International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

An Exploitation of the Internet of Things and Its Likely Resolution

Mr.A Srinivasan , Mr.K Ramanjulu , Dr.G Kishore Kumar
Assistant Professor[1,2] , Associate Professor[3]
Department of CSE,
Viswam Engineering College (VISM) Madanapalle-517325 Chittoor District, Andhra Pradesh, India

Abstract

Thanks to the IoT, people may now connect their real-world devices to the web. Tagging technologies such as near field communication (NFC), radio frequency identification (RFID), and two-dimensional barcode make this possible. 2D barcodes have become standard practice for creating an IoT system because of their simplicity and inexpensive development and deployment costs. In this work, we investigate the prospect of Internet of Things spam. It aims to prove that online spammers may utilize 2D barcodes to inundate the real-world IoT, deceive people into seeing or accessing unwanted and irrelevant material via the Internet, and potentially compromise the credibility of legitimate content. A first experiment's findings are described, which raise the problem's plausibility. To combat the issue of spamming the IoT, this article also suggests using digital signatures (ECDSA). This study presents experimental data and a prototype implementation of the proposed approach.

Keywords:

Elliptic curves, anti-spam solutions, Internet of Things, two-dimensional barcodes, quick response codes, digital signatures, e-cads, and quaternions.

Introduction

Spam has affected every aspect of our online life, from receiving unsolicited emails to having web sites maliciously altered. The goal is to improve the exposure of specific online sites and maybe reap financial advantages [1] by preying on unsuspecting people and weakening search engines by manipulating search results. The formal definition of spamming is "the practice of sending large numbers of electronic messages that are neither requested nor wanted" [2]. Internet of Things (IoT) is a new endeavour that uses low-cost embedded tags like RFID, NFC, and 2D barcode to bridge the gap between our digital and physical worlds. In order to establish a connection between real-world items and their digital counterparts, 2D barcodes have emerged as the major method due to their simplicity and inexpensive development and deployment costs. This analogy-digital connection has also been stoked by the widespread distribution of smartphones with built-in 2D barcode scanning capability. Numerous studies [3, 4, 5] and practical programs have emerged to take use of the physical-cyber connection. The capacity to encode public data into a 2D barcode and then put that barcode on a physical item or location is the fundamental idea behind the physical-cyber connection.

Fig. 1. Example 2D barcode (Website referral) in a public space

can easily be decoded by ordinary mobile phone users. Since the encoded data in 2D barcodes is always public Due of the low cost and ease of creating fresh 2D barcodes, the physical side of the IoT might be a soft target

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

for spammers. This article is an exploratory piece that proposes a possible answer to the issue of Spamming the Internet of Things. It seeks to prove that Spammers may utilize 2D barcodes to inundate the real-world IoT and trick people into accessing unwanted and irrelevant material online (raising traffic for specific URLs). As a result, potentially authoritative material will be discredited. An experiment is described that yields preliminary findings that raise the problem's likelihood. In addition, the issue is outlined, and its alternative solutions, including implementation details and experimental findings, are presented. There are five main parts to this study. In Section 2, we detail the nature of the issue at hand, the findings of our pilot study to determine whether or not such an issue is even possible, and some potential use cases. The article defines a problem, and Section 3 proposes a solution and describes created applications that use the proposed approach. The article is divided into four sections, with the fourth focusing on current methods and the fifth serving as a conclusion.

The issue of spamming the IoT network:

There's a chance the primary motivations for spamming include financial gain, religious or political goals [1], persuading individuals to purchase a product or increase website traffic, etc. The issue therefore becomes, what role does the Internet of Things play here? Internet of Things relies on the analogy-digital coupling described above to function. Two-dimensional barcodes (or "QR codes") are labels affixed to real-world items or locations that direct users to digital content. In the Internet of Things, "spamming" is the widespread distribution of fake or altered 2D barcodes in physical spaces that link to irrelevant online information in an effort to boost page views for certain websites. Even while this kind of spamming is most common in public places like museums, railway stations, movie theatres, and the public transit system, it may also occur in semi-private places like colleges, workplaces, and factories. Next, we'll look at several potential spamming methods and some sample spam able sites.

Referrals from the public and online

Referring to an online resource using a 2D barcode is now standard practice. Online service providers often generate 2D barcodes to direct customers to their sites. Users with mobile devices may go online everywhere there are these barcodes thanks to their widespread distribution. Spam may easily be directed to such 2D barcodes and physical locations by using the Internet. Imagine a public transportation organization that uses 2D barcodes at various bus terminals (see Figure 1) to direct riders to the organization's digital resources. The information provided by these services includes bus arrival and departure times and route details1. By deciphering the 2D barcode, the user would have access to the business's digital resources. The 2D barcodes stationed at various terminals stand in for the "physical" side of the company's system, while the "cyber" side is represented by the company's online services. There are two possible approaches a spammer may use when targeting these kinds of systems.

A widespread flood

Mass Flooding addresses the issue of overwhelming the physical side of an IoT system with many 2D barcodes, making it difficult for users to ascertain which barcode corresponds to the service they are seeking. In the above-described situation, spammers might simply produce countless website referrals in public locations (bus station) that link to unwanted information on the Internet. Since there will be several 2D barcodes put across the area, users, particularly visitors, may get confused and begin decoding them in an attempt to find a genuine business online. The terminal's various 2D barcodes raise the prospect of the user being shown stuff that has nothing to do with what they first sought out. It not only inhibits the services offered by the firm, but also damages the company's reputation. Accordingly, on the one hand, the widespread invasion of such ecosystems might quickly ruin the credibility of genuine websites while simultaneously driving more attention to the spammer's link.

Method of Redirection Disguise

A spammer might simply build a 2D barcode that leads to a spam site if they had access to the content (URL) of a valid 2D barcode inserted by the firm. A re-direction concealment method is used on the spammer's website to lead users to the correct content of the genuine 2D barcode. Here, we call this method of concealment "Redirection hiding technique" [1]. Assume, for the sake of argument, that a public 2D barcode really leads to the intended website (http://correctAddress.com). If spammers decoded this address, they might replace it with a 2D barcode that leads to the website http://spammerAddress.com. Eventually, visitors to the website at

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

(http://spammerAddress.com) will be sent to (http://correctAddress.com) through the Internet's automatic redirection system (either via meta tags or java script). This spammer uses a 2D barcode that, once decoded, takes the visitor to his own website before redirecting them to the right one. This method lends itself more naturally to public settings than to more intimate ones. The key aspect of this method is that the spammer is not required to flood the environment in large quantities. Spammer websites will get increased traffic as a result of this silent tag being placed on them. In this study, we use this method in an experiment to determine whether or not it is possible to Spam the Internet of Things.

Greeting/Business Cards

Information about a person or business may be found on a business card. As a courtesy and a memento, they are passed around at introductions. Business card encoding with 2D barcodes (particularly QR code) has become more popular in recent years, and many websites now provide simple and novel means of doing so. A sample of such a business card is shown in Figure 2. As a result, spammers may target these cards and distribute copies with altered 2D barcodes. Figure 3 is a sample of a business card with a QR code that has been altered. An unfamiliar user will have a hard time telling the difference between a legitimate and fake business card.

Fig. 2. Correct Version.

Fig. 3. Spammed Version

Table 1. Experimental statistics for establishing the possibility of spamming the Internet of Things.

Record	Spammer Link	Real Link	Spammer Hits	Real Hits
1	/site/elitefaizal	/site/elitefaisal	20	48
2	/site/referralS	Not Given	19	unknown
3	/site/referralA	Not Given	32	unknown
4	/site/referralU	Not Given	26	unknown

Initial Laboratory Tests

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

An experiment has been carried out to prove the viability of spamming the IoT. The goal of the experiment is to prove that it is possible to spam the IoT, not to capture the impact of such spamming on the system as a whole. The first findings from this experiment are shown in Table 1. For this study, we used the spam approach of redirection concealment (Section 2.1.2). The "Spammer Link" leads to the spammer's website, which often contains unwanted and irrelevant material. For the sake of the experiment, the spammer websites merely have simple hit counters that keep track of how many times each page is seen. The term "Real Link" is used to denote genuine websites that provide the service the user is seeking. The number of clicks on the Spammer Link and the number of clicks on the Real Link are shown under "Spammer Hits" and "Real Hits," respectively. We settled on the QR code as a means of encoding both spam and legitimate links. The Quick Response code, sometimes known as a QR code, is a kind of two-dimensional matrix bar code developed by the Japanese firm Denso-Wave in 1994. It was used since QR codes were designed with speedy decoding in mind, and many newer mobile phones come with QR-decoding software already installed. Each spammer and legitimate link had five 2D barcodes inserted in random places during the course of the six-day trial. QR tags with live connections were posted throughout the venue on day one. The following day, some of the QR codes were swapped out with ones that led to a spammer's website. Real Links were expected to go to external websites in the real world for records 2, 3, and 4. As a result, neither their physical nor their overall number of internet hits have been disclosed. However, clicks on spammy links are tracked. Record 1 is a web page that functions as a legitimate link. The actual webpage incorporates a hit counter that keeps track of how many times the page has been accessed.

Discussion

Web spammers may easily generate or alter QR codes in order to trick people into visiting malicious websites, as seen in Table 1. This is shown by the "Spammer Hits" column. It's also fascinating that this many hits were recorded after just 5 QR codes were placed. The author plans to do further research on the outcomes of controlled mass flooding. We need a method that identifies the QR code's author (the content provider) so that we can stop spammers from using them to deceive consumers into reading irrelevant material. In addition, the method should enable authentic content owners to generate QR codes without compromising the authenticity of the original message. The author believes that the issue outlined in this subsection may be avoided by the use of technique(s) that guarantee the originality of the material and the credibility of the content producer.

A Likely Answer

The author suggests digitally signing the information within 2D barcodes using Digital Signatures [6, 7] to guarantee the material's authenticity and to verify the author's identity (to solve the difficulty stated in Section 2). Digital Signatures, the practice of using cryptographic methods to verify the authenticity of a communication and its author, have been extensively explored in the subject of cryptography, therefore it makes sense to use these methods while solving a problem. A digital signature, or digital signature system, is a method of verifying the integrity of data stored in a digital format. It's a useful tool for verifying the user's identity and protecting the data they're accessing. A digital signature embedded inside a 2D barcode may be used to verify the authenticity of the material and verify the author's identity. In order to generate and validate digitally signed QR codes, two essential tools—a digitally signed QR Code Generator and an application to verify the signed QR Code—are required. The fundamental parts of the suggested approach and how they work together are shown in Figure 4. To begin, a QR Code generator should be used to digitally sign the material before encoding it in the QR code. It creates a digitally signed QR code and any necessary certifications based on the data provided (including any necessary public-private key pairs used in public-key cryptography). Original content/message (C), digitally signed content (DS), and the content creator's public key (PK) are all encoded into the modified QR code. Since the material is a link to an online resource, the certifications attesting to the author's credibility have been inserted in the URL. The second component is a mobile app that can scan the QR code and verify the certificate chain and the QR code's content integrity.

Below, we break out how the various parts of the proposed approach work together:

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

- If you provide a piece of content and the identity of the content's author (their public-private key pair and certificate), the "QR Code generator" will produce a QR code that contains the piece of content (C), the digitally signed version of the content (DS), and the content's creator's public key.
- It is not required to do this. The "QR Code generator" may create self-certified certificates that encode the identification of the content creator if the content creator does not have certificates authenticating the identity of the content creator.
- The certificates are placed at the URL specified in the content(C), assuming that C is a website reference.
- In order to get the unmodified content (C), the digitally signed version (DS), and the author's public key (PK), the "mobile application" must decode the QR code.
- The QR code can only be trusted if the "mobile application" uses the content creator's public key to validate the content and compare it to the digitally signed content (DS).
- The "mobile application" guarantees the root certificate is trusted by the user by verifying the certificate and certificate chain.
- The user is sent to the linked webpage.

Application Development and Testing

To test how well his method would work, the author put it into practice piece by piece. The Quick Response (QR) code was selected as the 2D barcode to be generated. A Java program called a "QR code generator" creates QR codes. To create QR Codes, it calls upon the ZXing library5. ZXing (pronounced "zebra crossing") is a Java package for processing images of 1D and 2D barcodes that is free source. The "QR code generator" employs an elliptic curve (EC) based public-private key pair to sign the information, as recommended by NIST 6 for future applications requiring encryption and digital signatures. Cryptography based on elliptic curves and

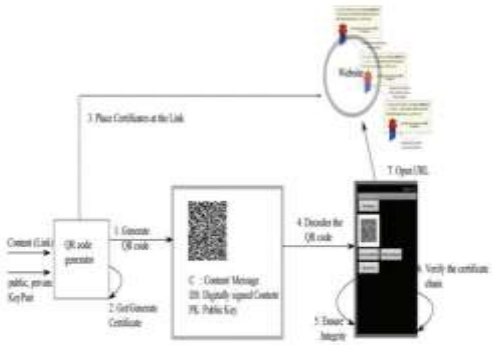

Fig. 4. Elements and their interaction inside the proposed solution

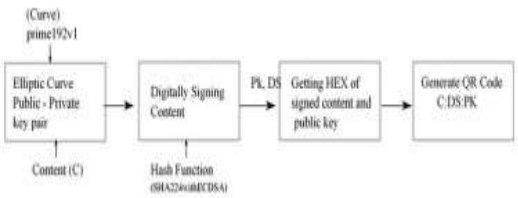

Fig. 5. QR code generator steps

Organizations are increasingly turning to digital signatures as a means of data encryption and digital signing due to the schemes' ability to offer the same degree of security with shorter key lengths than their predecessors, RSA and DSA. It's the backbone of Suite B 7, the next U.S. government cryptography standard. In order to digitally sign the material and (if necessary) issue certificates, the "QR code generator" employs an Elliptic Curve private-public key pair. Both theoretically and practically, the Elliptic Curve Digital Signature Algorithm

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

(ECDSA) [8] is used. Bounce house to digitally sign documents using Elliptic curves and establish a public private key pair, Java Security provider8 is utilized. However, the public key and the digitally signed information are both encoded in hexadecimal form before being included into the QR code. Figure 5 illustrates the procedure. The Android platform9 powers the mobile software that confirms the QR code's authenticity and the author's identity. Using a barcode scanner, the user can now decipher QR codes. Following successful decoding of a QR code, the app gives the user the choice to view the URL in their default browser, validate the content's integrity, and confirm the content creator's validity.

Table 2. Experimental statistics of the solution.

Elliptic Curve	Curve (Bits)	cryptographic hash functions	Dimensions of QR code	Message Size (bytes)	Verify Time (seconds)
prime192v1	192	SHA224withRSAEncryption	256 x 256	296	2.46
prime239v1	239	SHA224withRSAEncryption	256 x 256	342	3.31
prime256v1	256	SHA224withRSAEncryption	256 x 256	360	3.36
P-224	224	SHA224withRSAEncryption	256 x 256	322	3.21
P-256	256	SHA224withRSAEncryption	256 x 256	361	3.29
P-384	384	SHA384withRSAEncryption	512 x 512	402	7.5
P-521	521	SHA512withRSAEncryption	512 x 512	429	9.0

Experiment

Different elliptic curves have been used to produce public and private keys and a cryptographic hash function for content signing in an experiment to evaluate the production and verification of digitally signed QR codes. In the future, it will be useful for providing remarks detailing potential options, offering early suggestions for readers (should they want to implement it), and pointing out any flaws in the suggested solution. The experiment was repeated seven times (Table 2). For each cycle, a new cryptographic hash function was selected and a new elliptic curve was utilized to produce the public and private keys (Elliptic curve and curve (bits)). The created QR code's dimensions are shown in the Dimensions field. The average size, in bytes, of 50 randomly produced QR codes is shown in the Message Size column. The average amount of time it takes for the mobile app to decode the QR code and confirm the authenticity of the message is shown in the verify time. Each iteration is averaged across a sample size of 50 QR codes. Time to verify the content creator's identity (certificate chain) is not included in Table 2 since it is not the topic of this research and varies greatly depending on the length of the chain. The time required is in addition to the time needed to validate the QR code's integrity and varies depending on the length of the certificate chain.

Discussion

The data collected from running the experiment using the custom software is detailed in Table 2. It demonstrates that both the solution and its implementation are possible. The following, however, is gleaned from the data. The time it takes the mobile app to check the legitimacy of the material is shown in Table 2 and is given in seconds. Validating the certificate chain to determine the content creator's identity is a time-consuming process. The solution's resilience must be enhanced so that it can handle larger curves. The approach presupposes that the referred-to material is a website, and hence that certificates are hosted on the website. However, it is unclear where certificates establishing the identity of the content provider should be placed when the material relates to anything other than a website. One alternative answer is to include the link to the certificates' online repository in the QR code itself.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Analysis of the Literature

The risk of Spam on the IoT has been briefly discussed, and a possible remedy has been presented in the form of Digital Signatures. While there is a dearth of material on the identification of the problem (Spamming the IoT) and potential solutions, numerous academics have already used digital signature in signing papers and 2D barcode to tackle other issues.

Using a serial number (produced by a server) printed in the form of a 2D QR code and connected to the product, Katsu nori Seino et al. [9] presented a method to identify fishing products. The primary goal of this work was to develop a system for creating and encrypting a unique product identifier utilizing a public-key infrastructure. Since it is simple to forge a product's unique QR code, it is advised that digital signatures be used to ensure authenticity. However, instructions for digitally signing a QR code and installing certificates are not included in the article. This study takes a new approach to the issue at hand and provides a thorough explanation of how QR codes may be used to implement digital signatures. An effective and secure authentication technique for access control systems was presented by Yung-Wei Kao et al. [10] and makes use of mobile phones and QR codes. Using the OTP (One Time Password) method, it produces a secret and saves it in a QR code. While the architecture was described in the article, further information on the methodology and its application was lacking. There is no solution for the problems of fake QR codes or compromised information contained inside them. In [11], a printable digital signature technique was presented, which is based on the Korean Certificate-based Digital Signature Algorithm (KCDSA), which is used for safe transactions and binding electronic documents to their printed counterparts. The QR code is used to print the signature in a discrete region of the paper document. The method is described in full in [12]. In the realm of the Internet of Things (IoT), however, the QR code serves as the primary information carrier and bridges the gap between the real world and the virtual one. The present study summarizes the implementation and experiments conducted for the IoT field.

Conclusion

The prospect of spamming the IoT is explored and established, and a possible solution is proposed. We also provide our early experiment results, which show that spamming the IoT is possible. To combat the issue of IoT spam, this article also suggests using digital signatures. This article details the solution's implementation and the experimental findings that followed.

References

[1] Z. Gyongyi, H. Garcia-Molina, Spam: it's not just for Inboxes anymore, Computer 38 (10) (2005) 28 – 34.

[2] P. Hayati, V. Potdar, A. Talevski, N. Firoozeh, S. Sarenche, E. Yeganeh, Definition of Spam 2.0: New spamming boom, in: Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on, IEEE, 2010, pp. 580–584.

[3] F. Razzak, D. Bonino, F. Corno, Mobile interaction with smart environments through linked data, in: Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on, IEEE, 2010, pp. 2922–2929.

[4] J. Gao, L. Prakash, R. Jagatesan, Understanding 2d-barcode technology and applications in m-commerce-design and implementation of a 2d barcode processing solution, in: Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International, Vol. 2, IEEE, 2007, pp. 49–56.

[5] T. Liu, T. Tan, Y. Chu, 2d barcode and augmented reality supported english learning system, in: Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on, Ieee, 2007, pp. 5–10.

[6] W. Diffie, M. Hellman, New directions in cryptography, Information Theory, IEEE Transactions on 22 (6) (1976) 644–654.

[7] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key crypto systems, Communications of the ACM 21 (2) (1978) 120–126.

[8] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), International Journal of Information Security 1 (1) (2001) 36–63.

[9] K. Seine, S. Kuwabara, S. Mikami, Y. Takahashi, M. Yoshikawa, H. Narumi, K. Koganezaki, T. Wakabayashi, A. Nagano, Development of the traceability system which secures the safety of fishery products using the QR code and a digital signature, in: OCEANS'04. MTTS/IEEE TECHNO-OCEAN'04, Vol. 1, IEEE, 2004, pp. 476–481.

[10] Y. Kao, G. Luo, H. Lin, Y. Huang, S. Yuan, Physical access control based on QR code, in: Cyber-Enabled Distributed Computing and Knowledge Discovery, 2011 International Conference on, IEEE, 2011, pp. 285–288.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

[11] J. Lee, T. Kwon, S. Song, J. Song, A model for embedding and authorizing digital signatures in printed documents, Information Security and CryptologyICISC 2002 (2003) 465–477.

[12] C. Teoh, Two-dimensional barcodes for hardcopy document integrity verification (2008). URL http://eprints.utm.my/9467