Final Paper

Lakeidra Eady

School or Institution Name (University at Place or Town, State)

 **Abstract:**

Telecommunication is an umbrella term now. It deals with the transfer of information from one place to another using electronic means including emails, instant messaging and video data. Telecommunication has seen tremendous growth in recent decades. It is the fastest growing technology made by humans. It is transforming from traditional voice networks to next-generation data networks. Internet and communication technologies are evolving at an exponential rate. Along with the advancement in communication technologies latest trends are of securing the data in transit. Encryption algorithms and various security algorithms are being developed to secure communications. The paper describes the advancements made in the area of cryptography related to the latest trends in telecommunication and arising challenges for the technology.

**Introduction**

 Telecommunication is referred to the transfer of information from one place to another using electronic means such as satellite communications, wireless radio communications, and fiber optical communications, etc. Telecommunication has seen tremendous growth since the invention of radio technology. Telecommunication is not only limited to the transfer of voice like in traditional telephone (Xu, Qu, & Yang, 2016). Modern telecommunication is an umbrella term providing a plethora of different services ranging from traditional voice networks to next-generation video networks. The advent of the internet has made telecommunication the primary driving force behind global development and value creation.

 In recent decades many changes are occurring in the communication industry due to the advancement in technology. Telecommunication services providers and all of the industries that rely on communications technologies for their operations as well will feel the immediate and far-reaching impact of the significant trends that are being circulated in the communication sector. Internet of things has become a buzz word in the telecom world. With the advancement in communication technologies and miniaturization of the antenna technology, every possible thing is being connected to the internet making the world a global village (Kraijak & Tuwanut, 2015). Nowadays we have the ability to control a room air conditioner with the help of mobile phone. It is not appropriate to call a modern mobile phone just a mobile phone. It has transformed into a powerful computer. In fact, as powerful as supercomputer of the 1970s. It has been an established fact that the internet of things will be something more than just controlling home appliances using wireless networks. It is developing as an ecosystem that connects everything from the toaster in the kitchen to the car and from the workplace to the large-scale industrial networks.

 While there are tremendous developments being made in the telecommunication, the industry is not unaware of the potential growth in the internet of things ecosystem. Instead, the telecom industry has shown a keen interest in the internet of things market as well because no internet of things is possible without the backbone infrastructure of the telecom companies. In 2015, the telecom industry spent a total of $110 million in the development of the internet of things devices (Farooq, Waseem, Khairi, & Mazhar, 2015). The industry was also ranked at fourth place for investing in the research and development activities of the internet of things. According to the recent developments in the ecosystem, it is believed that there will be twenty billion connected devices to the internet. That will be a massive amount of data to be routed and transmitted from one location to another location globally.

Although all of the connectivity is being provided and continuously expanded by the telecom provider companies, there are growing concerns about protecting the data being transmitted over telecom networks. There are various measures and technologies implemented to ensure the security of the data in transit, but the most important technology is the cryptography. Cryptography is the technology that deals with the hiding of the transmitted message from prying eyes by encrypting the message (RU-nian, 2009). Telecom industry is focusing on implementing the cryptographic capabilities into the internet of things ecosystem using supporting technologies such as machine learning. The paper describes the efforts of the telecommunication industry to implement security in the internet of things and the challenges being faced by the industry.

**Literature review and background of the study:**

Communication has played a central role in human life since the beginning of the information age. In earlier days the conversations were based on mutual trust. In other words, if two persons were having a conversation, then they were not worried about someone listening to their conversation without permission. Privacy and security of mutual communication was the fundamental right of human being. No one was able to eavesdrop on someone else’s conversation (Miller & Alexander, 1996). With the advent of communication technology, it has become possible for people to eavesdrop on others. Eavesdrop means listening to someone's conversation secretly. Since then scientists and communication engineers are continuously working on making communications more secure. In early telephone days, the voice was transferred using the wired network only. With the advancement of science and technology, it was possible to record the telephone calls of the people as well. FBI agents were tasked with clamping the crocodile clips in the phone lines of the suspected party and to record their phone calls. That action strictly violated the previously laid out privacy culture.

 That was the initiating point of efforts to implement cryptography into the telephone networks. Cryptography is the practice of encoding the message so, that only intended recipient of the message can read the message. It was to ensure the confidentiality of the message being transferred over the insecure telecommunication networks. Various methods of securing communication have been developed and implemented. The method of encrypting or coding the message is known as cryptography (Sumi & Ranga, 2016). In cryptography simple message is also known as plain text is run through a code known as a cipher resulting in a ciphertext. The message is encoded by performing the cipher on the plain text at the sender side. On the other hand, the receiver will perform the exact opposite of coding known as the decoding operation on the received ciphertext to extract the original message. The practice was common in written letters during World War II for circulating confidential military-related intelligence to concerned parties. With the advancement of science and communication technologies cryptography is being implemented into the communication networks because all of the communication is now digital in nature.

 A simple example of the earliest form of the cryptography is the rotation 13 cipher. In which each letter of the message is replaced with the corresponding letter in the English alphabets at number 13. Thus, the ciphertext obtained by the ROT13 cipher can only be decrypted by reversing the action known as deciphering or the decoding of the message. In this way, the message can only be understood by the recipient parties (Dawson, 2017). The rotation is particularly thirteen, and it is known as the key of the encryption. The receiver can only decode the message if the key is known to the receiving party. In the above example, the key is thirteen meaning that each letter needs to be rotated thirteen places (Stallings, 2017). The technique is known as the symmetric cryptography because the key for the encrypting the message and decrypting the message is the same that is thirteen.

 Symmetric cryptographic techniques are as secure as the key of encryption. Modern encryption systems use various sophisticated encryption algorithms. The example of ROT13 is just a simple example of understanding the encryption. Modern encryption systems are not as simple as ROT13. Rather they are complex and sophisticated in their design. They need to be sophisticated because while the security researchers are developing new encryption algorithms, the criminals are also working on new methods to crack the encryption codes (Icart & Coron, 2018). The encryption mechanism and algorithm implemented to secure internet traffic was known as the RC4 algorithm. It was known to be the trusted encryption method for securing internet traffic so that no one can intercept the message in transit. But in 2014, it was cracked by the RC4 No more project. The team demonstrated the vulnerabilities into the algorithm of encrypting the message using RC4 encryption. Since then the algorithm has been replaced with modern algorithms of securing the data.

 In earlier days the channels for data transfer were only limited to the voice traffic. But given to the fact that the world will be having twenty billion devices connected to the internet transferring the data in various formats the security will be more crucial than ever. Therefore, the telecommunication industry is investing more in security than ever to ensure the privacy and security of the data being transmitted. Almost all of the internet of things devices works on wireless networks (Dodis, 2017). Data transferred over wireless networks can be intercepted by anyone having access to a radio system. Wireless channels are more prone to man in the middle attacks than the wired channels for data transfer. It is not possible to build an internet of things over wired channels for the sake of security because it would not be physically and economically possible to connect billions of devices using wires. Hence, the solution is to improve the encryption capabilities of the modern ecosystem of the internet of things and build a secure network for transferring valuable information.

**Discussion**

 Internet of things coupled with artificial intelligence and machine learning is the future of modern communication systems. It is expected that in a decade each and every gadget will be having internet connectivity thus building an internet of things. Internet of things corresponds to the machine to machine communication. A network in which machines can communicate and collaborate with other machines without any human intervention (Kumari et al., 2017). All of the devices will be transferring the data over wireless channels because the internet itself was not designed with much security in mind, so any ecosystem built over the backbone of the internet will be inherently insecure. Telecommunication industry will see tremendous growth in security technologies to make the internet of things ecosystem more secure than ever.

 As the symmetric key cryptography cannot be used in the internet of things because symmetric key cryptography requires the transfer of key via some secure channel. Therefore, more robust solutions such as public key cryptographic mechanisms are to be implemented into the IoT devices. Public key cryptographic algorithms require certification authorities to authenticate the requests to the protected resources. It is inevitable to implement cryptographic capabilities in the internet of things devices to protect the data transfer from intruders. Internet of things is penetrating the industries dealing with personally identifiable information such as healthcare organizations and financial institutions such as banks (Tewari & Gupta, 2017). An IoT device in a healthcare facility may be collecting health records of the patient and transferring them to the doctor in another country over an insecure channel. These communications over insecure channels can be intercepted by third parties while being transmitted to the destination.

 Telecommunication industry can provide the backbone to transfer the data and implement the security mechanisms, but the cryptography must be implemented within the electronic devices. It is crucial because many organizations may not even trust their telecom or internet service providers to handle their data for encryption. It is important because in this way the third party which the service provider, in this case, may be aware of the encryption keys as well (Liu & Seo, 2019). The problem is not only with the telecom service providers but with the device manufacturers as well. Each of the IoT devices is powered by some type of processing chip capable of processing the data. These chips are not manufactured at a single place. Reports and research studies reveal that almost millions of the IoT device processing chips are manufactured in unknown factories across the globe putting the question mark on the security of such devices.

 It has been revealed in recent years that most of the IoT devices can be hijacked and remotely controlled by the criminals for data harvesting. Headlines are filled with the news of such data breaches on insecure networks of the internet of things. The manufacturing issues restrict the implementation of inbuilt encryption capabilities to IoT devices. All of the devices are so small in size that their limited processing power cannot support encryption algorithms. Encryption and decryption of the data require considerable processing power that cannot be provided by the tiny internet of things devices such as wearable technologies. On the other hand, if the telecom industry will try to implement encryption capabilities into their network backbone, then it will not be possible for the industry to maintain the quality of the service due to the processing overhead created by the encryption jobs (Naru, Saini, & Sharma, 2017). With the advancement in science and technology if the scientists and engineers are able to build the encryption algorithms and incorporate trusted platform modules into tiny internet of things devices, then there will be other problems as well. A huge number of connected devices are powered by the batteries. All of the manufacturers claim long-lasting battery lifetimes to increase their revenues. It will be a difficult job to convince all of the manufacturers worldwide to compromise battery life for security. So here is the tradeoff between the battery life of the internet of things devices and security of the data being transmitted by these devices without any encryption.

 In recent years cyber crimes have been increased tremendously, and criminals are developing sophisticated attacks. Depending on the complexity of design and development involved in the manufacturing process, it is not possible for a single manufacturer to build all of the required electronic parts in a single factory. Therefore, they license different parts from different manufacturers across the globe (Liu, Choo, & Grossschadl, 2018). So, the security of the supply chains is also critical because if the encryption is important or data security, then protection from internal backdoors of the device is also inevitable. Hardcoded threats will not be eliminated by software innovations. Without implementing encryption as an essential technology in the internet of things devices, we will be creating a world of internet of threats instead of building an internet of things.

 To build a secure internet of things telecom industry in conjunction with the software industry is developing complementary technologies. Many companies such as the Kaspersky lab a Russian cybersecurity organization, has developed an operating system for the internet of things devices to implement basic security features into the devices. It is an important step for creating a secure infrastructure for the optimal operation of the internet of things (Tiwari & Kim, 2018). Insecure devices connected to the internet can compromise the security of the whole internet infrastructure. IoT devices are closely connected to a single access point; it is relatively easy for the attacker to compromise a single vulnerability in the device and take control of the entire network intercepting the critical information being transferred.

 Along with telecom companies, the cybersecurity companies such as AVIRA, a Germany based information security company, now building secure network routers to implement basic encryption algorithms in their routers to protect the data from hackers and eavesdroppers. Telecom companies will not only invest and grow in the security aspect of the internet of things but will continue to develop their connectivity backbone infrastructure as well to support billions of connected devices (Thota, Sundarasekar, Manogaran, Varatharajan, & Priyan, 2018). Telecom industry will invest massively in fifth and sixth generation networks to move the machine to machine communication data of internet of things devices quickly and securely. Recent investments by the telecom service provider Verizon in telematics shows that it will invest in any technology requiring location services powered by their network infrastructure. Telecom equipment manufacturers such as Nokia, Huawei and ZTE are among the names investing in artificial intelligence and machine learning capabilities to enhance the security for the internet of things.

**Summary and Conclusion:**

Security of the transferred data over the communication backbone or insecure channels is inevitable for the growth in the internet of things ecosystem. Currently, the complexity of implementing encryption technologies in the internet of things devices is the major bottleneck in the development of the ecosystem. Telecom industry has recognized the potential of tremendous growth in the internet of things. Therefore, telecom service providers and equipment manufacturers are making investments in the field of the internet of things to create a secure environment for connected devices along with building and improving the backbone infrastructure for communications. Along with the development of the latest technologies of data transfer such as the fifth generation of networks the security of the internet of things will also be improved by incorporating machine learning and artificial intelligence into the ecosystem. By developing and implementing these technologies, the world will soon be able to see a sustainable ecosystem powered by the internet f things and telecommunication revolution.

References

Dawson, M. (2017). Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity. *Security solutions for hyperconnectivity and the internet of things* (pp. 1–12). IGI Global.

Dodis, Y. (2017). Basing cryptography on biometrics and other noisy data. In *2017 51st Annual Conference on Information Sciences and Systems (CISS)* (pp. 1–1). IEEE.

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7).

Icart, T., & Coron, J.-S. (2018). *Cryptography on an elliptical curve*. Google Patents.

Kraijak, S., & Tuwanut, P. (2015). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In *2015 IEEE 16th International Conference on Communication Technology (ICCT)* (pp. 26–31). IEEE.

Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Kumar, N. (2017). A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *The Journal of Supercomputing*, 1–26.

Liu, Z., Choo, K.-K. R., & Grossschadl, J. (2018). Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography. *IEEE Communications Magazine*, *56*(2), 158–162.

Liu, Z., & Seo, H. (2019). IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms. *IEEE Transactions on Information Forensics and Security*, *14*(3), 720–729.

Miller, S. E., & Alexander, J. (1996). *Civilizing cyberspace: Policy, power, and the information superhighway* (Vol. 14). ACM Press New York.

Naru, E. R., Saini, H., & Sharma, M. (2017). A recent review on lightweight cryptography in IoT. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 887–890). IEEE.

RU-nian, L. I. (2009). Study on the Internet of Things Based on RFID Technique [J]. *Journal of China Academy of Electronics and Information Technology*, *6*, 595–597.

Stallings, W. (2017). *Cryptography and network security: principles and practice*. Pearson Upper Saddle River.

Sumi, L., & Ranga, V. (2016). Sensor enabled Internet of Things for smart cities. In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 295–300). IEEE.

Tewari, A., & Gupta, B. B. (2017). A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms*, *9*(2–3), 111–121.

Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. In *Fog Computing: Breakthroughs in Research and Practice* (pp. 365–378). IGI Global.

Tiwari, H. D., & Kim, J. H. (2018). Novel Method for DNA‐Based Elliptic Curve Cryptography for IoT Devices. *ETRI Journal*, *40*(3), 396–409.

Xu, K., Qu, Y., & Yang, K. (2016). A tutorial on the internet of things: from a heterogeneous network integration perspective. *IEEE Network*, *30*(2), 102–108.