Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Using Cryptography as a Peer-To-Peer Security Protocol for Internet of Things (IoT)

Samuel Opoku Daniels
School of Technology
Ghana Institute of Management & Public Administration
GreenHill, Accra Ghana
E-mails: samuel@fucah.com

ABSTRACT

The Internet of Things (IoT) is a system with an ever-growing complexity; it is the next breakthrough that will humanize every object in our lives, as well as the next stage of automation. People are eager to embrace the convenience and practicalities brought by the rapidly evolving Internet-connected gadgets and applications. The IoT, which connects a variety of devices, systems, and applications beyond traditional machine-to-machine communication, evolves as technology generally advances and provides users more sophisticated services. Devices that are part of the IoT generate, analyse, and communicate enormous volumes of data that is sensitive to privacy as well as security, making them attractive targets for various cyberattacks. The number of attacks and types of attacks have increased tremendously in comparison to older IoT technology over the past decade of technological advancements in the domain of IoT security. Despite the numerous Internet protocols that have been proposed, they are still unable to satisfy the IoT's increasingly complicated requirements. Many of them are not effective enough to adapt to the environment of diverse devices and quick communication. One of the major ways perpetrators use to compromise IoT devices is via the server. They leverage vulnerabilities, un-updated software packages or dependencies and server misconfigurations to launch attacks against IoT technologies. The most effective way to battle the ever growing cyberattacks on IoT is to deliberately reduce the attack surface. This can be achieved by deploying a peer-to-peer security protocol for IoT, instead of the usual server-to-peer implementation. By doing so, all the vulnerabilities and problems that come with server and the leverage it gives to perpetrators will be eliminated. One sure way to drastically reduce attacks on IoT technology in general is the reduce the attack surface during IoT implementation, and eliminating servers and allowing peer-to-peer communication between IoT devices help to achieve that. This research project attempts to mitigate attacks on IoT by putting forward a peer-to-peer security protocol to drastically reduce the attack surface and to accommodate the diverse IoT environment so has to enhance IoT security.

Keywords: Protocols, Security, Peer-to-Peer, IoTs, Cyber Security, Internet

Proceedings Citation Format
Samuel Opoku Daniels (2022): Using Cryptography As A Peer-To-Peer Security Protocol For Internet Of Things (IoT). Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 71-76. www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P9

1. INTRODUCTION

In the context of contemporary wireless telecommunications, the Internet of Things (IoT) is a unique paradigm that is quickly gaining traction. The fundamental tenet of this concept is that there are numerous items or things all around us, including Radio Frequency IDentification (RFID) tags, sensors, actuators and home appliances such as light bulbs, fans, air conditioners, fridges, cookers, etc., which can communicate with one another and work together with peers to accomplish shared objectives (Luigi et al, 2021). According to the National Intelligence Council (NIC), by 2025 Internet nodes may reside in everyday things—food packages, furniture, paper documents, and more. It highlights future opportunities that will arise, starting from the idea that “popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development”.

The possible threats deriving from a widespread adoption of such a technology are also stressed. Indeed, it is emphasized that “to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date” (Luigi Atzori, Antonio Lera, Giacomo Morabito, 2010). The IoT is vulnerable to various security threats due to the nature of its technology. In particular, it has a limited hardware specification such as low power consumption, small amount of memory, etc., and tends to be distributed in an environment where it is difficult to manage, which potentially has various security threat factors including physical attacks, replay attacks and man-in-the-middle attacks (Sunghyuck Hong, 2019). Another concern stems from the fact that most of these devices use wireless as a main communication medium, as such, threat actors can easily eavesdrop or intercept the message, thereby compromising security and privacy.

Different types of security mechanisms have been employed to safeguard some IoT devices. One of the biggest obstacles to securing an IoT network is lack of standardisation at the manufacturing level, which leaves the hardware, software, and data vulnerable to numerous threats and assaults. Also, many IoT devices have limited storage and processing power. As such, any security mechanism employed should necessarily be light in terms of storage and processing to be effective. Considering the fact that it is difficult to find one solution that can be adapted everywhere, the protocol should be flexible enough to adapt to different situations. Symmetric algorithms are light weight compared to asymmetric algorithms and therefore are recommended for securing data transmission. However, they have problems in key exchange, confidentiality, digital signature and message authentication.

Hence public key algorithms are recommended as they are able to provide key management, node authentication, scalability and security (J. Cynthia et al, 2020). Multiple layers of security is required to mitigate all the attacks on IoT. Figure 1 below is the summary of the attacks that are commonly used on IoT.

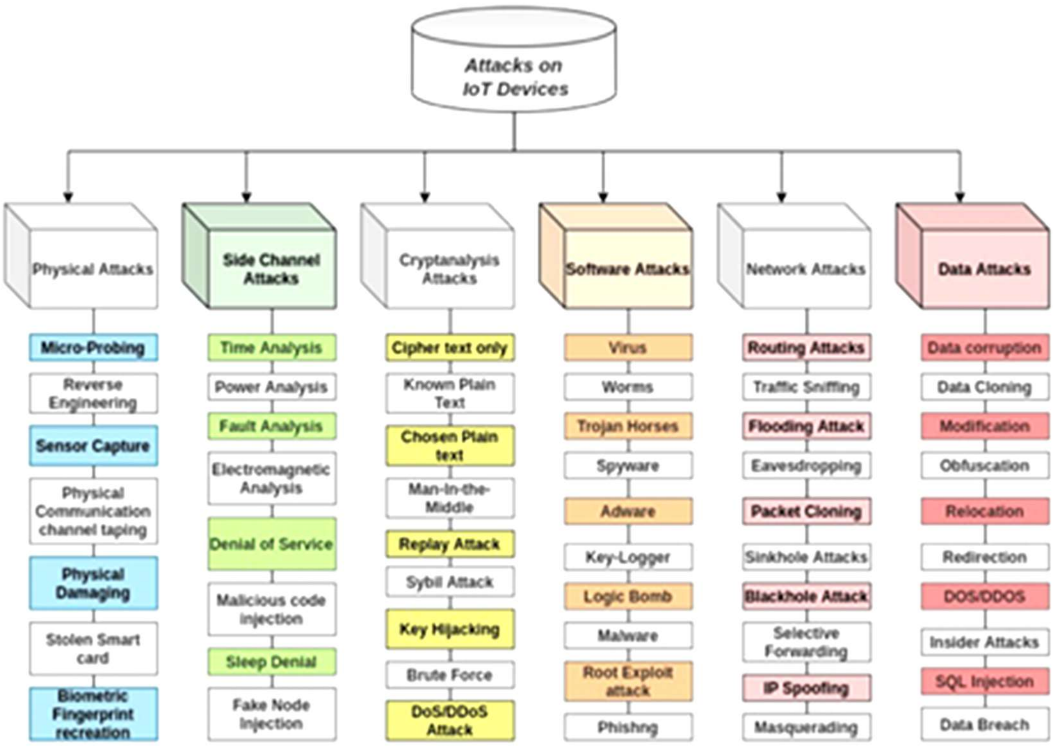

Figure 1: Typical Attacks on IoT Devices

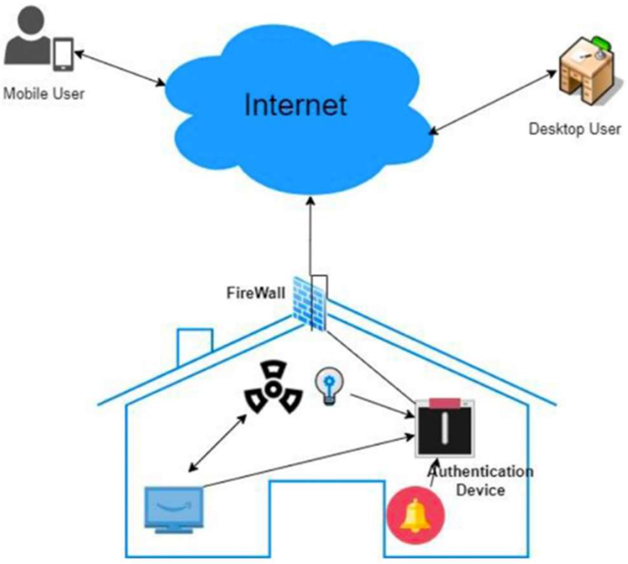

Figure 2: Secured implementation of IoT.

A proper implementation of a good cryptographic algorithms can help mitigate all these attacks, with the exception of physical attacks. Evidently, we cannot overestimate the importance of cryptography is IoT. Figure 2 below illustrates a secured implementation of IoT. In order to create a secured peer-to-peer security protocol for IoT, there is the need for more than just one layer of security. In the event where a user wants to operates the home device from a remote location, the user uses the internet to send a command to the home appliances. Every communication done through the internet must go through a secured hypertext transfer protocol (https), implemented over the latest Transfer Layer Security (TLS).

At the time of writing this paper, the latest version of TLS is version 1.3. This ensures that traffic over the internet is encrypted, therefore can prevent some attacks such as man-in-the-middle attacks. For an advance implementation, a virtual private network (VPN) is recommended to prevent https stripping. The VPN creates a secure tunnel to the traffic in the home network. Every traffic to and from the home network must go through a firewall with required rules to block illegitimate traffic, to avoid denial of service attacks and buffer overflow. The best way to implement the peer-to-peer security in IoT technology is by using a blockchain. This will prevent man-in-the-middle (MitM) and replay attacks with part of the most common attacks against IoT technology. Blockchain provides a decentralised mechanism to store validated session keys that can be allotted to the network devices (Ankit Attkan and Virender Ranga, 2022). Blockchain is has been very successful in real life application such as bitcoin and other cryptocurrencies.

3. RELATED LITERATURE

There has been some work on various protocols put forward to secure IoT. Various research streams focus on cryptographic encryptions as part of recommended ways to secure IoT.

TITLE OF PAPER	AUTHOR(S)	FINDINGS
Survey on secure communication protocols for the Internet of Things	(Kim Thuat, Nguyen, Maryline Laurent & Nouha Oualha, 2015)	The applicability and limitations of existing IP-based Internet security protocols and other security protocols used in wireless sensor networks, which are potentially suitable in the context of IoT.
Security Protocols for IoT	(J. Cynthia et al, 2020)	Elaborates on various security attacks and the solutions offered by IoT protocols and IoT protocols that deals with securing an IoT network.
Analysis on functionalities and security features of Internet of Things related protocols	(Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini, 2022)	Investigate security features, which are often combined with native functionalities, in the most known IoT-related protocols: MQTT, CoAP, LoRaWAN, AMQP, RFID, ZigBee, and Sigfox.
P2P networking based internet of things (IoT) sensor node authentication by Blockchain	(Sunghyuck Hong, 2019)	Block-chain-based IoT device is proposed to get a more secure authentication scheme.
ASSURE: A hardware-baSed SecUrity pRotocol for resourcE-constrained IoT systems	(Yildiran Yilmaz, Leonardo Aniello, Basel Halak, 2021)	Propose a lightweight mutual authentication and key agreement protocol named ASSURE based on Rivest Cipher (RC5) and physically unclonable functions (PUFs).
Light Weight Authentication Scheme for Smart Home IoT Devices	(Vipin Kumar et. al, 2022)	proposes a home device authentication scheme when these are accessed from a remote place.

4. RESEARCH GAPS/FINDINGS

Computer networks are widely used today, and we utilize the Internet to access our home network. IoT networks are a brand-new category of these networks where we attempt to connect various home equipment and attempt to issue commands from a distance. Privacy and security have been the most prevailing issues in IoT domain. Many researchers have strived to come up with various ways to secure IoT technologies. Most IoT devices fall prey into the hands of perpetrators because they leverage one or more vulnerabilities. Many researchers have come up with various research streams to improve upon the security of IoT. The problem however, is that, the attackers leverage on the areas that are neglected as far as security is concern to launch their attacks. For proper security, the implementation should be such that every aspect of the communication is secured.

5. CONCLUSION

Setting up a security mechanism that effectively protects communication traffic has become a significant issue for systems and applications due to the growing complexity and risks to security. To solve this issue, I proposed a peer-to-peer security protocol. The required features of this protocol are achieved through a series of mechanisms. It is scalable as no central server is used and no third party involved when communicating between two entities. To be able to fully secure IoT technology, server-to-client implementation should be eliminated while peer-to-peer security protocol used. Also, blockchain must be the underlining cryptographic implementation behind the peer-to-peer protocol.

6. RECOMMENDATION FOR POLICY AND PRACTICES

Reducing the attack surface also means reducing the possibility of cyber threat actors gaining access to devices and recking havoc to them. Eliminating servers form IoT technology will pretty much eliminate all attacks against servers. A peer-to-peer security protocol with blockchain implementation is the way forward.

7. DIRECTION FOR FUTURE WORKS

Fucah research should focus on how to implement blockchain effectively on most IoT technologies to enforce peer-to-peer security protocol, despite the limitations of some IoT devices, specifically, some IoT devices have low memory space and processing capabilities. Blockchain stores session keys on all the nodes of the connected devices, as such the database increases with time, and requires high processing power and large memory space. However, because of relatively low memory size and processing power of most IoT devices, it is not feasible to deploy blockchain on them.

REFERENCES

1. Alessandra Rizzardi, Sabrina Sicari & Alberto Coen-Porisini, "Analysis on functionalities and security features of Internet of Things related protocols", 2022.
2. Ankit Attkan and Virender Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security", 2022.

3. Atzori, Luigi ; Iera, Antonio ; Morabito, Giacomo, "The Internet of Things: A survey" Computer Networks, 2010, Vol.54(15), pp.2787-2805 [Peer Reviewed Journal].
4. Guedda Hassan Mohammed, "The Truth About Blockchain", 2017. https://hbr.org/2017/01/the-truth-about-blockchain
5. Hao Zhang, "A Peer to Peer Security Protocol for the Internet of Things – Secure Communication for the Sensible Things Platform", 2014.
6. J. Cynthia et al, "Security Protocols for IoT", 2020.
7. Kim Thuat, Nguyen, Maryline Laurent & Nouha Oualha, 'Survey on secure communication protocols for the Internet of Things", 2015.
8. Luigi Atzori, Antonio Lera, Giacomo Morabito, "The Internet of Things: a survey", 2010.
9. Sunghyuck Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain", 2019.
10. Yildiran Yilmaz, Leonardo Aniello & Basel Halak, "ASSURE: A hardware-baSed SecUrity pRotocol for resourcE-constrained IoT systems", 2021.
11. Zhang, Hao. "A Peer to Peer Security Protocol for the Internet of Things: Secure Communication for the Sensible Things Platform", 2014.