

Smart Cities: A Survey on Security Concerns

Sidra Ijaz, Munam Ali Shah, Abid Khan and Mansoor Ahmed
Department of Computer Science
COMSATS Institute of Information Technology(CIIT)
Islamabad

Abstract—A smart city is developed, deployed and maintained with the help of Internet of Things (IoT). The smart cities have become an emerging phenomena with rapid urban growth and boost in the field of information technology. However, the function and operation of a smart city is subject to the pivotal development of security architectures. The contribution made in this paper is twofold. Firstly, it aims to provide a detailed, categorized and comprehensive overview of the research on security problems and their existing solutions for smart cities. The categorization is based on several factors such as governance, socioeconomic and technological factors. This classification provides an easy and concise view of the security threats, vulnerabilities and available solutions for the respective technologies areas that are proposed over the period 2010-2015. Secondly, an IoT testbed for smart cities architecture, i.e., SmartSantander is also analyzed with respect to security threats and vulnerabilities to smart cities. The existing best practices regarding smart city security are discussed and analyzed with respect to their performance, which could be used by different stakeholders of the smart cities.

Index Terms—Smart city, ICT, IoT, Information security, RFID, M2M, WSN, Smart grids, Biometrics

I. INTRODUCTION

The concept of smart cities is very vast as its vision encompasses management and organization of the whole city through embedded technology. These are ideally the cities that monitor and integrate status of all their infrastructures, management, governance, people and communities, health, education, and natural environment through information and communication technologies (ICT). The smart city is designed, constructed, and maintained by using highly advanced integrated technologies, that include sensors, electronics, and networks which are linked with computerized systems comprised of databases, tracking, and decision-making algorithms [1]. With increasing boost in urbanization, the concerns about economic restructuring, environmental issues, governance issues and public sector problems need to be dealt in a smarter approach. The challenges of modern cities are becoming complex as the pace of change has become very gigantic. This requires organizational changes specially focusing on the latest technologies and communication through Internet.

The term global village seems very coherent with the smart city as urbanization is dependent on latest technologies and Internet. The concept is also influenced by the industries promoting and selling their products like GPS, ipad, smartphones and other technologies [2]. The smart city hence promises smarter growth. It is said that proper investments in developing the systems of a city through embedded technologies will

help in immense growth in economic system as well [3]. There are certain pioneering cities that are considered as the next generation smart cities. Names of such cities include Barcelona, Amsterdam, Masder, Singapore and France[4]. The general idea of a smart city and it's major components is given in the Figure 1.

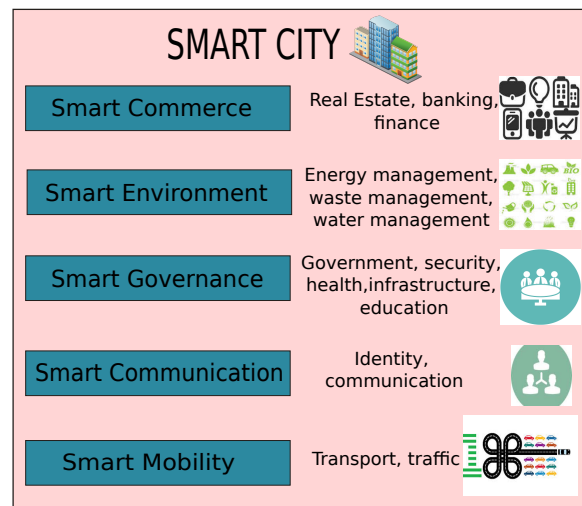


Fig. 1. Major components of a Smart City

It should be considered that the latest information and communication technologies (ICT) that are the core part of an efficient smart city are the Internet of things (IoT), smartphone technology, RFID(Radio Frequency Identification System), smart meters, semantic web, linked data, ontologies, artificial intelligence, cloud computing, collective intelligence, softwares, smart apps, and biometrics. The Internet of Things (IoT) is the network of physical/tangible objects integrated with computational devices, software, electronics, smart sensors and connectivity so that it can be used to achieve greater value and service by exchanging data with the maker, operator and other connected devices. Each thing is unambiguously distinctive through its embedded computing system but is able to inter-operate within the infrastructure of Internet. The concept of IoT play a vital role in development of ideal and secure smart city, as a smart city is solely dependent on the embedded technology. The IoT is considered as a major research and innovation idea that leads to a lot of opportunities

for new services by interconnecting physical and virtual worlds with a huge amount of electronics distributed in different places including houses, vehicles, streets, buildings and many other environments [5].

The concept of smart cities is distinguished on the fact that it is solely dependent on embedded systems, smart technologies and the IoT. In general term, a smart city relies on information technology and the embedded infrastructure to facilitate it for a better living standard.

Though smart cities are facing many problems through their development, including socioeconomic and political issues, but the most important hurdle here is the technical issues. In technical problems, along with the other issues like system interoperability and cost efficient technology, the concern of security and privacy is very important [6]. The field of information security particularly deals with the issues of security and privacy of information. The goal of information security is to protect the information from attacks, viruses, frauds, and many other vicious activities that may cause harm either to the information, or the need of information in the technologically embedded smart cities. The security is very important in the infrastructures of smart cities because the networks will be prone to a large range of malicious attacks, and the internal and external parties are not trusted so security is a vital prerequisite to consumer acceptance [7]. As the concept of smart cities is still developing, the need to identify the core requirements of information security in various technologies is important.

In order to identify the correct requirements, and limitations, the aspiring smart cities should also be studied to identify the achievements and flaws in information security. As smart cities are exposed to malicious attacks which can alter or damage the whole infrastructure and communication systems, so the security of a smart city regarding the information point of view is very crucial. In other words, the key goals of a smart city would not be achieved if the information is not properly secured. Moreover, privacy should also be considered in a smart city environment. Privacy of systems that gather data and trigger emergency response when needed are also technological challenges that go hand in hand with the continuous security challenges [8].

The influence of information security is not in technical side only, but it also effects the economic concerns as well [9]. The issues of information security also needs to be addressed for a better economic development of a smart city. The requirements of of ideally secured and reliable smart cities need to be recognized considering most of the technologies, specially focusing on IoT, cloud computing, real world user interfaces, smart sensors, smartphones, semantic web etc. The factor of commercialization also needs to be considered as many IT companies have new solutions for the smart cities as well. The example is launch of Global Intelligent Urbanization by Cisco [10].

The objective of this paper is to survey pivotal problems and the solutions in practice regarding information security in a smart city in the light of key influencing factors. The rest of the paper is organized as follows: The Section II describes factors

influencing a smart city. In Section III, the security issues of smart cities in perspective of governance, social and economic point of view are identified. The technologies that play part in making a smart city are considered in light of information security in Section IV. Section V gives comparative analysis of selected literature. Conclusions are discussed in Section VI.

II. INFORMATION SECURITY IN A SMART CITY

The security and privacy of information in a smart city has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a smart city, the information security must be fool proof. The factors that are taken under consideration in order to identify the issues in information security in a smart city include governance factors, social/economic factors and most importantly economic factors. These factors are elaborated in the Figure (2). The researchers identify, explain and propose solutions to the information security issues by considering the mentioned factors. Most of the research work discuss the components and architecture of a smart city and then describe solutions for the security and privacy concerns.

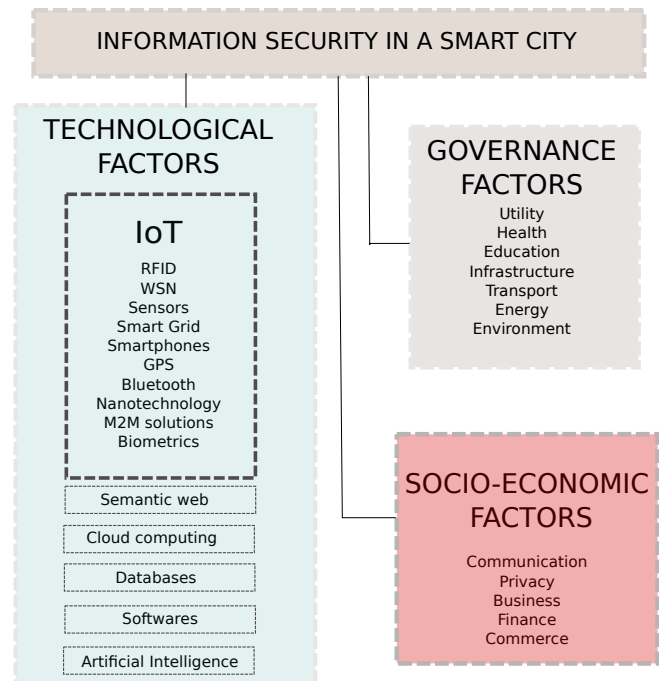


Fig. 2. Influencing factors on information security in a smart city

The IoT has been the key interest of the researchers as it is the core technology on which the smart cities are being developed and maintained [11]. For instance, in [7], the key hurdles and problems faced regarding security and privacy are discussed, keeping in the context of technological standards. the paper particularly focuses on Machine to Machine (M2M) standard solutions that are helpful in better implementation of IoT in a smart city.

A very important factor that plays key role in developing a smart city is "big data". The production of large data sets in a smart city is an inevitable phenomenon including national consensuses, government records, and other information about the citizens[12]. From such data, the smart cities can extract very important information helping real time analysis and ubiquitous computing. The author in paper [13] elaborates that though the big data provides various opportunities for smarter life, still it brings challenges of security and privacy. The challenges include lack of tools for management of big data, third party data sharing, threats in growing public databases, data leakage and concerns on digital security.

In another paper, the cyber security challenges are addressed [8]. Here the authors focus on two main challenges, security and privacy. They present a mathematical model depicting the interaction between people, IoT, and servers which are vulnerable to information security threats. Though the mathematical and graphical model for the IoT, people and servers is given stating that it will help in locating the problems in security and privacy, but the methodology to do so is not discussed. Moreover, Bohli et al [14] propose a distributed framework for IoT applications, which promises security, trust and privacy in information delivery. As IoT applications play a key role on building the smarter city, so some information security issues in a smart city can be addressed through the distributive framework.

The identification and classification of stakeholders of a smart city help in addressing the security problems in smart city in a better way. In this paper [15] all the concerned stakeholders regarding the security and privacy of information are identified by using onion model approach. The authors proposed that by identifying all the stakeholders, the security requirements and issues are identified in a better way. They also propose a comprehensive framework to deal with these issues.

In [16] the role of smart software is discussed in context of information security. The role of smart software in developing a smarter city is discussed specifically throwing light upon limitations regarding security issues. Certain security software models are also discussed. Another paper discusses the issue of security problems in sensing and querying in urbanization[17]. The authors propose an encryption scheme to deal with the issues of data integrity and privacy.

Smart grids are considered an important component of a smart city as they provide the services of very novel and efficient energy supply chain and information management[18]. In [19] the authors discuss the information security issues in a smart grid. The requirements of information security are identified by the authors and various models are discussed and compared regarding the concerned issues with methodologies.

Sanjay Goel in his paper [20] discuss the relationship between anonymity and security thus proving that there is a need of balance between anonymity and security in smart grids. The author then proposes a new idea for designing Internet in a way that security issues are dealt in a better way. The restructuring of Internet seems an interesting idea

as author believes that redesigning and creation of multiple Internets with attempt to have a balance and anonymity can create a difference.

The paper [21] describes the main application systems for a smart city, and discuss various problem issues in constructing a smart city, particularly in China. Though the authors have discussed many hurdles in developing a smart city, but the information security issue has been overlooked and not been discussed by authors specifically.

Suciu et al [22] propose that by defining the platform of cloud computing and IoT properly for a smart city, better security can be achieved. For that, they have proposed a framework for the information that can be automatically be managed by the distributed cloud computing services. The privacy concerns of a common citizen of a smart city also need to be discussed. For example in [23] the privacy issues of citizens of a smart city are analyzed. This includes five dimensions according to the authors: identity privacy, query privacy, location privacy, footprint privacy and owner privacy. They propose a 5D model that addresses these five issues. The authors conclude that by following the model, privacy aware smart city is achievable.

The credibility of a smart city is questioned by Galdon-Clavell and Gemma [24] particularly on various problem areas in the implementation of smart cities, including security and privacy in context of individuals as well as institutions and governments. They describe the smart solutions and elaborate the issues regarding the implementation of such solutions. They propose is that by understanding the problem areas efficiently, smarter cities can be built. The issue of privacy is also discussed in [25] where the authors provide the issues and problem areas in trace analysis and mining for the smart cities. They conclude that though data mining and trace analysis play a key role in smart cities, still it is a challenging task to be done keeping in mind the privacy concerns and usage of limited and relevant data only.

III. SECURITY CONCERNS IN GOVERNANCE, SOCIAL AND ECONOMIC PERSPECTIVE

It is important to identify the core requirements in a smart city in context of information security, as this will help to develop a better understanding of the problem areas. Moreover it will also help to identify the correct and feasible solutions to those problems. As it was discussed in section II, the information security in smart city is mostly dependent on three factors: governance factors, socio-economic factors and the technological factors. These factors influence and identify the information security issues in a smart city. The ICT technologies work together to form a smart city, so not only these implement the whole infrastructure of a smart city and provide solutions to information security problems, but also trigger new concerns and problems regarding security, privacy, protection and resilience. The dependence of socio-economic and governance factors on the technological factors and the relationship of information security with them is shown in Figure 3.

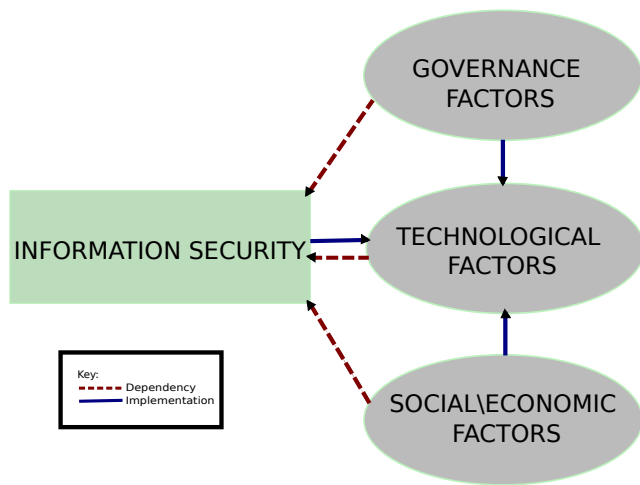


Fig. 3. Relationship between various factors influencing information security

Here it is illustrated that the governance factors and socio economic factors are dependent on the technological factors as these are implemented in a smart city through technology. These factors combine together to influence the information security issues in a smart city, which can again be managed through technology as it is a major driving force in this scenario. So the role of technology in security management and the issues of information security in implementation of all the technology requires the major focus. But in order to identify the core information security requirements, there is need to study the governance, social and economic factors as well. In this section, these factors are analyzed in the light of information security.

A. Governance factors

As discussed in Figure 2, the governance factors that influence and trigger the security issues include utility, health sector, infrastructure, education, transport, etc. The biggest concern for the researchers is that a smart city though promises to provide all the ways to maintain whole infrastructure and management issues, but it's improper implementation can lead us to attacks and frauds. These malicious attacks and frauds can be very harmful to the core purpose of smart cities. In fact they could cause more damage than good they promise.

1) *Need of security testing:* Cesar Cerrudo, chief technology officer at security research firm IOActive Labs [26] have pointed on an important problem that the governance authorities that are the customers of technology firms don't bother to test the security of the systems they buy. Their priority is on testing the functionality of the technology, and they do not bother to focus on the security testing. So the awareness among the authorities to have a genuine concern over security issues is a key requirement.

2) *Threats to critical infrastructures:* The most important and crucial area is the critical infrastructure where changing a single process in a critical system can cause delay or loss of critical services [27]. The main critical infrastructures include health care, industry and telecommunication. The

implementation of critical infrastructures in smart cities is mainly on the IoT and smart grids. So the threats posing to these two technologies should be taken under consideration. Moreover the big data generated by critical systems can pose big problems regarding data integrity and resilience as it need to be properly stored, managed and protected. This is the responsibility of a smart city's critical infrastructure to maintain its security, resilience and data integrity [28]. Therefore, critical infrastructure need protection from malicious attacks that may cause crucial damage to smart cities and their promised services. The health sector is one of the most important type of critical infrastructure as if it is prone to security threats, it can not only cause privacy concerns of a patient [29] but may also pose threats to his life as the critical information can be changed by the attacker. So the health information systems in a smart city should have very secure encryption systems.

3) *Smart mobility security and privacy requirements:* Smart mobility may cause privacy concerns as personal information disclosure could happen in collecting, publishing, and utilizing trace data. Here, localization techniques include GPS, GSM, WiFi, Bluetooth, and RFID because centric servers do not need to know device IDs. [25] Some of the smartphone apps that provide services of smart mobility take mobile data and use trace analysis and data mining techniques. Moreover, The information sent and received from devices used in smart mobility infrastructure may subject to malicious attacks causing wrong traffic reports in satellite navigation systems [28]. Hence, it is clear by analyzing the problems in smart mobility that this domain requires optimized use of ICT technologies keeping in mind the security and privacy threats.

4) *Energy and utility optimization:* Energy and utility services are increasingly relying on smart grids that use bi-directional communication with the users in order to manage the distributed energy efficiently. Cloud computing also plays its role by providing features that are well suited for smart grid software platforms [30]. Data security and privacy remain top concerns for utilities and and the users that is playing a crucial setback in the adoption of smart grids [31]. Moreover the problem increases if it is implemented with clouds. In order to save energy and utilities from frauds and malicious attacks, a proper strategy should be made. This report by Semantic [28] suggests that public key infrastructure (PKI) or managed PKI can be used to tackle security issues in smart grids. The security problems and their solutions in a smart grid will be discussed in detail in section IV.

B. Social and economic factors

In a smart city, peoples' requests for assistance and personal management of social issues, are managed through technology that provides basic platform services for urban planning, emergency and community management, thus turning the smart city into a one-stop service system [21]. Moreover, the smart city promises smarter economic growth as it provides services to enhance the banking, finance and business activities more efficiently. The social and economic factors in a smart

city include communication, individual identity, banking and finance. All of these are a critical part of a smart city and vulnerable to security and privacy issues.

1) *Challenges in smart communication:* The telecommunication sector is part of critical infrastructure of a smart city and is vulnerable to various malicious attacks, viruses, frauds and privacy attacks. As various financial and governance activities are also carried out through telecommunication and wireless networks so the need of security and authentication even increases. Moreover, Machine to machine (M2M) communications also help providing services offered to citizens of a smart city [32]. So the security threats relating to M2M communications should also be taken under consideration. The use of smartphones and tablets has brought new horizons in the communication between the citizens of a smart city. Moreover, it has also led to new threats to their privacy and information security. It is evident that more widely a technology is in use, it is more prone to attacks and viruses. As the smartphones have become very popular in recent years so they have become keen target of the hackers [33]. Wireless networking, bluetooth, cloud computing, IoT, in fact almost all ICT technologies play their part in smart communication and the security concerns relating to them should be considered while developing smart solutions.

2) *Individual Privacy:* The privacy of individuals is a fundamental right that should be guaranteed in a smart city. The individuals of a smart city use various services and communicate with each other through latest technology that is connected using heterogeneous networks and systems, which are the target for hackers who want to intrude in their personal privacy thus depriving them from their personal right [23]. Here the role of social networking should also be considered regarding privacy and information security. The privacy concerns linked with the social networking depend on the level of identification of the provided information by the individual, the receivers and the way it may be used. Those social networking providers that promise not to expose their users identities openly still may provide the required enough data to identify the individual's profile [34].

3) *Banking, finance and business:* The banking, finance and business are all part of smart economy that is a fundamental component of a smart city. Though smart cities promise growth in economy, and better banking and business services, but this component of a smart city is most vulnerable to security threats as it can be attacked for personal financial use. The attackers also intend to sabotage the economy of certain organization, or a whole city.

IV. TECHNOLOGICAL FACTORS

Technology plays key role in making all the promises of a smart city functional. The smart city is solely dependent on technology in order to provide better services to the government and citizens. Smart city promises smarter economic growth, smarter governance and smarter services to the people through integrated and up to date technology. As this seems a very beautiful promise, but the concerns in security, privacy

and data questions to its credibility. In fact, smart cities are not so smart if the concerns in security and privacy are not properly catered. A summarized view of various security threats in a smart city are illustrated in Figure 4.

In this section, some of the core technologies used in developing and maintaining a smart city are discussed and analyzed under security.

A. IoT

The Internet of Things (IoT) incorporate a huge number of distinguished and heterogeneous devices, and gives free access to information for various on-line services for smart cities. IoT plays a gigantic role in developing and maintaining the services of a smart city, hence making the issue of secure information flow a huge task with respect to it. There are various IoT architectures such as urban IoTs [35] that are designed with respect to the needs of a smart city. There are numerous European projects that are made to tackle the research challenges in different aspects of the IoT. One of those is the SmartSantander, a real life experimental testbed for a smart city.

1) *RFID tags:* Radio frequency identification (RFID) tags are being used immensely in the various components of smart city including smart environment [36], industry [37] and mobility [38], etc. It has brought significant benefits in many other areas as well through improving real-time information visibility and traceability. This widespread technology is also prone to many threats and attacks thus making it vulnerable to security [39]. According to [40] the RFID tag is prone to give away sensitive information through unauthorized access, creating problem of data confidentiality and privacy. The problems to data integrity may also occur due to information leakage.

- Abuse of tags [40]

The size of RFID tag is small making it cost efficient. As RFID tag can be embedded into various functions, so the margin for establish security protection system is very little due to its small size. The RFID tags are prone to illegal use by unauthorized users. Moreover the communication between RFID tag and RFID reader is done through a unique Electronic Product Code (EPC), which may be sabotaged by the attacker if they collect the EPC. Another problem is detaching the tag. In this case the transponders, that identify the tagged items in the RFID system, may be associated to some other thing and may be detached from its tag [41].

- Tag killing

The tags are made useless through application of delete or kill commands by the attacker, or through physical destruction [41]. The reader in result cannot identify or read the tag. The DoS attacks are mainly used for this purpose. One important point to know that the tag killing process may also be used for enhancing the security of

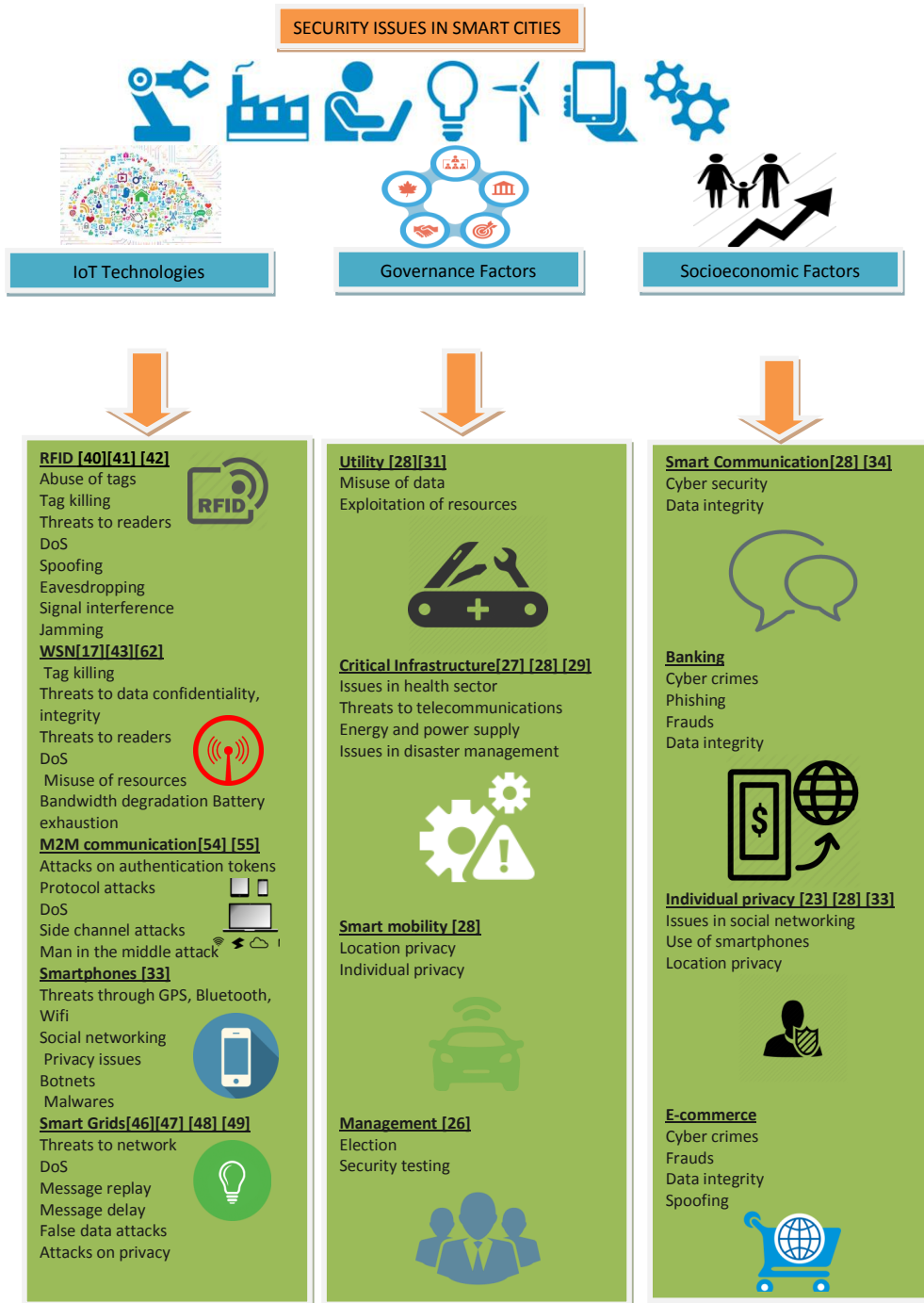


Fig. 4. Security issues in a smart city

the system by addressing privacy issues [40].

- **Tag cloning**
Tag cloning is a process that gains the data from a original tag and makes an unauthorized copy of the captured data on a new tag. The copied data is transferred onto a tag of the attacker.
- **Threats to readers**
One of the big security issue for RFID is sabotage of the reader. If the attacker gets control of the RFID reader, it can be sabotaged thus emitting some electromagnetic waves to destroy the data in the RFID tag [40].
- **Threats to privacy**
The RFID tag can be tracked without the consent of users of a system [40]. Moreover, the uniqueness of tag's EPC makes it easy for hacker to track tags. Thus traceability and identification of the tags causes leakage of private information of the users of the system. So tag tracking is the main issue which harms the individual privacy [42]. Location privacy is also an issue that need to be addressed.
- **Signal interference**
The RFID system adopts two frequency signals: low-frequency signal (125kHz, 225kHz, 13.65MHz) and high-frequency signal (433MHz, 915MHz, 2.45GHz, 5.8GHz) [40], so there is signal interference between the two adjacent band. The attacker can induce signal interference that lead to issues of data integrity in the communication between the reader and tag.
- **Jamming**
Jamming is an attempt to disturb the air interface disturbing the communication. This can effect the integrity of the system communication. This attack is done by powerful transmitters at a significant distance, and by passive means as well such as shielding [41].
- **Threats to communication**
In RFID system the readers and tags communicate through wireless communication. The availability of the wireless signals, makes it easy for an attacker to search, manipulate, and jam wireless signals [40]. So encryption and authentication are crucial in order to protect the wireless transmission between the RFID readers and RFID tags. Attacks on wireless communications include active attacks and passive attacks [43].
Wired communication between the RFID readers and the middle-ware system, through the Internet also has its security concerns. The need to ensure data confidentiality and integrity is very important.
- **Denial of Service (DoS)**
An important type of attacks on RFID system are the Denial of Service (DoS) attacks. The purpose of the DoS is to disable the system making it useless. Device that broadcasts the radio signals can be used for malicious purposes and can disrupt or block the working of a RFID reader. There are many possibilities to perform DoS attacks including the possibility of placing the information in Faraday's cage [44].
- **Spoofing**
Spoofing is a security threat in which tag data is duplicated and communicated to a reader. This occurs in case when the security protocol used in the RFID channel is revealed [41]. For instance, in case of an electronic seal, the e-seal information is transmitted to the reader from some other source that is the duplicate e-seal.
- **Software attacks**
Software attacks are the most well known attacks including viruses, buffer overflows and worms injected in the RFID system to effect its functionality. These are the coded malicious programs aiming to infect and disturb the system making its performance slow or none.
- **Cryptanalysis and eavesdropping**
Eavesdropping and cryptanalysis are the most frequent and talked about attacks on a RFID system. As cryptanalysis is getting stronger side by side with the cryptographic techniques so the need of better cryptography techniques is more evident than ever. The attacks include man in the middle attack, chosen plain text and chosen cipher-text attacks, and known plain-text and known cipher-text attacks. RFID tag emits data that is usually a unique identifier. When the data is communicated to RFID reader, it is prone to the risk of eavesdropping. In this particular case, eavesdropping is done by the attacker by catching data with a reader one for the correct tag family and frequency during a tag is being read by authorized reader [41].
- **Suggestions and techniques for better security**
It is important to discuss various techniques and strategies that may play part in better security performance of RFID in a smart city. Privacy protection is an important need and right of the citizens and as discussed previously, that tag killing may play role in privacy protection but this also may lead to loss data permanently. A better option is tag sleeping. When the tag does not need to be read, it is put to sleep temporarily [45]. There is another concept of tag blocking and selective blocking [40]. Other techniques include relabeling approach, re-encryption and minimalist cryptography [45].
The interference problems in the RFID system can be dealt by data coding, multiple re transmission and data integrity check.
Hash-Lock and Hash Link techniques are also important as they provide better authentication. There are other

authentication techniques based on hash such as ID exchange and distributed RFID challenge/answer authentication [39].

The authentication supported by hash requires the symmetric key distribution. So it is evident that protecting the shared key is essential in the procedure of authentication. The shared key is saved in the tag of the RFID.

2) *Smart grids*: Smart grids play core part in a smart city regarding energy deployment and management. These are actually communicating instruments including sensors and communication networks that help in communicating data in real time [18]. When the data is shared in real time scenario among power generator, distributed resources, the service provider and the users, any information that is prone to attacks, that would take the system to failure. This will unfortunately lead to user's uncertainty and discontentment with the system. Through literature review [46][47] [48], we classify main threats that should be kept under consideration while constructing and deploying a smart grid as follows:

- Threats to network availability
The most vindictive attacks that target the network availability are the denial-of-service (DoS) attacks. These attacks attempt to delay, block or corrupt services by abusing information in the smart grid. It is evident [46] that mostly of the smart grid use IP based protocols. As TCP/IP is open to DoS attacks, so such attacks are becoming huge problem in a smart grid.
- Threats to data Integrity
In case of smart grids particularly, data integrity is needed in case of data like sensor values and control commands. The main objective of data integrity includes defense mechanism for information modification through various means such as message injection, message replay, and message delay on the network. Threats to data integrity cause many issues like infrastructure or people of the smart city may be harmed. The main goal of the integrity attacks is either customers information or network operation information. These attacks tend to abuse critical data in a smart grid.
False data [49] injection attacks are very powerful attacks against the state estimation in the power grid. In this case the hacker takes advantage of the configuration of a power system to launch malicious attacks by infusing wrong data to the monitoring center questioning data integrity.
- Threats to information privacy
Privacy of smart grid communication systems is important as it is the main concern and right of the consumers. Smart grid communications should take care of the privacy during communication in real time.

- Threats to devices
Smart meters are prone to physical attacks like battery change, removal, and modification. Moreover, functions including remote connect/disconnect meters and outage reporting may be used by unwarranted third parties.
- Proposed solutions for smart grids
According to literature [48] [47] the possible solutions for threats to devices in a smart grid include ensuring the integrity of meter data and maintaining meter securely. Moreover for wireless networking, TCP/IP for smart grid networks is a better choice for Internet. Moreover the M2M solutions prosed by IEEE including 802.11i, 802.16e, and 3GPP LTE should be used. For sensor networks various encryption standards should be adopted for authentication. Public key infrastructure (PKI) and managed PKI are also a good choice for smart grids security.

3) *Biometrics*: Biometrics is an automated recognition of a person through unique behavioral and biological characteristics. There are two main types of biometric characteristics: physiological and behavioral. Both are acquired by applying proper sensors and distinctive features are taken in use to get a biometric template in authentication process [50]. In fact, it is generally thought that any other substitute to biometrics for identification in integrated security applications does not exist.

Biometrics is said to play a key role in information security issues in a smart city. According to Bill Maheu, who is senior director for Qualcomm Government Technologies, every year 3.7 trillion dollars are lost to global frauds, which can be solved sufficiently by implementing biometrics [51]. Biometrics in fact can make various components of a smart city secure with respect to frauds and malicious attacks[51]:

- Health
- Education
- Institution
- Utility
- Patrol and security

4) *Smartphones*: Smart phones are one of the core component of IoT infrastructure in a smart city as they give access to various services and smart applications that help in maintaining and developing a better smart city. These are also the main source of people's role in a smart city. Smartphones have become immensely popular in recent years, making them an attractive thing to be attacked by hackers and viruses. The main security threats in smartphones are illustrated as under [33]:

- Malicious smart applications
In some cases, hackers upload vindictive applications to application marketplaces for iphone and android devices. Such applications may also be present in Internet. Such

smart applications can infect the smart-phone devices and may cause many security and information privacy issues.

- Botnets
Botnet is formed by attackers by contaminating multiple devices with malwares that victimize broadly through the e-mail attachments or from smart applications or malicious websites.
- Spyware
Attackers may misuse the available spyware to hijack a smart-phone, allowing them to locate and hear calls, check messages and e-mails, and track a user's location through GPS updates. So the user's privacy is totally sabotaged in this way.
- Threats from bluetooth
Wireless devices show their existence and permit unrequested connections and in case the end users do not know how to manage and configure their bluetooth settings properly.
- Location and GPS
The location privacy of individuals can be sabotaged by the attackers by various attempts on the GPS feature provided in the smart-phone.
- Threats through WiFi
Attacker on a smartphone can catch information during the communication between smartphones and Wi-Fi hotspots. The main problem is extreme vulnerability of the Wifi hotspot architecture where there is no encryption to protect transmitted data
- Threats in social networks
As smartphone usage has gone through a major boost, so has mobile social networking flourished. People give a lot of personal information and time to social networks. Many links on social networking websites and applications may effectively spread malicious malware. Moreover individual privacy is also prone to major attacks on social networking websites.

Literature [52] proposes various solutions to threats to smartphones, illustrated as under:

- Anti Viruses and firewalls
Anti-viruses for smartphones scan every data including files, memory, SMS, MMS, emails etc. These solutions can help in preventing the malicious malwares. Moreover the threat of access to phishing site is also controlled. The firewalls on the other hand block connections that are unauthorized preventing the network attacks.
- Secure API

The secure APIs have the cryptography properties helping program and application developers for implementation of secure functionality.

- Authentication and access control
The process of authentication process can prevent unauthorized use of smartphone devices. Moreover, access control is also important as it limits the access of malicious processes and attacker to resources and services.
- Filters
Filters include SPAM filters that blocks SPAM MMS, SMS, emails and calls from unknown origins.
- Cellular M2M solutions
Cellular Smart City M2M technology advancements are tacking momentum with time, and good number of organizations envision the future IoT applications to run over cellular networks. There are specific M2M solutions for smartphones [7]:
 - ETSI M2M
It is made by different manufacturers and it provides the framework, requirements and architecture, for the technologies like 3GPP that can be used to populate the developed architecture.
 - 3GPP LTE-M
It is OFDM based LTE making cellular M2M has suddenly become of interest for a significant target market.

5) *M2M communication*: Machine to machine (M2M) communications promise dramatic achievements in the applications and services offered to citizens, making smart city a reality [32]. Machine to machine protocols are used for communication fix the rules of engagement for at least two nodes of a network. Internet Protocol (IP) has become the standard for such communication purposes. Examples of protocols that can be used for communication are: ISA 100A, link Layer, Wireless HART, IPv6 and ZigBee [53]. IPv6 plays a gigantic role in the IoT. The plus of IPv6 is that it fulfills the demands of portability and helps variant systems to work together. According to [54] [55] the main security concerns in M2M communications include:

- Physical Attacks
These attacks include using modified softwares for the purpose of fraud. The main breaches that occur due to these attacks are in integrity of data and M2M softwares.
- Attacks on authentication tokens
The threats include physical attacks as discussed above and side-channel attacks. The authentication tokens can also be cloned for malicious purposes.

- Configuration Attacks
The example of configuration attacks include malicious software updates configuration changes that lead to fraud. Moreover, mis-configuration by the user may also occur.
- Protocol Attacks
The protocol attacks are mainly designed against the devices. For example: man-in-the-middle attacks, DoS attacks, and attacks on OAM and its traffic.
- Threats in network security
These attacks mainly target mobile networks. The examples of such threats include impersonation of devices and traffic tunneling between them. Moreover, mis-configuration of the firewall in the devices is also a serious network security breach. The DoS attacks on the network also pose a major problem.
- Breaches in privacy
Privacy is a huge concern of the individuals of a smart city as it is a basic human right. But it becomes very difficult to take care of the privacy of citizens through M2M communications as the ways in which data collection, mining, and provisioning is accomplished are totally different from those that we now know and there are a huge amount of occasions for personal data to be collected.
Eavesdropping can cause major concerns over individual privacy and data integrity. Moreover, masquerading as other user's devices is also a gigantic security problem.

There are various M2M standard solutions available to establish a smart city with respect to security [7]:

- IEEE Standards Solutions
The IEEE provides standard mechanisms for the physical (PHY) and medium access control (MAC) layers which are useful in implementation of a smart city. There exist three families that can provide low-power and short-range IoT operation for a smart city [7].
IEEE 802.15.4:
Important characteristics include real-time quality by guarantying time slots, collision dodging through CSMA/CA and merged assistance for secure communication. Moreover, the devices include power management functions for example, energy detection and link quality. IEEE 802.15.1 is used in Bluetooth.
IEEE 802.15.11 This technology is provided from WiFi Alliance, a trade association in control of the certifying products if they adjust to particular standards of interpretability. The Wifi Protected Access (WPA) [56] is a security protocol that has become the regulation for providing security .11 networks. Here by using an already shared encryption key (PSK) or digital certificates, the WPA algorithm Temporal Key Integrity Protocol (TKIP) encrypts

information providing authentication to the particular networks. The WPA algorithm (TKIP) further improved upon to the new WPA2 [57] [56] that utilize more securer encryption algorithm that is Advanced Encryption Standard (AES). Moreover this protocol also uses better and advanced key distribution techniques, which help in improved session security to avoid eavesdropping.

6) *SmartSantander: An IoT testbed for a smart city*: This facility is an IoT infrastructure deployment in Santander, Spain [58]. This unique arrangement contains more than 2000 IoT devices deployed in an urban scenario [59]. This project aims at developing an architecture of a smart city through of IoT by a twofold approach [60]:

i. Experimentation support:

It provides the platform for the research community to get results for their experimental research in a real life scenario. It is an amazing opportunity for the researchers that they can allocate and manage the required IoT resources to run their experiments.

ii. Service provision:

SmartSantander provides the services promised by a smart city in accordance with the needs and requirements of people described in form of use cases.

In SmartSantander a detailed network deployment is done on basis of the use cases oriented to define all the services and technological support needed over them. Moreover, many applications for smartphone operating systems are developed in order to add in the people's role in this environment of sensing and connecting. SmartSantander has a 3-tiered architecture: IoT nodes/End points, IoT nodes/Repeaters and Gateways [58]. Endpoints and repeaters are used for sensing various parameters, but the main difference is that endpoints don't forward the information, and the repeaters send the information to the required places. Gateway gathers all the information sent. The interface for the communication used in this scenario is IEEE 802.15.4 interface [61]. This architecture forms into wireless sensor networks (WSN) for the information sharing. There are various security concerns for a WSN, categorized as under [62]:

- Attack on data confidentiality
There are various crypt-analysis attacks that cause threats to data confidentiality on a WSN during information sending and receiving.
- Threats to data integrity
The data may be abused, changed and modified due to various attacks.
- Misuse of resources
Another problem that arises in the scenario of a smart city is the misuse of the IoT devices for malicious purposes.
- Bandwidth degradation
Bandwidth degradation may effect the information flow and prone to abuse of data.
- Battery or resource exhaustion
The malicious attacks infect the IoT devices making their battery life and resources poor.

- Unauthorized Access
An attacker can access to WSN resources to obtain the keys for malicious purposes.
- Threats to Authentication
Authentication service ensures security of a system by restraining any attacker from entering the system. In WSN, the attacker may get hold of the user id and password hence getting over the authentication process. In this way attackers can get hold of all the services provided by the WSN. So it should be made sure that SmartSantander has a foolproof authentication system.
- DoS
The denial of service attacks are a huge problem in WSNs as these attack suspend the services of whole system.

Following goals in SmartSantander are reached regarding security of information in IoT infrastructure:

- Data confidentiality
Cryptographic techniques are used in order to ensure data confidentiality. The literature [63] compares various encryption techniques that makes it easy to choose the technique better for the system:
PKI distribution mechanism provides the best security and on the other hand, symmetric cryptography mechanism requires significantly less computational complexity on the node but higher memory requirements. The ID-based encryption mechanisms provide asymmetric cryptography which is cost effective in terms of memory as well, but it is more complex to maintain. A qualitative analysis on the comparison of these schemes is given in [63] which is modified into quantitative analysis in Figure 5.

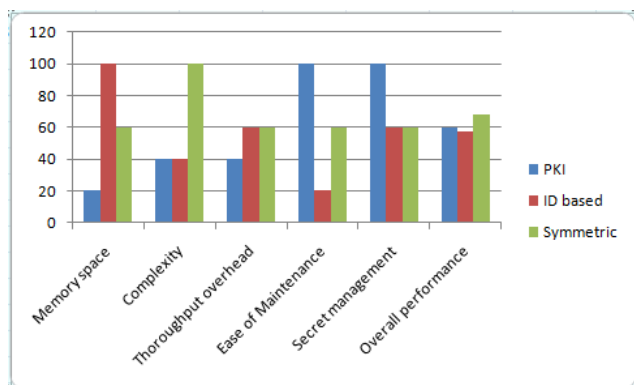


Fig. 5. PERFORMANCE ANALYSIS OF VARIOUS CRYPTOGRAPHY TECHNIQUES IN PERCENTAGE [63]

- Integrity
For data integrity Cyclic Redundancy Code (CRC) or a Message Authentication Code (MAC) is used in this scenario.
- Authentication
Here the message authentication code (MAC) is used for symmetric cryptography. A digital signature for asymmetric cryptography may also be used.

- No repudiation
For no repudiation, secure protocol is used with acknowledgment.
- Freshness
nonce is a random number that is used only once for a given time. It is used inside the secure protocol for achieving freshness.

The SmartSantander is setting position at the assemblage between providing different types of services and the deployment of a huge experimental testbed. This includes many stakeholders, including citizens, experimentalists, government and authorities. It is an ideal testbed to check and manage the security issues for a smart city.

V. COMPARATIVE ANALYSIS

As the conception of smart cities is still under evolution, the need to identify the core threats of information security in various technologies is important. The security of information in a smart city has been interest of researchers because, in order to guarantee the provision of all the services in a smart city, the information security issues must be catered properly. Smart city involves various services in different components including mobility, communication and critical infrastructure. The need to achieve secure information sharing through the technology being used is crucial. The measures for secure information flow can be taken by identifying the problem areas and threats to security. So the purpose of research on information security in a smart city is that by understanding the problem areas and available solutions efficiently, smarter cities can be deployed and maintained. The IoT has been the key interest of the researchers as it is the core technology on which the smart cities are being developed and maintained. Through literature review, various security breaches along with their existing solutions have been identified and illustrated in Table II. The security threats and solutions are illustrated with reference to the papers reviewed. This summarized review will help learning the core security threats and available solutions that are being discussed in latest research.

VI. CONCLUSIONS

The issue of information security in a smart city ranges over on a variety of aspects including social, economic, structural and governance factors. This paper provides a comprehensive overview on the threats, vulnerabilities and available solutions in order to facilitate much needed research in addressing the problem areas in smart city security. The technological factors are pivotal in deployment and maintenance of a smart city. In fact, technology is the driving force that establishes and maintains a smart city to deliver the promised services. Nonetheless, the significance of studying security of a smart city with regards to governance and socioeconomic factors help in identifying security concerns and requirements of the concerned stakeholders. Moreover, this practice also facilitates in identifying risks and vulnerabilities in plausible manner. It is evident that security is the weakest link in the implementation

IoT Technologies	Application in smart city	Security threats	Available solutions	Related literature
RFID	Industry, environment utility, mobility, infrastructure	Threats to readers, threats to privacy, abuse of tags, tag killing, signal interference, jamming, threats to communication, DoS, spoofing, software attacks, cryptanalysis and eavesdropping	Selective blocking, minimalist cryptography, tag sleeping, tag blocking re encryption, data coding, multiple retransmission, hash lock, hash link, SKD	[36] [37] [38] [41] [40] [39] [42] [45]
WSN	Environment, utility, Health, energy, infrastructure, governance and commerce	DoS attacks on data confidentiality, threats to data integrity, Misuse of resources' bandwidth degradation, battery exhaustion, unauthorized access	CRC, MAC, PKI, symmetric cryptography, and light weight asymmetric cryptography digital signatures, secure protocols	[17] [43] [62]
M2M communication	Smart communication, governance, health, critical infrastructure, education	Physical Attacks, Attacks on authentication tokens, Protocol Attacks, man-in-the-middle attack, DoS attacks, attacks on privacy, side-channel attacks, fraudulent software updates	IEEE standard solutions: 802.15.4, 802.15.1, 802.15.11	[54] [55] [32] [7]
Smart grids	Smart energy, power, utility critical infrastructure smart Appliances and smart homes	threats to network availability, DoS, breaches in data integrity, message replay, message delay, false data attacks, attacks on privacy,	Public key infrastructure (PKI) or managed PKI, AES for sensor networks, protected routing protocols, 802.11i, 802.16e, 3GPPLTE - M	[18] [28] [46] [47]
Smartphones	Smart communication, Smart mobility, Entertainment,	Malicious smart applications, bot-nets, spy-wares, threats from Bluetooth, Location privacy and GPS, threats through WiFi, threats in social networking, privacy issues	Antivirus, firewalls, secure APIs, authentication and access control filters, ETSI M2M, 3GPPLTE - M	[33] [52]
Biometrics	Health, atrol and security, education, institutions, corporate sector, and utility	N.A	N.A	[50]

TABLE I
INFORMATION SECURITY ANALYSIS OF VARIOUS TECHNOLOGIES USED IN A SMART CITY

of a smart city. The serious repercussions of flawed security may undo the value of promised features and services of a smart city. The excellent functionality of smart solutions would have no value if the system has security loopholes. The smart solution manufacturers and decision making authorities, both are stakeholders and responsible for ensuring the security of a deployed system.

REFERENCES

- [1] B. Bowerman, J. Braverman, J. Taylor, H. Todosow, and U. Von Wimmersperg, "The vision of a smart city," in *2nd International Life Extension Technology Workshop, Paris*, 2000.
- [2] K. R. Kunzmann, "Smart cities: A new paradigm of urban development," *Crios*, vol. 4, no. 1, pp. 9–20, 2014.
- [3] S. Dirks, C. Gurdgiev, and M. Keeling, "Smarter cities for smarter growth: How cities can optimize their systems for the talent-based economy," *IBM Institute for Business Value*, 2010.
- [4] "Top five smart cities in the world," <http://www.forbes.com/sites/peterhigh/2015/03/09/the-top-five-smart-cities-in-the-world/>, accessed: 2015-04-03.
- [5] N. Komninos, H. Schaffers, and M. Pallot, "Developing a policy roadmap for smart cities and the future internet," in *eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation*. IMC International Information Management Corporation, 2011.
- [6] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris, "Smarter cities and their innovation challenges," *Computer*, vol. 44, no. 6, pp. 32–39, 2011.
- [7] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Security and privacy in your smart city," in *Proceedings of the Barcelona Smart Cities Congress*, 2011.

- [8] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014.
- [9] R. Anderson, "Why information security is hard-an economic perspective," in *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*. IEEE, 2001, pp. 358–365.
- [10] "Cisco intelligent urbanisation," <http://www.urenio.org/2009/03/13/cisco-intelligent-urbanisation/>, accessed: 2015-04-22.
- [11] M. Dohler, I. Vilajosana, X. Vilajosana, and J. LLoa, "Smart cities: An action plan," in *Barcelona Smart Cities Congress*, 2011.
- [12] R. Kitchin, "The real-time city? big data and smart urbanism," *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014.
- [13] C. Schmitt, "Security and privacy in the era of big data," 2014.
- [14] J.-M. Bohli, P. Langendörfer, and A. F. Skarmeta, "Security and privacy challenge in data aggregation for the iot in smart cities," *River Publisher Series in Cmounications*, p. 225, 2013.
- [15] Z. Khan, Z. Pervez, and A. Ghafoor, "Towards cloud based smart cities data security and privacy management," 2014.
- [16] M. Sen, A. Dutt, S. Agarwal, and A. Nath, "Issues of privacy and security in the role of software in smart cities," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*. IEEE, 2013, pp. 518–523.
- [17] M. Wen, J. Lei, and Z. Bi, "Sse: A secure searchable encryption scheme for urban sensing and querying," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.
- [18] C. Clastres, "Smart grids: Another step towards competition, energy security and climate change objectives," *Energy Policy*, vol. 39, no. 9, pp. 5399–5408, 2011.
- [19] A. P. A. Ling and M. Masao, "Selection of model in developing information security criteria on smart grid security system," in *Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on*. IEEE, 2011, pp. 91–98.
- [20] S. Goel, "Anonymity vs. security: The right balance for the smart grid," *Communications of the Association for Information Systems*, vol. 36, no. 1, p. 2, 2015.
- [21] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *Electronics, Communications and Control (ICECC), 2011 International Conference on*. IEEE, 2011, pp. 1028–1031.
- [22] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart cities built on resilient cloud computing and secure internet of things," in *Control Systems and Computer Science (CSCS), 2013 19th International Conference on*. IEEE, 2013, pp. 513–518.
- [23] A. Martinez-Balleste, P. A. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *Communications Magazine, IEEE*, vol. 51, no. 6, pp. 136–141, 2013.
- [24] G. Galdon-Clavell, "(not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments," *Science and Public Policy*, vol. 40, no. 6, pp. 717–723, 2013.
- [25] W. Z. S. L. Gang Pan, Guande Qi and Z. Wu, "Trace analysis and mining for smart cities: issues, methods, and applications," *IEEE Communications Magazine*, vol. 121, 2013.
- [26] "Why smart cities need to get wise to security and fast," <http://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs>, accessed: 2015-05-14.
- [27] N. Abouzakhar, "Critical infrastructure cybersecurity: A review of recent threats and violations," 2013.
- [28] Semantic, "Transformational smart cities: cyber security and resilience," 2010.
- [29] A. Solanas, C. Patsakis, M. Conti, I. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. Di Pietro, D. N. Perrea *et al.*, "Smart health: a context-aware health paradigm within smart cities," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 74–81, 2014.
- [30] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An analysis of security and privacy issues in smart grid software architectures on clouds," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*. IEEE, 2011, pp. 582–589.
- [31] J. Polonetsky and C. Wolf, "How privacy (or lack of it) could sabotage the grid," *Smart grid news*, 2009.
- [32] J. Wan, D. Li, C. Zou, and K. Zhou, "M2m communications for smart city: An event-based architecture," in *Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on*. IEEE, 2012, pp. 895–900.
- [33] N. Leavitt, "Mobile security: finally a serious problem?" *Computer*, vol. 44, no. 6, pp. 11–14, 2011.
- [34] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 2005, pp. 71–80.
- [35] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, 2014.
- [36] A. Luvisi and G. Lorenzini, "Rfid-plants in the smart city: Applications and outlook for urban green management," *Urban Forestry & Urban Greening*, vol. 13, no. 4, pp. 630–637, 2014.
- [37] X. Zhu, S. K. Mukhopadhyay, and H. Kurata, "A review of rfid technology and its managerial applications in different industries," *Journal of Engineering and Technology Management*, vol. 29, no. 1, pp. 152–167, 2012.
- [38] A. Ramos, A. Lazaro, and D. Girbau, "Multi-sensor uwb time-coded rfid tags for smart cities applications," in *European Microwave Conference (EuMC), 2014 44th*. IEEE, 2014, pp. 259–262.
- [39] S. Xiwen, "Study on security issue of internet of things based on rfid," in *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*. IEEE, 2012, pp. 566–569.
- [40] X. Nie and X. Zhong, "Security in the internet of things based on rfid: Issues and current countermeasures," in *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*. Atlantis Press, 2013.
- [41] S. Mohite, G. Kulkarni, and R. Sutar, "Rfid security issues," in *International Journal of Engineering Research and Technology*, vol. 2, no. 9 (September-2013). ESRSA Publications, 2013.
- [42] R. Aggarwal and M. L. Das, "Rfid security in the context of internet of things," in *Proceedings of the First International Conference on Security of Internet of Things*. ACM, 2012, pp. 51–56.
- [43] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for internet of things (iot)," in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*. IEEE, 2011, pp. 1–5.
- [44] Q. Xiao, C. Boulet, and T. Gibbons, "Rfid security issues in military supply chains," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*. IEEE, 2007, pp. 599–605.
- [45] R. Pateriya and S. Sharma, "The evolution of rfid security and privacy: a research survey," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*. IEEE, 2011, pp. 115–119.
- [46] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010*. IEEE, 2010, pp. 1830–1835.
- [47] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 998–1010, 2012.
- [48] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, 2012.
- [49] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.
- [50] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, pp. 1–25, 2011.
- [51] "How connectivity and biometrics are making cities safer," <http://smartcitiescouncil.com/article/how-connectivity-and-biometrics-are-making-cities-safer>, accessed: 2015-05-31.
- [52] W. Jeon, J. Kim, Y. Lee, and D. Won, "A practical analysis of smartphone security," in *Human Interface and the Management of Information. Interacting with Information*. Springer, 2011, pp. 311–320.
- [53] N. Dlodlo, T. Foko, P. Mvelase, and S. Mathaba, "The state of affairs in internet of things research." Academic Conferences International Ltd, 2012.
- [54] C. Hongsong, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in *Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on*. IEEE, 2011, pp. 286–290.

- [55] D. Jiang and C. ShiWei, "A study of information security for m2m of iot," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 3. IEEE, 2010, pp. V3–576.
- [56] S. Bai, Y. Wang, and Z. Xue, "Research on security of wpa/wpa2 protocol," *Information Security and Communications Privacy*, vol. 1, pp. 106–108, 2012.
- [57] J.-C. Chen, M.-C. Jiang, and Y.-w. Liu, "Wireless lan security and ieee 802.11 i," *Wireless Communications, IEEE*, vol. 12, no. 1, pp. 27–36, 2005.
- [58] "Smart santander," <http://www.fed4fire.eu/smart-santander/>, accessed: 2015-05-22.
- [59] L. Sanchez, J. Galache, V. Gutierrez, J. Hernandez, J. Bernat, A. Gluhak, T. Garcia, P. Cunningham, and M. Cunningham, "Smartsantander: The meeting point between future internet research and experimentation and the smart cities ist future networks & mobile summit poland," in *Conference Proceedings Cunningham, P. and Cunningham, M.(Eds) IIMC International Information Management Corporation, Warsaw, Poland*, 2011.
- [60] A. G. Jose, V. Gutiérrez, J. R. Santana, L. Sánchez, P. Sotres, J. Casanueva, and L. Muñoz, "Smartsantander: A joint service provision facility and experimentation-oriented testbed, within a smart city environment," 2013.
- [61] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis *et al.*, "Smart-santander: Iot experimentation over a smart city testbed," *Computer Networks*, vol. 61, pp. 217–238, 2014.
- [62] C. Hennebert, "Internet of things: Security management for large scale deployment in the city," 2013.
- [63] C. Hennebert and V. Berg, "A framework of deployment strategy for hierarchical wsn security management," in *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2012, pp. 310–318.