International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 2, February 2022, pg.119 – 126

Security of IoT Automated Devices Using Different Authentication Methods

Nikhil Kumar

Research Scholar, Bhagwant Institute of Technology, Muzaffarnagar, UP, India
nikhilkumarhere@gmail.com

Dr. Pushpneel Verma

Associate Professor, Bhagwant Institute of Technology, Muzaffarnagar, UP, India
pushpneelverma@gmail.com

Ajay Singh

Assistant Professor, Bhagwant Institute of Technology, Muzaffarnagar, UP, India
ajaysingh221985@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2022.v11i02.014>

Abstract— Internet of Things (IoT) has brought significant change to the real world and has impacted every aspect of our lives. The acceptance by users of IoT is extremely significant and its widespread use is due to the availability of autonomous devices. A wide acceptance of IoT in applications in every field is constantly gathering sensitive data and providing an increased surface for hackers. Therefore, privacy-preserving authentication and access control are major issues in the field of research. Methods/Statistical Analysis This paper will look at the ways to secure the authentication of sensors-enabled autonomous devices in the IoT. Additionally, for the purpose of ensuring confidentiality during communications, there are a variety of Authentication methods that meet the requirements of Security. Results: Insecure authentication process biometrics, PINs, and other methods offer additional security for IoT that is autonomously implemented. Also, Finger vein technology is one part that IoT could have a significant impact in protecting their devices. 3D Face detection is the most advanced form of 2D face detection. It enhances the processing and processing speed of image capture.

Keywords— IoT (Internet of Things) IoT, Authentication, Autonomous Things PIN Biometrics and Finger Vein

I. INTRODUCTION

This IoT is now a reality via the Internet where everything from objects, people, data, and other objects can connect via wired or wireless networks anytime, any location. In this new era, Internet has expanded beyond communication devices to enterprise products and assets as well as consumer products. IoT makes a smart environment. It also provides unique addressing is employed to facilitate effective communication[1]. Therefore, every device connected to the internet can be identified. Each participant independently interacts with the other via the internet and no central authority exists to regulate the objects.

IoT enabled the interaction of humans with people around the world using a sensor device. IoT incorporates technologies to collect and process information about context, such as sensors Near Field Communicators, Global Positioning Systems, etc. The IoT offers many possibilities to society, but these technologies affect all aspects that are connected to the communications device and demand solutions to enhance security and privacy. There are now billions of internet-connected devices that have been identified and provide worldwide network connectivity that allows users to enhance their lives. This has led to billions of connected devices via the internet, and even more IoT applications are being developed. IoT offers a myriad of opportunities in the industry, commerce as well as technology to enhance its performance while simultaneously adding complexity to the field of information technology[2]. From a technology standpoint, the data generated by IoT is created by machines and increases the density due to Moore's law. Smart objects with sufficient memory can recognize and store data about people and other objects in the network. Therefore, a key requirement of IoT is the protection of privacy and security enhancements.

Figure 1. Internet of Things in an intelligent environment.

Data security is a significant concern when devices are connected to the outside. In IoT the person is identifiable and smart devices gather the information and data without their permission, which is why they infringe on security standards alone. The majority of information gathered by these sensors is protected and confidential. Therefore, security-related issues have to be dealt with by researchers. IoT communications, an interplay between smart objects and social media. It is susceptible to Trudy interactions. The dynamic nature, mobility, and weak physical security of Mobile devices have also created an attack target. IoT connected devices result in the leakage of private information and exposure of authentication credentials to hackers. Thus, a secure authentication method from the client device is essential for safe browsing[3]. This study provides a review of the literature as well as an interesting model of authenticating in the IoT environment. Authentication elements can be classified into three categories that include: something you are familiar with: a password or personal identification number (PIN) or something you possess an item like a token, like a credit card, things you're biometrics such as the fingerprint and the voice.

II. AUTHENTICATION

In order to build confidence in IoT communications and achieve the objectives of information security, it is necessary to be attentive to the authentication of the server and for users. Authentication is the act that validates your identity when communicating. It assures the authenticity of the source of the communication it is among the most important objectives in security. It acts as a gateway to the inside to a safe system in order to ensure that there are no errors. If there are more connected devices the need for a new system to be created to authenticate users as well as devices. The authentication mechanisms utilized in commercial applications can be classified into four categories namely, things you're aware of, things you own as well as something that you have, and an area where you are. One of the most commonly used security methods is the use of authentication by user name and password using the Secure Socket Layer connection. Sometimes algorithms calculate the cryptographic hash and block encryption of passwords in plain text. However, the credentials are transmitted via the internet, and the proliferation of wireless hotspots is increasing which makes them vulnerable to access by intruders, even if they are hashed. Furthermore, the 3G GSM connection is risky and is easily cracked in less than 2 hours. So we're looking for the solution that doesn't reveal our secret to authenticate. Traditional authentication to a system will always result in overhead for the server as well as a lengthy process at the end-user machine. To solve this issue, current research is focused on solutions to Memory and Battery constrained Smart devices. This research offers an easy-to-use solution with a compact footprint that is high-performance and low price for IoT environments. When we look at IoT devices, it was discovered that many devices are not equipped with passwords and authentication methods. The usage of weak passwords and encryption of traffic is a significant problem in IoT [4]. Nowadays, people are increasingly using their mobile phones to make payments, do banking shopping, and more. Therefore it's important to secure their identity and provide the authenticity of their devices. It is important to protect their identity and ensure authentication. IoT the possibilities of communication include device-to-device devices to humans, the human to the human and enable heterogeneous entities and networks. Because devices don't have any prior knowledge of any other entity and since no SSL communication is available, eavesdropping is feasible. Furthermore, IoT smart devices that have actuators and sensors exchange data and collect personal data for authentication, and have the potential to reveal unauthorized identities. Therefore, for the protection of personal data and security, we require completely different access control systems and authorization techniques. The separation of sensors' output is a major issue and privacy law isn't yet fully prepared for IoT. Traditional authentication processes require that the user sends their user id and password. The machine on the client creates the password's hash and then sends the user's id and password hash to the networks. The replies from the server can also be sent via the network. A Wi-Fi connection or 3G mobile broadband is utilized to transfer these credentials and is susceptible to hacking. Hackers can access the credentials and make use of it later to obtain services from the server, or the software to retrieve the password using the hashes. The authentication methods are generally divided into private keys as well as public key-based one-time signature-based. Systems that rely on public keys require large computation, communication in addition to storage. Private Key mechanisms aren't suitable for devices with limited resources and the internet security standard TLS cannot be used with tiny embedded devices[5].

A. Authentication Methods

1) *Login using a password*: Passwords are one of the most commonly used methods for identification. Passwords may take the form of an alphabet and numbers or other specific characters. To safeguard yourself, you must make secure passwords that incorporate the best of all possibilities.

However, passwords are susceptible to fraud attacks and poor hygiene, which can reduce their effectiveness. A typical person has around 25 online accounts, however, only 54 percent of users have different passwords for each of their accounts.[6]

The reality is that there are many passwords to keep track of. Therefore, many people prefer ease over security. The majority of people choose simple passwords instead of making solid passwords as they are easier to remember. The main point is that passwords come with numerous security flaws and are not adequate to protect online data. Hackers can easily decipher passwords by going through every possible combination until they discover the right that matches.

2) *Multi-factor authentication*: Multi-Factor Authentication (MFA) is an authentication process that makes use of two or different methods to substantiate the accuracy for the individual. Most commonly, these are the codes generated by the phone that the person is using, Captcha testing, fingerprints, voice biometrics as well as facial recognition[7].

MFA authentication techniques and methods improve the security of users through the addition of several levels of protection. MFA can be a useful protection against the majority of accounts hacks but it also has its own set of pitfalls. Users could have their phone is stolen or SIM cards, and be able to create an authentication code.

3) *Certificate-based verification*: Certificate-based authentication technology identifies the users, devices, or machines with digital certificates. Digital certificates are digital documents that are based on the idea of a driver's license or passport.

The certificate shows the digital identity of the person who is issued it, which includes a public key along with the digital signatures of authority for certification. Digital certificates verify the authenticity of the key public and are issued by a certified authority. Users sign their digital certificates each time they sign into servers. The server checks the authenticity of the certificate's digital signature as well as an authority for certificates. The server then employs cryptography to verify that the certificate holder has the correct private key to the certification[8].

4) *Biometric verification*: Biometrics authentication is a secure method that is based on the particular biological traits of an individual. There are many advantages to the use of biometric authentication technology:

The biological characteristics of a person can easily be compared with approved features that are stored in a database. Biometric authentication allows physical access by installing it on doors and gates. You can incorporate biometrics into your multi-factor authentication system. Biometric authentication is utilized by governments, consumers, and private companies, including airports, military bases as well as national border crossings. The technology is becoming more popular because of its ability to attain the highest level of security without causing friction for the users. The most popular biometric authentication methods are:

Recognition of facial features--matches the distinct facial features of the person who is trying to access an approved face in databases. Face recognition is often unreliable when comparing faces at different angles, or when comparing people who are similar to close relatives. Face liveness, similar to ID R&D's active facial liveness stops fake faces. Fingerprint scanners--match the distinctive patterns of the fingerprints of an individual. Newer versions of fingerprint scanners even detect the vascular patterns on people's fingers. Fingerprint

scanners are the most used biometric technology for the everyday user however, they can be inaccurate at times. The reason can be attributed to iPhones.

Speaker Recognition is also known by the name of voice biometrics studies the patterns of speech in a person's voice to determine the formation of certain forms and sounds. A device that is voice-protected usually utilizes standard words to identify the user as passwords. Eye scanners--include technologies such as retina scanners and iris recognition. Iris scanners beam bright light toward the eye and look for distinctive patterns within the colored ring surrounding the eyes' pupil. These patterns are then compared against information accepted to be stored in databases. Which will become the topic of further study in the near future. Eye-based authentication could be inaccurate depending on whether the user wears contact lenses or glasses.

5) *A token-based method of authentication:* Token-based authentication systems allow users to input their credentials once and get a unique secure string of randomly generated characters. You can then use this token to gain access to protected systems, instead of having to enter your credentials over and over. The digital token is proof that you have access rights. The use cases for token-based authentication are RESTful APIs, which are utilized by various frameworks and clients[6].

B. Functionality

1) *Multiple multi-factor authentication methods:* Multi-way authentication systems require users to install client applications to enable multi-factor authentication. Some companies have created separate installation programs for network logins as well as Web access credentials and VPN connections. For these types of products, there could be up to five software applications that can be pushed down onto clients' PC to use tokens or smart cards. Token or smart card. This means that there are five or four applications where revision control must be

implemented and the four or five programs that examine for conflicts with enterprise applications[7]. If access is managed through websites it is possible to reduce the above-mentioned overheads to one application. Other multi-factor authentication options include "virtual" tokens, as well as hardware tokens there is no software that must be installed by the end-users.

2) *Biometric authentication*: The choice of a biometric for an application requires the weighting of various factors. Jain and colleagues. (1999) [3] discovered seven aspects to be considered to determine the appropriateness of any particular trait for biometric authentication. Universality implies that everyone who uses a system must possess the characteristic. Uniqueness means that the characters should be distinct enough for each person within the population in question so that they are distinct from each other. Permanence refers to the manner that which a trait changes over time. Particularly, a characteristic that has good permanence is likely to be fairly stable over time in relation to the exact algorithm that matches it. Measurability (collectability) is a measure of the ability to acquire or measure the characteristics of the characteristic. Furthermore, data that is acquired must be presented in a format that permits processing later and extraction of relevant features. Performance is determined by the accuracy speed, speed, and durability of the technology employed. Acceptability refers to the degree to which people from the appropriate group of people accept the technology in a way that they're willing to capture their biometrics and evaluated. Circumvention is the way that a particular characteristic can be duplicated with the aid of an object or substituting.

3) *Certificate-based authentication*: In cryptography, a certificate of the public key or digital certificate, also known as an identity certificate can be described as an electronic certificate that can be used to verify the authenticity of an official key. The certificate contains details about the key, details about the identity of the person who owns it (called "the subject") as well as an electronic signature from the entity who has confirmed the contents of the certificate (called "issuer"). When the certificate's signature appears to be legitimate and the program that examines the certificate believes in its issuer then the software will be able to utilize that key to secure communication with the certificate's owner. In the case of email security, encryption, code signing as well as electronic signature systems the certificate's subject is usually a particular individual or an organization. In the case of Transport Layer Security (TLS) certificates, the user is usually an electronic device or computer but TLS certificates can be used to identify businesses or individuals in addition to their main function in the identification of devices. TLS often referred to as its earlier designation Secure Sockets Layer (SSL) is notable because it is a component of HTTPS which is a protocol to secure browsing on the internet.

III.CONCLUSIONS

Technology for authentication is constantly changing. Businesses must move beyond passwords and look at authentication as a way of improving the user experience. Biometric authentication methods can make it unnecessary to remember long and intricate passwords. Due to the advancement of technology and authentication methods security, hackers won't be able to hack passwords, as well as data breaches, are prevented.

IoT is a rapidly growing technology field that gives an opportunity to create a variety of possibilities with a variety of efficient, cost-effective, and user-friendly applications and services available to users. Security is, however, one of the major issues in the direction of greater use of IoT systems. In the paper, we've reviewed and identified the most current security requirements for the IoT and suggested an array of security specifications to be included in the IoT security framework. We provided a comprehensive analysis of the problems that must be taken into consideration to construct an effective and secure IoT architecture, based on the requirements proposed. We've observed that the security requirements currently in place in IoT security aren't sufficient. IoT is not designed to deal with a variety of attacks and threats in a systematic manner. We found an urgent need for a coherent approach to address IoT security needs that is capable of capturing the fundamental requirements for a secure IoT architecture. Distinct categories, including threats and attacks on communications, mobile devices, user services, and integration of resources as well as the possible threats and threats for each. In light of these classifications and the available solutions, we've formulated the security requirements which are essential to secure the security of an IoT system. It is important to note that the proposed specifications are not only

ones that are mandatory for IoT but using them, can be more effective in achieving the majority of the promised advantages of scalability, reliability, usability and trust, identity, and more. It is also important to remember that without an accurate analysis of potential security threats and the incorporation of appropriate security standards the IoT system could be susceptible to attack. We have looked at and explained the security concerns in the different levels of the IoT security framework. We have outlined the various crucial security needs in five different layers within one IoT security architecture. They are the device sensing layer management layer and service composition layer application layer, and user interfaces layer. We discovered that there could overlap certain security requirements within two different layers. However, they're dependent on the system's requirements as well as the choice of the designer. In the near future, we intend to conduct research using the security requirements that are proposed to evaluate security concerns in greater detail in a real-world IoT system. We will also conduct an extensive test with various scenarios for use cases that will help in gaining further insights on what makes the most secured IoT device in an actual setting.

IV.FUTURE DIRECTIONS

Technology Biometrics for finger veins is the subject where biometric authentication will be improved on IoT devices. It is often referred to as vein match also known as vascular technology. It is a method for biometric authentication that examines the blood vessel patterns visible from the finger's skin. This method is based on the capture of images of veins within one's hand, by shining near-infrared lights on the fingers of those who use it.[9]

Fig Process of Finger vein Authentication.

3D facial recognition is an important area that can be secured by our devices. 3D face recognition is not fooled by videos or images. Additionally, it is very hard to deceive the

machine by using 3D masks or dummies since a precise stereolithographic model must be created using the exact smaller sub-millimeter measurements.[10]

We developed an extension of our approach mostly Biometrics as well as a Multi-way authentication method to authenticate on autonomous objects in IoT to minimize the amount of computation and communication. This work employs a similar OTP to verify and hash preparation. We also intend to develop an algorithm to exchange keys for key exchange in IoT. With the advent of the use of GPS, NFC, and RFID devices, the location of these devices can be tracked, but on certain occasions, users need to conceal their location from services. We propose a contextual filter that will protect privacy, based on the current situation. The work to come will also focus on designing a small server that functions as an intermediary between the requester and server. This will help create a complete, secure, and robust device for use within IoT.

Sensor Interoperability is another area of study to come in the future. Sensor Interoperability is an ideal option for companies that use various types of sensors. There are a myriad of fingerprint capture devices, or fingerprint sensor technologies that are available on the market today and each has its own advantages. While some sensors are suitable for certain situations but they are not adequate, or even suitable.

REFERENCES

- [1]. Vermesan O Friess P. Internet of Things From research and developments to deployment in the market. River Publishers; 2015.
- [2]. Peppet SR. Controlling what is known as the Internet of Things: The first step in tackling discrimination Privacy Security and Consent Texas Law Reviews 2014.
- [3]. Sen J. Privacy preservation technologies for the Internet of Things. International Journal BITM Transactions on EECC. 2009 Aug; 1(4):496-504.
- [4]. Oleshchuk V. Internet of things and privacy-preserving technologies. IEEE Wireless VITAE'09; 2009.
- [5]. Indian Journal of Science and Technology. <https://www.indjst.org>.
- [6]. AUTHENTICATION METHODS <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach>
- [7]. Multi-Factor Authentication https://en.wikipedia.org/wiki/Multi-factor_authentication
- [8]. Rehiman K.A, Veni S. Security privacy, trust and security for mobile devices with smart security in the internet of things. A study in the literature. IJARCET. 2015 May; 4(5):1775-9.
- [9]. Finger vein technology (Wiki) https://en.wikipedia.org/wiki/Vein_matching.
- [10]. 3D Face Recognition and Sensor interoperability <https://www.miteksystems.com/blog/finger-vein-recognition-biometrics>.