Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 03, pp. 28411-28420, March, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

REVIEWING TRENDS AND TECHNOLOGY SHAPING THE FUTURE OF PUBLIC KEY INFRASTRUCTURE

[1]Mishra, P. K., [2]Dongale, T. D., [3]Kamath, R. S. and [1,*]Kamat, R. K.

[1]Department of Computer Science, Shivaji University, Kolhapur, 416004, India
[2]School of Nanoscience and Biotechnology, Shivaji University, Kolhapur- 416004, India
[3]Department of Computer Studies, Chhatrapati Shahu Institute of Business Education and Research, Kolhapur, 416004, India

ARTICLE INFO

Article History:
Received 15th December, 2015
Received in revised form
26th January, 2016
Accepted 29th February, 2016
Published online 31st March, 2016

Key words:

Public key infrastructure (PKI),
Internet of things (IoT),
Information Security,
Cryptographic algorithms.

ABSTRACT

The present manuscript reviews trends and technologies pertaining to the future of public key infrastructure. Public key infrastructure (PKI) is one such technology that may offer benefits to net-centric organizations, being a system of services, technology, protocols and standards that can be used as a solution for providing secure transactions. Here we have reviewed some early work in the field of PKI's as well as some recent technological advance in the PKI's. We have also reviewed some issues with the traditional PKI and suggested some technological measures to overcome the limitation of conventional PKI's.

Citation: Mishra, P. K., Dongale, T. D., Kamath, R. S. and Kamat, R. K., 2016. "Reviewing Trends and Technology Shaping the Future of Public Key Infrastructure", *International Journal of Current Research*, 8, (03), 28411-28420.

INTRODUCTION

Information encompasses the connotation and understanding that is used to express facts, or data. The worth of information is determined by the mechanism used for comprehension and its usage to come out interms of products, services, etc. Information comprises the meanings and interpretations that people place upon facts, or data. The value of information springs from the ways it is interpreted and applied to make products, to provide services, and so on (An introduction to information security, 2015). Organizations not only use the information but they are solely reliant on the same. Protection of information is of utmost important as the same being the sole asset of the organization. Especially in today's era of pronounced interconnection, protection and security of information is vital and the same has become challenging owing to the exponential growth of it along with the increasing instances f threats, attacks, vulnerabilities and so on. Few grounds of damage of information are malicious code, computer hacking, and denial of service attacks which have become more common, more ambitious, and increasingly sophisticated (Why is Information Security Important, 2015). Information security, as a familiar business movement, has emerged mainly in the past decade. Awide range of factors have led the discipline to grown-up and it has now accomplished its "licence to operate" within the corporate and public sector environments, becoming one of the core business and organisational enablers. However, there is little room for error, as the consequences of insecure systems and information are almost always costly and distracting (Computer Weekly.com, 2015).

Widely agreed notions of Information Security

There are different notions and definitions of the information security. "Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious intentions. Confidentiality, integrity and availability are sometimes referred to as the CIA Triad of information security. This triad has evolved into what is commonly termed the Parkerian hexad, which includes confidentiality, possession (or control), integrity, authenticity, availability and utility (Techopedia.com, 2015).

***Corresponding author: Kamat, R.K.**
Department of Computer Science, Shivaji University, Kolhapur, 416004, India.

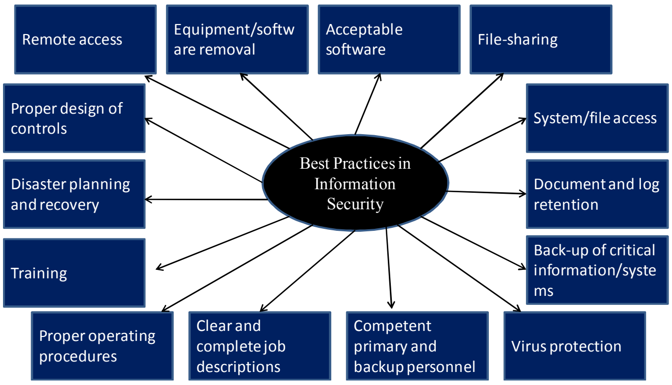
Best Practices in Information Security
Remote access
Equipment/software removal
Acceptable software
File-sharing
Proper design of controls
System/file access
Disaster planning and recovery
Document and log retention
Training
Back-up of critical information/systems
Proper operating procedures
Clear and complete job descriptions
Competent primary and backup personnel
Virus protection

Fig. 1. Best practices in Information Security

Safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity (BusinessDictionary.com, 2015). The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- Availability, which means ensuring timely and reliable access to and use of information (Ishandbook.bsewall.com, 2015).

Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption (Sans.org, 2015) ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes (Search Security.co.UK, 2015)."

Authentication in Information Security

"Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access (Search Security, 'What is authentication?, 2015)".

"In computing systems, authentication and authorization must work in tandem to provide effective security. Without authentication, there would be no way to determine if individuals are who they claim to be. Without some sort of authorization in place, it may not matter who they claim to be — as with no authorization in place, essentially anyone could access anything simply by telling the truth about who they are (Assurance, 2015)". Organizations ought to cautiously think about the authentication mechanisms and weigh up whether their chosen mechanism provides a solid ground on which the additional requirements for their security controls can be resorted. Just as a house built on a weak foundation will crumble, an authorization, encryption, integrity or audit scheme built on a weak foundation may also crumble when it comes down to a forensic evaluation after an incident has occurred (Sans.org, 2015). "Whether a security system serves the purposes of information asset protection or provides for general security outside the scope of IT, it is common to have three main security processes working together to provide access to assets in a controlled manner. These processes are (Infosectoday.com, 2015):

- Authentication: Often referred to as Identification and Authentication, determining and validating user identity.
- Authorization: Providing users with the access to resources that they are allowed to have and preventing users from accessing resources that they are not allowed to access.
- Accounting: Providing an audit trail of user actions. This is sometimes referred to as auditing."

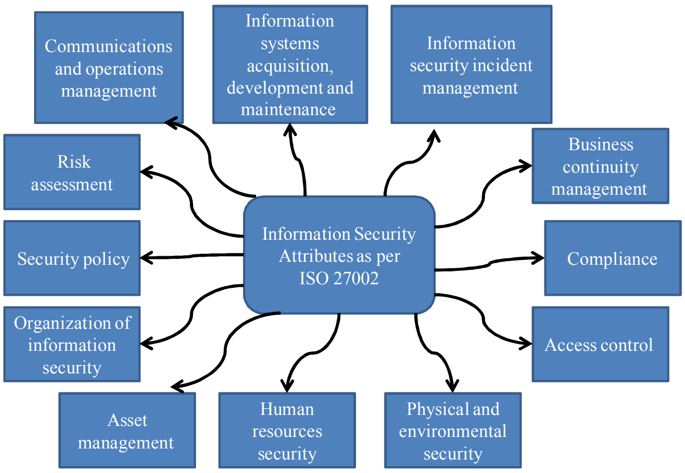
Communications and operations management
Information systems acquisition, development and maintenance
Information security incident management
Risk assessment
Business continuity management
Information Security Attributes as per ISO 27002
Security policy
Compliance
Organization of information security
Access control
Asset management
Human resources security
Physical and environmental security

Fig. 2. Different attributes of Information Security as per ISO 27002

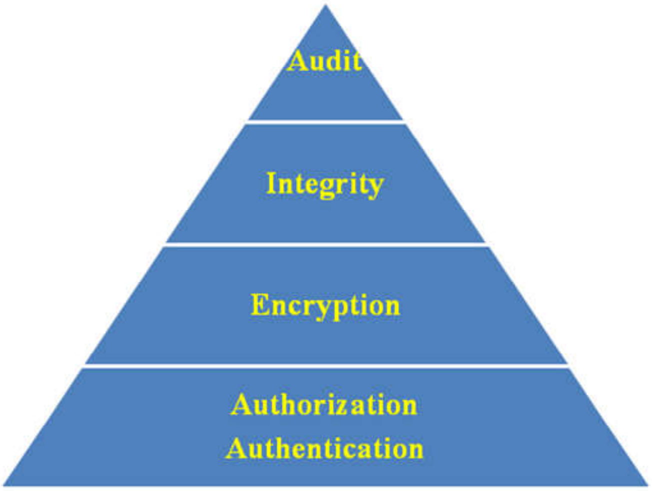

Fig. 3. Security pyramid

Cryptography and Information Security

Information security falls under the broad arena of Cryptography. Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Achieving strong encryption, the hiding of data's meaning, also requires intuitive leaps that allow creative application of known or new methods. So cryptography is also an art (InfoSec Institute, 2015). It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The Internet and the World Wide Web have brought many changes that provide huge benefits, in particular by giving people easy access to information that was previously unavailable, or simply hard to find. Unfortunately, these changes have raised many new challenges in the security of computer systems and the protection of information against unauthorized access (Vulimiri *et al*., 2012).

Public-key cryptography facilitates the following tasks (Mozilla Developer Network, 2015):

- Encryption and decryption allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- Tamper detection allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected.
- Authentication allows the recipient of information to determine its origin-that is, to confirm the sender's identity.
- Nonrepudiation prevents the sender of information from claiming at a later date that the information was never sent.

Public Key Infrastructure (PKI)

Public Key Infrastructure or PKI is a very complex but important subject. PKI is a loaded term that involves the hardware, software, policies, and standards that are necessary to manage SSL certificates. A PKI (Sslshopper.com, 2015) lets you:

- Authenticate users more securely than standard usernames and passwords
- Encrypt sensitive information
- Electronically sign documents more efficiently

PKI has lots of different uses, but it is used primarily for encrypting and / or signing data. Encrypting data refers to scrambling it in a way that makes it unreadable except to authorized persons. Signing data basically refers to authenticating it. A good example of this is signing an E-mail message. If an E-mail message contains a valid digital signature, it proves two things. First, it proves that the message has not been tampered with in transit. Second, it proves that the message is from the person that it claims to be from. E-mail messages are not the only thing that can be signed though (Posey, 2015). It provides cryptographic services through the use of special algorithms. These do not as traditionally done rely on symmetric keys for encrypting and decrypting. With symmetric algorithms the same key that is used to encrypt data is used to decrypt. Whereas PKI uses matched key pairs where one key is used to encrypt data and the other matching key is used to decrypt the data (Sans.org, 2015).

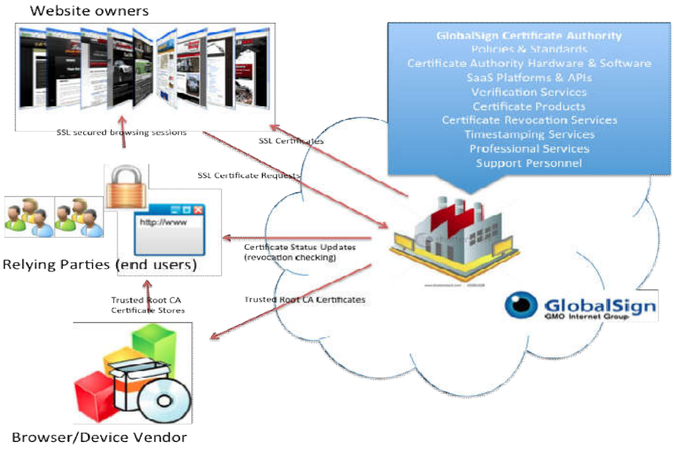
Website owners
GlobalSign Certificate Authority
Policies & Standards
Certificate Authority Hardware & Software
SaaS Platforms & APIs
Verification Services
Certificate Products
Certificate Revocation Services
Timestamping Services
Professional Services
Support Personnel
SSL secured browsing sessions
SSL Certificates
SSL Certificate Requests
http://www
Relying Parties (end users)
Certificate Status Updates (revocation checking)
Trusted Root CA Certificate Stores
Trusted Root CA Certificates
GlobalSign GMO Internet Group
Browser/Device Vendor

Fig. 4. A Public Domain Illustration to exemplify PKI

A PKI is generally considered to be associated with three primary services (Technet.microsoft.com, 2015):

- Authentication—The assurance to one entity that another entity is who he/she/it claims to be.
- Integrity—The assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here," or between "then" and "now."
- Confidentiality—The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.

Some of the issues with the traditional PKI are:

- Cost of issuance
- Cost of Smartcard / USB Token
- Card personalization
- Cost of deployment
- Massive Logistics
- Helpdesk support
- Cost of Certificates
- High upfront and recurrent certificates
- Lack of mobility
- Client installation

There are many research groups working on the above mentioned issues.

Research on PKI in 1970s

Hellman in (Hellman, 1979) put forth the mathematics behind the PKI in early 1970. Technological implementation in those early days is seen to be reported by R. Conway in (Conway *et al*., 1972). However the core issues handled were only the mathematical basis as seen in (Denning, 1976). It reports security system wherein the central component of the model is a lattice structure derived from the security classes and justified by the semantics of information flow. The lattice properties permit concise formulations of the security requirements of different existing systems and facilitate the construction of mechanisms that enforce security. The model provides a unifying view of all systems that restrict information flow, enables a classification of them according to security objectives, and suggests some new approaches. It also leads to the construction of automatic program certification mechanisms for verifying the secure flow of information through a program. A research paper (Diffie and Hellman, 1976) however seems to open new directions in the field by reporting two kinds of contemporary developments in cryptography. IT reported widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing. The decade has also witnessed application of Shanon's theory to information security. Shannon's information-theoretic approach to cryptography is reviewed and extended in (Hellman, 1977). It is shown that Shannon's random cipher model is conservative in that a randomly chosen cipher is essentially the worst possible. This is in contrast with error-correcting codes where a randomly chosen code is essentially the best possible. The concepts of matching a cipher to a language and of the trade-off between local and global uncertainty are also developed.

However the real conceptualization of the PKI emerged at the end of the decade in a pape reported in 1980. New definitions are proposed for the security of Transient-Key Cryptography (a variant on Public-Key Cryptography) that account for the possibility of super-polynomial-time,Monte Carlo cryptanalytic attacks. The basic question we address is: how can one relate the amount of time a cryptanalyst is willing to spend decoding cryptograms to his likelihood of success? This question and others are partially answered in a relativized model of computation in which there provably exists a transient-key cryptosystem such that even a cryptanalyst willing to spend as much as (almost) O (2n/log n) steps on length n cryptograms cannot hope to break but an exponentially small fraction of them, even if he is allowed to make use of a true random bit generator (Brassard, 1981).

Research on PKI in 1980s

Owing to increase in the group communication in the decade of 1980 to 90, the security in view of group was the main focus of the research. Diffe (Diffie, 1981) has taken a review of these developments. He has reported the development of public-key cryptography and its principles. The discussion covers exponential key exchange, the trap-door knapsack public-key cryptosystem, the Rivest-Shamir-Adleman (RSA) system, and the breaking of the knapsack cryptosystem. In a book by KONHEIM (Konheim, 1981) in 1981 a thorough analysis of development of the principles and technology underlying the disguising of text and computer data has been done. The said book formulated the principles underlying encipherment, analyzes a number of basic systems including the ``Enigma machine," and treats applications to data processing: public key systems, electronic signatures, communication and file security. A "promise problem" reported as a formulation of partial decision problem was reported in (Even *et al*., 1984). Complexity issues about promise problems arise from considerations about cracking problems for public-key cryptosystems. Using a notion of Turing reducibility between promise problems, this paper disproved a conjecture made by Even and Yacobi (1980), that would imply nonexistence of public-key cryptosystems with NP-hard cracking problems. In its place a new conjecture is raised having the same consequence. In addition, the new conjecture implies that NP-complete sets cannot be accepted by Turing machines that have at most one accepting computation for each input word. Brassard (Brassard, 1983) has reported about the difficulty in formally defining computational security for public-key cryptography.

A slightly different notion, called transient-key cryptography, was defined by him for whom a natural definition of security against chosen-plaintext attacks was given. The main result presented here was the existence of a relativized model of computation under which there does exist a secure transient-key cryptosystem. A cryptography processor was reported in (Sedlak and Golze, 1986) with a single-chip implementation of the RSA algorithm as an RSA Cryptography Processor (CP). The design of a secure file system based on user controlled cryptographic (UCC) transformations was investigated by Gudes (Gudes, 1980). With UCC transformations, cryptography not only complements other protection mechanisms, but can also enforce protection specifications. Files with different access permissions are enciphered by different cryptographic keys supplied by authorized users at access time. Several classes of protection policies such as: compartmentalized, hierarchical, and data dependent were discussed. Several protection implementation schemes were suggested and analyzed according to criteria such as: security, efficiency, and user convenience. These schemes found to provide a versatile and powerful set of design alternatives. A cost-effective public key cryptographic architecture and its implementation in 2-&mu;m double-level-metal CMOS was also presented during this decade (Ishii *et al*., 1998). The latter consists of a 593-bit arithmetic processing element, an 8-bit microcontroller, and an intelligent bus interface unit. The device uses 95000 transistors, has an area of 115000 mil2 assembled in a 40-pin package, and is capable of an average throughput of 500 kb/s.

Up surge of research in 1990s

In a informative book by Menezes in 1990s, which was the then regarded as the major contribution to the field of cryptography narrated a rigorous encyclopedia of known techniques, with an emphasis on those that are both (believed to be) secure and practically useful. It presents in a coherent manner most of the important cryptographic tools one needs to implement secure cryptographic systems, and explains many of the cryptographic principles and protocols of existing systems. The topics covered range from low-level considerations such as random-number generation and efficient modular exponentiation algorithms and medium-level items such as publickey signature techniques, to higher-level topics such as zero-knowledge protocols (Menezes *et al*., 1997). With PKI in full swing several types of PKI and their advantages and disadvantages were discussed in (Perlman, 1999). ELLISON in his paper (Ellison, 1999) questioned the underlying assumptions, suggests workable alternative assumptions and presents elements of a public key certification structure appropriate to the new assumptions. In a paper during early 21st century, an emphasis was placed on the emerging use of elliptic curve cryptography (ECC) as an alternative to more widely accepted public key algorithms.

Overall, the need to allow for multiple algorithms was emphasized as being prudent and a safeguard against any unforeseen 'cracking' of a particular algorithm that may be in use. Both technical and policy parameters in this area were outlined in the paper. However, the paper concludes that lack of government, and particularly parliamentary, leadership and firm decision making in the area of public key infrastructure and associated legal and management regulation means that resulting reliance on market forces may simply cause disparate regimes to be created that will impede orderly global electronic commerce. Somewhere in 2000, researchers started gaining an insight regarding the vulnerabilities of the traditional PKI and started proposing new solutions (Caelli *et al*., 1999).

Research in the last decade 2000 – 2010

Few rich research oriented reference books have been reported in this period. One such noteworthy book is by SCHNEIER, B (Ellison and Schneier, 2000). This book provides a comprehensive survey of modern cryptography. The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. Another similar book is by Stallings William that gives important case studies in this area (Schneier *et al*., 1999). The notion of the notion of nonmalleable cryptography, an extension of semantically secure cryptography, is defined in this decade (Stallings and Stallings, 1999). Reportedly it is the first proven to be secure against a strong type of chosen ciphertext attack proposed by Rackoff and Simon, in which the attacker knows the ciphertext she wishes to break and can query the decryption oracle on any ciphertext other than the target. Oded Regev a well known researcher in this field presented a (classical) public-key cryptosystem whose security is based on the hardness of the learning problem. By the main result, its security is also based on the worst-case quantum hardness of Gap SVP and SIVP. The new cryptosystem is much more efficient than previous lattice-based cryptosystems: the public key is of size $\tilde{O}(n_2)$ and encrypting a message increases its size by a factor of $\tilde{O}(n)$ (in previous cryptosystems these values are $\tilde{O}(n4)$ and $\tilde{O}(n_2)$, respectively). In fact, under the assumption that all parties share a random bit string of length $\tilde{O}(n_2)$, the size of the public key can be reduced to $\tilde{O}(n)$ (Regev, 2009). Yet another interesting direction has been discussed in (Kocarev, 2001) applications of chaos in cryptography. Gutmann (Gutmann, 2002) reported renaissance in this field by relating to other flexible objects, the public key infrastructure sacrifices some utility in trying to be all things to all people. Mainly, PKI's generic, all-purpose identity certificates fall short of what the marketplace demands, forcing vendors to develop more economically efficient, useful, and imaginative business models. Thus, we must adapt the PKI design to the real world rather than trying to constrain the real world to match the PKI. The use of electronic communication channels to conduct businesses without the need for physical conduct or presence has already been established and accepted warmly. But the issue of paying electronically still remains risky and muddy. A noteworthy paper (Tsiakis and Sthephanides, 2005) implicates the security and trust issues that are essential for every electronic payment mechanism in order to be accepted and established as a common medium of financial transactions. The link between usability and security has been explored in (Balfanz *et al*., 2004). Not only will this better protect users, it will actually enable them to accomplish tasks they couldn't accomplish before due to the lack of a trustworthy infrastructure.

Certificate less public key cryptography was introduced to overcome the key escrow limitation of the identity-based cryptography. It combines the advantages of the identity-based cryptography and the traditional PKI. Many certificate less public key encryption and signature schemes have been proposed. However, the key agreement in CL-PKE is seldom discussed. In (Shi and Li, 2007) authors present a new certificate less two party authentication key agreement protocol and prove its security attributes. Compared with the existing protocol, our protocol is more efficient. Public key infrastructure (PKI) is a key component for most of the current and future secure communications architectures and distributed application environments. Thus, the process of migrating UMU-PKI to IPv6 is important for the successful deployment of IPv6 as a basic component of the future Internet. A recent European research project provides an ideal opportunity to migrate the Java-based UMU-PKI to IPv6 and build new security services over it (Gomez Skarmeta *et al*., 2003).

Status of research in last five years (2010- 2015)

Mobile USB based tokens are now appearing on the scene in last few years. Such a system is Moserbaer Crypto USB token based on Public Key Infrastructure (PKI) Technology. The purpose of this technology is to manage digital keys and certificates. PKI systems can enable the use of digital signature, digital receipt, encryption and permissions management services across a wide variety of applications. PKI-based security solutions are enhanced by "something you have" technologies, providing secure storage of digital identities backed up by strong two-factor authentication (Moserbaer.com, 2015). Many new protocols are also emerging on the scene. The need to secure networks has grown substantially over the last few years. One of the security challenges organizations face is authentication. There are few protocols that can be used for authentication-one of which, Internet Protocol Security (IPSec), uses X509 version 3 certificates as a means to identify the entities involved in a secure session. However, the challenge has moved from authentication to issuance certificate to these end entities. Moreover, our network includes devices that do not run with established credentials (domain known), for example, routers. SCEP enables network devices that do not run with domain credentials to enroll for x509 version 3 certificates from a Certification Authority (CA) (Social.technet.microsoft.com, 2015).

Good number of latest research papers also evident to showcase work in this direction. Providing secure and efficient access to large scale data is an important component of cloud computing. In (Wang and Lin, 2012), a PKI-based access control mechanism is proposed. The mechanism is based on encryption-based access control and over-encryption, it not only ensures secure access to the outsourced data, but also relieve the data owner from user's every access procedure, thus avoid the owner will become the bottleneck during the access and archieve high efficiency. Moreover, the mechanism is easy and flexible when users are granted or revoked. Preliminary analysis demonstrates the effectiveness and security of the mechanism. With fast evolution of mobile devices and mobile network, the need of protecting user sensitive information locally and performing secure user authentication remotely become ever more increasing. Bio-cryptography is emerging as a powerful solution which can combine the advantages of conventional cryptography and biometric security. In (Xi *et al*., 2010), authors have presented an efficient bio-cryptographic security protocol designed for client/server authentication in current mobile computing environment, with a reasonable assumption that server is secure. In this protocol, fingerprint biometric is used in user verification, protected by a computationally efficient Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC).

Today's P2P applications require security services such as privacy, anonymity, authentication, and non-repudiation. Such services could be provided through a hierarchical Public Key Infrastructure. However, P2P networks are usually Internet-scale distributed systems comprised of nodes with an undetermined trust level, thus making hierarchical solutions unrealistic. In (Avramidis *et al*., 2012), authors have proposed Chord-PKI, a distributed PKI architecture which is build upon the Chord overlay network, in order to provide security services for P2P applications. One major direction in last few years is the application of PKI for Internet of Things (IoT). As the Internet of Things (IoT) continues to connect objects and relay information to people, new possibilities for business and personal life abound. IDC projects that by 2020, the IoT will grow to 200 billion objects. Yet, for all of the IoT's possibilities, hackers are innovating as well. In light of the reams of sensitive data that the IoT generates, the need for security has never been greater. One answer comes from a solution that has been working quietly to protect data for 20 years: Public Key Infrastructure (PKI). Its full capabilities have never been explored, but that is about to change thanks to the IoT (Magazine, 2015). Few interesting applications are arising out of this. Such an application is Ambient Assisted Living (AAL) that aims at providing unobtrusive support to frail and elderly people for their daily life based on their context and situation. To this end, systems and services are required which are user-centric and adaptable towards the needs and capabilities of the people in need of care. The continuous integration of leading-edge technologies, such as cloud and wireless communication technologies, in the context of the Internet of the Things (IoT), can meet this requirement by enabling a new form of communication between frail and elderly people, their environment and relevant groups of care givers. However, for IoT-based systems to reach their full potential, sound answers need to be provided to the important security questions arisen, particularly those regarding authentication of entities (people and environmental objects) and data privacy. This paper presents a system based on Gateways (GW) that aggregate health sensor data and resolve security issues through digital certificates and PKI data encryption (Doukas *et al*., 2012). Although X.509-based PKI has some well-known problems, they're being, or can be, addressed. In the past, those problems led to proposals for reinventing PKI based on other technologies. However, none of the proposals provided sufficient additional benefit to gain broad adoption. While there are reasons to change and evolve X.509-based PKI, for the present there are no compelling reasons to reinvent the technology (Farrell, 2011).

Overview of Cryptographic algorithms

There are two basic kinds of encryption algorithms in use today (Diablotin.com, 2015):

- Private key cryptography, which uses the same key to encrypt and decrypt the message. This type is also known as symmetric key cryptography.
- Public key cryptography, which uses a public key to encrypt the message and a private key to decrypt it. The name public key comes from the fact that you can make the encryption key public without compromising the secrecy of the message or the decryption key. Public key systems are also known as asymmetric key cryptography.

Private Key systems

ROT13

ROT13 ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the letter 13 letters after it in the alphabet. ROT13 is an example of the Caesar cipher, developed in ancient Rome (Dictionary.sensagent.com, 2015).

CRYPT

This is the original cryptographic tool available in UNIX.

DES, AES and BLOWFISH

The Data Encryption Standard (DES, /ˌdiːˌiːˈɛs/ or /ˈdɛz/) was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world (Wikipedia, 'Data Encryption Standard', 2015). The origins of AES date back to 1997 when the National Institute of Standards and Technology (NIST) announced that it needed a successor to the aging Data Encryption Standard (DES) which was becoming vulnerable to brute-force attacks (Search Security, 'What is Advanced Encryption Standard, 2015). Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variablelength key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use (Schneier.com, 2015). Some recent study, however indicates that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm (Kumar Verma and Kumar Singh, 2012).

RC2, RC4, RC5 and RC6

There are many Symmetric key cryptography algorithms which have been proposed. The Rivest Cipher Algorithm is one among those. Different versions of this algorithm have been released. In this paper, a comparative study of the various Rivest Cipher Algorithms has been done. The RC6 algorithm although is not found vulnerable to any practical attack, while some theoretical attacks still exist. Nowadays, as computing power is increasing, RC6 could be broken in some years. So, the need for a stronger algorithm arises. Therefore, the algorithm should be improved in order to make it safe against security attacks (Ahmad *et al*., 2010).

IDEA

The IDEA (International Data Encryption Algorithm) is a strong block-cipher. Though there are many operations involved in the entire algorithm, only three different of operations are involved (as mentioned above). As the cipher key size is 128bits, in that respect IDEA is too strong (having taken care for weak keys) (Data-encryption-algorithms, 2015).

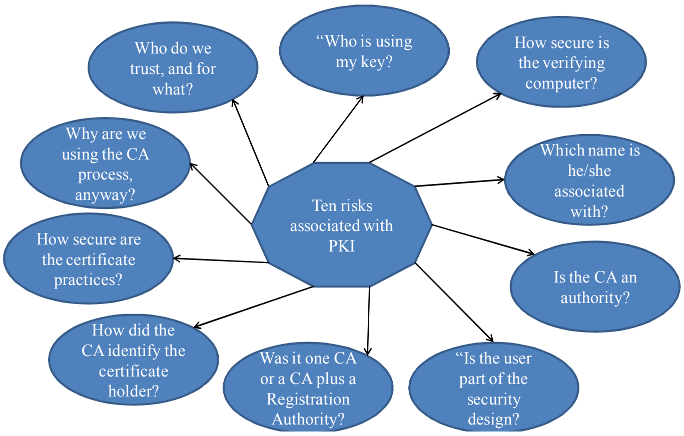
Who do we trust, and for what?
"Who is using my key?
How secure is the verifying computer?
Why are we using the CA process, anyway?
Which name is he/she associated with?
Ten risks associated with PKI
How secure are the certificate practices?
Is the CA an authority?
How did the CA identify the certificate holder?
Was it one CA or a CA plus a Registration Authority?
"Is the user part of the security design?

Fig. 5. Ten risks associated with PKI

Discussion, Conclusion and Way Forward

The explosive growth of e-commerce has resulted in organizations sharing data over the Internet with other net-centric organizations. Advances in telecommunications and networked applications are forcing dramatic changes in corporate functions, such as supply chain management, enterprise resource planning and customer relationship management. Online transactions with business partners and customers has prompted e-businesses to re-evaluate their security strategy, to avoid network downtime and being unable to connect to upstream partners and suppliers. Presence of a robust security architecture is essential to the success of net-centric organizations. Public key infrastructure (PKI) is one such technology that offer benefits to net-centric organizations, being a system of services, technology, protocols and standards that can be used as a solution for providing secure transactions. There are many factors that make PKI implementation difficult. Literature survey reveals that the arguments for adopting Public-Key Infrastructure (PKI) are strong and yet PKI products have suffered from relatively low adoption rates.

Convergence of mobile phones and the Internet opens up unlimited opportunities to service providers and users alike. For service providers, it offers an opportunity to deploy innovative services for a large base of users and boost revenue. For users, it brings them closer to the dream of "anytime-anywhere" services available in "all-in-one" device. However, exploiting these opportunities into real world requires an assurance to both service providers and mobile users that the services adhere to well known security models. The Public Key Infrastructure for mobile phones (mobile PKI) is emerging as enabling technology for accessing services over the Internet. Yet, authentication of service providers and users in the mobile PKI brings its own set of challenges. For example, check for certificate revocation is vital but it is resource consuming and requires connectivity. Security of the private key is central to PKI but portable natures of mobile phones worsen the issue. Existing practices of offline credential verification to issue a certificate restrict usability of certificates for mobile users.

Thus secure storage of private keys in mobile devices is an active research area. On one hand, hand-held based solutions provide more flexibility in terms greater availability of storage and computation resources as well as rich set of support for applications. On the other hand, SIM based solutions offer higher level of security as the private keys never leave the SIM but provides less flexibility in application support. Also, SIM based solutions have restricted storage and computing resources. Online registration and issuance of certificates is another challenging area in mobile authentication. This requires some form of user credentials availability (transparentto mobile client) with CA. However, there is no industry-level agreement for procedures of online registration and issuance. Further, though offline credentials are available with mobile user's home identity provider (such as National Identity Providers), lack of interoperability agreements and functionality limit the access of these credentials to home environment only.

As with many young and expanding fields, the issues of security and privacy of Public Key Infrastructures are involved and complex. PKI has proven to be a relatively complex and expensive solution and from the perspective of diffusion into applications it has been notably less successful than expected. Nevertheless it is still considered to be a very secure technology for authentication and electronic signatures. That said, the core premise underlying the public key cryptography, and thus PKI systems, is that secret keys always remain secret. This is just one of many security issues that PKIs face. In this case technical solutions are available which lead to increasing costs for the users' infrastructure for electronic signatures. Another critical aspect of PKI systems is the underlying concept of trust (who trusts whom for what ?) and the role of the certificate authority (CA) taken therein. In the case of signature fraud in a multilateral, not secured technological system the consequences of this fraud are largely borne by the PKI user, not the CA.

Additionally, PKIs suffer from privacy issues because traditional public-key certificates contain information about the holder. As such, a digital certificate can be traced uniquely to the person to whom it has been issued (or to the device in which it has been incorporated) and can be followed around instantaneously and automatically as it moves through the system. In spite of these threats, the protection of privacy has never been a core issue in the legal and policy discussions about PKI. However, the use of such certificates has rarely been implemented into national European legislation so far. Based on the market penetration rate of qualified electronic signatures to date it can be seen that only a fraction of the potential market has adopted this innovation. Notably, successful implementations can be found especially where the signature is used in a process that has an added value such as within a central organization. Informally, it is believed, that most potential adopters have not even reached the knowledge stage, meaning they are not even aware that this technology exists. Possibly the awareness of this technology could create a need to adopt. This study suggests six concrete measures to improve the diffusion of PKI into the market:

- To shift costs in order to achieve a fair distribution
- Measures to reach the critical mass of users
- Increasing awareness and knowledge about this technology
- To especially target the user group called ‘early adopters’
- To increase triability e.g. by trial versions of electronic signatures
- To further reduce complexity of the private infrastructure required

Researchers need to address more on the last aspect to reduce the complexity and attempt to reduce the vulnerability of PKI. Further looking at the active area of research for mobiles and Internet of Things a new type of PKI is need of the hour.

REFERENCES

Ahmad, S., Beg, D. and Abbas, D. 2010. J. Ahmad and S. Atif, 'Comparative Study between Stream Cipher and Block Cipher using RC4 and Hill Cipher', *International Journal of Computer Applications*, vol. 1, no. 25, pp.15-21.

Assurance, I. 2015. 'Authentication vs. Authorization | Protect IU', *Protect.iu.edu*, 2015. (Online). Available: https://protect.iu.edu/cybersecurity/authn-authz. (Accessed: 21- Mar- 2015).

Avramidis, A., Kotzanikolaou, P., Douligeris, C. and Burmester, M. 2012. 'Chord-PKI: A distributed trust infrastructure based on P2P networks', *Computer Networks*, vol. 56, no. 1, pp. 378-398, 2012.

Balfanz, D., Durfee, G., Smetters, D. and Grinter, R. 2004. 'In search of usable security: five lessons from the field', *IEEE Security & Privacy Magazine*, vol. 2, no. 5, pp. 19-24.

Brassard, G. 1981. 'A time-luck tradeoff in relativized cryptography', *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 280-311.

Brassard, G. 1983. 'Relativized cryptography', *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 877-894, 1983.

BusinessDictionary.com, 'What is information security? definition and meaning', 2015. (Online). Available: http://www.businessdictionary.com/definition/information-security.html. (Accessed: 20- Mar- 2015).

Caelli, W. Dawson, E. and Rea, S. 1999. 'PKI, elliptic curve cryptography, and digital signatures', *Computers & Security*, vol. 18, no. 1, pp. 47-66.

ComputerWeekly.com, 'Information security means better business', 2015. (Online). Available: http://www.computerweekly.com/opinion/Information-security-means-better-business. (Accessed: 20- Mar- 2015).

Conway, R., Maxwell, W. and Morgan, H. 1972. 'On the implementation of security measures in information systems', *Commun. ACM*, vol. 15, no. 4, pp. 211-220, 1972.

Data-encryption-algorithms, Available: http://rroij.com/open-access/international-data-encryption-algorithm-idea-a-typical-illustration-116-118.pdf. (Accessed:22- Mar- 2015).

Denning, D. 1976. 'A lattice model of secure information flow', *Commun. ACM*, vol. 19, no. 5, pp. 236-243.

Diablotin.com, '(Chapter 6) 6.4 Common Cryptographic Algorithms', 2015. (Online). Available: http://www.diablotin.com/librairie/networking/puis/ch06_04.htm. (Accessed: 22- Mar- 2015).

Dictionary.sensagent.com, 'ROT13 : definition of ROT13 and synonyms of ROT13 (English)', 2015. (Online). Available: http://dictionary.sensagent.com/ROT13/en-en/. (Accessed: 22- Mar- 2015).

Diffie, W. 1988. 'The first ten years of public-key cryptography', *Proc. IEEE*, vol. 76, no. 5, pp. 560-577.

Diffie, W. and Hellman, M. 1976. 'New directions in cryptography', *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654.

Dolev, D. Dwork, C. and Naor, M. 2003. 'Nonmalleable Cryptography', *SIAM Rev.*, vol. 45, no. 4, pp. 727-784.

Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F. and Vassilacopoulos, G. 2012. 'Enabling data protection through PKI encryption in IoT m-Health devices', *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)*.

Ellison, C. 1999. 'The nature of a useable PKI', *Computer Networks*, vol. 31, no. 8, pp. 823-830.

Ellison, C. and Schneier, B. 2000. 'Inside risks: risks of PKI: secure email', *Commun. ACM*, vol. 43, no. 1, p. 160, 2000.

Even, S. Selman, A. and Yacobi, Y. 1984. 'The complexity of promise problems with applications to public-key cryptography', *Information and Control*, vol. 61, no. 2, pp. 159-173.

Farrell, S. 2011. 'Not Reinventing PKI until We Have Something Better', *IEEE Internet Comput.*, vol. 15, no. 5, pp. 95-98.

Gomez Skarmeta, G., Martinez Perez, A., Canovas Reverte, O. and Lopez Millan, G. 2003. 'PKI services for IPv6', *IEEE Internet Comput.*, vol. 7, no. 3, pp. 36-42.

Gudes, E. 1980. 'The Design of a Cryptography Based Secure File System', *IIEEE Trans. Software Eng.*, vol-6, no. 5, pp. 411-420.

Gutmann, P. 2002. 'PKI: it's not dead, just resting', *Computer*, vol. 35, no. 8, pp. 41-49.

Hellman, M. 1979. 'The Mathematics of Public-Key Cryptography', *Sci Am*, vol. 241, no. 2, pp. 146-157.

Hellman, M. 1977. 'An extension of the Shannon theory approach to cryptography', *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 289-294.

InfoSec Institute, 'Chapter 7: The Role of Cryptography in Information Security - InfoSec Institute', 2012. (Online). Available: http://resources.infosecinstitute.com/role-of-cryptography/. (Accessed: 21- Mar- 2015).

Infosectoday.com, 'Authentication, Authorization, and Accounting', 2015. (Online). Available: http://www.infosectoday.com/Articles/Authentication.htm. (Accessed: 21- Mar- 2015).

Ishandbook.bsewall.com, 'Definition of Information Security', 2015. (Online). Available: http://ishandbook.bsewall.com/risk/Methodology/IS.html. (Accessed: 20- Mar- 2015).

Ishii, S. Oyama, K. and Yamanaka, K. 1998. 'A high-speed public key encryption processor', *Syst. Comp. Jpn.*, vol. 29, no. 1, pp. 20-32.

Kocarev, L. 2001. 'Chaos-based cryptography: a brief overview', *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6-21.

Konheim, A. 1981. *Cryptography, a primer*. New York: Wiley.

Kumar Verma, H. and Kumar Singh, R. 2012. 'Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms', *International Journal of Computer Applications*, vol. 42, no. 16, pp. 8-14.

Magazine, S.C. 2015. 'PKI for the Internet of Things', 2014. (Online). Available: http://www.scmagazine.com/pki-for-the-internet-of-things/article/359724/. (Accessed: 21- Mar- 2015).

Menezes, A. Van Oorschot, P. and Vanstone, S. 1997. *Handbook of applied cryptography*. Boca Raton: CRC Press.

Moserbaer.com, 'PKI Token | IT Security Solutions | Crypto USB Token | Digital Signature | Security Token', 2015. (Online). Available: http://www.moserbaer.com/iss-pki-token.asp. (Accessed: 21- Mar- 2015).

Mozilla Developer Network, 2015, 'Introduction to Public-Key Cryptography', 2015. (Online). Available:https://developer.mozilla.org/en/docs/Introduction_to_Public-Key_ Cryptography. (Accessed: 21- Mar- 2015).

Open Learn, 2015. 'An introduction to information security', 2015. (Online). Available: http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-4.1. (Accessed: 20- Mar- 2015).

Perlman, R. 1999. 'An overview of PKI trust models', *IEEE Network*, vol. 13, no. 6, pp. 38-43, 1999.

Posey, 2005. 'A beginner's guide to Public Key Infrastructure', *Tech. Republic*, 2005. (Online). Available:http://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/. (Accessed: 21- Mar- 2015).

Regev, O. 2009. 'On lattices, learning with errors, random linear codes, and cryptography', *JACM*, vol. 56, no. 6, pp. 1-40.

Sans.org, 2015. (Online). Available: http://www.sans.org/reading-room/whitepapers/authentication/its-about-authentication-1070. (Accessed: 21- Mar- 2015).

Sans.org, Available: http://www.sans.org/reading-room/whitepapers/vpns/pki-what-why-764. (Accessed: 21- Mar- 2015).

Sans.org, 'SANS Institute: Information Security Resources', 2015. (Online). Available: http://www.sans.org/information-security/(Accessed: 20- Mar- 2015).

Schneier, B. Meyer, C. Denning, D. Stinson, D. Menezes, A. and Friedman, W. 1999. *Dr. Dobb's essential books on cryptography and security*. San Mateo, CA: Miller Freeman, Inc., 1999.

Schneier.com, 'Schneier on Security: Blowfish', 2015. (Online). Available: https://www.schneier.com/blowfish.html. (Accessed: 22- Mar- 2015).

Search Security, 'What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com', 2015. (Online). Available: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. (Accessed: 22- Mar- 2015).

Search Security, 'What is authentication? - Definition from WhatIs.com', 2015. (Online). Available: http://searchsecurity.techtarget.com/definition/authentication. (Accessed: 21- Mar- 2015).

Search Security.co.UK, 'What is ISO 27001? - Definition from WhatIs.com', 2015. (Online). Available: http://searchsecurity.techtarget.co.uk/definition/ISO-27001. (Accessed: 20- Mar- 2015).

Sedlak, H. and Golze, U. 1986. 'An RSA cryptography processor', *Microprocessing and Microprogramming*, vol. 18, no. 1-5, pp. 583-590.

Shi, Y. and Li, J. 2007. 'Two-party authenticated key agreement in certificateless public key cryptography', *Wuhan Univ. J. of Nat. Sci.*, vol. 12, no. 1, pp. 71-74.

Social.technet.microsoft.com, 'Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS) - TechNet Articles - United States (English) - TechNet Wiki', 2015. (Online). Available: http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx. (Accessed: 21- Mar- 2015).

Sslshopper.com, 'Public Key Infrastructure (PKI) Overview', 2015. (Online). Available: https://www.sslshopper.com/public-key-infrastructure-pki-overview.html. (Accessed: 21- Mar- 2015).

Stallings, W. and Stallings, W. 1999. *Cryptography and network security*. Upper Saddle River, N.J.: Prentice Hall.

Technet.microsoft.com, 'Core PKI Services: Authentication, Integrity, and Confidentiality', 2015. (Online). Available: https://technet.microsoft.com/en-us/library/cc700808.aspx. (Accessed: 21- Mar- 2015).

Techopedia.com, 'What is Information Security (IS)? - Definition from Techopedia', 2015. (Online). Available: http://www.techopedia.com/definition/10282/information-security-is. (Accessed: 20- Mar- 2015).

Tsiakis, T. and Sthephanides, G. 2005. 'The concept of security and trust in electronic payments', *Computers & Security*, vol. 24, no. 1, pp. 10-15.

Vulimiri, A., Agha, G., Godfrey, P. and K. Lakshminarayanan, 'How well can congestion pricing neutralize denial of service attacks?', *Proceedings of the 12th ACM Sigmetrics/Performance joint international conference on Measurement and Modeling of Computer*

Systems - SIGMETRICS '12, 2012.

Wang, X. and Lin, Y. 2012. 'An Efficient Access control scheme for Outsourced Data', *JCP*, vol. 7, no. 4.

Why is Information Security Important? 2015. Available: http://www.senseofsecurity.com.au/articles/information-security. (Accessed: 20- Mar- 2015).

Wikipedia, 'Data Encryption Standard', 2015. (Online). Available: http://en.wikipedia.org/wiki/Data_Encryption_Standard. (Accessed: 22- Mar- 2015).

Xi, K., Ahmad, T., Han, F. and Hu, J. 2010. 'A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment', *Security Comm. Networks*, vol. 4, no. 5, pp. 487-499.

****