Comparative Analysis of Applications of Identity-Based Cryptosystem in IoT

Ramesh, C. H, Vasumathi, D
Jawaharlal Nehru Technological University
Hyderabad, Telangana
India
chramesh23@gmail.com

Venugopal Rao, K
G Narayannamma Institute of Technology and Science for women
Hyderabad, Telangana
India
kvgrao1234@gmail.com

ABSTRACT: Although it has been with us in some form and under different names for many years, the Internet of Things (IoT) is suddenly the thing. The ability to connect, communicate with, and remotely manage an incalculable number of networked, automated devices via the Internet is becoming pervasive, from the factory floor to the hospital operating room to the residential basement. The transition from closed networks to enterprise IT networks to the public Internet is accelerating at an alarming pace—and justly raising alarms about security. As we become increasingly reliant on intelligent, interconnected devices in every aspect of our lives, how do we protect potentially billions of them from intrusions and interference that could compromise personal privacy or threaten public safety. As every player with a stake in IoT is well aware, security is paramount for the safe and reliable operation of IoT connected devices. In this aspect Identity-Based Cryptography which makes use of user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification is promising in Internet of Things (IoT) due to its benefits, such as facilitating public key management. However, different aspects on IBC (e.g. the need for bilinear pairing) require attention when applied to IoT in order to meet basic security requirements on these environments. This paper gives a detailed feasibility study of applicability of IBC in IoT.

Keywords: Identity-Based Cryptosystems, Tate Pair, Elliptic Curves and Digital Certificates

Received: 6 May 2018, Revised 4 July 2018, Accepted 13 July 2018

DOI: 10.6025/isej/2018/5/2/63-70

© 2018 DLINE. All Rights Reserved

1. Introduction

IoT (Internet of Things) is a network of highly connected devices, supporting ubiquitous applications in a number of areas (Ex. Health, physical security, industrial automation and transportation) in addition to facilitate day to day activities [1]. The IoT includes different types of devices such as sensors, actuators, RFID tags, smart phones and servers, with different computing capabilities, features and sizes. Security is the key requirement for many of these applications to deal with the characteristics of this new environment, expectations and needs computational safety of users [1].
Cryptographic techniques have been applied for several years to protect the digital data from unauthorized access and illegal theft. The concept of identity-based encryption (IBC - Identity-Based Cryptography) [6] has excelled since the public keys are derived from public information to identifying a User uniquely (Ex. PAN no for individuals or IP for machine) and not require authentication mechanisms. IBC has several advantages positively contributing to the protection of digital data in complex IoT environment [1]. It simplifies the management of public keys by eliminating the use of digital certificates, in addition to reduce the burden of communication with trade certificates check messages and the applications response time. There is a considerable gain in efficiency, as for as secure communication and authentication, there is no need for key exchange, in addition to a reduction of complexity and cost to establish and maintain the infrastructure of public keys. Such characteristics make the IBC converge with the needs of the IoT.

The IBC has disadvantages, for example the need for a reliable third party (Public Key Generator - PKG), responsible for generating and maintaining custody of private key system. Another requirement of the IBC is that keys must be delivered to users through confidential and authenticated channels. However, as the encryption mechanism in general needs to be used to provide the security scheme, such channels not yet exist. Thus, this paper aimed to contribute to the literature through a comparative analysis between cryptosystems based on identity and adjustments when applied in the context of IoT. Comparative analysis considers the characteristics of each cryptosystem as well as the characteristics and requirements for the safety of users in ubiquitous environment are analyzed. This paper points out the strengths and weaknesses of each cryptosystem for the environment of IoT.

2. Internet of Things (IOT)

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

However, according to Singer [3] define what in fact is the Internet of Things (IoT) becomes extremely difficult in the face of several studies and publications on this subject. With emerging attempts of definitions and statements about this new concept, various names are confused with the IoT in order to try to convey what you can compose your circle of studies.

In the publications that the researcher Singer collected, there are articles dealing with the topic of Internet of Things involving subjects on “spatial intelligence, data collection sensors, low energy consumption, middleware, network security, encryption, information architecture and issues related to legality and transparency” [3].

In some cases, the subject is treated as the interests of the country. Europeans and Chinese are drawing efficient use and beneficial impact to the society, by generating greater academic interest for the conceptualization of this subject while the United States focused on technology in itself does not give much credibility to the term IoT. [3].

The term Internet of Things can be mentioned in a number of ways in countries that are researching on the subject, modifying the name thing for objects or otherwise [5]. This reveals a lack of unity rating that may seem simple, but it can generate diverge conceptual paths.

To Ayres and Sales [4] the concept of Internet of Things (IoT) - had its beginning at MIT (Massachusetts Institute of Technology) in 1999 in the AutoID Center. In the early 2000s, Kevin Ashton laid the foundation for what would be the Internet of Things (IoT) in a AutoID Lab at MIT. Ashton was one of the pioneers who created this notion, while researching ways to Procter & Gamble improve their business transactions connecting RFID information to the Internet. The concept was simple but effective. If all objects of daily life were equipped with handles and wireless connectivity, they could communicate and be managed by computers. Since then, for these researchers, the Internet of Things (IoT) began to be defined as: “a network of interconnected objects, which could have unique IP address, be incorporated into the complex systems and use sensors to monitor the environment, responding to different contexts” [4].

According to the authors, Ayres and Sales [4], there are four things that can characterize the Internet of Things (IoT). The first is the possibility of being independent, i.e., connecting its processes to the Internet today. The second is that the IoT is implemented in cooperation with new services. The third is that it provides the communication of objects-to-people, but also of objects to objects. And lastly is that networks can be free for all or restricted to a few.
To Read (2013), The IoT is a new concept where objects have abilities to communicate with human beings and producing new real quality.

In this way, we can observe that the IoT comes to objects or things by means of other objects and human actions, scheduled to be able to act independently of direct action, transforming the simple use of the object in a new dimension of real action ever seen in other times. In fact it is a new paradigm in the era of Information Technology serving as a useful beneficial to society.

3. Identity Based Cryptosystems (IBC)

The central idea of the public key cryptographic system based on Identity is very simple, because of the fact that the public key is a numeric value without explicit direction and which can be calculated from string of any significance?. In [6], it was proposed that the public key can be the user’s identity, such as name, email address, social security number, cell phone number, IP address, serial number of electronic devices, etc.

Is the public key is predetermined (equal to the identity), and then calculate the secret key? The answer to this question comes with the first model of security assumptions: there is a CA, with the following main responsibilities:

• Create and maintain safe custody of a secret master key SAC.
• Identify and record all users of the system.
• Calculate the secret keys of the users.
• Deliver the secret keys securely (with confidentiality and authenticity).

In 1984, Shamir described the model and algorithms for digital signature. It took almost two decades until efficient encryption algorithms were discovered and demonstrated for the identity-based model to create interest among researchers and industry.

For comparison, in Table 1, we see that the secret key is calculated according to the secret system of authority and the user’s identity. For a convenient f, it is not feasible to recover the master key from the ID values. And just the authority is able to generate secret keys, so that secret itself is a guarantee that the use of ID will work in cryptographic operations involving the owner’s identity.

To encrypt a message to the owner ID or verify a signature ID, user ID using the identity over the public parameters of the system, they include the public key of the authority (see Figure 1).

![Figure 1. Encrypting the model based on the identity](image)

To decrypt a message to ID or to create a signature, the secret key ID is required.

3.1 Advantages
The identity-based model is attractive because it has many interesting advantages. The first is that the public key can in most
Information Security Education Journal  Volume  5   Number  2   December 2018

Table 1. Attributes of cryptographic identity -based public key style

<table>
<thead>
<tr>
<th>Secret key</th>
<th>Public key</th>
<th>Warranty</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S = f (ID, S_{AC})$</td>
<td>ID</td>
<td>$S$</td>
</tr>
<tr>
<td>Calculated by the authority and chosen by the user or shared with the user</td>
<td>Chosen by the user or shared with the user formatted for authority</td>
<td></td>
</tr>
</tbody>
</table>

cases be easily remembered by humans. Very different from the conventional public key, which is usually a binary string with hundreds or thousands of bits? The identity can be informed by the user to their partners and there is no requirement to maintain key directories.

To be able to view the saving processing time, storage costs and data transmissions, we will recall, for example, as it is generally a cryptographic operation with PCI. If Bob wants to encrypt a message to Alice, first of all, he must obtain the certificate that was issued to Alice (consulting a public directory or Alice itself). Bob needs check the validity period and the signature contained in the certificate. The signature verification is a process that sometimes runs the certification path of the certifying authorities involved in the hierarchy until they reach the root certification authority. If nothing goes wrong, Bob can save the Alice certificate for future use. However, before each use, Bob need to consult a validation authority to verify that the certificate has not been revoked (often, a referral to a server that is online). Once the certificate is valid and not revoked, Bob extracts the public key of Alice, encrypts the message and transmits.

In identity -based model, just if the system parameters are authentic Bob can encrypt a message based on the identity of Alice and send (considering that identity withdrawal is treated as explained below).

A peculiarity of identity -based model is that the public key can be used before the secret key calculation. Thus, it is possible to encrypt a message for those who have not registered with the system authority or has secret key for decryption. In contrast to the model based on certificates, the user must first register and get the certificate, and then to receive an encrypted message under your public key.

3.2 Disadvantages

The first disadvantage, which is characteristic of identity -based systems is the custody of keys. As explained above, the system authority has the ability to generate secret keys of all users under their responsibility. This implies that the authority reaches to the level of confidence that defined in [10] . Consequently, you can decrypt any encrypted texts that have access (if you can identify the recipient’s identity). You can also sign on behalf of any user and there is no irreversibility guarantee. Therefore, it is essential that the system of authority is reliable enough for eavesdropping of shares or counterfeiting as these are controllable.

Custody of property keys, referenced by key escrow in English texts is not always undesirable. Within a company, for example, if all sensitive documents and data are encrypted by the employee who created it, the board may have access to decryption in case of death or termination of the employee. When there is need for monitoring the content of encrypted e-mail, it can also be justifiable custody of keys. However, for most applications, custodial key is a disadvantage.

Another point unfavourable to identity -based model is the need for a secure channel for distribution of secret keys. If delivery occurs in networked and remote environment, it is necessary to ensure mutual authentication and delivery with secrecy.

Another concern that one must have in identity -based model is the possibility of identity revocation. If the secret key of a user is compromised, its identity should be repealed. Therefore, it is not recommended to simply use the number of CPF or mobile phone, for example, as a user identifier.
3.3 Additional Features

As noted by [6], the identity-based model is ideal for groups of users, such as executives of a multinational company or branch of a bank, once the headquarters of these corporations can serve as system authority in all trust. Applications small scale, where the cost of deploying and maintaining an ICP are prohibitive, are candidates for the use of identity-based model. When the disadvantages cited above are not critical, the characteristics model allow interesting implementations.

Some examples of services with time availability confidential document that can be revealed to the press or to a particular group, only from certain date and time; bids an auction that should be kept secret until the end of negotiations; or view a film that should be enabled only within the rental period contracted.

The identity-based model has also been the subject of studies in search for alternatives to SSL/TLS, to Web applications, as shown in [7]. With the elimination of certificates the process of distributing public keys and access control will be simplified. Similarly, the model has been explored to provide security in a number of other application areas, such as grid computing and sensor networks (see for example [8] and [9]) and other applications.

4. Comparative Analysis

In literature the following are the five identity-based cryptosystems which are identified for the comparative analysis in this section. The cryptosystems are: Identity Based Encryption (IBE), Cocks, Boneh-Gentry-Hamburg (BGH), Secure Key Issuing (SKI) and ID-based Authenticated Key Agreement (AKA-ID). They are represented in two main groups classified by their form of implementation: i) supported by pairings and ii) supported by alternatives to pairing strategies, such as quadratic residues and the problem of Diffie-Hellman, i.e. use of operations which are easy to compute but difficult to reverse. These two groups are different for their computing costs. For example, The IBC based on pairings calculation, generates a high computational cost making it inadequate for the IoT devices.

For comparative analysis the following aspects are observed besides the support for pairing, they are custody of keys, the size of the cryptograms, need for random algorithms and need for key agreement. The following are the main characteristics of the five approaches analyzed are briefly described in order to contextualize the main aspects of each approach summarized in Table 2.

IBE [Boneh and Franklin 2001]: One of the implementations of the 1st IBC is based on bilinear pairings. Furthermore, it relies on a reliable PKG unconditionally, introducing the problem of key escrow.

Cocks [Cocks 2001]: Strategy that emerged alongside the IBE proposal, supported by quadratic residues, which are computationally cheaper than pairings. This scheme has the same structure as reliable entity adopted in IBE therefore not address the problem of key escrow. An important feature is that the cipher algorithm includes every bit of the original message, yielding very large cipher text.

BGH [Boneh. 2007]: Supported by quadratic residues, the BGH has the same structure as IBE and the Cocks, keeping the issue of custody of keys. Aiming to reduce the problem of the size of messages encrypted by Cocks, the BGH suggests a new encryption algorithm where random elements are reused. However, this algorithm has polynomial complexity of order four, which considerably decreases the efficiency of the method.

SKI [Lee. 2004] Based on the bilinear pairing, the differential SKI and the adoption of a hierarchical structure of reliable authorities, consisting of a central key generation (Key Generation Center - KGC), which produces private keys, in addition to maintenance of Private Key Authorities (Private Key Authorities - KPAs). This structure partially solves the problem of key escrow, because it allows the KPAs to cooperate with each other to retrieve the contents of encrypted messages in this system. This co-operation is known as collusion by message. A negative aspect of the addition of the KPAs and the rising cost of implantation and maintenance of the cryptosystem, because there are more elements involved.

ID-AKA [Cao. 2010] is based on the Diffie-Hellman problem and the most efficient use of bilinear pairings. The confidence in a PKG is maintained, but not solving the problem of key escrow. The main difference of ID-AKA in relation to other IBC mechanisms is that exchange of only two messages, significantly reducing the overhead of communication.
Table 2. Comparison between identity-based cryptosystems

Table 2 explains the characteristics of IBC systems compared in this study. The first aspect to be considered in a IoT environment are the computational costs. In this sense, the IBE and SKI strategies are the most expensive because they are based on bilinear pairings. The adoption of quadratic residues in the work Cocks in fact reaches temporal efficiency. However, the encryption algorithm it produces a very large encrypted messages that require more space for storage and generates overload of communication due to its transmission. This characteristic may not be appropriate if the IoT environment is considered involve devices with low storage capacity or communication. Already in the proposal of BGH, the idea is to solve the problem of large cryptograms by Cocks but the encryption algorithm that reduces the size of ciphers and polynomial complexity of order four, making the system inefficient computationally. Thus, the system appears more suitable to IoT scenario where the main factor is efficiency. The strategy ID-AKA, which adopts the Diffie-Hellman problem to solve the problems of BGH. AKA-ID also seems adequate when considering the communication of the IoT devices, since it allows to exchange keys with only two messages.

The second aspect considered is custody of keys, which can derail the implantation of an IoT environment if the device cannot trust unconditionally in a single central authority. The only cryptosystem compared in this work that addresses this problem is SKI, which adopts a hierarchical structure of reliable authority by adding multiple Public Key Authorities. However, the problem is not addressed in a definitive way, since there is the possibility of Collusion by message, which may occur when the intermediate authorities cooperate with each other to retrieve the contents of encrypted messages in this system. The negative aspect in addition to KPAs are the rising cost of implantation and maintenance of the cryptosystem, which can hamper its adoption in IoT environments. Furthermore, the inclusion of KPAs also increases response times of applications.

5. Conclusion

Wireless communication, scalability, restrictions of computer resources and requirements such as low latency and high flow applications are some characteristics that should be considered in the definition of security systems adopted in a IoT environment. In this context, the identity-based encryption features several advantages that contribute positively to the protection of digital data, the main one and the simplification of public key management. However, IBC has some disadvantages, for example, the problem of custody of the private key system. This paper has contributed to the literature by presenting a comparative analysis of identity-based cryptosystems and their adjustments when applied in the context of IoT. As a conclusion, it is observed that there is no ideal solution which satisfies all requirements of IoT, their applications and users are treated together. Not even basic requirements are dealt together by a single scheme and is therefore a matter for open research to develop more schemes to meet the requirements of devices, applications and users of IoT.

References

Computers, and Communication Systems (TAACCS), NIST Technical Note (TN) 1867, National Institute of Standards and Technology, G aithersburg, Maryland, (February), 26 p.


in Computer Science, 3152. 41–55.


