International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 2, March 2020 |

Application of Cryptography for the Internet of Things

Dr. Rajendra Kumar Bharti

Associate Professor, Computer Science & Engineering, Bipin Tripathi Kumaon Institute of Technology,
Dwarahat, Uttarakhand, India

ABSTRACT: As CIOs and their organizations deploy more connected devices and build out more extensive IoT environments, many struggle to secure those ecosystems and all the data generated.Cryptography is a useful counter to those challenges.Cryptography uses codes to protect information and communications, making it inaccessible to all but those authorized to decipher the codes.Security leaders advocate for its use in IoT environments, saying it's an optimal way to secure data at rest and in transit, secure the channels that transmit data and even authenticate devices within the IoT mesh, thereby providing a blanket of protection against hacks.

KEYWORDS: cryptography, IoT, security, hacks, ecosystems, data transmit, communications, informations

I. INTRODUCTION

"Encryption in general is a security best practice, and that applies to IoT use cases to encrypt data in transit from device to back end and at rest. It should be used everywhere, because the more you can encrypt data, the stronger protection you're offering," said Merritt Maxim, vice president and research director at the research firm Forrester Research.Any electronic device that holds data can be compromised, regardless of whether it's connected to the internet. A bad actor can steal a laptop and break into the files it holds, for example.But the risk of unauthorized access to electronic devices and the data they hold skyrockets as soon as those devices connect to the internet.IoT significantly expands that risk of unauthorized access simply due to the huge number of devices being connected to the internet.[1]

That number is staggering. IoT Analytics, an IoT market research firm, calculated the number of active endpoints in the world in 2019 at 12.3 billion; it predicts more than 27 billion IoT connections by future.[2] Meanwhile, IDC researchers predict that there will be 55.7 billion connected devices in the world by 2025, with 75% of them connected to an IoT platform. They further estimate that those IoT devices will generate 73.1 zettabytes of data by future, up from 18.3 zettabytes in 2019.That massive volume isn't the only security challenge.IoT deployments also increase hacking risks because their data exists in different places: in endpoint devices, on gateways and in centralized servers, as well as in transit among all those points. Minimizing those risks is where cryptography comes in.[3]

Cryptography can be used in various areas of an IoT deployment.Organizations can use cryptography to secure communication channels. For example, developers can use the cryptographic protocol Transport Layer Security for secure communications.They can also use cryptography for encrypting and decrypting the data within the IoT ecosystem, using one of the various available options. [4]Options including single-key or symmetric-key encryption algorithms such as the Advanced Encryption Standard (AES), public-key infrastructure (PKI) or asymmetric-key encryption algorithms such as the Rivest-Shamir-Adleman algorithm and the digital signature algorithm.When it comes to how it works and the benefits it provides, the use of cryptography in IoT deployments is the essentially the same as it is when used in other types of IT infrastructure, said Jason Pittman, a faculty member at the School of Cybersecurity and Information Technology at the University of Maryland Global Campus."A primary principle of technology and cybersecurity is that only the people who should have access should gain access. And the best way to ensure that no one has [unauthorized] access to a device or the data is to encrypt it," Pittman said. "So even if you're not worried about an attack, you should be mindful that no one should access something if they're not authorized to do that and the primary way to do that is encryption."[5]

However, there are challenges and technical considerations within IoT environments that can influence cryptography decisions.

"What [IoT] managers need to think about is the constraints of the devices, mostly because the devices are low-powered, and cryptography, because of the mathematics involved, is hardware intensive," Pittman said.The hardware-level constraints -- specifically restricted power and restricted memory -- can add considerations to decisions that don't exist when using cryptography in more conventional IT environments, said Yale Fox, IEEE member, TED fellow and CEO of Rentlogic, a platform that analyzes vast amounts of public data to generate letter grades for buildings across New York City.Speed requirements can be a factor in cryptography decisions within an IoT deployment, too.IoT managers must consider those constraints when choosing which cryptographic protocols to use."There are different protocols that are better for transmitting information in a more energy efficient way," Fox added.For example, some experts have found that AES isn't lightweight enough for some IoT use cases, while others have determined that some lightweight options don't offer strong enough protection for highly sensitive IoT use cases.Another potential challenge with cryptography in IoT is the management of encryption keys due to the high volume of devices involved. Some IoT deployments involve hundreds of thousands of devices generating encrypted data, creating a complexity that doesn't exist in non-IoT environments.[6]

II. DISCUSSIONS

Organizations must ensure that their cryptography choices offer enough protection for the use cases they're securing. No security solution delivers a full guarantee of security and cryptography is no exception to that.For example, the Data Encryption Standard is significantly more susceptible to brute-force cryptographic hacks than other options; that's one reason the standard, one of the oldest encryption algorithms, has fallen out of favor and isn't in much use today."So, you have to be careful about how the encryption is implemented,[7] and companies must make sure that even if they implement the most advanced algorithms that the devices themselves can't be compromised," Maxim added.Security experts and analysts didn't have figures available on cryptography use in IoT environments, but they said its use seems to be on the rise."It's being used more than it was, but I'm not sure it's being used as much as it should be," Pittman said. "All modern devices come with the ability to facilitate encryption natively. It's no longer something you have to put on devices, so its implementation is trivial compared to what it was just five years ago."[8]

Still, experts said many organizations aren't using cryptography to secure their IoT deployments.They said they hear IT leaders and IoT managers give different reasons for forgoing cryptography.For instance, some IT admin don't employ cryptography capabilities because it blocks visibility, making network analysis and troubleshooting difficult. Others opt not to use it because they believe managing it or configuring it is beyond their existing expertise and their ability to pay for needed skills. Some organizations decide to use cryptography to secure only part of their IoT environment, such as encrypting data at rest.Some experts countered those reasons, saying cryptography's benefits outpaces its challenges."Security is often a cost center and an afterthought," Fox said. "But using cryptography can be a quick win when you want to persuade people [of its worth].[9]" New IoT devices can exchange significant volumes of data — often sensitive — every second. Without the proper protections, hackers can siphon off valuable information they shouldn’t have access to. In some cases, they may even be able to send messages or data of their own.Cryptography — and specifically, the encryption and decryption of transferred information — has to be an essential part of IoT design as a result. It can keep IoT devices and the data they transfer secure, which should be at the forefront of everyone’s minds. After all, nobody wants their sensitive information to be compromised.[10]

III. RESULTS

With cryptography, it’s possible to encrypt this data. Messages are encoded with a special key so they can only be decoded by a specific user, device or set of users.When developers or manufacturers implement end-to-end encryption, no one but the sender and intended recipient can access that data as it moves from device to device — even if it travels across the internet to reach its destination. This means that with the right encryption standards in place, even the manufacturer of a particular device won’t have access to that information.This kind of protection is essential for businesses working with highly sensitive data that want to keep that information safe.[11] Encryption effectively reduces the angles of attack a hacker would have if they were trying to steal data transferred across different IoT devices.The data most IoT devices transfer is encrypted at some point as it moves across the web and to other devices. Few manufacturers, however, implement on-device or centralized encryption, meaning that information may only be safe some of the time that it's in transit.While cryptography is essential for good IoT device security, there are some significant challenges to implanting encryption standards. Because these devices have different, less powerful hardware specifications than other items, like computers or smartphones, standard approaches to encryption may be less workable.There are a few different cryptographic standards for manufacturers to choose from. [12]Most data protection tools on the market — as well as many governments and security organizations — use the gold standard encryption method, which is the Advanced Encryption Standard.However, not every manufacturer is convinced that popular encryption standards, like the AES, are right for IoT devices.IoT devices are unique, however. In many cases, they have specialized hardware that provides just enough processing power for whatever task they need to complete. In industrial settings, an IoT device may only have the equipment to track one type of data and send that information to a central server.Some manufacturers have pushed back against the idea of using tried-and-true encryption standards like the AES. This is because the AES isn't designed to be lightweight — meaning that for devices with little processing power, like IoT sensors, implementing the standard could be challenging.[13]

Research on leading IoT devices has found that manufacturers probably don't need to work with lighter-weight — but less secure — security standards. Instead, it's often possible to find a way to make AES work, even on these low-power devices.However, for IoT devices with very little processing power — like internet-connected microcontrollers in heavy equipment — lightweight encryption may be a necessity.New, lightweight encryption standards for IoT devices haven't been used at scale yet, mostly because there hasn't really been a need for that kind of measure in the past. While developers, cryptographers and cybersecurity experts know the strengths and weaknesses of AES, they won't have the same knowledge about a new encryption standard. This could make IoT devices that use these new standards more vulnerable.Waiting for lightweight encryption technology to become available could also present significant issues. It may be difficult to retrofit existing IoT technology with new security standards at scale, meaning that owners would either need to replace old devices or accept limited data security. Even if older items can be secured, waiting may mean leaving vast amounts of device communication unsecured in the meantime.[14]

IV. CONCLUSIONS

Cybersecurity developers are starting to create new technology that can handle this problem. Projects — like the open-source E4 developed by Swiss cryptography firm Teserakt — aim to help manufacturers ensure data is protected as often as possible, no matter where it's from or where it's going.The number of IoT devices in use is likely to grow at a fast pace over the coming years. Growth of Industry 4.0 tech will likely make sensors and other devices even more useful, encouraging businesses to adopt the technology.This trend will likely make cryptography much more important, as well. Without end-to-end encryption, data transferred between IoT devices will remain unsecured and vulnerable to eavesdropping and manipulation.New and old cryptographic standards can help keep IoT devices safe. While manufacturers have pushed back against the idea of including encryption on some devices — citing issues like the resources needed to encrypt information using some standards — developers are at work creating new technology that may be able to help.[15]

REFERENCES

1. Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon. Oxford University Press.
2. ^ Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science. Vol. 1. Elsevier.
3. ^ Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
4. ^ Sadkhan, Sattar B. (December 2013). "Key note lecture multidisciplinary in cryptology and information security". 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE): 1–2. doi:10.1109/ICECCPCE.2013.6998773. ISBN 978-1-4799-5633-3. S2CID 22378547.
5. ^ Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. (1997). Handbook of Applied Cryptography. ISBN 978-0-8493-8523-0.
6. ^ Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.

7. ^ "Overview per country". Crypto Law Survey. February 2013. Retrieved 26 March 2015.
8. ^ "UK Data Encryption Disclosure Law Takes Effect". PC World. 1 October 2007. Archived from the original on 20 January 2012. Retrieved 26 March 2015.
9. ^ Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web". TechRepublic. Archived from the original on 12 June 2016. Retrieved 12 June 2016.
10. ^ Doctorow, Cory (2 May 2007). "Digg users revolt over AACS key". Boing Boing. Retrieved 26 March 2015.
11. ^ Whalen, Terence (1994). "The Code for Gold: Edgar Allan Poe and Cryptography". Representations. University of California Press. 46 (46): 35–57. doi:10.2307/2928778. JSTOR 2928778.
12. ^ Rosenheim, Shawn (1997). The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet. Johns Hopkins University Press. p. 20. ISBN 9780801853319.
13. ^ Kahn, David (1967). The Codebreakers. ISBN 978-0-684-83130-5.
14. ^ "An Introduction to Modern Cryptosystems".
15. ^ Sharbaf, M.S. (1 November 2011). "Quantum cryptography: An emerging technology in network security". 2011 IEEE International Conference on Technologies for Homeland Security (HST): 13–19. doi:10.1109/THS.2011.6107841. ISBN 978-1-4577-1376-7. S2CID 17915038.