Authentication of IoT Device and IoT Server Using Security Key

Abstract

The Internet of Things (IoT) is an emerging topic in the field of information technology (IT) that has attracted the interest of researchers from different parts of the world. Authentication of IoT includes the establishment of a model for controlling access to IoT devices through the internet and other unsecured network platforms. Strong authentication of IoT is necessary for ensuring that machines and devices could be trusted when it comes to data sharing. The whole idea of authentication further prevents cybercriminals from using loopholes in IoT devices to access data that they are not allowed to access. Various authentication techniques could be used to secure IoT servers and devices. Establishing mutual authentication between IoT servers and IoT devices has attracted a lot of research interests because it helps enhance the effectiveness and overall security of data sharing. Therefore, this research provides the basis for analyzing the whole idea of using security keys to encrypt both IoT servers and IoT devices.

Keywords: Authentication, IoT, Security Key, Device, Server

1. Introduction

The Internet of Things (IoT) is one of the latest technological innovations that has attracted a lot of interest from researchers and IT (information technology) experts in the last couple of years. Mutual authentication between IoT servers and IoT devices is considered by experts as a critical step of securing the entire IoT system. The use of authentication systems that are based on single passwords is vulnerable to dictionary and side-channel attacks (Shah and Venkatesan, 2018). Authentication in the context of IoT servers and IoT devices is simply a model for the establishment of a trust in the identity of IoT devices and servers to control access and protect data when information is conveyed through the internet or other unsecured network. It is important to have strong IoT authentication because it helps ensure that connected servers and devices could earn the trust of protecting data against possible control commands from malicious actors and unauthorized machines. Additionally, authentication plays an integral role in preventing potential attackers from pretending to be authorized IoT servers and IoT devices hoping that they will access sensitive data.

Different pieces of research have been conducted to establish the best way of attaining the right level of authentication for IoT devices and IoT servers. This includes and is not limited to centralized, distributed, two-way, and one-way authentication. It is equally vital to note

January 26, 2021

that the IoT is not just one technology but rather a connected environment that is comprised of different "things" or machines that function independently without human intervention. The purpose of the IoT authorization process is to provide the basis for validating the identity of every single endpoint within the larger IoT system. The underlying process of certification is usually configured following the enrollment entry and also offers the service providers with information about the method that can be used to check the identity of the system during registration.

Consequently, machine identity management usually focuses on managing and building confidence in the identity of machines that are meant to interact with other gateways, clouds, applications, and devices. The rationale could include authorization and authentication of IoT devices like smart outlets, lights, and speakers, mobile devices, home security systems, security cameras, vehicle engine control units, and industrial control systems. Every single IoT device should have a unique digital identity that can be used when connecting to the central server or gateway to help prevent unauthorized parties from accessing the system. This is attained by binding identities to cryptographic keys that are unique to each IoT device. Approaches for machine identity management are especially essential when it comes to discovering the credentials that are utilized by various machines. The unique ID of IoT servers and IoT devices enables system administrators to track them throughout their lifecycles, establish secure communication with them, and prevent them from executing processes that could be harmful. Should an IoT server or device start to exhibit a behavior that is not expected, the system administrators could revoke their privileges with ease.

1.1. Definition of the Problem

The IoT platform has been subjected to constant changes over recent years (El-Hajj et al., 2017). The applicability and functionality of the technology have increasingly grown in a manner that allows for their integration in different domains like smart cities, public health, and environmental monitoring. As a technology, IoT is a clear representation of a revolutionary change of conceptualization of the internet from communication between people to communication that has rooms for everything. The problem is that this has come in handy with a fair share of risks and challenges. More precisely, information management and gathering, access control, authentication, and privacy have become increasingly vital functions that should be maintained and handled accordingly (El-Hajj et al., 2017). Undoubtedly, hackers and other malicious actors find the IoT platform an attractive and new platform that makes it easier for them to engage in their actions while expanding the scope and sophistication of the attack techniques. Based on their fields of application, the security requirements for IoT servers and IoT devices have to touch on the aspects of information availability, integrity, and confidentiality which to some extent is a great challenge. Even more, recent studies have not been redirecting a lot of attention to establishing better authentication mechanisms that could be used when securing IoT servers and IoT devices. This research gap has heightened the vulnerabilities and weaknesses that are associated with these devices, thus paving the way for unauthorized parties such as hackers (El-Hajj et al., 2017).

1.2. Main Motivations

This research is motivated by the fact that connectivity and big data have significantly impacted our daily lives. Connecting everyday systems, products, and devices to the global internet gives us the capability of accessing rich data in real-time. This is especially important because it enhances our abilities to carry out our business activities, analyze patterns, and make sound decisions. This transition towards connecting everything to the IoT calls for corresponding adoption and implementation of effective security keys when authenticating IoT servers and IoT devices. Many of us are in the rush of seeing the launch of the next smart car, connected medical device, or home automation systems but without proper security authentication protocols in place, it might be difficult to attain any of that. Designing IoT servers and IoT devices with the required security levels is considered as the next step towards the attainment of full-scale incorporation of IoT in our daily lives. System authentication is the fundamental way of preventing catastrophic attacks on sensitive data and IoT servers and IoT devices. PKI (public key infrastructure) is considered by many as one of the most innovative ways of encrypting data and authenticating websites. The secure approach offers a flexible and scalable solution that could provide the basis for securing IoT servers and IoT devices today. For organizations that are still struggling to address their authentication problems, this could be an ideal solution. The flexibility of PKI is especially vital in the context of changing requirements as well as during the representation of identity in a multiprotocol and cross-platform approach. By focusing on using security keys to authenticate IoT servers and IoT devices, this study offers a foundation for making more discoveries of even more effective authentication techniques.

Evolving cyber threats has also been part of the motivation behind this research. The number of IoT devices has been rising every day with the market expected to attain exponential expansion in the next couple of years. As of now, it is estimated that each individual has an average of three IoT devices. The increase in the number of these devices has also increased the scope of attacks. New vulnerabilities and threats are continuing to emerge, thus compromising the growth capability of the IoT. There have been recent cases of hacking in healthcare facilities, financial institutions, transport systems, and so forth. Even though many of these attacks have been carried out in the wild, it is just a matter of time before smart hacking becomes the order of the day. Unless the IT industry and all its stakeholders pay close attention to the security needs when it comes to IoT servers and IoT devices, it will become difficult to contain the extent of the damage that could be realized on end. Security keys offer a scalable way forward for data encryption, authentication, and discovering devices.

This research has further been motivated by the basic understanding that with increased data amounts that are being exchanged over the internet, it has become especially vital to have a coherent understanding of devices that are authorized to receive and send data. This partly involves using strong authentication such as security keys among devices users and cloud service providers. The stakes are a little bit higher when it comes to the IoT. That is bearing in mind that if by any chance data or information gets into the wrong hands or data integrity is compromised, it could lead to life-threatening situations. For instance, compromising an IoT device that is supposed to convey sensitive data about patients' treatment

could even lead to the death of the subject. Corporations should provision their systems and IoT servers and IoT devices with credentials that are trustable enough and to ensure that they do so on a large scale. Many security keys use open interoperability standards that could be applied in different use cases and across a wide range of platforms and protocols. Unlike the traditional authentication techniques, security keys could be scaled to suit the needs of the users. That means that billions of IoT servers and devices in different parts of the world could be customized or provisioned with digital certificates that can then be managed on specific centralized locations. Offering unique security keys to every single user and IoT device and IoT server will help create a secure digital tunnel that only authorized data can flow. The data will remain encrypted and out of reach to intruders and other unauthorized parties. Whereas the IoT is still evolving, we can all agree that we still have time to take the right security precautionary measures and ensure that these devices function in a manner that cannot limit their capabilities because of security vulnerabilities and faults. The IoT platform needs trustworthy, scalable, and fast deployments of digital certificates. For companies that rely on the internet for their daily operations, it is important to implement publicly trusted certificate root authorities that could enable users to understand that they are connecting to web locations that have been authorized. Of course, some IoT environments do not depend on public trust since they function under closed systems. Such networks could use security keys coupled with certificate management and sophisticated automation that can only be provided by a trusted partner.

Moreover, this study has partly been motivated by the underlying need of enhancing the security of IoT servers and IoT devices. We are currently living in the era of the IoT. That means that different IoT devices are now part and parcel of almost every aspect of our lives starting from wearables in our bodies to devices in our offices and homes. It is clear that in as much as the IoT has opened a wide range of opportunities that had not been explored initially, the related risks have been translating into costly challenges. The security of IoT devices has further been amplified by the fact that many users relate the functionality of the IoT platform with the traditional internet thus convincing them to have the same security approach to security as the past techniques. Nonetheless, the truth is that IoT security is way off different from the traditional internet security schemes. Although it could be easy to secure the entire network, blocking the infiltration of IoT devices before their activation has been a constant threat that has been identified by many experts in the field of information technology. Consequently, hackers can find their way into devices that have been connected or linked together during deployment. That is why it is important to rethink our approaches to the security of IoT servers and IoT devices. It is essential to understand the significance of building IoT security starting from the bottom up. This should also be embedded in the core project and organizational architectures when still at the conceptualization stage. This could further be developed into a multi-security system featuring bespoke solutions that can meet the exact corporate or individual requirements.

January 26, 2021

2. Problem Statement

The number of IoT servers and devices have been increasing exponentially year in year out. The limitations and requirements of these connected devices have also continued to increase related problems that mostly revolve around weak authentications (El-Hajj et al., 2019). The issue is, even more, augmented considering limited resources that have rendered the traditional security schemed and protocols ineffective and infeasible for the Internet of Things. Security issues that are associated with the IoT servers and IoT devices are continuing to create concerns because of the iniquitousness of those devices as well as the integration of the IoT in critical apps that could aggregate the potential effect of any security breach. Ideally, the security needs for an IoT network solely rely on the type of apps that it serves and the need for authentication, integrity, confidentiality, and availability (El-Hajj et al., 2019). Authentication is especially vital because it is regarded by experts as the key requirement for the effectiveness of IoT servers and IoT devices. Having trust in these IoT devices is the cornerstone for the attainment of a well-functioning network. That is bearing in mind that even one node that has been compromised could be used by malicious actors to the extent of bringing down the entire system or cause other disasters. In essence, the specific nature of IoT servers and IoT devices renders the traditional authentication schemes inapplicable and infeasible. Cryptographic schemes that are specifically meant for large memory, high processing devices, or main-powered devices cannot meet the needs of the IoT nodes that have limited resources. This has partly paved the way for the establishment of lightweight authentication techniques with some being specific to particular IoT contexts (El-Hajj et al., 2019).

As mentioned earlier, the use of connecting devices in our everyday lives could make the extent of security challenges that arise from poor authentication of IoT servers and IoT devices life-threatening (El-Hajj et al., 2019). The smartness that has been incorporated into electric grids, cars, and homes could be diverted into harmful scenarios once malicious actors have started exploiting them. The various hacking scenarios that have thus far been presented showcase the extent to which poor authentication could cause harm to society at large. Because of that, it is easy to note different types of attacks that could be associated with the IoT layers. At the perception layer, poor authentication could create loopholes on gateways or nodes that can then be manipulated by attackers with ease (El-Hajj et al., 2019). Loopholes in nodes can enable malicious actors to assume control over protocol states and cryptographic keys. Also, these vulnerabilities could as well give hackers a unique opportunity of cloning and redistributing malicious nodes within a network setup, thus compromising the security of the whole network (El-Hajj et al., 2019).

There is also the issue of DoS (Denial of Services) that could result because of poor authentication (El-Hajj et al., 2019). DoS is considered as a type of attack whereby the entire network or system is shut down by attackers, thereby preventing authorized parties or users from accessing them. This could overwhelmingly be attained through vast amounts of simultaneous spam requests that could end up overloading the network and prevent authorized users from receiving or delivering normal services. Next, poor authentication of IoT devices could lead to Denial of Sleep Attack. It is vital to note that one of the core purposes of the

IoT network is to sense via an extensive number of nodes that are widely distributed. In this case, the nodes offer different pieces of data such as vibration, humidity, and temperature data. These data are in this case provided at specific intervals after which the IoT devices could sleep and wait for the subsequent interval (El-Hajj et al., 2019). However, when it comes to the Denial of Sleep Attack, the power supply of the nodes is compromised leading to an increase in power consumption and reduced lifetime of services of the nodes. This is attained by preventing the nodes from sleeping once necessary data has been sent.

Poor authentication has further been associated with the problem of DDoS (Distributed Denial of Service) attacks. Here, the most challenging concern is the underlying capability of using a vast number of IoT nodes to pass traffic that has been gathered towards the servers of the victims (El-Hajj et al., 2019). Several studies associated DDoS attacks with IoT servers and IoT devices with some ending up compromising the whole networks or systems. Moreover, there have also been incidences of Sybil attacks on the fake node. Such attacks are whereby malicious actors tend to use fake nodes to deploy fake identities. In the event of a Sybil attack, the entire network or system could end up generating wrong data and even making neighboring nodes start receiving spam data that could compromise authentication protocols that have been implemented (El-Hajj et al., 2019). These fake nodes could be used by the attackers to transmit or convey data to nodes that are legitimate making them consume more energy and making services go down. Other attacks include and are not limited to mass node authentication, side-channel attack, routing attacks, and replay attack. Thus, the bottom line of this is that by putting all the above issues into consideration, it is clear that there is a dire need for the implementation of better authentication techniques for IoT servers and IoT devices (El-Hajj et al., 2019).

3. Material and methods

IoT servers and devices can be hacked remotely by malicious actors and unauthorized parties who might attempt to find their way into the device using an internet connection. If IoT devices could have been configured in a manner that allows for communication only with authorized servers, the outside communication attempts could have been ignored. The number of attacks targeting IoT servers and devices has continued to increase year in year out. Thus, as these devices are being integrated into corporate networks, special attention should be redirected to the essence of security. Powerful and efficient cryptographic solutions should be utilized because they can assist with the standardization of secure lines of communications between different devices and machines. Nonetheless, it is also a tough decision to select the most appropriate authentication model that can get the job done. Before choosing the architecture model that is ideal for IoT authentication, it is first of all essential to consider a wide range of factors that includes and are not limited to connectivity, security requirements, security expertise, financial budgets, hardware capacity, and energy resources. Therefore, the following models will be used to address the authentication problem that relates to IoT servers and IoT devices:

3.1. The Chain of Trust Model

The core purpose of the chain of trust model is to prove that a specific certificate comes from a given trusted source (Cheng et al., 2020). The model is comprised of three basic entities that form the valid chain of trust. They include end-entity, intermediate, and root. Consequently, the end-entity offers compliance, scalability, and security with certificate authority standards. Nonetheless, certificates, in this case, does not offer a guarantee that the subject under consideration is reputable or trustworthy in his business activities, safe to carry out business with, or compliant with specific laws. The end-entity offers vital pieces of information to the issuing certificate authority through a form of certificate signing request. This certificate has to be signed before being issued by a trusted certificate authority showing that the information that has been provided is correct at the time of issuance. The Secure Sockets Layer connection to the IoT server will not be successful if the certificate has not been signed or verified (Cheng et al., 2020).

Next, when it comes to the intermediate entity, the idea is that at least a single certificate should be present in the chain of the Secure Sockets Layer certificate (Cheng et al., 2020). They offer an important connection that allows the Root certificate authority to the extent their reputation of trustworthiness to entities that cannot be trusted. In this case, the issuing certificate authority is allowed to remain secure while being stored offline, thus offering additional security. In as far as the certificate authority is concerned, trust should always remain as explicit as possible. All custom applications, third party web browsers, and operating systems will have the opportunity of shipping more than one hundred trusted root certificate authorities that had been installed initially. This is different from non-root certificates that are implicitly trusted and do not have to be necessarily shipped with a certificate-ware app, a web browser, or an operating system (Cheng et al., 2020).

Lastly, the root certificate entity is an individual-signed certificate that has been designed to follow the X.509 certificate standards (Chau et al., 2017). It includes a hierarchical chain of trust with multiple levels that give web applications and clients the opportunity of verifying that particular trusted sources have been able to validate the identities of different end-entities. If by any chance the trust anchor private key is breached or become compromised, then every single certificate that has been signed under that private key are also going to be compromised and this will eventually mean that all certificates that have been provided by that certificate authority are also going to be affected. This will force the certificate authority to issue new certificates to each intermediate certificate authority as well as the end-entities in the underlying certificate chain. Because of that, the root entity certificate authority should monitor the private key closely and ensure that end-entity certificates are signed on a rare basis. If anything, the root authority should go ahead and create and sign at least one intermediate certificate authorities that will be tasked with issuing certificates and making sure that they have been linked back to the root certificate authority.

The chain of trust model could be further categorized into three models including the BA certificate authority architecture, web of trust, and hierarchical trust model (Roosa and Schultze, 2013). For the hierarchical trust model, there has to be a single root certificate authority or more subordinate certificate authorities. In this case, subordinated certificate authorities are meant to offer load balancing and redundancy when the root certificate au-

thority is offline. That means that even if the subordinate certificate authority has been compromised, the root certificate authority will have the opportunity to revoke the subordinate certificate authority, thus offering redundancy. Apart from that, the web of trust model which is also regarded as the cross-certification model has been designed such that the certificate authorities can form what could be considered as a peer-to-peer relationship. According to experts, this model is somehow challenging to manage with an increase in the number of certificate authorities (Roosa and Schultze, 2013). This type of trust relationship that is formed in this case could only take place when other company divisions have their unique certificate authorities that must work together. Lastly, the bridge certificate authority architecture model is different in the sense that it can overcome the challenges and complexities of the web of trust model. In this case, the bride certificate authority serves as the central point of coordination. That implies that other principals or certificate authorities have to trust the bridge certificate authority only.

3.2. The Threat Model

The IoT servers have been deployed at the cloud architecture and have the underlying capability of communicating with the IoT devices or the client over a wide area network (WAN) (Shah and Venkatesan, 2018). The use of single key authentication cannot be sufficient when it comes to the authentication of IoT devices and IoT servers. There are additional side-channel cyber-attacks that can provide the basis for the retrieval of shared keys when communication has been established between the IoT server and the IoT device. If passwords are not changed regularly, they become vulnerable to the brute force of dictionary attacks. As soon as adversaries have acquired the key that has been shared, fake devices could be created with that same key. Thus, while establishing the right model for the documentation of this task, a set of keys known as a secure vault could be used to authenticate both IoT devices and IoT servers (Shah and Venkatesan, 2018). Initially, the secure vault must be shared between the IoT devices and the servers and could change their values depending on the underlying data exchanges that might be taking place between these IoT devices and IoT servers (Shah and Venkatesan, 2018). With such a level of organization, the contents of the secure vault will be subject to constant change. No other messages will be exchanged between these IoT devices and IoT servers to the extent of modifying the value of the secure vault (Shah and Venkatesan, 2018).

In essence, a three-way mutual authentication technique for authenticating both the IoT devices and IoT servers are used (Shah and Venkatesan, 2018). The IoT devices will be responsible for the initiation of communication by redirecting the request for connection to the server. Once the request has been received by the IoT servers, the IoT servers will then send back challenges to the IoT devices. To this point, the IoT devices can then respond to the challenges by redirecting further challenges for authentication to the IoT servers. The IoT servers will then make a verification for the responses that have been provided and if by any chance they are valid, the IoT servers would eventually end up responding to the challenge that has been sent by the IoT devices. In the course of this session, the IoT devices and IoT servers have to create a shared secret also known as the session key. The session key has to fulfill fundamental purposes (Shah and Venkatesan, 2018). Firstly, they should

help encrypt all messages that have been exchanged between the IoT devices and the IoT servers. Secondly, they serve as encryption keys for message authentication codes that are relied upon for authentication of messages. All messages that in one or another are going to be exchanged between the two authentications that have been established are regarded as sessions. Session keys usually remain unmodified throughout the entire session even though varied sessions utilize different, unique session keys (Shah and Venkatesan, 2018).

4. Discussion

4.1. Security Keys

The advent of the IoT is arguably amongst the most exciting and dynamic developments in ICT (information and communications technology) (U.Farooq et al., 2015). The past two decades have seen networking devices becoming increasingly ubiquitous. However, these devices are largely been restricted to connect to the traditional end-user devices like tablets, smartphones, laptop and desktop computers, mainframes, and so forth. The past few years have seen have experienced more attachment of more and more devices to the network. These devices include and are not limited to digital assistants like Google Home and Amazon Alexa, smart TVs, traffic controls, street lights, electric controls and meters, medical devices, household appliances, and vehicles (F., 2012).

In essence, the IoT can be defined as a system of interrelated and interconnected digital and mechanical machines, computing devices, people, animals, or objects that have unique identifiers as well as the underlying capability of transferring data over a network without necessarily requiring human-to-computer or human-to-human interaction. In the light of the IoT, a thing can be any man-made or natural objects that could be assigned an IP (Internet Protocol) and have the ability to initiate data transfer over a network. Examples include automobiles with in-built sensors, farm animals with a biochip transponder, or an individual with an implant to monitor heart rate. Once these devices have been integrated with automated systems, it becomes easier to collect and analyze information and take appropriate action (Burgess, 2018). Many organizations in different industries are increasingly using IoT to enhance the effectiveness of their operations. They rely on technology to increase their business values, enhance decision-making capabilities, and establish a coherent understanding of their customer needs.

The need to authenticate IoT servers and IoT devices using security keys has attracted the attention of different groups of researchers and scholars in the field of information technology. According to (Das et al., 2018), authentication of online accounts is something that many people understand as something you have, something you are, or something you know. This partly implies to the use of passphrases, PINs, and passwords as knowledge; physical tokens as possessions, and biometric identity as a form of being intrinsic to oneself (Das et al., 2018). Other authentication techniques might include someone that you are conversant with and where you are. Once any of these methods of authentication are used together, the practice is considered as 2FA (two-factor-authentication). Although there exist different kinds of authentication options, the use of passwords is still continuing to dominate when it

comes to online authentication. In this case, the main concern is that passwords are associated with a wide range of security vulnerabilities and flaws with sheer amounts of generated passwords causing even greater risks (Das et al., 2018). Despite the continuing instances of passwords being compromised, many people are still using a single-factor authentication method that has greatly been associated with misalignment in human cognition, vulnerability in the event of social engineering, and difficulties when it comes to creating necessary policies. Even though a two-factor authentication is being adopted on a large scope, a simple examination of the benefits and risks that are associated with them could call for further evaluation of their adoption (Das et al., 2018).

To be in the sole position of assessing some of the reasons behind the limited adoption of two-factor authentication (Das et al., 2018) decided to implement a two-phase acceptability and usability assessment. The USB token that was subjected to tests in this case was the Yubico security key. The security key was selected because of its design focus on privacy and usability. A think-aloud protocol was implemented to help determine perceived costs, perceived benefits, and stop points. According to (Das et al., 2018), their research work was centered around previous studies about usable authentications using passphrases and passwords. The initial evaluation that was made about the security keys were made based on different frameworks that had been developed to evaluate various authentication approaches. It was evident that for authentication protocols to be accepted in a large scale, they must outperform the use of passwords in many fronts that includes and are not limited to preservation or privacy, scalability, physical burden, and cognitive burden (Das et al., 2018). Further research has also seen five important attributes being proposed for tokens namely; theft resistant, loss resistant, scalable, memoryless, and secure (Das et al., 2018). Despite the fact the use of security keys does not come in handy with a physical burden, it is physically effortless, and is lightweight because their operations are based on the pressing of buttons. Even more, security keys are unlikely to be stolen or get lost and are also scalable and secure besides being compatible with the use of passwords (Das et al., 2018). Once an individual has enrolled in the service, security keys are further considered as cognitively effortless (Das et al., 2018).

In a study that was conducted by (Guirat and Halpin, 2018), the science behind the establishment of security systems could be established based on firm grounds of formal protocols of verification. There are new protocols that could have their designs being validated in manner that is more mechanized to ensure that they are in sole positions of dealing with possible security flaws (Guirat and Halpin, 2018). One of the core risks that has been compromising the effectiveness of security of current information systems is the ability of different groups of users to create and subsequently utilize high-entropy passwords that are unique to specific domains. Even more, the whole idea of using passwords as what could be termed as symmetric secret when it comes to authentication includes the need to replace those passwords with symmetric cryptography (Guirat and Halpin, 2018). That is bearing in mind that security has for a long time now been perceived as a black art that is highly based on intuition as contrasted to science. That is amidst the context of cryptographic primitives and protocols being mostly judged because of the reputation that their creators exhibit. Contrastingly, the science of security would actually position security features of

different techno-social systems on the basis of science. This task is not only challenging but also demanding. That is why formal authentication approaches have paved the way for tremendous progress when coming up with the right definition for and varication fundamentals of security features (Guirat and Halpin, 2018). Game-hopping proofs that have been formalized have placed cryptographic field on what could be regarded as a sound basis and could function on complex protocols despite the fact that a lot is still to be done (Guirat and Halpin, 2018).

Science usually requires the use of methodologies. Apparently, methodologies that are relied upon by formal verification tools offer a very promising path when it comes to the verification of various security features including the privacy features of cryptographic protocols and primitives. The essence of formal verification includes the checking and establishment of different properties of cryptographic primitives and tools not through some of the proofs that have been created using hands, but via proofs that have been developed in a manner that has been mechanized fully (Guirat and Halpin, 2018). It is equally vital to note that whereas testing could assist in assessing the security requirements of particular programs, there is a possibility of failing to test a particular aspect, thus paving the way for security loopholes (Guirat and Halpin, 2018).

According to (Joye and Michalevsky, 2018), choosing a small public exponent creates room for less and faster computationally verification of signatures of RSA. This could be partly vital for devices with small power and modest budget for processing. Whereas practical attacks that could break accurate the deployment of RSA encryptions, studies have been able to unveil some of the attacks that have ended up emerging thereafter (Joye and Michalevsky, 2018). For instance, Coppersmith's theorem is one of the widely known theoretic attack that tend to target RSA encryption with the aid of low public-exponent. This theorem offers an efficient algorithm that could be used to determine small roots of various polynomial equations. The technique has already been applied by other researchers on some old attacks due to the underlying capability of encrypted messages that were meant for many recipients with each of them having their unique RSA public key. If anything, such attacks could have been prevented even better with the aid of widely-used and standard cryptographic libraries (Joye and Michalevsky, 2018). The research further shows that once malicious actors have been able to in one way or another recover particular bits that constitute the private key, it might become easier for them to go ahead and recover the whole private key, especially in instances where the public exponent is considerably low (Joye and Michalevsky, 2018). That is why it is essential to make sure that the whole RSA private key has been secured accordingly.

Practically, many cyber-attackers are highly likely to find it challenging to gain access to the private key at all or even to some extent manage to get all the bits of the private key (Joye and Michalevsky, 2018). In some instances, the whole notion of exposure of partial bits tend to make some sense when it comes to side-channel attacks like cache-timing or power-timing attacks. In such a case, attackers might be able to figure out specific bits with reasonable probability but end up encountering noise that are time-consuming and makes it harder to obtain all bits of the private key. The use of a larger component in such a scenario would make it generally challenging for the cyber-attackers to succeed in their malicious acts. That

means that even though there are many arguments out there that tend to favor the use of RSA alongside small public exponents, some security vendors might decide to restrict their support to exponents that are relatively larger (Joye and Michalevsky, 2018).

According to (Omorog et al., 2018), the fact that Wi-Fi networks or WLAN technology relies on radio frequency technology for the transmission of connection, it is associated with a wide range of security vulnerabilities. Its broadcast nature makes it easy even for the traffic that has already been encrypted to intercepted with ease making it vulnerable to attacks like jamming and eavesdropping (Omorog et al., 2018). Nonetheless, the security challenges that have thus far been linked with these Wi-Fi networks have not been sufficient enough to constraint the need for the establishment of ubiquitous connectivity. As a matter of fact, many individuals like the essence of being online, thus rendering the commonplace for Wi-Fi APs (access points) as hotspots. The rate of malicious activities that are carried out by cyber criminals have also been on the rise. They include computer hacking, financial heists, identity theft, and so forth. The major concern here is that these activities are mainly encouraged by poor security behavior and practices as well as weak understanding of the whole idea of internet security and their effects (Omorog et al., 2018).

The moment everything seems to be proper and secure, some internet users barely put the issue of security into consideration. This creates an avenue for hackers and other malicious actors to engage in their activities. Today, WAP2 or the IEEE 802.11i is considered as the core security standard that is applied globally when it comes to the encryption of Wi-Fi networks that could in some way become compromised by cyber-attackers. Experts believe that because Wi-Fi networks could be intercepted or sniffed with ease, it is important to use strong passwords that could counter or slow down the use of brute force or dictionary techniques (Omorog et al., 2018). Amidst such security recommendations, it is still unfortunate that key generation algorithms for routers of Wi-Fi networks have been receiving less attention from research bodies amidst the time when blog posts, videos, and hacker websites are continuing to flourish while offering enlightenment on how to crack WPA2 security standards. Besides the underlying knowledge to the contrary, recent studies have mainly focused on four-way handshake dauthentication/authentication, frames, and encryption.

According to (Omorog et al., 2018) are imperative that despite being overlooked in many instances, microcontrollers are the central components that have been embodied in systems that have the underlying capability of driving the transition towards the adoption of the IoT. Consequently, microcontrollers have not only less costly but are small and can be handled with ease leave alone the fact that they can be applied in a wide range of applications (Strobel et al., 2014). The increase in the number of systems that have been equipped with microcontrollers also raises questions about safety and security. The continued evolution of the IoT technology can only increase the underlying need for embedded apps that have been designed with strong security features. As such, it is high time for users and design engineers to go back to the drawing board and evaluate the feasibility of microcontrollers as part of the body of security devices (Strobel et al., 2014).

While trying to conduct an automated analysis of different security protocols at the global scale, (Kremer and Künnemann, 2016) established that it is important to security of protocols, key servers, and APIs that are required to keep the statuses of various transactions

should be in sole positions of maintaining non-monotonic and global state such as the form of registers or databases. Nonetheless, verification tools that exist today cannot allow for the analysis of this kind of stateful security protocols (Kremer and Künnemann, 2016). That is amidst the past success of automated analysis of a wide range of security protocols. The use of automated tools has made it easier to discover flaws and vulnerabilities in different platforms such as the Google Single Sign on Protocol. Whereas there exist more efficient tools like Maude-NPA and AVISPA, it is apparent that some of these tools are unable to conduct a full analysis of protocols that to some extent by need non-monotonic global state. Such an abstraction is considered is ideal for the monotonic prior knowledge of cyber-attackers, thus making the tools to be very effective during the verification of unbounded number of sessions of protocols. They further make it easy to build on techniques that are already there for the attainment of what could be termed as the Horn clause resolution (Kremer and Künnemann, 2016).

The study further reviews various case studies that sheds light on simple APIs such as Yubikey security token (Kremer and Künnemann, 2016). The security token is based on the basic assumption that as our online presence continues to increase it becomes increasingly ideal to bolster our online security practices. Yubikey security token functions based on the principles of two-factor authentication. This is a kind of hardware that can be plugged into a computer or a mobile device. The security token can be utilized alongside passwords when trying to authenticate logins to different websites (Kremer and Künnemann, 2016). It is easy to think of it as a physical that rather than being used to unlock the door, it can be used to unlock online life. There are many manufacturers in different parts of the world who manufacture these security tokens and the function almost the same way. As mentioned earlier, the security token operates based on the two-factor authentication standards and by integrating public key cryptography with authentication that is based on hardware. Being somehow challenging to compromise, the hardware can be used for secure access to a wide range of online services like Mac OS, Windows, Dropbox, Facebook, and Google. Also, the tool comes in handy with the underlying capability of supporting password managers such as Keepass, Dashlane, and Lastpass (Kremer and Künnemann, 2016).

According to (Crocker and Querido, 2015), the cloud platform is widely used to share, back-up, and store different pieces of information. Issues of data privacy and confidentiality are vital and topical concerns in the context of the current cloud technology that is subject to change. Considering the increase in the identity of users who use the cloud platform, difficulties have as well been associated with the ability to manage keys and passwords. Despite the fact that different cloud providers might decide to offer contract guarantees that data that has been stored cannot be accessed by both their administrators and malicious actors, a real mechanism of barring them from establishing access does not actually exist (Crocker and Querido, 2015). One of the possible approaches that could be used to address this issue includes the establishment of secure containers whereby users' data and files could be added and that it is only the users who could be granted access. The use of master keys that have been retrieved from the passphrases that have been selected by the users provides users with the convenience of decrypting and encrypting these secure containers and have access to files. For instance, once an attacker has been able to guess the passphrase of specific users, they

could end up compromising all data files that will have been stored in the container. Additionally, if by any chance a single file is modified or compromised, the entire file container has to be synchronized using the existing cloud environment (Crocker and Querido, 2015). A further approach that could be used to address this problem is using a system that has the underlying capability of individually encrypting every single file rather than relying on the secure container. Despite the fact that the problem that is associated with synchronization can be addressed, security concerns will still be there. This is partly due to the fact that attackers will still be able to have access to all files as soon as the users' passphrases have been figured out. Ideally, this security approach does not have the right proponents like the BoxCrypt application. Therefore, to implement appropriate security measures against such kind of threat, it is advisable to have a second aspect of encryption and of different nature (Crocker and Querido, 2015). That will imply that should passphrases belonging to various users become compromised by cyber-attackers through techniques like social engineering, and keyloggers, the attackers would still not be able to have access to the second authentication factor. This is generally beneficial because it helps standardize and at the same time simplify key management and authentication (Crocker and Querido, 2015).

4.2. Cloud Computing

The IoT technology is considered to be an extension of cloud computing. Cloud computing is a general term referring to the delivery of a wide range of hosted services over the internet. In other words, cloud computing is the provision of various on-demand computing services like processing power, storage, and applications, typically on a pay-as-you-go basis and over the internet. These services are placed into three broad categories including SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), and IaaS (Infrastructure-as-a-Service). According to (Vasanth.C.Bhagawat, 2015), cloud computing has evolved into one of the most inspiring technology in industry and research. It is a model that necessitates convenient, ubiquitous, on-demand network access to a wide range of configurable computing resources including, services, applications, storage, servers, and network that can be provisioned and subsequently released with minimal interaction with the service providers and management efforts. Due to its high computational value, cloud computing has continued to grow and allow companies such as Microsoft Azure to offer their cloud computing services through the internet (Vasanth.C.Bhagawat, 2015).

The vast cloud's capability to store and ensure availability of different applications and contents poses a lot of risks that relate to security and privacy (Kshetri, 2013). This is an important issue of concern, especially for diffusion of the cloud because many organizations rely on the cloud for their mission critical and strategic functions. In that same regard, cloud providers are said to be experiencing numerous challenges and pressure from different stakeholders including the members of the society to protect information and other sensitive data assets that belongs to the customers Kshetri (2013). Today, there is a huge gap between what cloud providers claim to be offering, and what potential and existing adopters think about cloud computing's cloud security. On the flip side, players in the industry are starting to realize the need to establish standards that can be used to offer guidance for promoting privacy and security. Because of a wide range of individual and organized efforts, the society

at large is anticipating for significant security changes in cloud-related institutions (Kshetri, 2013).

Cloud computing can be classified into different architecture models, types, and classifications (Krishna et al., 2016). The public cloud, private cloud, and hybrid cloud are the three major transformative types of networked computing model. The underlying cloud infrastructure could assume different features and forms including hyper-converged models, software-defined, virtualized models, and so forth. The public cloud can be described as the cloud computing model in which IT services are offered through the internet. Consequently, the service could be charged, subscription-based, freemium, or free depending on the type of computing resources that are being used or consumed. The corresponding computing functionality vary and might include services such as infrastructure environment, storage, apps, and emails. It is the responsibility of the cloud vendors to maintain, manage, and develop the different pools of computing resources that are provided to different tenants. The main defining features of public cloud solutions are scalability of the IT-enabled services and high elasticity that are provided at relatively low costs and based on pricing tier. The public cloud has developed into the most common way for cloud computing deployment (Persico et al., 2016). Consequently, cloud resources such as storage and servers are operated and owned by third party cloud vendors after which they are delivered through the internet. A great example of a public cloud is Microsoft Azure. The cloud provider manages and owns all software, hardware, and related supporting infrastructure in public cloud. In this type of cloud, tenants share network, storage, and hardware with fellow tenants. These tenants manage their accounts through web browsers. A majority of public cloud deployments offer online office applications, web-based email, testing, storage, and development environments. Some of the advantages that are associated with the use of public clouds include high reliability, near-unlimited scalability, no maintenance, and lower costs.

The private cloud is widely known as a cloud solution that is mainly dictated for use by a single corporation or organization. Here, the data center resources could either be operated by third-party vendor off-site or on-site. The underlying computing resources are isolated before being delivered through secure private networks rather than being shared with fellow customers. Private cloud can be customized to meet the various security and business needs of an organization at large (Sridhar and Smys, 2016). With greater control and visibility into such infrastructure, companies can operate IT workloads that are compliance sensitive without necessarily having implications on performance and security. The private cloud is comprised of a wide range of computing resources that are exclusively used by a single organization or business. Besides, the private cloud can be located physically on an organization's on-site datacenter, or could be hosted by third-party service providers. Infrastructure and services in the private cloud are usually maintained on what could be termed as a private network whereas software and hardware are typically dedicated to solely fulfill organizational needs. Private clouds are in most cases used by financial institutions, government agencies, and other middle to large government corporations that have business-critical functions aimed at promoting control over a cloud environment. Advantages of the private cloud includes and are not limited to high scalability, improved security, and more flexibility.

Lastly, a hybrid cloud is defined as the cloud infrastructure environment that constitutes the mix of private and public cloud solutions. In this case, resources are mainly orchestrated as infrastructural environments that have been integrated. Data workloads and applications can share a wide range of resources between private and public cloud deployment depending on organizational efficiency and cost, scalability, performance, technical policies that revolve around the subject of security, and so forth (Linthicum, 2016). For example, a company can use a private cloud for its information technology workloads and at the same time complement the underlying infrastructure with some public cloud resources with the hope of accommodating spikes in network traffic that are likely to be experienced on occasional basis. Because of that, access to other computing capability will not necessarily need high CapEx of the private cloud environment. Instead, it will be delivered through the public cloud solution as a short-term IT service. Here, the environment is by itself integrated to attain a high level of scalability and performance to the changing or evolving business needs. Many would describe a hybrid cloud as the best of the two worlds because it includes combination of private clouds, or on-premise infrastructure, with the public cloud to provide corporations with the convenience of reaping or gaining from the advantages of both. Here, applications and data can move between public and private clouds for enhanced deployment options and greater flexibility. For example, private cloud can be used for highly sensitive and business-critical activities such as reporting on financial issues and public cloud for lower-security and high-volume needs like web-based mail. Cloud bursting is also an option in hybrid cloud (Yangui et al., 2016). This is where a resource or application is configured to run in the private cloud up to the point where spike in demand like tax filing or any other seasonal event is realized. From there, the organization can proceed further and burst through all the way to the public cloud to tap or capture more computing resources. Some of the advantages of hybrid clouds includes and are not limited to transitioning ease, cost-effectiveness, flexibility, and enhanced control.

4.3. Authentications

Authentications are processes that are involved in verifying whether something or someone is what or who is declared to be. In other words, an authentication is an approach that is employed when trying to recognize the identity of users. The mechanism entails relating incoming requests to various sets of identifying credentials. Credentials that have been provided are first of all compared to those that have been filed in the authentication servers, operating systems, and databases for information about authorized users. Authentication processes will always run at the start of applications before any other code is given the green light to proceed. Multiple systems might need varied credentials to determine the identity of the users. These credentials normally assume the form of passwords that could either be known or secret to a system or individuals.

There are three authentication techniques. They include something that you are such as a scanned body part, something that you have like token keys and something that you know like a password. Essentially, something that you are is considered as the strongest authentication method that is the hardest to crack. For instance, it is not easy for one to duplicate fingerprints or replicate an iris scan. Something that you have has continued to

gain popularity because of people's unwillingness to be detached from their mobile devices. This access control technique usually assumes the form of a one-time toke key that can be retrieved from external sources. Lastly, something you know does not require special hardware. Just like the use of passwords, there are no additional tools that are required to offer secret codes. That is why people are highly encouraged to come up with passwords that are difficult to guess.

4.4. Multi-Factor Authentication (MFA)

MFA is an authentication technique whereby users offer at least two verification factors to establish access over resources like virtual private networks, online accounts, or applications MFA is considered to be an important aspect of strong policy for identity and access management. For instance, instead of being required to provide a password and a username only, MFA requires the use of an additional verification factor, thus minimizing cyber-attacks. In information technology, credentials that form MFA can take the form of locations, time, biometrics, numerical codes, hardware tokens, passwords, and so forth (Das et al., 2019). Technically, combining any two of such credentials is considered as MFA. That is despite the fact that a majority of implementations tend to capitalize on two factors or what is considered as two-factor authentication. Using many credentials rather than one makes authentication process more secure even if one of the combinations that has been used is compromised. For MFA to work, users' credentials must come from a minimum of two of three different factors or categories (what you are, what you have, and what you know) (Ibrokhimov et al., 2019).

4.5. Weak Passwords

Passwords are arguably the most common authentication forms that are used to establish control over information such as voice mail systems, calling cards, telephone, credit cards, automated teller machines, and personal identification numbers. Many people use passwords because they are convenient, inexpensive, and simple mechanisms to implement and use. Similarly, passwords are regarded as extremely poor forms of authentication or protection. It is very difficult to manage password problems since one computer network could possibly have thousands or hundreds of accounts that have been protected using passwords and that only one of them could be compromised to provide potential attackers with access to the network or system. With the current nature interconnected internet, skillful hackers can use passwords to compromise millions of systems (Vakilinia et al., 2019).

Weak passwords usually play significant roles in any form of hacking activity (Sudhanshu and Chauhan, 2015). Some systems and applications do not promote password complexity, thus encouraging users to use simple passwords like their phone numbers, god, 12345, and 123. Weak passwords are not necessarily characterized by the characters or length that has been used. They could as well be associated with guess ability. For instance, a password like name@12345 appears to be pretty complex, but could be guessed (Sudhanshu and Chauhan, 2015). Users are encouraged to avoid passwords that relates to mobile numbers, places, or names. Weak passwords are easy to guess and, in some instances, especially when they are too short, attackers can use brute force. That is why users are highly encouraged to

utilize special characters alongside random strings. Even though it might be difficult to remember such a password combination, the truth is that they are quite secure (Sudhanshu and Chauhan, 2015).

4.6. Importance of Multi-factor Authentication (MFA)

The core importance of MFA is that it increases organizational security (Dasgupta et al., 2017). The technique requires all users such as organizational employees to identify themselves using additional credentials rather than just usernames and passwords. Essentially, usernames and passwords are vulnerable to brute force attacks and could be compromised or get stolen by unauthorized third parties. Promoting the use of MFA at the organizational level promotes the sense of confidence that an organization remains safe from potential cyber-attacks.

Passwords are considered as the most popular authentication technique. However, they provide very little protection because once stolen, they can be used by hackers or unauthorized users to wreak serious havoc, bypass other access controls, and log in to business systems and applications. According to research, stolen login credentials are the most common means that hackers use to carry out data breaches. There are many other attack vectors out there that cyber criminals can use to gain access and steal passwords such as stolen hardware, point of sale intrusions, web app attacks, brute force attacks, and phishing attacks. Some users make things easier to cyber-attackers by keeping the same passwords for considerably long period of time, storing their passwords in locations that are not secure, using the same passwords different applications, and going for weak passwords. Thankfully, MFA comes in handy with an additional protection layer that makes it easier to deal with these problems. This technique addresses the ripple implications of credentials that have been compromised because even if malicious actors might steal users' password and usernames, they will be prompted to offer another factor before being allowed to access sensitive data.

MFA is also important because based on recent surveys, a majority of security and information technology (IT) professionals think that it is the most effective security control for both public cloud and on-premise data. Additionally, many current MFA solutions that are also available in the market are easy and fast to implement. The solutions make it easy for companies to implement the security controls without redirecting a lot of effort and time on the same. That is besides the level of cost-effectiveness that come in handy with the same solutions.

Another vital significance of MFA authentication is that it offers an excellent way of enabling enterprise mobility (Acar et al., 2019). This is especially important since enterprise mobility is a significant initiative that is prioritized by many companies that are still undergoing digital transformation. Level of productivity usually increases when workers or employees are able to use devices that they prefer with securely and easily to access resources that they need to fulfill their tasks. The use of MFA authentication to remotely log in to a network using virtual private networks or long into business applications provides a high level of flexibility. Besides, encouraging the use of MFA at the organizational level is a clear indication that a firm is committed at both network and date protection measures.

MFA is also important because it forms part of compliance with specific geographical and industry regulations. For instance, PCI-DSS requires implementation of MFA on specific instances to prevent unauthorized users and malicious actors from accessing systems that are used to process payment transactions. Additionally, MFA provides healthcare institutions and providers to have the convenience of complying with HIPAA. The authentication method is considered to be an integral part of making sure that strong customer authentication has been met, especially in financial institutions.

MFA helps promote cybersecurity. As the scope and number of cybercrimes continue to increase, enterprises are soon starting to realize the scope of threats that they are facing. In the world of today, cyber-attackers do not target large organizations only. Approximately 31% of companies that have less than 250 employees have been popular targets of cyber-crimes. It is equally vital to note that the intention of cyber-attackers is not just stealing data. Some of them try to destroy or corrupt it completely. Because of this concern, the market for MFA is expected to hit about $12.51 billion in the next four years.

Further, implementation of MFA is important when it comes to setting security expectations (Henricks and Kettani, 2019). As a matter of fact, identification of organizational security requirements is considered to be an integral part of any implementation of MFA. For instance, it is important to consider things like business model, industry, type of data that should be stored, utilized, or captured, and applicable compliance regulations to attain normal business functions. Implementation of MFA provides all organizations with the opportunity to single out and classify typical business scenarios depending on the level of risks and to figure out situations when MFA should be applied. For example, based on different sets of factors, companies could choose to use MFA when workers are logging in remotely, when specific databases or applications are being accessed or for high-risk scenarios. Apart from that, MFA could also be used to limit locations where users can access data or information from, thus enhancing access restriction measures.

4.7. Different Implementations of Multi-factor Authentication (MFA)

There are various ways of implementing MFA. Examples include:

- Using a time-based one-time password (TOTP). TOTP functions by generating a one-time password from the current timestamp and shared secret key using particular types of cryptographic function. Here, the cryptographic functions tend to vary across the board.
- The use of short message service (SMS). Once you try to log in to systems or resource, a text message with a code is automatically sent to your phone. Because you are the only person who has access to your phone, you will automatically receive notification of any attempt made to log into your system, resource, or account.
- The use of electronic mail (email).
- Push notifications.

4.8. Statistics and Numbers on Security

The field of information technology (IT) is complex and subject to change. Any security change has the potential of setting off a chain of adjustments and tweaks that could irritate users. Streamlined authentication processes helps maintain productivity level in the IT

sector a high as possible. That is why IT administrators are encouraged to make sure that all emerging upgrades are integrated to increase security. With MFA, IT administrators have a unique opportunity of adapting the required level of security support with the aid of contextual information like geo-location and behavioral patterns.

Identity theft is a high-reward, low-risk, and an easy type of crime and threat to individuals and organizations. It is one of the fastest growing crimes that is increasingly becoming more profitable compared to crimes that relates to drugs. Research has shown that stolen and weak user credentials are important weapons to hackers who have been using them in almost 95% of all attacks that have been orchestrated on web applications. Malicious actors seem to be on the winning side because between 2013 and 2014, the total number of attack breaches that ended up being successful had gone up by approximately 27.5%. Even though these breaches have been associated with companies that bear household names, there has been a further concern because out of all target attacks, about 31% have been targeting business enterprises with less than 250 employees.

Advanced firewalls and anti-virus systems are as important as vulnerability tests. However, the front door will always remain open without proper user authentication. Password theft has continued to evolve as attackers attempt to utilize highly sophisticated techniques like pharming, phishing, and keylogging. The bitter truth is that cyber-attackers have been trying to do more than just steal data. They change services or programs, destroy data, or use servers to transmit malicious code, spam, or propaganda.

4.9. Effectiveness of Multi-factor Authentications (MFA)

Many IT departments would agree that implementing MFA across all access points could bolster organizational security. The problem is that the nature of MFAs could be tedious leaving some people wondering about their effectiveness. Therefore, to truly understand the effectiveness of multifactor authentications, it is first of all important to develop a coherent understanding of how hackers and other malicious actors engage in their activities in the absence of MFA. In a nutshell, cyber-attackers are required to access your password and username. Some of the typical access techniques that hackers have been using to steal sensitive information include:

- Dark Web: In both small and large organizations, data breaches can always mean that confidential information has been made available on the Dark Web where people with bad intentions can purchase or sell them. Such information could be corporate login information or personal information such as bank information, credit card numbers, driver's license information, and addresses.
- Malware: There are different ways in which malware can find its way into your computer. This could be through thumb drives, network shares, attachments, websites, emails, and so forth. The problem is that once malware has entered your computer, it can do a lot of terrible things including keylogger that can be used to record anything that you type and forwards them to cyber-attackers. Logging in into a website where keylogger is active and running can only mean that your password and username are going to be shared immediately.

- Social engineering: Just like phishing, social engineering takes place when cyber-attackers decide to impersonate other people in an organization or corporation. Once they do so, they can then send you an email requesting that they are granted access to resources like network servers. If the individual who has been impersonated is a senior person, there are high chances that those who have been tricked will share requested information without asking a lot of questions.
- Smishing/Phishing: A majority of phishing activities occurs when cyber criminals decide to send millions of emails to specific individuals. These emails could be offering warnings about compromised passwords, thus prompting the receivers to change them. In such a case, the link that will be provided is always fictious and will make it possible to immediately gather all login credentials that is shared. The malicious actors can then attempt to use the credentials to gain access to sensitive information of their victims including their banks. Smishing works the same way except that initial messages come in form of texts.
- Brute Force: Brute force is an automated technique of attempting thousands or hundreds of passwords in order to gain access over a system. It is often based on personal information about an individual such as anniversary dates, pet names, spouse names, and birthdays as well as common passwords.

Thousands of people from different parts of the world including prominent and intelligent ones get hacked everyday using either of the above methods. As soon as malicious actors have been able to acquire your login credentials, they can cause a lot of damage.

According to Microsoft, MFA blocks approximately 99% of account hacking attempts. Users who want to prevent 99% of automated attacks should consider implementing MFA because it does the trick pretty well. This strategy is not just effective for Microsoft accounts only, but also for other accounts. That is why it is highly encouraged that MFA is enabled regardless of whether there are complex or simple security measures in place. The advice was further echoed by Google by encouraging users who were using phone number for account recovery purposes because the rationale helps strengthen security of their accounts. That among others is a clear indication of the overall effectiveness of MFA.

MFA is an effective and proven technique than just using credentials. Its effectiveness revolves around the fact that whereas malicious actors might obtain users' credentials through credential stuffing or phishing attempts, they cannot easily obtain second verification. The method is considered to be an integral aspect of the zero-trust security and requires that users should offer at least two credentials if they want to gain access over sensitive information and resources. So far, this form of security approach has been proved to protect resources, sensitive information, accounts, and so forth from cyber-attackers. MFA functions by preventing attacks that could result from cyber criminals attempting to guess or obtain users' credentials.

The effectiveness of MFA is further demonstrated through its applicability in various industries including education, communication and media, technology, and financial services among others. Being a process whereby users are required to pass at least two authentication levels to access information, resources, accounts, or data, MFA has continued to gain popularity. It has become increasingly important to implement MFA, especially now that companies are facing cyber threats of different scopes and nature. The chances of suffering

from cyber-attacks will usually decrease by adding another security layer. Essentially, this is because of the difficulty that is associated with attempts to surpass multiple levels of authentication.

5. Conclusions

To sum up, MFA is one of the proven approaches that could be used to increase cyber security. It is clear that even though passwords play an integral part of promoting security, they are not entirely infallible. Cyber-attackers can use different methods to compromise, steal, or guess your passwords. However, MFA can assist significantly because it makes it more challenging for malicious actors to access accounts or devices. That is why many companies have been providing MFA features in most of their product offerings.

6. Results

6.1. Proof of Concept

There was a demonstration of how fake domains and social engineering could be used to bypass the use of passwords. To address this concern, further research was conducted to determine the effectiveness of 2FA technique. Even though 2FA has some weaknesses that could be explored through push notifications, the security approach emerged as an excellent first step that can help keep attackers at bay. In this research, evaluations were made on IoT servers and IoT devices that had been configured using 2FA and results documented. It emerged that in as much as this research was seeking a basis for assessing the effectiveness of security keys in the authentication of IoT servers and IoT devices, the core objectives were met. 2FA comes in handy with the scalability and adaptability that can enable both organizations and individuals to meet their security needs.

6.2. Research Evaluation

This prototype that came up in this study was evaluated based on the dominant nature of the use of passwords. Whereas some people go for weak passwords that could be compromised easily using brute force and dictionary attacks, 2FA enhances the effectiveness of promoting security. An evaluation about the scope of the use of 2FA was conducted and the extent to which the security approach is being adopted and implemented assessed even further. Two models were used to help bolster the testability of the authentication technique in the light of similar researches that have thus far been carried out by other scholars. It emerged that as contrasted to overreliance on the use of passwords, it appeared that many users find it more secure to use 2FA. Therefore, it will be especially vital to encourage users to start accepting the use of this authentication approach.

Acknowledgment

I wish to thank my parents for their support and encouragement throughout my studies and special thanks to my supervisor Dr. Mohammad Tabrez Quasim.

January 26, 2021

References

Acar, A., Liu, W., Beyah, R., Akkaya, K., Uluagac, A.S., 2019. A privacy-preserving multifactor authentication system. Security and Privacy 2, 1–19.

Burgess, M., 2018. What Is the Internet of Things? Wired explains. MicroPython for the Internet of Things , 1–25.

Chau, S.Y., Chowdhury, O., Hoque, E., Ge, H., Kate, A., Nita-Rotaru, C., Li, N., 2017. SymCerts: Practical Symbolic Execution for Exposing Noncompliance in X.509 Certificate Validation Implementations. Proceedings - IEEE Symposium on Security and Privacy , 503–520.

Cheng, G., Xie, H., Zhang, D., 2020. Analyzing the Chain of Trust Model Based on Entity Dependence. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12472 LNCS, 146–159.

Crocker, P., Querido, P., 2015. Two factor encryption in cloud storage providers using hardware tokens. 2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings.

Das, S., Russo, G., Dingman, A.C., Dev, J., Kenny, O., Camp, L.J., 2018. A qualitative study on usability and acceptability of Yubico security key. ACM International Conference Proceeding Series.

Das, S., Wang, B., Tingle, Z., Camp, L.J., 2019. Evaluating user perception of multi-factor authentication a systematic review. arXiv.

Dasgupta, D., Roy, A., Nag, A., 2017. Advances in User Authentication.

El-Hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A., 2017. Analysis of authentication techniques in Internet of Things (IoT). 2017 1st Cyber Security in Networking Conference, CSNet 2017 2017-Janua, 1–3.

El-Hajj, M., Fadlallah, A., Chamoun, M., Serhrouchni, A., 2019. A survey of internet of things (IoT) authentication schemes. Sensors (Switzerland) 19, 1–43.

F., Yang, L.T.W.L..V.A.X., 2012. Internet of Things. International Journal of Communication Systems 23, 633–652.

Guirat, I.B., Halpin, H., 2018. Formal verification of the w3c web authentication protocol. ACM International Conference Proceeding Series.

Henricks, A., Kettani, H., 2019. On Data Protection Using Multi-Factor Authentication. ACM International Conference Proceeding Series , 1–4.

Ibrokhimov, S., Hui, K.L., Al-Absi, A.A., Lee, H.J., Sain, M., 2019. Multi-Factor Authentication in Cyber Physical System: A State of Art Survey. International Conference on Advanced Communication Technology, ICACT 2019-Febru, 279–284.

Joye, M., Michalevsky, Y., 2018. RSA signatures under hardware restrictions. Proceedings of the ACM Conference on Computer and Communications Security , 51–54.

Kremer, S., Künnemann, R., 2016. Automated analysis of security protocols with global state. Journal of Computer Security 24, 583–616.

Krishna, B.H., Kiran, S., Murali, G., Reddy, R.P.K., 2016. Security Issues in Service Model of Cloud Computing Environment. Procedia Computer Science 87, 246–251.

Kshetri, N., 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy 37, 372–386.

Linthicum, D.S., 2016. Emerging Hybrid Cloud Patterns. IEEE Cloud Computing 3, 88–91.

Omorog, C.D., Gerardo, B.D., Medina, R.P., 2018. The performance of blum-blum-shub elliptic curve Pseudorandom Number Generator as WiFi protected access 2 security key generator. ACM International Conference Proceeding Series , 23–28.

Persico, V., Montieri, A., Pescape, A., 2016. CloudSurf: A platform for monitoring public-cloud networks. 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow, RTSI 2016.

Roosa, S.B., Schultze, S., 2013. Trust darknet: Control and compromise in the internetś certificate authority model. IEEE Internet Computing 17, 18–25.

Shah, T., Venkatesan, S., 2018. Authentication of IoT Device and IoT Server Using Secure Vaults. Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and

Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 , 819–824.
Sridhar, S., Smys, S., 2016. A hybrid multilevel authentication scheme for private cloud environment. Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016.
Strobel, D., Oswald, D., Richter, B., Schellenberg, F., Paar, C., 2014. Microcontrollers as (In)Security Devices for Pervasive Computing Applications. Proceedings of the IEEE 102, 1157–1173.
Sudhanshu, Chauhan, N.K.P., 2015. Hacking web intelligence: open source intelligence and web reconnaissance concepts and techniques. volume 53.
U.Farooq, M., Waseem, M., Mazhar, S., Khairi, A., Kamal, T., 2015. A Review on Internet of Things (IoT).International Journal of Computer Applications 113, 1–7.
Vakilinia, I., Cheung, S., Sengupta, S., 2019. Sharing Susceptible Passwords as Cyber Threat Intelligence Feed. Proceedings - IEEE Military Communications Conference MILCOM 2019-Octob, 774–779.
Vasanth.C.Bhagawat, D.A.L., 2015. Survey on Data security Issues in Cloud Environment. International Journal of Innovative Research in Advanced Engineering 2, 31–35.
Yangui, S., Ravindran, P., Bibani, O., Glitho, R.H., Hadj-Alouane, N.B., Morrow, M.J., Polakos, P.A., 2016. A platform as-a-service for hybrid cloud/fog environments, in: 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1–7.