibility and access control enforcement [40,41]. If there is a chance for an attacker like from input device an insecure transmission takes place through an extraction and to the database matches the blocks. To provide protection is response of these risks guarantee for a level of data safety is needed.

6. CONCLUSION AND FUTURE WORK

There is an expectation with the Multi-Factor authentication for an improved level of assurance in the field of security. Let us consider an example to complete the process of authentication in business network the user may be asked to give a password and from a security token any random number. Identification of a person can be to a high degree when the user knows the password as well as the security token. Some new challenges were introduced in the field of usability especially by the two-factor authentication. As there is no standardization of two-factor authentication is one of the challenges of the usability. With different implementations there are only few different authentication factors. There is not necessary interoperability when at the same time same authentication factor is employed by different institutes. As a result of which there is an expectation on the user to remember dozens of unique passwords and for second authentication factor have multiple physical objects.

ISSN: 2233-7857 IJFGCN

An effective and feasible solution is proposed by the mentioned framework with the help of a mixture of user-ID and passwords-based process of authentication based on dynamic multi-factor method of secret-splitting approach of authentication. Various different kinds of attack protecting authentication system is designed by this. Rather than static authentication the user usually authenticates dynamically this is the fact on which this mechanism's strength lies. Security features like mutual dynamic authentication, credential and identity management, user friendliness and in between the user and the cloud access management server session uses token agreement. For cloud computing and resources dynamic level of security for the user reaches the specific security level by the user authentication system this is the final result of this.

REFERENCES

1. 1.Tarun Dhar Diwan, Upasana Sinha "The Machine Learning Method Regarding Efficient Soft Computing and ICT Using SVM" international journal of computer engineering & technology (ijcet), issn 0976 – 6367(print) issn 0976 – 6375(online) volume 4, issue 1, january- february (2013), pp. 124-130.
2. 2.Tarun Dhar Diwan,Upasana Sinha" performance analysis is basis on color based image retrieval technique" international journal of computer engineering & technology (ijcet) issn 0976 – 6367(print) issn 0976 – 6375(online) volume 4, issue 1, january- february (2013), pp. 131-140.
3. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen and Yevgeni Koucheryavy, Multi-Factor Authentication: A Survey, Published: 5 January 2018, doi:10.3390/cryptography2010001.2-31.
4. 4.VNI Cisco Global Mobile Data Traffic Forecast 2016–2021. White Paper, 2017. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/ complete-white-paper-c11-481360.pdf (accessed on 4 January 2018).
5. Benarous, L.; Kadri, B.; Bouridane, A. A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. In Biometric Security and Privacy; Springer: Berlin, Germany, 2017; pp. 371–411.
6. Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39.
7. Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.
8. Bonneau, J.; Herley, C.; Van Oorschot, P.C.; Stajano, F. Passwords and the evolution of imperfect authentication. Commun. ACM 2015, 58, 78–87.
9. 9 Wang, D.; Wang, P. Offline dictionary attack on password authentication schemes using smart cards. In Information Security; Springer: Berlin, Germany, 2015; pp. 221–237.
10. Banyal, R.K.; Jain, P.; Jain, V.K. Multi-factor authentication framework for cloud computing. In Proceedings of the Fifth International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), Seoul, Korea, 24–25 September 2013; pp. 105–110.
11. SC Media UK. 68% of Europeans Want to Use Biometric Authentication for Payments. 2016. Available online: https://www.scmagazineuk.com/68-of-europeans-want-to-use-biometric-authentication-forpayments/article/530818/ (accessed on 4 January 2018).
12. Khan, R.; Hasan, R.; Xu, J. SEPIA: Secure-PIN-authentication-as-a-service for ATM using mobile and wearable devices. In Proceedings of the 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, USA, 30 March–3 April 2015; pp. 41–50.
13. Security Intelligence. The Move to Multifactor Authentication: Are Passwords Past Their Prime? 2016. Available online: https://securityintelligence.com/news/the-move-to-multifactor-authenticationare-passwords-past-their-prime/ (accessed on 4 January 2018).

ISSN: 2233-7857 IJFGCN

14. Neha; Chatterjee, K. Authentication techniques for e-commerce applications: A review. In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 693–698.
15. Labati, R.D.; Genovese, A.; Muñoz, E.; Piuri, V.; Scotti, F.; Sforza, G. Biometric recognition in automated border control: A survey. ACM Comput. Surv. (CSUR) 2016, 49, 24.
16. De Cristofaro, E.; Du, H.; Freudiger, J.; Norcie, G. A comparative usability study of two-factor authentication. arXiv 2013, arXiv:1309.5344.
17. Khan, S.H.; Akbar, M.A.; Shahzad, F.; Farooq, M.; Khan, Z. Secure biometric template generation for multi-factor authentication. Pattern Recognit. 2015, 48, 458–472.
18. Acharya, S.; Polawar, A.; Pawar, P. Two factor authentication using smartphone generated one time password. J. Comput. Eng. (IOSR-JCE) 2013, 11, 85–90.
19. 122. Sae-Bae, N.; Ahmed, K.; Isbister, K.; Memon, N. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 22–27 April 2006; ACM: New York, NY, USA, 2012; pp. 977–986.
20. Lee, W.H.; Lee, R.B. Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning. In Proceedings of the 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 26–29 June 2017; pp. 297–308.
21. Van Goethem, T.; Scheepers, W.; Preventers, D.; Joosen, W. Accelerometer-based device fingerprinting for multi-factor mobile authentication. In Proceedings of the International Symposium on Engineering Secure Software and Systems, London, UK, 6–8 April 2016; Springer: Berlin, Germany, 2016; pp. 106–121
22. Raja, K.B.; Raghavendra, R.; Stokkenes, M.; Busch, C. Multi-modal authentication system for smartphones using face, iris and periocular. In Proceedings of the International Conference on Biometrics (ICB), Phuket, Thailand, 19–22 May 2015; pp. 143–150.
23. Townsend, K. Passive Authentication May Be the Future for User Authentication, and It's Just Beginning to Appear. 2016. Available online: http://www.securityweek.com/passive-authentication-future-userauthentication (accessed on 4 January 2018).
24. Walters, R. Continuous Authentication: The Future of Identity and Access Management (IAM). 2016. Available online: https://www.networkworld.com/article/3121240/security/continuous-authenticationthe-future-of-identity-and-access-management-iam.html (accessed on 4 January 2018).
25. N.Ye,Y.Zhu,R.-C.Wang,R.Malekian, and Q.-M.Lin,“ An efficient authentication and access control scheme for perception layer of internet of things, “Applied Mathematics &Information Sciences,vol.8,no.4,pp.1617–1624,2014.
26. Q. Tasali, C. Chowdhury, and E. Y. Vasserman,“Aflexibleauthorizationarchitectureforsystemsofinteroperablemedicaldevices,”inProceedingsofthe22ndACMSymposiumonAccessControlModelsandTechnologies,SACMAT2017,pp.9–20,USA,June2017.
27. M. TrnkaandT.Cerny, “Authentication and authorization rules sharing for internet of things,” Software Networking, no. 1, pp. 35–52,2017.
28. 28.J.L.H.Ramos,M.P.Pawlowski,A.J.Jara,A.F.Skarmeta,andL.Ladid,“Towardalightweight authentication and authorization framework for smart objects, ”IEEE Journal on Selected Areas inCommunications,vol.33,no.4,pp.690702,2015.
29. S.-H. Lee, K.-W. Huang, and C.-S. Yang, “TBAS: Token-based authorization service architecture in Internet of things scenarios,” International Journal of Distributed Sensor Networks,vol.13,no.7,2017.
30. 30 L.Liu,B.Fang,andB.Yi,AGeneralFrameworkofNonleakageBased Authentication Using CSP for the Internet of Things, SpringerInternationalPublishing,Cham,Switzerland,2014.
31. M. Shahzad and M. P. Singh, “Continuous authentication and authorization for the internet ofthings,”IEEEInternetComputing,vol.21,no.2,pp.86–90,2017.

ISSN: 2233-7857 IJFGCN

32. M.Cagnazzo, M.Hertlein,and N.Pohlmann, An Usable Application for Authentication, Communication and Access Management in the Internet of Things, Springer International Publishing,Cham,Switzerland,2016.
33. G. Alpar, L. Batina, L. Batten et al., "New directions in IoT privacy using attribute-based authentication," in Proceedings of the ACM International Conference on Computing Frontiers, CF 2016, pp.461–466, NY, USA, May2016.
34. M. Khamis, M. Hassib, E. Zezschwits, A. Bulling, and F. Alt "GazeTouchPIN:Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication," In Proceedings of 19th ACM International Conference on Multimodal Interaction, Glasgow, UK, 2017, pp. 446-450.
35. V. Rajanna, P. Taele, S. Polsley, and T. Hammond., "A gaze gesture-based user authentication system to counter shoulder surfing attacks," In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA '17. ACM, 2017, pp. 1978-1986.
36. V. Rajanna, and T. Hammond.," Gaze-Assisted User Authentication to Counter Shoulder–surfing Attacks," In Proceedings of the 2018 CHI Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA '18. ACM, 2018.
37. M. Mehrubeoglu and V. Nguyem, "Real-time Tracking for Password Authentication" IEEE International Conference on Consumer Electronics (ICCE), 2018.
38. 38.C.Y.Chen, Efficient Authentication for Tiered Internet of Things Networks, Springer International Publishing, Cham, Switzerland,2017.
39. Ignacio Velásquez, Angélica Caro and Alfonso Rodríguez, Multifactor Authentication Methods: A Framework for Their Comparison and Selection DOI: http://dx.doi.org/10.5772/intechopen.89876
40. Dina M. Ibrahim, Sadaf Ambreen Gaze touch cross pin: secure multimodal Authentication using Gaze and Touch PIN" International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-9 Issue-1, October 2019.
41. Alzahraa J. Mohammed and Ali A. Yassin "Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device" 2019, 3, 24; doi:10.3390/cryptography3030024.

ISSN: 2233-7857 IJFGCN