Disclaimer — This paper partially fulfills a writing requirement for first year (freshman) engineering students at the University of Pittsburgh Swanson School of Engineering. This paper is a student, not a professional, paper. This paper is based on publicly available information and may not provide complete analyses of all relevant data. If this paper is used for any purpose other than these authors’ partial fulfillment of a writing requirement for first year (freshman) engineering students at the University of Pittsburgh Swanson School of Engineering, the user does so at his or her own risk.

END TO END ENCRYPTION: AN ANSWER TO SECURITY CONCERNS IN THE PRIVATE SECTOR

Erik Wehner, edw34@pitt.edu, Lora, 3:00, Evan Moran, ecm61@pitt.edu, Lora, 1:00

Abstract—Personal online security is becoming an extremely important topic in engineering. This is due to the increased popularity of online communication. The best technology to ensure a user’s data is safe is end to end encryption. Ever since electronic mailing services became available to the public, questions arose about how secure these messages were. In addition, the popularity of online shopping, banking, and other financial online transactions brought forth an even higher demand for the security of the internet. An example of technology that can provide a high level of privacy is end to end encryption. Hardware embedded into phones and computers allows for the random locks and keys that make up end to end encryption only work on the devices involved in the conversation. This allows for the data that is being transmitted to be completely secure. End to End encryption is very useful for the sustainability of privacy online, as it protects users from attacks and it is very hard to crack. iMessage is the best example of this extremely important technology in action on a large scale. The end to end encryption of the messages makes it almost impossible to intercept an iMessage message. In addition, the history of encryption as it relates to this software being used by the public is important to the understanding of how end to end encryption evolved into how it is known today in applications like iMessage. Apple’s iMessage software is one of the most popular publicly available messaging software in use, therefore serving as a representative of the effectiveness of end to end encryption technology. Although this technology allows extremely high levels of security for users, this comes with some concerns, such as the limits encryption places on government surveillance.

Key Words- AES, Cryptography, Cybersecurity, Encryption, End to End, Internet Privacy, Private Messaging

THE IMPORTANCE OF ONLINE SECURITY

As more and more people use the internet as a means to communicate, the importance of securing people’s and business’ online communications becomes more imperative and a much more difficult engineering challenge. According to the Central Intelligence Agency, there were an estimated 276 million internet users in the United States in 2014, and that number is predicted to rise [1]. With this many users, the incentive for hackers to execute attacks increases. CNET reported that in September of 2016, Yahoo! confirmed that 500 million accounts were hacked into, making it the largest data breach in history. Through this massive number of email accounts, names, other email addresses, contacts, phone numbers, security question answers, and contacts were all stolen. With this information, hackers had the ability to send out emails in the victim’s name and also read through all of the emails associated with the account. A majority of these hacked accounts are still being sold on the internet to people with the intent of stealing personal information, hacking into other accounts, and possibly even using the email to hack into an associated bank account [2]. According to a Javelin Strategy and Research Report in 2012, one in every four people that have a breach in their online data become a victim of identity theft as a result of that. [3]. This reveals the connection between online data breaches and hackers using this information to steal a victim’s identity. End to end encryption provides an effective way to prevent against these attacks through technology that allows the algorithms to be almost unbreakable. This technology, if implemented properly, could have prevented this large-scale attack. End to end encryption offers a sustainable solution to the ongoing problem of online security. According to Urban Sustainability in Theory and Practice, sustainability is referred to as intersecting “with other social conditions, such as resilience, livability, adaptation, innovation and reconciliation, as basic conditions of positive social life.” [4]. This technology offers peace of mind to users on the internet that their data is safe. In addition, end to end encryption is a technology that will remain relevant and in use for a long period of time, due to its security and adaptability. Overall, online security is very important in today’s society, however the concept of encryption has been around for centuries.

THE HISTORY OF ENCRYPTION

Earliest Forms of Encryption

The idea of encrypting information so it is not available to be understood by anyone but the ended recipient of a message is not a new idea. An article published by the University of Utah reports that the first known example of cryptography dates back to an Egyptian town in 1900 BCE. A series of hieroglyphics with a number of unusual symbols was
found in the tomb of Khnumhotep II. These unusual symbols were used to obscure the history of his life and was the first example of a substitution cipher, where one symbol is substituted for an arbitrary one to confuse an unintended reader [5]. Overall, ciphers and encryption techniques remained relatively simple until electronic communication in World War I drove countries to devise ways to prevent important information from being intercepted by the opposition.

**World War Era Encryption**

One of the most famous examples of encryption being used in World War I, was known as ‘The Zimmerman Telegraph,’ named after the German Foreign minister during the war, Arthur Zimmerman. According to the United States National Security Administration, the Zimmerman Telegraph was sent to Mexico by Germany in order to propose an alliance where Germany would supply Mexico with enough supplies to invade the United States and reclaim Texas, New Mexico, and Arizona. This telegraph was encrypted by the Germans to prevent the United States or its allies from intercepting this message and learning its contents, which would enable the United States to prepare for such an attack, therefore ruining the element of surprise. The Germans used a cipher known as ‘Code 0075,’ which was a series of numbers that corresponded to words in a physical cipher book. Unfortunately, for the Germans, the British government had already partially decoded Code 0075 by using past events and aligning them with intercepted telegrams. The British intercepted the Zimmerman Telegraph as it passed through Sweden and then began work on decoding the message. While they were not able to fully decode the message, they gained enough information to realize that the Germans were planning on encouraging Mexico to attack the United States. They then passed this information on to the United States, and this encouraged the United States to join the war against Germany [6]. Following World War I, encryption technology expanded greatly with electronic encryption methods making their debut in the late 1920s. Through the use of electronic encryption methods, much more complicated ciphers were possible, that would otherwise take years to code/decode. The most famous electronic encryption device was the Enigma Machine. An article published by Williams College states that the Enigma Machine was first used by Germany in the 1920s to send encrypted telegraphs throughout the country. This complex machine consists of a lamp board, a keyboard, plugboard, and four rotors. When a user types a letter on the keyboard the select letter travels by an electrical signal through each of the four rotors where it is scrambled. Every rotor has 26 different combinations and the rotors themselves can be arranged in six different ways. In addition, every time a letter is entered on the keyboard, the rotor moves, and this can be adjusted by the user. After a letter goes through the rotors, it is then scrambled by a plugboard that swaps the letters around a final time, all through different paths the electricity can take as it reaches its final destination, the lamp board, where the user sees what the typed letter results in. Overall this process results in approximately $3 \cdot 10^{14}$ different combinations [7]. The image below shows a World War II Era Enigma machine. In this photo the plugboard is seen at the very front of the machine, followed by the keyboard and the lamp board. The four rotors can be seen near the back of the machine with each of the rotors’ display window next to each rotor.

**FIGURE 1 [8]**

German World War II Era Enigma Machine.

According to the Central Intelligence Agency, the Enigma machine was cracked by Alan Turing, who created an electromechanical device called the ‘bombe’ which could detect the settings on an enemy’s enigma machine, therefore allowing him to decrypt it. This machine paved the way for modern computing and forced the creation of more complex encryption techniques [9]. Without these advances in encryption, current encryption techniques would not be possible. Today’s encryption techniques are very similar to these older technologies in which they all have some form of cipher that randomizes the message in a way only the intended recipient can understand. Modern day computers allow for extremely secure algorithms to improve security techniques to protect people online. This is because they are capable of doing repeated processes very rapidly to scramble a message more than a person was able to in the past. End to end encryption is a very good example of what modern day computers are capable of in regards to making an almost unbreakable cipher. This long history of encryption illustrates how sustainable it is as a technology as it has lasted centuries. The technology kept evolving as ways to break the encryption were developed. This applies to end to end encryption as all of the individual components can change as weakness are found, providing for a long lasting solution to internet privacy.

**WHAT MAKES END TO END ENCRYPTION SECURE**

**Overview of End to End Encryption**

End to End Encryption (E2EE) is one of the most commonly used ways to securely send information across the
internet. In principal, E2EE is a way to send information over a network in such a way that only the recipient and sender can access it. According to Lead Engineer at Cisco Systems, Michael Behringer, E2EE contains the following components: identity and protocols, algorithms, secure implementation, and secure operation. The identity and protocols component acts as a security guard to check verify that the parties involved are who they say they are. A protocol is used to set up everything needed for E2EE, such as the key exchange and the algorithm. The algorithm uses mathematical processes to scramble the data in such a way that it is near impossible to unscramble without the predetermined key. Secure implementation and operation are necessary to ensure that the E2EE process is not susceptible from cyberattacks on the hardware side, such as viruses and malware. These components all work together in order to provide a fluid system that runs efficiently to provide the best security possible to the end users. This helps E2EE adapt to different threats posed by hackers, because an indivial component can evolve to solve an indivial weakness, rather than having to reinvent the entire system. There are many different variations of each of these components that have been developed over the years for different applications. [10].

**Identity and Protocols**

Identity and protocols outline how the encryption process will take place and what algorithms will be used. This is very similar in function to the plugboards and rotors mentioned on the German enigma machine. In the identity component, a user or server that is sending data through E2EE verifies itself through a username and password, or in the case of a server, a security certificate issued by a website to prove its identity as valid. This component is very important in verifying that both the sender and the recipient in an E2EE exchange are the intended parties. For example, if a user was sending encrypted information to a banking website, the server hosting the website would have a security certificate showing the user that this website is the website it claims to be. In the next component, a transport protocol is used to ensure a connection is private and prepare data to be encrypted. The Internet Engineering Task Force describes an example of one of these protocols, the Transport Layer Security (TLS) Handshake Protocol, “the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.” Essentially, a protocol outlines what algorithm is going to be used and ensures that no unwanted party is participating in the exchange of data [11]. This is an integral part of the E2EE process because it allows for both parties to have a secure link and receive keys to decode the encrypted data.

**Diffie-Hellman Key Exchange Algorithm**

Key exchange algorithms allow for the keys used to code and decode encrypted information to be transmitted in such a way that they cannot be intercepted. A paper published in 1976 by Whitfield Diffie and Martin Hellman, unveiled a groundbreaking way of delivering the key needed to decrypt encrypted data, named the Diffie-Hellman Key Exchange Algorithm. This algorithm allows for the key to be transmitted across a public channel without the risk of compromising the encryption process. In addition, this algorithm enables users to send encrypted data without having to communicate with the recipient beforehand, which makes E2EE a much more practical process. Overall, the process is simple, it is extremely effective and secure. This paper written by Diffie and Hellman describes this process using a sender of an encrypted message named Alice, a recipient of the message named Bob, and another user on the same network named Sally. To begin, Alice and Bob are randomly assigned a prime modulus and a generator that is shared publicly, so Sally has access to this as well. For this example, a generator of 11 will be used and 23 will be the randomly selected number to be used in the prime modulus (mod). Next, Alice is assigned a randomly generated number, for example 6, and keeps that privately. She then calculates 11^6 mod 23, which is equal to 9. That nine is then shared publicly across the network. Bob does the same thing, taking his random number, say 5 and calculating 11^5 mod 23, which is equal to 5. Next, Alice takes Bob’s public result, five, and calculates 5^5 mod 23 which equals 8. Bob then takes Alice’s public result, 9, and calculates 9^6 mod 23, which equals 8. Notice that this is the same value that Alice got, this value is their shared secret key. This is due to the mathematical properties of the prime modulus function. Sally only ever receives the generator 11, the prime modulus 23, Bob’s result of 5, and Alice’s Result 9. Sally is left with no way of figuring out what the shared secret value is, therefore making the Diffie-Hellman key exchange very secure. Once this key is determined, it is sent along to another algorithm which scrambles the data based off of this key. Since both the sender and the recipient work to create a key, this process is truly ‘end to end.’ In real world applications, these numbers would be even larger to prevent Sally from being able to determine the key through guess and check techniques [12]. In the figure below, ‘n’ represents the prime modulus, ‘g’ represents the chosen generator, ‘x’ is Alice’s chosen secret number, and ‘y’ represents Bob’s secret number.

**FIGURE 2 [13]**

A visual representation of the Diffie-Hellman Exchange Algorithm

This diagram shows how the algorithm flows and transmits data over a public network and provides an example using
variables. A paper published for the 22nd Conference on Computer and Communications Security illustrated the difficulty in cracking the Diffie-Hellman Exchange Algorithm. The researchers that published this paper entitled, Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice, discuss an attack called Logjam that is capable of cracking Diffie-Hellman keys through computing by computing the discrete logarithm of the public values shared in the Diffie-Hellman process. Essentially, finding the discrete logarithm of the shared values can result in the discovery of the private values that Alice and Bob determined in the example mentioned earlier. However, this is still a trial and error method, which takes longer to solve the larger the numbers used in the process are. For example. with the Logjam algorithm, the researchers could crack a 512-bit key, a key that is 512 numbers long, in around 5 days, using 2,000-3,000 CPU cores in parallel. However, it would take the most powerful supercomputer in the United States, the National Security Agency’s Titan, 117 years to crack a 1024 bit key, which is the largest Diffie-Hellman key in use. This proves that this key exchange method is a long-term solution, as it will take a long time for a computer to be able to crack a key of this size in a reasonable amount of time. The adaptability of this technology illustrates its sustainability, as simply increasing the key size makes the entire system much more secure. Overall, the Diffie-Hellman Key Exchange is extremely secure and safe from ‘Man in the Middle’ attacks. This key exchange method is used most commonly by websites that require a secure connection, such as shopping websites that handle credit card information. Diffie-Hellman is less common in messaging applications since it can take longer to perform due to its complexity [14]. In conclusion, the Diffie-Hellman Exchange Algorithm is a very powerful and secure algorithm to determine the key to be used in End to End Encryption.

**Advanced Encryption Standard Algorithm**

The algorithm used to encrypt data is one of the most important steps, as this is what determines how difficult it is for the publicly transmitted encrypted data to be decrypted by an unwanted party. One of the most commonly used cipher algorithms is the Advanced Encryption Standard (AES). A National Institute of Standards and Technology (NIST) publication released on November 26, 2001, outlined AES to be the standard for securing sensitive information within Federal departments and agencies. According to this publication, AES is a specified form of the Rijndael algorithm, which is a block cipher that can process data blocks of 128 bits using cipher keys with lengths of 128,192, or 256 bits. These cipher keys are typically obtained from the Diffie-Hellman key exchange mentioned earlier. Next, the text is converted into hexadecimal format and stored in arrays, so it can be interpreted by the computer. From there, the data that is to be encrypted undergoes four transformations for every round. The number of rounds is decided by the length of the cipher key mentioned earlier, and are 10, 12, and 14 in order of increasing key length. All of these steps work to scramble the data as much as possible, making a user’s data even more difficult to intercept. The first step in a round is to perform the subBytes transformation. This transformation aligns with a substitution box (S-box), which corresponds to a hexa2--decimal value and that value is then substituted for the value indicated in the table. An example of one of these S-boxes is shown below.

![Figure 3](image)

**An S-box illustrating substitution values for the subBytes transformation**

This S-box corresponds with hexadecimal values for a byte (x,y). For example, if the byte to be substituted was 7c it would be substituted with the value 10. The next transformation in the AES algorithm is known as the ShiftRows transformation. This transformation is much simpler, as the row of an array is just shifted over by a value specified by the key. The figure below shows this transformation.

![Figure 4](image)

**A visualization of the ShiftRows transformation**

This shows the array S of bytes $s_{xy}$ being transformed into the array $S'$, by not moving the first row, transposing the middle row, and placing the first 3 columns of the last row to become the last three columns of that row. The third transformation in a round is the MixColumns transformation, which treats each column of an array as a four-term polynomial equation, then multiplies that by a different array, determined by the key, to produce a scrambled column. The last transformation in a round is the AddRoundKey transformation. In this transformation, a subkey is derived from the main key, and then added bitwise to each element using the exclusive or function. This figure illustrates how much an array of data changes as it passes through one round of this algorithm. The
first array represents the original data, then each following array is after each of the individual transformations.

![Table](image)

**Figure 5 [15]**

This shows how much an array of data changes after one round of the AES algorithm.

It is obvious that this algorithm is complex, and with a 256-bit key, it is near impossible to crack [14]. Since this algorithm is so complex, it would have taken the first computers a very long time to perform this scrambling of data. However, due to the increase in performance of computers and the increased efficiency, this algorithm provides a fast and efficient way to scramble data beyond recognition, and as this process evolves it will become more efficient. Therefore, it offers and adaptive and sustainable method to secure a user’s data. However, often the weakest link in an E2EE system is the users, so secure implementation is extremely important.

### Secure Implementation

Secure implementation is an essential component to ensuring that the E2EE process is secure. For example, if malware is installed on a client’s computer that is capable of stealing data from the computer’s memory, the entire encryption process is useless, because the hacker has access to the data after it has already been decrypted. Behringer also mentions malware that is capable of logging keystrokes which means that passwords and usernames can be stolen and used to impersonate the user. Due to this vulnerability, often businesses using E2EE will require users in a network to have an antivirus service installed on their computer to prevent against malware attacks compromising the security that E2EE offers [9]. Overall, E2EE is an extremely safe and secure way of sending information across the internet and is the best solution to enhancing privacy online. This is due to its adaptability, use of privately generated keys, and complex algorithms that allow for the maximum security possible.

### CHALLENGES OF AND ATTACKS ON END TO END ENCRYPTION

Although end to end encryption is a very secure method of communication, there are still ways to gain access to information inside an encrypted file, through such methods as Man in the Middle Attacks. These attacks are made on messages that are in transit from sender to receiver, but taken advantage of because of connection the internet network, which depends on the type of network.

### Man in the Middle Attacks

Man in the Middle Attacks are strikes on a line of communication in which the attacker intercepts and can manipulate a message that is sent from a sender to a recipient. In a Man in the Middle attack, the person attacking is able to retrieve the message sent, through a set of public keys. After opening the message, the eavesdropper is able to view data and even edit the message. After intercepting the message and doing whatever they want, they can send it using a similar set of keys, which will send it to the intended recipient, and no trace is left behind [16]. These attacks are very complicated, but there is a simple way to prevent these attacks. Simply by using a private and secure network, you are keeping people out of your internet connection and they are unable to intercept messages. Unfortunately, not many people stay away from public networks with no passwords and are exposed to these assaults on personal, digital information. Even though public network connections are available, there is a great risk with connecting and not many people know.

![Diagram](image)

**Figure 5 [16]**

A visualization of MiMA

An encrypted message is sent from a remote connection and received on the network of the end user. The attacker is also connected to the same network and therefore, has access to the encrypted message. Through using a set of public or stolen keys the attacker can look at the information and even change it. The attacker re-encrypts the message and send is to the end user, who is not able to tell that a message was tampered with.

### APPLICATIONS OF END TO END ENCRYPTION

**Communication on Messaging Platforms**

The first widely used platform was named Pretty Good Privacy, or PGP, and was released in 1991. PGP was released by Phil Zimmerman, because he believed that everybody deserves privacy [17]. When Apple launched iMessage in 2011, the service had end to end encryption built in upon launch of the platform. Another one of the main platforms to offer end to end encryption is WhatsApp, a popular messaging service owned by Facebook, which implemented the system in 2014. Other popular platforms that host end to end encryption include Facebook Messenger (although it is not turned on by default), Threema, Google Allo, Signal, Telegram, and OTR.
Encryption on Other Platforms

In addition to the different messaging applications, there are also different systems that use end to end encryption on different platforms. End to end encryption is often found on email, telephone, and even radio. Different platforms that are commonly used on email include, GnuPG, Protonmail, Mailfence, S/MIME, Inky, and pEp. On telephone end to end encryption, software like ZRTP and FaceTime use Voice over Internet Protocol, or VoIP, based on Real-time Transport Protocol. The software that uses end to end encryption for radio is called TETRA. There are many more applications or services that use end to end encryption for communication and messaging. Encryption on all of these platforms is important because is allows safe, private communication methods between two or more people.

Encryption of Medical Records and Patient Data

Sensitive personal information isn’t found only in communication platforms; it is also found in hospitals where the patient’s data is used to keep track of history, problems, and documentation. There are often thieves, who take advantage of information that is left in the open, who try to steal information, or to gain access to drugs or any other thing people usually don’t have access to. To prevent this from occurring, documents and information is encrypted with a code initially, so that it is not able to be intercepted by the wrong eyes. The intended receiver also has a key that is able to decrypt the information and is able to use the information that has been encrypted and is able to help the patient. This is a process that is based on end to end encryption, and also directly is able to help out people, by keeping their health information safe and kept from the wrong people [18].

ETHICS OF END TO END ENCRYPTION

As stated by the Software Engineering Code of Ethics and Professional Practice in Principle 4, line 1, the engineer must “Temper all technical judgments by the need to support and maintain human values.” [19]. Access to one’s own privacy is a basic human right, and such should be the same on all means, including internet. Every person has information that is only for them, such as their Social Security Number, driver’s License, and credit card number. In the new age of technology more people are putting their important information on the web, in an attempt to make their lives easier. However, there is a large risk when one puts their private information on a service that is available to anybody that has a connection and a device. Unfortunately, there are people that attempt to and succeed at breaking into and stealing people’s private information. This is where end to end encryption, when applied to this technology comes in, and protects the user’s sensitive information.

To the contrary of the previous view, some believe that the risk of malicious use of this technology outweighs the rewards of personal privacy on the internet. As stated by the National Society of Professional Engineers’ Code of Ethics, “Engineers, in the fulfillment of their professional duties, shall…. Hold paramount the safety, health, and welfare of the public.” [20]. This is the very first of the fundamental canons in the society's Code of Ethics. This canon can be interpreted that the engineer in such dilemma must always operate so that there is the least amount of risk to the public. With the technology of end to end encryption, the public is more open to physical attacks, that may be coordinated with end to end encryption to avoid being detected under monitored communication platforms. Without end to end encryption, regular users would have to avoid putting confidential information on any platform, or they risk giving information that people should not see to people that should not have access to the information.

Setting a Precedence

In December 2015, a shooting otherwise known as the San Bernardino shooting took place. There were fourteen people killed by two attackers. After the fact, the Federal Bureau of Investigations discovered one of the attacker’s cell phone, a blue iPhone 5C that was locked. The phone was brought to Apple and was requested to be unlocked, but however Apple refused the request, in an attempt to set a precedence of keeping the customer’s security first. The FBI did not stop and a federal magistrate judge, with the Justice Department’s request, sent an order for Apple to bypass security functions on the device. Apple still resisted and went into court.

On February 16, 2016, Apple sent a message to their customers explaining their decisions and answering questions about privacy and security. The message talks about the importance of encryption, the risk of compromising the security, the San Bernardino Case, the threat to data security, and setting precedent [21]. The letter outright states, “But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.” Apple absolutely refused because they have always had the ideology against what the government was asking of them. This was not the first time that a company was asked to decrypt its own software and programs, but it defined the precedence of companies having to decrypt their own devices.

Backdoors

Companies implement a backdoor end to end encryption platforms, and sometimes will not tell their customers about having a backdoor. A backdoor is a system in place by the service provider in which they can go in and get the messages that were sent, decrypt them, and hand them over to a third party, such as the NSA, CIA and other government
organizations. This is commonly looked down upon by consumers, because they are not getting a service that is truly encrypted end to end.

A very common example of an end to end encryption service with a backdoor as a part of the system is Microsoft’s Skype. The service was previously thought to be fully end to end encrypted without a way for Microsoft to see what is sent. In 2013, Edward Snowden shared that the platform did in fact have back door, in which enabled Microsoft access to all messages and communications on the service. Microsoft and Skype denied that statement many times, but in the end, it was shown that Skype messaging and voice backdoors. [22] Skype users protested the system, because it allowed attackers an easier way to access anybody’s information, because Microsoft has already decrypted their own technology, which means that it is easier to decrypt it.

There is an ethical dilemma that Microsoft faced when they had to implement backdoors. By implementing back doors, it meant that the service was not truly end to end encrypted, which meant that it was not as secure as it was thought out to be. In order to protect the general public, the backdoor was implemented, which meant that Microsoft and Skype had to protect the public. Usually, Microsoft would not really need to access messages sent, for most people do not have ill intentions. It can be understood, that after the fact, Microsoft and Skype wants to be able to access records to provide the government any government agencies with information that is able to protect the public in the future.

**FUTURE OF ENCRYPTION**

Encryption and end to end encryption has long been a great tool that has helped us many times, and the future of end to end encryption as a tool in the public really depends on the decisions of today and soon to come. If end to end encryption is accepted generally as the normal, then there is a wild amount of possibilities open in the future for encryption and cryptography. In 2010, and Idea was put forth for a type of encryption called fully homomorphic encryption, which allows access to data without ever decrypting it. Another idea is called honey encryption, in which upon many wrong guesses of a key creates data that is not accurate but looks like it is. Next is called functional encryption, in which restricted keys enable the key holder to learn only about a function of data and nothing else. The final approach is called quantum key encryption, in which the quantum nature of atoms actually is responsible for protecting all of the user’s data [23]. These methods could be even more secure than end to end encryption, which can help keep people’s information safe, in both the communication platforms and patient data. Data of a person could potentially be saved on that persons atoms and cells, which could potentially be very safe, because only the person could decrypt the information on their atoms, plus the have access to their atoms. Encryption is a very safe way to protect a user’s confidential data, and is essential in this age, an age that is filled with technology and progressive, creative thinkers who will further accomplishment and achievement.

**SOURCES**


ACKNOWLEDGMENTS

We would like to thank our parents for their guidance along our transition to college thus far. In addition, we would like to thank Rachel McTernan for her assistance in revising and improving this paper. Also, we would like to thank Patrick Loyn for his guidance with this paper.

ADDITIONAL SOURCES
