A survey on authentication methods for the Internet of Things

Dylan Sey[1]

[1]**School of Computing, Mathematics and Digital Technology**
[1]**Manchester Metropolitan University**

Corresponding author:
Dylan Sey[1]

Email address: dylan.sey@stu.mmu.ac.uk

ABSTRACT

This survey focuses on authentication methods for the Internet of Things (IoT). There are many different authentication methods that are used in the IT industry but not all of these can be adapted for the IoT. Lightweight and mutual authentication methods will be covered in this paper, alongside two authentication methods that are commonly used in other areas of the industry, rather than the IoT area, which are Kerberos and Group audio-based authentication. The survey will find that Mutual authentication is vital for the IoT and, due to the constraints that are apparent within the IoT devices; the lightweight option is very useful when it comes to dealing with areas like low bandwidth. As a result, there will be gaps that could be further investigated such as the advancement of the IoT technology so that more types of authentication are feasible. A conclusion to this paper is that, by combining different methods of encryption and authentication methods, there are always possibilities to make the proposed protocols more lightweight and secure.

1 INTRODUCTION

This survey will discuss the different methods of the authentication within the Internet of Things (IoT) and then go into one of these methods in further detail. This is a significant part of the computing industry because so many devices in everyday life are affected by IoT, so it is vital that users on this are secure and not vulnerable to attacks or illegitimate users Atwady and Hammoudeh (2017); Mohsin et al. (2017); Aloraini and Hammoudeh (2017); Moffat et al. (2017). The target audience for this survey is young Computer Science or Computing Students/Professionals that are looking to extend their knowledge on Authentication, the IoT and more specifically the different authentication methods that are used in IoT.

Authentication is a term used frequently in the Computing Industry, but what is Authentication? Authentication in everyday terms is described as establishing the identity of an entity that has not been through the authentication process to prove they are who they say they are Lopez-Research (2017). For example, when using your passport to travel, the serial number will be checked to see its legitimacy and then a visual comparison will be made by the person authenticating it. Furthermore, the Authentication problem can be a bit trickier within the Internet, due to networks not always having physical access to entities they are granting authentication. There is a huge problem when authentications are granted to malicious users Lopez-Research (2017), malicious entities can try and obtain sensitive information, disrupt service to the network/programs or even forge fake data by impersonating valid users of the service.

Mutual Authentication is when two entities will authenticate one another at the same time. Mutual Authentication is included in several different areas of authentication such as SSH. The two types of authentication used by mutual authentication will be either certificate based, or username and password based. This means that the majority of people are using mutual authentication daily without realizing; it is a very fast and efficient way of authentication Ghafir et al. (2017).

The Internet of Things (IoT) is one of the most predominant topics in the computing industry today, however, this is not a new notion McDaniel (2017); Alsboui et al. (2012); Hammoudeh (2015); Hammoudeh et al. (2008). The ground work for the Internet of Things was laid in the early 2000's by a

man named Kevin Aston, his "concept was simple If all objects in daily life were equipped with identifiers and wireless connectivity, these objects could be communicating with each other and be managed by computers McDaniel (2017); Hammoudeh and Alsbou'i (2011)". The article explains that at the time of these ideas, the technology available was in need of substantial improvements. This problem has been minimised today as the technology available has vastly improved and continues to do so. The article goes on to explain that, with technologies like IPv6 allowing us to have billions assigned with communications addresses and the ever-decreasing cost of wireless technologies, it is estimated by Cisco's Internet of Things Group, that by the year 2020 there will be 50 billion devices all communicating with each other in the IoT.

2 SURVEY BODY

This section of the paper will analyse two different types of authentication methods that reside in the IOT; Lightweight and Mutual Authentication in IoT infrastructure. After the critical analysis of these, further research will take place and two papers will be surveyed looking into future methods that may be used.

2.1 Lightweight authentication

Lightweight Authentication is a popular authentication method within the Internet of Things with extensive research written based on it Newman and Hammoudeh (2008); Hammoudeh et al. (2009). The first is Esfahani et al. (2017). This article was written about the technique of Lightweight Authentication for the communication between machines i.e. M2M communication in the industrial IoT Environment which is meant to be the next industrial revolution making this task extremely important. Another challenge that is faced when dealing with such a task is that, although numerous different authentication ideas were proposed to help with the security in the IoT, once the element of Industrial IoT were added this wasn't simple, due to the potential limitations that this area may have which include; computing power, Communication bandwidth. The proposed idea was to apply Lightweight Authentication mechanism to have M2M communication eliminating the constraints for future production systems, the devices that needed to communicate was a Smart sensor which included a Secure Element and Router with Trusted Platform Module which is a secure cryptography process that is embedded into devices.

This process can be achieved in several ways. The chosen method to complete this task was getting the Industrial devices registered with the chosen authentication service, and then carrying out the authentication process between the router and sensor. This is achieved by Mutual Authentication which will be explained later when discussing Mutual Authentication. It may be unclear why they have used Mutual Authentication, when the paper is talking about Lightweight Authentication but what Lightweight Authentication actually means is trying to get authentication in the most cost effective/economically/environmentally friendly solution possible.

In order to complete the registration 3 steps had to be carried out. Firstly, they had to ensure that every smart sensor was transmitting unique ID's to the Authentication Servers (AS) via a secure channel to have the lowest possible chance of malicious interception. The next step runs immediately after the first, due to the necessity to receive the information in order for the AS to calculate each unique parameter for the process. The calculation that is processed is to create relations between the Sensor ID and the AS. Once this relation has been established, the AS will send the parameters that have Smart sensor which will store it in the SE. This part is vital for the rest of the process of working to having a lightweight authentication for Industrial IoT. Each Smart Sensor will now be able to get authentication to the router. Then, the main authentication steps were processed after the registration stage. When carrying out these steps, mutual authentication was used. Firstly, the smart sensor generates a random number and stores it within its Secure Element. Once this is achieved, it will continue to generate Message 1 which consists of hashing generated function XOR a random number and also the Alias ID of id is generated via hash function encryption. Then, message 2 is generated which contains an encrypted message with all the information that has been generated so far. The second step is as simple as getting the message with all the information to the router. Upon receiving message 3, the router will decrypt via a pre-shared key. Using a pre-shared key is just one of many ways that the creators could have used to supply the decryption key to the router. After the decryption, the router will check if the correct information is received i.e. if when message 2 is decrypted, does it match the hash functions that are generated? If they do match, then the next step of authentication can begin. If they do not match, the request is rejected. Assuming the process moves on, the next step will be to send more information back to the sensor where they will generate shared keys.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

The sensor will then send another message including the shared key which, upon the router receiving the information; will check if it is the equal to the equation that it has calculated. If everything matches, it proves that the sensor has a legitimate key and the authentication process is complete Ghafir et al. (2016a).

The reason why this is a vital sequence is that this concept is a good base to explain future articles, because the authentication methods will be similar but with different devices, this article successfully explains the authentication method in a very informative table Esfahani et al. (2017). It clarifies the different notations of the equation so that a vast knowledge of how authentication works is not needed Ghafir et al. (2014b).

Linking to the previous article, the next paper also relates to lightweight authentication but has a different problem. This survey determines how much of the work crosses over when dealing with lightweight authentication for the IoT. The title for this paper is Lightweight, Anonymous and Mutual Authentication in IoT Infrastructure Janbabaei et al. (2016). This article's main goal was to create a lightweight authentication method that connects to sensors in a stationary mode and a mobile mode to each other. The article begins like most other articles covering this topic; explaining what the IoT actually is and what it consists of. Related work has included all the essential pieces that were required to create this method for explain they have wrote about not using RSA encryption and instead using Elliptic Curve Cryptography. As explained earlier there are many different encryption methods that can be used to encrypt the messages that are being sent from sensor to sensor Ghafir and Prenosil (2016b).

The full proposed scheme was as follows; firstly, the assumed Architecture that the IoT would be using, was a Authentication Cloud Sever (ACS) and a home IoT Server (HIoTS) also edge devices like sensor nodes (SNs).

Similarly, to the previous paper, there are two main steps to gaining secure authentication the Registration Phase and the Authentication Phase. This trend will be discussed throughout this survey as the similarities between each method will more often than not only have minor differences, where it makes it more secure or changes the method to suit the constraints.

The Registration Phase involves the sensor node sending the HIoTS its identity through a secure channel. Many similarities are already becoming apparent between the two articles at this early stage. This phase leaves the HIoTS to generate a Random number. Once it has done this, it will also generate a track sequence number that is also generated randomly. After this, it will send the track sequence number to the sensor node via the secure channel again, but also keeping a copy for itself. This is similar to the previous registration steps but the it's a track sequence number and not a shared key that will identify a legitimate entity. Following these steps, the process will then move onto the main authentication mechanisms.

They explained that this isn't the simple authentication method covered in the first survey, where the sensor gets authentication with the router. This method gets two sensors authenticating each other via sensor to sensor communication. The first step to gaining authentication at this stage is for sensor 1 to generate a onetime alias, then sends it as message 1 which includes the secure tracking sequence number that has been determined. Upon receiving this, sensor 2 will do the same process as before and send it to sensor 1 but it will be called message 2. The chosen ACS will send message 2 to the current HIoTS where the HIoTS will check both identities of the sensors. If they are equal to each other, it will then compare both their tracking sequence numbers. After this, it will verify the alias IDs. The HIoTS will then compute some more algorithms and after they have been computed it will send a message 3 to sensor 2, the message that has been generated will contains session keys the Tracking sequence numbers and other vital information to continue the authentication process. Sensor 2 now confirms this information by decrypting and comparing to its information that is already gathered, it then sends a new message to sensor 1 where sensor 1 will do the same decryption and comparing. Once all this has been complete authentication has been granted.

The reason for this being classed as Anonymous, which is not discussed until the security analysis is the use of one time alias due to the real identity always being hidden. This is very similar to the first surveyed paper because, in that process, the real identity was always hidden. Furthermore, there are trends that have begun to emerge after just two papers and will continue to become clearer through this survey.

The desired result of this paper was to create a lightweight, anonymous and mutual authentication method which has been achieved to a certain extent. The only part that this paper has not provided, was the part where the authentication method that was provided was classed as lightweight as they have provided evidence of previous work that shows the product that has been produced isn't as lightweight as previous work this can be seen in the table 3 in their paper Janbabaei et al. (2016). Although they did

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

not achieve their end goal perfectly, the end goal was still a success due to mutual authentication being granted in a similar way that we have previously discussed. Overall, this paper has been useful to show how common trends are becoming apparent within these authentication methods. The next paper that will be surveyed will be solely on Mutual Authentication to see if the trends continue when the focus isn't on making the authentication lightweight.

2.2 Mutual Authentication

The following paper has a great fundamental explanation of the methodology of Mutual Authentication Aman et al. (2017). The aim of this paper was to create an authentication protocol for the IoT service that is secure. The extra constraints demonstrated in this paper, making it interesting, they are that it will have to provide protecting from physical attacks and cloning attacks. This has not been a factor in any of the other papers that have been surveyed. Each authentication problem has its own constraints that make it individually challenging and its essential they are overcome for the future of IoT.

Similarly to the previous papers, the introduction explains what the IoT consists of. However, it also discusses how Physical Unclonable Functions (PUFs), are protocols that provide security to physically unsecure devices. Using PUFs it reduces the risk of authenticated physical devices being cloned Ghafir and Prenosil (2015c).

This paper contributes lots of in-depth knowledge that helps the reader fully understand their task and the devices they used. For example, one sub-heading, 'Preliminary Background', explained exactly what a PUF is. Its properties are as follows; "Output depends on a physical system, Easy to evaluate and construct, Output is unpredictable and looks like a random function, Virtually impossible to duplicate or clone a PUF Aman et al. (2017)." After this was established, they explained the different assumptions that they would be making with regards to the system and the potential risks of attacks that may occur for this paper. It is vital to note that instead of saying that the attacks will definitely take place, they are making the reader aware of the possibilities of such attacks, such as packet inject.

The next paper is significant when it discusses their proposed Mutual Authentication protocols. These protocols tend to all follow a similar pattern, but with changes within the algorithms of the protocols. Within this method; they explained that there would be two different types scenarios where mutual authentication would be used. The first being between the IoT device and a server. The second being with two IoT devices. These areas have already been covered in this survey, showing another trend of the devices that are being authenticated. Mutual authentication between device and server was achieved like the other papers by forming an identity along with a random number generated and sending it as message one. Once received, the server will search to find if the ID is in the authentication requests. If the ID isn't there or an incorrect ID it will reject the authentication. The remainder of this step is identical to the first survey. Once both the device and server have their own ID's, the IoT device will adapt the new feature that makes this paper unique, PUF, which generates a response to continue. The remainder of the steps follow the same pattern of paper 1. After this protocol was achieved, they also gained mutual authentication between two devices that was safe and worked within the constraints that had been laid out.

Unlike the previous papers, this paper did not have a notation table which made the algorithms quite difficult to understand. Therefore, a recommendation for any paper with algorithms would be to explain the notations so that someone with relative but not a deep understanding of authentication could learn from the papers.

Overall, this paper was the most in-depth of the three papers that have been surveyed. With the challenge of malicious users having physical access to the devices they proved that they can still make it safe from malicious activity. In the future, they could advance this project by adding a constraint, such as making it a lightweight authentication. This paper made the case for not storing secret keys and added a new dynamic that other papers could implement in the future. Paper 1 and 2 could look into this in the future to try and make their methodologies more lightweight Ghafir and Prenosil (2014b).

Although we have mainly surveyed mutual authentication so far, it is necessary to make sure that lightweight and non-lightweight mutual authentication do not have any major differences, except for being lightweight. Because of this, the fourth paper that will be surveyed is "Mutual Authentication for IoT Smart Environment Using Certificate-less Public Key Cryptography" Bala et al. (2017). The aim for this paper was to create a mutual authentication between sensor nodes inside a smart environment and a remote end-user which adds a channelling task for IoT authentication. The proposed proctor was to eliminate the use of certificate management by using certificate-less public key cryptography. This

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

added a new challenge to a very similar problem to paper 1 but with the constraint of taking away the certificate Ghafir et al. (2015b).

Cryptography is a vital part of every authentication method and without it, messages between devices and servers or device to device communication would be very vulnerable to attacks, compromising the integrity of the devices and servers. It is interesting how we have seen three different types of cryptography within these papers. This shows that there are numerous ways that this can be achieved. In future papers, there will be further methods of cryptography that may be used. Cryptography is always being updated and making it more difficult for malicious activity to be carried out.

The final proposed protocol was as follows; Firstly, they had to understand the network architecture. This had five main entities; they included the key generation centre, End-user, Senor Node, Workstation and the Gateway. Without these five main aspects, the authentication and communication wouldn't have been possible to create. To generate the authentication method, they explained that there were three main modules. These were the network initialization module, the node registration module and the session key establishment module. These are very similar methods to the methods in previous surveys but are worded differently. For example, by first establishing the network, communication lines and by registering nodes via session keys that are generated from the Key Generation Centre, to prove their legitimacy. If the keys and messages match authentication will be granted.

This paper successfully produced a certificate-less public key cryptography within a mutual authentication method. Although in a novel aspect the certificate-less public key cryptography is consider a lightweight cryptography. They could try make the full authentication method lightweight when it came to actual creation. This question should be presented to the authors. Adding an automatic update feature to not just this authentication method, but all the methods that have been discussed thus far, could have been discussed. Why? Because as authentication and cryptography are safe and always improving, there are malicious activities that go with this. If one authentication process gets attacked it would be beneficial if once the problem is dealt with an automatic patch could be rolled out for all future/current authentication methods.

One of the main constraints we have seen so far is limited bandwidth for wireless devices. This is currently a massive issue but with technology advancing, this constraint will potentially become obsolete. However, the drawbacks with having wireless communication are discussed below. The next paper that will be discussed is "Secure Authentication and Access Mechanism for IoT Wireless Sensors Azarmehr et al. (2017)". Their challenge was to create an integrated approach to solving the authentication and access control between wireless sensors. Which used mutual message authentication code, another type of mutual authentication that can be used.

The paper provides a good background on possible threats and therefore reasons for security measures to make the IoT as safe as possible. For example, they describe how integrated mechanics can be vulnerable to both remote and physical attacks, such as side channel attacks and eavesdropping. Without studies like the papers that have been surveyed, these attacks would remain undefended against, leaving the IoT vulnerable. Although these attacks are noted at the moment, there are several strains of each of these attacks and no system should be regarded as completely secure. It is vital to keep on top of new strains that may bypass the security measures put in place. A lot of the papers that have been studied never refer to this as being a problem. The study looked into these problems in more detail which was useful to the reader. It was very similar to previous papers for reasons such as low bandwidth and how using IPv6 provides unique IP addresses for IoT. In contrast to other papers, the background of this paper provided a very clear and concise overview of what the rest of the paper would consist of and provided the information that would make the understanding of their proposed methodology easier to comprehend.

Based on the security problems that may occur, this process of authentication and access control was produced. They explained how if an illegitimate entity got access, they could DDoS the sensors by never letting them go to sleep. This is a very concerning scenario as DDoS is one of the most accessible/common attacks in the hacking community and even someone with very little knowledge of hacks could proceed to orchestrate this attack. This is something that should have been highlighted more in the other papers because a lot of IoT systems using sensors to communicate and they can be attacked easily without authentication. Their solution to this problem was to add a wake-up radio, which is very simple to implement. Other projects in the future would be advised to use something similar in case a malicious entity gained access. Gaining their proposed method of authentication has three main aspects, consisting of Token Establishment, where they established tokens for sensors and hash them. Secondly, they added

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

the wake-up radio technique. In the second stage, which doesn't only protect against DDoS it also is used to communicate. also in the second stage, the Session Key Agreement which is fundamentally the same as we have seen in numerous mutual authentication method, which is when they create a session key that is used to validate if the entity is legitimate by checking the session key throughout the steps of authentication This is a very common method used throughout multiple authentication methods. Finally, the Data Transmission step used session keys but the function comes as a hash function that is irrevocable. The only way for sender and receiver to verify the legitimacy of the session key is to create the hash function to see if it is a match.

This paper could be classed as being lightweight due to how energy efficient it is, as it uses very low powered equipment algorithms such as the wake-up radio etc. This paper was successful in creating a secure authentication method for IoT wireless sensors, by using mutual message authentication. This paper was very similar in the approach it took to complete the authentication method, however, the reasons it was in this paper is due to the theoretical approach that it took to explaining the exact areas that could be under threat and how they may be. One aspect they could have added to the paper was a table of notations to make the algorithms clearer Azarmehr et al. (2017). Creating both access control and authentication in the same process is a good example of how to create methods that can serve multiple purposes for future work Ghafir and Prenosil (2016a).

As this survey leads on to another section of authentication methods, there is something that cannot be overlooked. Mutual authentication is the most important and most used type of authentication method within the IoT. It would be nice to see if there were other options but not in the circumstance that would make mutual authentication obsolete, because that is very unlikely. To make other options more accessible for projects to experiment with different authentication methods to see if they can find another method that produces the same/equal/better results similar to mutual authentication. As there has been previous methods that have failed it would be interesting as a reader to see someone succeed in this challenge.

The next survey is something a bit different but also similar to previous papers. It is on lightweight mutual authentication again but within constrained application protocol based Lavanya and Natarajan (2016). The paper planned to use constrained application protocol in exchange of HTTP by utilising DTLS. In the introduction of the following paper, they explain that the method of encryption they planned to use was Diffie Hellman for key exchange and RSA for signature. These are two very useful techniques when it comes to cryptography and the strongest cryptography is the cryptographies that use many different techniques together. A prime example has been displayed in this project Ghafir and Prenosil (2015a).

Their proposed protocol had two phases. The first was to grant mutual authentication and session key establishment. Phase Two will be to continue the communication via security association which is gained in Phase One. Their key agreement was similar to one of the previous papers as they used certificate-less key agreement.

This report carried out extensive testing on their proposed protocol. Firstly, they determined if it was fully secure against man in the middle attacks. They determined this by determining that due to their authentication method using IP addresses to generate the messages that are sent, if there is a malicious parameter in the message it won't match the IP address and the malicious entity will never be authenticated, eliminating the risk of the man-in-the-middle attack. Not only does their proposed authentication method defend against this attack, it also defends against Replay Attack. The way that this project and many other projects negate this attack is by using the nonce feature, which means that each number is only used once so the replay attack isn't viable. These two attacks are the main attacks that the majority of protocols try and negate along with DDoS. As attacks become more sophisticated alongside technology, the malicious user's ability to bypass older security is increased. It is because of this that all security measures need to be up-to-date with the latest attacks.

In conclusion for this paper, they succeeded by using Elliptic Curve Cryptography instead of RSA. The reason they chose this instead of RSA is because it produces the same security whilst reducing the key size, having a knock-on effect on one of the constraints, which kept the authentication process lightweight. Area of improvement for this paper, although they spoke about the key size making it lightweight they didn't explain that certificate-less key agreement also adds great lightweight elements and how they benefit the protocol.

For the final part of this paper, we will discuss two papers that have different constraints and authentication methods. They have been included to ensure that the reader understands it doesn't have to always be similar authentication methods and adding different papers will produce that.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

2.3 Different Authentication Methods

When looking for papers on authentication in the IoT, I noticed that a very common method, Kerberos, wasn't in any of the main searches and it only appeared when it was searched for specifically. Kerberos was designed by MIT and is a very intelligent authentication method. It can use mutual authentication but can be also used in a number of different ways. It is widely used in the security industry so it is only reasonable that it is included in this article. When thinking about Kerberos, you must remember a few vital points in order to understand its authentication; Kerberos is a protocol for authentication, it uses tickets to authenticate the entities, it uses a 3rd-party that is trusted and is built on a symmetric-key cryptography.

The paper that has been chosen for the purpose of surveying Kerberos in IoT is "3-Level Secure Kerberos Authentication for Smart Home Systems Using IoT." The main objective of this paper was to make smart home System that has implemented the IoT, secured by using 3-leve Kerberos authentication. This was achieved eco-friendly and low cost Gaikwad et al. (2015).

A smart home involves appliances such as heating, lights and electrical devices that are all attached to a remote device, which is able to control settings and turn the devices off and on. This is another area of the computing industry that is very interesting and would be worth further study on. If you would like to read more into how the smart home was laid out, read Gaikwad et al. (2015) as the main focus of this article is the authentication method.

Their proposed authentication protocol had three layers for the authentication process, as stated in the title of the article. The first layer was used to initiate the authentication method by asking the user to logon into their smart home services with a username and password. Then, the information would be sent to the key distribution centre for authentication, all the information that gets to the key distribution centre would be encrypted with a hash function - the two that may have been used are Secure Hash Algorithm 1 (SHA-1) and MD5. These two hash functions are used widely in the computer forensic industry and can determine the legitimacy and a lot of other information, but in this instance they were for encrypting the information sent to make it secure.

Level Two is where the main part of Kerberos authentication takes place. After receiving all the information from Level One, the username and password are decrypted and checked against the authentication database. If the credentials are wrong, the system would assume it was an illegitimate user and would terminate the request. This is similar to most authentication methods that have been discussed. On the other hand, if the credentials matched, the authentication server would reply with a key that has been generated and a ticket. This is part of the Kerberos method if this ticket is not obtained the user wouldn't get access to their systems. Level Two also has another method that checks the timestamp with the request. If the time is longer than allowed, then the user wouldn't gain access. This service is used to negate replay attacks. This is different to other methods because it has the timestamp mechanism; however, this is common practice in a lot of different authentication methods, such as services at universities and different establishments that requires you to log onto their networks. Kerberos is widely used for areas within Windows, Linux and Apple Mac. Once all of these steps have been completed, the authentication process moves on to Level Three. where they have collected all the users profile in the authentication server, upon receiving they would hash the information using SHA1. The shared secret key would then get shared with the Authentication Server by using Advanced Encryption Standard. After all encryption and checks have been completed, the final Kerberos step would generate a ticket for the session which includes credentials such as a current time Server IP address. There is a very good safety feature that the ticket aspect of Kerberos adds to this system; if the IP address is changed at any stage throughout the authentication stage, the system would automatically log the user out.

As a service, Kerberos is a very useful authentication method, especially in the aspect of smart homes which is an up and coming area of IoT. This authentication method has many great features. Some of its drawbacks are that passwords from a human aspect can never be fully secure, and this authentication method could be problematic due to its reliance on user interaction where human error could be a factor. If a higher budget was available, some technologies that could be used to reduce this are retinal scanners or other biometric passwords. These are very accessible as smart homes can rely on smart phones or computers. Smart phones, for example the new iPhones, have this technology already built in so could be utilised.

This paper was successful for the small smart home equipment that was used it. In the future, they could try this with a fully built in smart home that is using IoT technology. It makes the users more secure

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

when connecting to their devices and removes the threat of unauthorised users taking control, or using the smart home devices maliciously. Kerberos is one technique that could be used more in the IoT. If utilised properly, it is very secure and widely used in other areas of authentication for other technology Ghafir and Prenosil (2015b).

The final paper that will be surveyed focuses on audio-based authentication. This is an area of authentication that also needs user input, similar to the previous paper. The title of this paper is "Scalable Group Audio-Based Authentication Scheme for IoT Devices Gu and Liu (2016)". The main goal for this paper was to make the authentication method both scalable and group-based, something that will be vital for the increasing number of IoT devices that are in today's industry.

This paper explains that it reduces the amount of shared information that Mutual Authentication relies on. Their idea was to use senses signals or radio frequency signals for the devices to extract information to generate authentication keys. They explained that they were adding their own contribution to the related work that had already produced, so firstly they added a key authentication scheme by using their protocol, which included audio sensing and affordable user interaction.

The authentication process used three main aspects, similar to many authentication processes. The user, a smartphone and IoT devices. Majority of Authentication methods that require user input will usually require a smart device. All of the devices that are being authenticated have to be in a range where they can receive the audio signals, meaning that all of the audio authentication will be the same. This concept is intelligent because it reduces the amount of user input. However, the drawbacks are that if the IoT devices aren't in range to receive this audio signal, then they will never be authenticated Ghafir et al. (2015a).

Like the Kerberos method, the user will have to enter a username and password on their smart device. Once this has been achieved, they would send a signal that would request the protocol to start - this will only commence if the device is within the appropriate distance to commence the authentication. Similarly to the other authentication methods, once the request has been sent and received the IoT device will then determine if it is ready for the authentication process to commence. The user's job was to send a piece of audio out, to which when the IoT device receives this it will use error correction to make sure the audio is highly similar to previous audio that has been sent. Error correction is a very useful tool when it comes to authentication and more authentication methods could use it when user input is necessary. This aspect of the term group audio-based authentication is derived from the concept that all authentication methods can be done in a group format is very useful for future professionals to work with Raza et al. (2017).

To generate the key, all of the previous steps need to be achieved. The vital process is that the error correction has produced a similar audio bit, from this audio bit the key would be generated, this key sets up a session key which is produced using similar methods as Kerberos, in that they use authentication key exchange and that it is based on a symmetric key solution, which is what Kerberos uses for their key generation. They added a very secure aspect, in which all of the devices that are being authenticated will be sent to the user's smart device and if the user notices a malicious IoT device i.e. one that shouldn't have been involved in the group authentication process, they could terminate the authentication process for that device Ghafir and Prenosil (2014a).

One main advantage of this authentication method, that has been made apparent over many surveys, is the aspect of group authentication. This is beneficial because all devices can be authenticated at once, reducing time and energy consumption, making this quite a lightweight aspect. In conclusion, this has been a hugely successful paper and a lot of aspects could be adapted especially for areas like smart house IoT authentication. This could be a very useful protocol of authentication, although, if this was a solution proposed for a long range in a wide variety of areas, this wouldn't be the best solution that could be proposed Ghafir et al. (2016b).

3 GAPS AND OPPORTUNITIES

After reading and surveying all of the papers in this article, there are some gaps and opportunities that I have noticed and think could be used to create and produce an overall benefit to the industry. Firstly, researchers that are trying to make their papers more accessible could add a notation table for their algorithms to make their paper more accessible for those with less prior knowledge. I noticed this when I was getting the basis of how their authentication algorithm worked and the different concepts they used in it. The first paper that was surveyed had an effective notations table and this was one of the reasons I chose to begin with this survey, as it was easy to understand.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Secondly, assuming that a lot of the authentication that is being completed is wireless, more studies should be focused on whether wireless communications in restricted areas, i.e., areas that have no cellular signal or any form of wireless communication whether authentication protocols could be in place for people like mountain rescue and other areas that work in restricted areas Svoboda et al. (2015); Dibb and Hammoudeh (2013); Carlin et al. (2015a,b).

Also, one constraint and gap in the market is that touch/voice or different forms of authentication of IoT devices aren't being utilised. As IoT devices became more sophisticated these types of authentication are very feasible with devices like smart phones having the technology already embedded this leaves a lot of thought for the future of IoT authentication, this would take a lot of money for extensive testing but with how fast technology is moving in this era it would be a great way to move authentication within IoT forward Ghafir et al. (2014a).

4 CONCLUSION

To conclude, this survey has covered a wide variety of areas in which IoT can be used and a wide variety of constraints that authentication processes can come under; whether it is low-bandwidth, communication problems or that the technology is not as advanced as it needs to be. Lightweight authentication is a great choice when it comes to authentication within IoT, due to the constraints that have been mentioned and by having a lightweight authentication method Hammoudeh (2008); Aldabbas et al. (2016). This satisfies all of these constraints and is good for the future of the industry when you use lightweight solutions. Mutual authentication was the main focus of this survey with almost every paper that was surveyed using Mutual authentication due to its concurrent authentication protocol being very useful within the Internet of Things. The survey paper also went into other authentication methods due to the necessity to provide a full view of different types of authentication and not just stay one dimensional. The two that were surveyed are vital for the future of authentication in IoT as they both add aspects that can change the future and benefit the industry. Authentication is ever changing, as is the IoT, and with this there is also a wide variety of areas that can be exploited. Authentication always needs to be a step ahead and with the aspects that have been already discovered there are numerous opportunities to improve these, by make them more lightweight or combining a protocols and encryption methods together to make the authentication protocols even more secure, such as using the likes of RSA and Diffie Hellman along with Elliptic Curve Cryptography to make everything even more secure.

REFERENCES

Aldabbas, O., Abuarqoub, A., Hammoudeh, M., Raza, U., and Bounceur, A. (2016). Unmanned ground vehicle for data collection in wireless sensor networks: mobility-aware sink selection. *The Open Automation and Control Systems Journal*, 8(1).

Aloraini, A. and Hammoudeh, M. (2017). A survey on data confidentiality and privacy in cloud computing. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, pages 10:1–10:7, New York, NY, USA. ACM.

Alsboui, T., Abuarqoub, A., Hammoudeh, M., Bandar, Z., and Nisbet, A. (2012). Information extraction from wireless sensor networks: System and approaches. *Sensors & Transducers*, 14(2):1.

Aman, M. N., Chua, K. C., and Sikdar, B. (2017). Physically secure mutual authentication for iot. In *Dependable and Secure Computing, 2017 IEEE Conference on*, pages 310–317. IEEE.

Atwady, Y. and Hammoudeh, M. (2017). A survey on authentication techniques for the internet of things. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, New York, NY, USA. ACM.

Azarmehr, M., Ahmadi, A., and Rashidzadeh, R. (2017). Secure authentication and access mechanism for iot wireless sensors. In *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*, pages 1–4. IEEE.

Bala, D. Q., Maity, S., and Jena, S. K. (2017). Mutual authentication for iot smart environment using certificate-less public key cryptography. In *Sensing, Signal Processing and Security (ICSSS), 2017 Third International Conference on*, pages 29–34. IEEE.

Carlin, A., Hammoudeh, M., and Aldabbas, O. (2015a). Defence for distributed denial of service attacks in cloud computing. *Procedia Computer Science*, 73:490–497.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Carlin, A., Hammoudeh, M., and Aldabbas, O. (2015b). Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *International Journal of Advanced Computer Science and Applications*, 6(6).

Dibb, P. and Hammoudeh, M. (2013). Forensic data recovery from android os devices: an open source toolkit. In *Intelligence and Security Informatics Conference (EISIC), 2013 European*, pages 226–226. IEEE.

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M., Schmittner, C., and Bastos, J. (2017). A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet of Things Journal*.

Gaikwad, P. P., Gabhane, J. P., and Golait, S. S. (2015). 3-level secure kerberos authentication for smart home systems using iot. In *Next Generation Computing Technologies (NGCT), 2015 1st International Conference on*, pages 262–268. IEEE.

Ghafir, I., Husák, M., and Přenosil, V. (2014a). A survey on intrusion detection and prevention systems. In *Proceedings of student conference Zvule, IEEE/UREL*, pages 10–14. Brno University of Technology.

Ghafir, I. and Prenosil, V. (2014a). Advanced persistent threat attack detection: An overview. *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, vol. 4(Issue 4):50–54.

Ghafir, I. and Prenosil, V. (2014b). Dns query failure and algorithmically generated domain-flux detection. In *International Conference on Frontiers of Communications, Networks and Applications (ICFCNA)*, pages 1–5. IEEE Xplore Digital Library.

Ghafir, I. and Prenosil, V. (2015a). Advanced persistent threat and spear phishing emails. In *Proceedings of International Conference on Distance Learning, Simulation and Communication*, pages 34–41. University of Defence.

Ghafir, I. and Prenosil, V. (2015b). Blacklist-based malicious ip traffic detection. In *Global Conference on Communication Technologies (GCCT)*, pages 229–233. IEEE Xplore Digital Library.

Ghafir, I. and Prenosil, V. (2015c). Dns traffic analysis for malicious domains detection. In *2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 613–918. IEEE Xplore Digital Library.

Ghafir, I. and Prenosil, V. (2016a). Malicious file hash detection and drive-by download attacks. In *Proceedings of the Second International Conference on Computer and Communication Technologies*, pages 661–669. Springer.

Ghafir, I. and Prenosil, V. (2016b). Proposed approach for targeted attacks detection. In *Advanced Computer and Communication Engineering Technology*, pages 73–80. Springer.

Ghafir, I., Prenosil, V., Alhejailan, A., and Hammoudeh, M. (2016a). Social engineering attack strategies and defence approaches. In *IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 145–149. IEEE Xplore Digital Library.

Ghafir, I., Prenosil, V., and Hammoudeh, M. (2015a). Botnet command and control traffic detection challenges: A correlation-based solution. *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, vol. 7(Issue 2):27–31.

Ghafir, I., Prenosil, V., Hammoudeh, M., Han, L., and Raza, U. (2017). Malicious ssl certificate detection: A step towards advanced persistent threat defence. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, page 27. ACM.

Ghafir, I., Prenosil, V., Svoboda, J., and Hammoudeh, M. (2016b). A survey on network security monitoring systems. In *IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 77–82. IEEE Xplore Digital Library.

Ghafir, I., Svoboda, J., and Prenosil, V. (2014b). Tor-based malware and tor connection detection. In *International Conference on Frontiers of Communications, Networks and Applications (ICFCNA)*, pages 1–6. IEEE Xplore Digital Library.

Ghafir, I., Svoboda, J., and Prenosil, V. (2015b). A survey on botnet command and control traffic detection. *International Journal of Advances in Computer Networks and its security (ICJNS)*, vol. 5(Issue 2):75–80.

Gu, Z. and Liu, Y. (2016). Scalable group audio-based authentication scheme for iot devices. In *Computational Intelligence and Security (CIS), 2016 12th International Conference on*, pages 277–281. IEEE.

Hammoudeh, M. (2008). Modelling clustering of sensor networks with synchronised hyperedge replacement. In *International Conference on Graph Transformation*, pages 490–492. Springer.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Hammoudeh, M. (2015). Applying wireless sensor networks to solve real-world problems. In *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication*, page 1. ACM.

Hammoudeh, M. and Alsbou'i, T. A. (2011). Building programming abstractions for wireless sensor networks using watershed segmentation. In *Smart Spaces and Next Generation Wired/Wireless Networking*, pages 587–597. Springer.

Hammoudeh, M., Newman, R., Mount, S., and Dennett, C. (2009). A combined inductive and deductive sense data extraction and visualisation service. In *Proceedings of the 2009 international conference on Pervasive services*, pages 159–168. ACM.

Hammoudeh, M., Shuttleworth, J., Newman, R., and Mount, S. (2008). Experimental applications of hierarchical mapping services in wireless sensor networks. In *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pages 36–43. IEEE.

Janbabaei, S., Gharaee, H., and Mohammadzadeh, N. (2016). Lightweight, anonymous and mutual authentication in iot infrastructure. In *Telecommunications (IST), 2016 8th International Symposium on*, pages 162–166. IEEE.

Lavanya and Natarajan (2016). Lightweight authentication for coap based iot. In *IOT*, pages 167–168.

Lopez-Research (2017). An introduction to the internet of things (iot). `https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf`. Accessed: 15-01-2018.

McDaniel, P. (2017). Authentication. `https://pdfs.semanticscholar.org/dd3f/ba9b89a1f912a49463f2c9c28d9d726331a3.pdf`. Accessed: 15-01-2018.

Moffat, S., Hammoudeh, M., and Hegarty, R. (2017). A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, page 34. ACM.

Mohsin, J., Han, L., Hammoudeh, M., and Hegarty, R. (2017). Two factor vs multi-factor, an authentication battle in mobile cloud computing environments. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, page 39. ACM.

Newman, R. and Hammoudeh, M. (2008). Pennies from heaven: A retrospective on the use of wireless sensor networks for planetary exploration. In *Adaptive Hardware and Systems, 2008. AHS'08. NASA/ESA Conference on*, pages 263–270. IEEE.

Raza, U., Lomax, J., Ghafir, I., Kharel, R., and Whiteside, B. (2017). An iot and business processes based approach for the monitoring and control of high value-added manufacturing processes. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, page 28. ACM.

Svoboda, J., Ghafir, I., and Prenosil, V. (2015). Network monitoring approaches: An overview. *International Journal of Advances in Computer Networks and Its Security (IJCNS)*, vol. 5(Issue I).

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26474v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018