Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April - 2017

Protecting Smart Cities in India Using Blockchain Technology

Prof. R.R.Papalkar[1] Prof. P.R.Nerkar[2] Prof. N.M. Shivratriwar [3] Prof. S.N. Sarda[4] Prof. A.S.Mahalle

[1]*Information Technology Department, PRMIT & R, Badnera*
[2]*Information Technology Department, PRMIT & R, Badnera*
[3]*Information Technology Department, PRMIT & R, Badnera*
[4]*Information Technology Department, PRMIT & R, Badnera*
[5]*Information Technology Department, PRMIT & R, Badnera*

Abstract:

IoT play an important role for making smart cities.IoT application generate voluminous heterogeneous data, due to this it is typical to secure such data across the globe. In this paper we are going to address the approach to protect multiple IoT based application generated data using novel technique known as block chain technology. As we know Indian government mostly focus is on smart city, for this purposed it required IoT Technology. A smart city uses information technology to assimilate and manage physical, social, and business infrastructures in order to provide better services to its residents while ensuring efficient and optimal utilization of available resources. With the proliferation of technologies such as Internet of Things (IoT), cloud computing, and interconnected networks, smart cities can deliver innovative solutions and more direct interaction and collaboration between citizens and the local government. This paper proposes a security framework that integrates the blockchain technology with smart devices to provide a secure communication platform in a smart city.

Keywords: IoT, Cloud Platform, Blackchain technology

I. INTRODUCTION

Currently over half of the world's population live in urban areas, and this is forecasted by Cisco to rise to 60% by 2050. The steadily rising urban populations are placing huge strain on the world's cities, as resources are expected to meet the demand of more and more inhabitants. Supervision the anxiety on urban resources with the status quo is becomingly increasingly impossible, and so attention has turned to developing new systems that address the challenge of megacities. Combining cities with smart tech solutions has become the prospect of today's digital age. Aiming to bring the city into the age of the 'Fourth Industrial Revolution', companies are outfitting the Internet of Things (IoT) and big data solutions to their ordinary running. This is the 'smart city' concept – a promise to combine a city's physical infrastructure and services with the latest technological aids. As the IoT has become ever more bulbous in everyday life, the concept of the smart city has began to grow[1]. To survive with these crises, cities are focusing on modern technologies as well as aiming to reduce costs, use resources optimally, and create more comfortable urban environment. The significant advancements in IoTs and wireless communications have made it easy to interconnect a range of devices and enable them to transmit data universally even from secluded locations. However, these systems are more instrumented with open data such as locations, personal and financial information, and therefore, must be capable to defend against security attacks. The Kaspersky Lab shows that smart terminals such as bicycle rental terminals, self-service machines, and information kiosks have a number of security flaws. These devices can be oppressed by the cybercriminals and they may get access to personal and financial information of the users. It is also worth noting that implementation of traditional security mechanisms into a city's critical infrastructure to make it smarter has failed. Thus, new solutions based on the nature of the data (private or public) and communication platforms have to be developed to provide privacy, integrity, and data confidentiality. This paper proposes a security framework based on block chain technology which allows to communicate the entities in a smart city without compromising privacy and security [2]. IoTs Application generate huge data and for processing such data it require cloud platform but it is to difficult to succeed identity across distributed platform in [3] they provide approach to manage identity of user across the globe.

II. SMART CITY ELEMENTS

The Smart City standard development elements are forming the inclusive smart city framework. They need to be pondered starting from the infrastructure preparation stage. Old edifice of the utilities has to be re-studied and in this context three elements have to be taking into account to provide "smartness" [4]:

- Hardware/Software elements: The smart concept is embodied in transmitting and receiving the data using communication protocols from and to the network element (asset). The asset's data sending and receiving is the base of monitoring and controlling the functional operational framework needed for smartly network assets managing. The most practical way is to embed the essential hardware (operational sensors) and software during the design phase.
- Databases elements: The second element for creating Smart City is to build up the proper database that would
  reveal the existing/proposed infrastructure networks. The database has to imitate the completeness of the network chattels as well as the dependability and data integrity. The assets positional accuracy is extremely important aspect that has to be taken care for all of network assets which will reflect the physical reality of the system that would be the base for all network spatial analysis actions. On the other hand the database has to cope the data communication protocols between the chattels programmable logic controllers and the data servers.
- Management System elements: After concocting the database that reveals the physical certainty of the assets/ network components. The third element is to build up the most practical and proficient Management System (MS). The MS has to have an automation work frame that has to be vigorously functioned in order to save energy and accordingly condense the running cost. The magnitude of energy saving produced due to the economical automation and comfortable/easiness operation reflects the level of the elegance that the building has.

III. SMART CITY ARCHITECTURE

In India for smart city main important objective is on smart city architecture it provide all aspects those required for implementation of information services for nurture perilous infrastructures and organize the Smart City data-bases. The Smart City architecture, which is mainstream applied in five cities in the world (Malta, Dubai Internet City, Dubai Media City, Dubai Festival City and Kochi), has four principle unites that cover almost all the networks, processes, applications and several associated activities in different drifts[5].

These four unites are:

- *Application unit:* Applications are related to physical assets monitoring using fathoming technologies such as satellite imagery; WS, M2M and embedded networks; aerial mapping; GPS/GNSS reference station and laser/LIDAR technologies. These technologies permits to operate the following applications: city security processes, industrial monitoring, building management system for building's automation, Closed Circuit Television (CCTV) for several types of monitoring and controlling, Community Access Television (CATV), Geographic Information System (GIS) for inclusive conception, analysis and data banking.
- *Information unit:* The city information unit is very crucial in order to appreciate the function of using the mentioned applications. The mainstream of the information units that used to communicate the city applications are as follow: user information for monitoring the public behavior; document information for enhanced statistical and feasibility studies; industry information for monitoring the market demand, inflation and others; business information for more commerce and financial analysis; revenue information for better understanding of the market cash flow and daily business activities; rotation information for treating the new materialized business cases.
- *Management unit:* The third principle component is process management. It is really important because it defines the relationship, rules, strategies and policies between the city applications and related information unites. The administration has to partake in the following parties which will demonstrate the overall city modules.
- *Integration communication protocol unit*: The handier of this bustle city cycle is the connection between these three principle components. The connectors (integration communication protocols) might be utilizing the orthodox wiring network or using fiber optic cables for the systems that depending on the physical network connectivity concept. Wireless, Bluetooth, Wi-Fi and different GSM technologies are going to be mature in the near future, which make them more practical and realistic solutions for data sharing and information altercation processes. In addition of them, also M2M and embedded network will be implemented for low-power networks; they will be key actors for actual monitoring and networking communication in perilous parts of Smart City (e.g.: Smart Grid). More in details, smart nodes are responsible to produce and/or to munch (query/subscribe) notifications of events (application unit). Statements elaborate the events as observed locally by smart nodes and the decision to publish a notification is a core part of the publisher smart nodes internal logic. If is needed, notifications are simply stored in data-bases (information unit), otherwise, for example, if they are high priority notifications, they are sent to the decision maker unit (management unit). The management unit will elaborate them and the output result can be a announcement directed to the information unit or a query directed to both information and application units. The assistance between nodes, data-base, and decision-makers is

possible thanks the integration communication protocols unit. A set of appropriate security policies permits the system to control the notifications only to the smart nodes that have vowed with appropriate credentials and protect the sensible information with advanced security techniques.

IV. SECURITY THREATS

Due to the heterogeneous nature of resource constrained devices, a smart city is susceptible to a number of security attacks. It is imperative to recognize those coercions and their possible consequences in order to design an effective solution. A number of research has been conducted in this field such as Open Web Application Security Project (OWASP) enlisting common security attacks, Computer Emergency Response Teams (CERT) providing graphical representation of potential vulnerabilities, G-Cloud presenting a series of Cloud Computer Service Provider (CCSP) requirements [6], [7], [8]. The following threat categories are identified for the smart cities: i) Threats on Availability- are concerned with the (unofficial) upholding of resources, ii) Threats on Integrity- include unauthorized change to data such as manipulation and corruption of information, iii) Threats on Confidentiality- include disclose of sensitive information by unauthorized entity, iv) Threats on Authenticity- are concerned with gaining unauthorized access to resource and sensitive information, and v) Threats on Accountability include denial of transmission or reception of a message by the corresponding entity.

- SECURITY IN SMART GRID

As part of the development of Smart City, control systems have to become more sophisticated, allowing better control and higher reliability. Smart City will require higher degrees of network connectivity to support new sophisticated features. This higher degree of connectivity also has the potential to open up new vulnerabilities. For this reason, one of the biggest challenges facing Smart City development is related to Cyber Security of Systems [11]. Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against critical sectors in Smart City. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the system in unpredictable ways. To protect Smart City in a proper way, a number of security problems have to be faced according to a specific design/plan; here, some of the issues that have to be taking into account in the design phase are described:

- Privacy: If users deem a system as insecure for his/her sensitive information (privacy), it will not be able to establish itself successfully in the market. Important social challenges stem from the necessity to adapt Smart City services to the specific characteristics of every user. A service has many configurations options, depending on user expectations and preferences; the knowledge of these preferences usually means the success or failure of a service. In order to adapt a service to the specific user's preferences, it is necessary to know them, and this is basically done based on a characterization of that specific user. Nevertheless, a complete characterization of user preferences and behavior can be considered as a personal threat, so the great societal challenge for this, and for any service requiring user characterization, is to assure user's privacy and security. Thus, in order to achieve user consent, trust in, and acceptance of Smart Cities, integration of security and privacy preserving mechanisms must be a key concern of future research. The overall priority must be to establish user confidence in the upcoming technologies, as otherwise users will hesitate to accept the services provided by Smart Cities.
- Networking connectivity: Keeping the network private, i.e. where all transport facilities are wholly owned by the utility, would greatly minimize the threats from intruders, as there would be no potential for access from intruders over the Internet. But having a completely separate network is not feasible in today's highly connected world; it makes good business sense to reuse communications facilities, such as the Internet. A minimally secured Internet-connected Smart City approach, as commonly found with commercial networks, opens the door to threats from multiple types of attacks. These include cyber attacks from hostile groups looking to cause an interruption of the services. Another type of attack is worm infestations which have proven to negatively impact critical network infrastructures. Such threats have largely been the result of leaving a network vulnerable to threats from the Internet. For example, there have been denial of service ("DoS") attacks on a single network that disrupted all directory name servers, thus prohibiting users from connecting to any of the resources. This demonstrates the fragility of an Internet-connected network.
- Complexity: By interconnecting systems that serve totally different purposes (e.g., traffic control and energy management), and thereby creating a "system of systems", the complexity of such collaborating systems increases exponentially. As a result, the number of vulnerabilities in a Smart City system will be significantly higher than that of each of its sub-systems. Furthermore, the pure interconnection of two systems might open the door to new attacks that have not been considered before, when securing either of the individual systems. Therefore, research into ways of handling the increasing complexity of distributed systems from the security perspective is required, which includes: cost-effective and tamper resistant smart systems or device architectures (crypto and key management for platforms with limited memory and computation);

evolutionary trust models (i.e., trust is not static but dynamic, and associated values can change a long time) for scalable and secure inter-system interaction; abstract and comprehensive security policy languages; self-monitoring and self-protecting systems, as well as development of (formal) methods for designing security and privacy into complex and interdependent systems; overall thread models that allow to take multiple sub-systems into account.

- Security services: The Smart City industry requires access to cost-effective, high-performance security services, including expertise in mobility, security, and systems integration. These security services can be tailored per utility to best fit their needs and help them achieve their organizational objectives. An experienced security services organization would need to provide the following capabilities: Proven expertise in information security, for organizations such as governments, large enterprisers and service providers; holistic security framework that operationalizes security across the people, process, policy and technology foundations of each organization; experience in Security and Compliance Pre-Audit Assessments; threat Management expertise - Design, Managed Service, and Integration; policy Design and Related Services - Incident Response Planning, Risk Management, Compliance. Sensitive data organization: The number of users, and the volume and quality of collected data, will also increase with the development of Smart Cities. When personal data is collected by smart meters, smart phones, connected plug-in hybrid electric vehicles, and other types of ubiquitous sensors, privacy becomes all the more important. The challenge is, on the one hand, in he area of identity and privacy management, where, for instance, pseudo-nomination must be applied throughout the whole system, in order to separate the data collected about a user (which is required in order to provide high quality personalized services) from the user's real identity (which is required for purposes such as accounting); this includes that the usage of addressing identifiers, such as IP or MAC addresses, for the purpose of identification must be avoided in future systems. On the other hand, security technologies, such as advanced encryption and access control, and intelligent data aggregation techniques (interesting secure data aggregation scheme for low power networks)[12] must be integrated into all systems, in order to reduce the amount of personal data as far as possible, without limiting the quality of service.
- Availability: The availability of the services depends on the proper operations of many components and the proper connectivity between these components. To disrupt a service, an attacker might attempt to gain electronic access to a component and misconfigure it or to impersonate another component and report a false condition or alarm, but one of the simplest types of attacks that an adversary might attempt is the denial of service attack, where the adversary prevents authorized devices from communicating by consuming excessive resources on one device. For example, it is a well-known issue that if a node, such as server or an access control device uses an authentication protocol which is stateful prior to authentication and authorization, then the node may be subject to denial of service attacks. Smart City protocol designers must ensure that proper care and attention is given to this threat during protocol development. Interesting solution to provide availability against DoS attacks is presented in [5].
- Emergency plan: The components, systems, networks, and architecture are all important to the security design and reliability of the Smart City communications solution. But it's inevitable that an incident will occur at some point and one must be prepared with the proper Incident Response plan. This can vary between commercial providers and private utility networks. A private utility network is likely to provide better consistency of the incident response plan in the event of a security incident, assuming the private network is build upon a standardized framework of hardware and software. The speed of the response decreases exponentially as the number of parties involved increases. Conversely, a private network would ideally depend on fewer parties, therefore a more efficient incident response process would provide for more rapid response and resolution. The rapidity of the response is critical during emergency situations.
- Key management: Some sort of key management is necessary to provide a reliable crypto security. Considering that the Smart City will contain millions of devices, spread across hundreds of organizations, the key management systems used must be scalable to amazing levels. Further, key management must offer strong security (authentication and authorization), inter organization interoperability, and the highest possible levels of efficiency to ensure that unnecessary cost due to overhead, provisioning, and maintenance are minimized. It is likely that new key management systems (specialized to meet the requirements of Smart City) will be needed State of Art is poor in this specific field.

V. THE PROPOSED SECURITY FRAMEWORK

A. Blockchain Technology

Blockchain is a peer-to-peer scattered register technology which annals transactions, agreements, contracts, and sales [9]. Originally developed to support crypto-currency, blockchain can be utilized for any form of transactions without an intermediary. The advantage of blockchain is that an invader has to compromise 51% of the systems to surpass the hashing power of the target network. Thus, it is computationally impractical to launch an attack against the blockchain network. The following example demonstrates working procedures of the blockchain

technology. Let A and B be two entities in a blockchain based parking system and A is paying parking fee to B, the parking authority. This transaction is represented online as a block including information such as block number, proof of work, previous block, and transaction records and this block is broadcast to every entity in the network. The other entities verify the block and if more than 50% of the entities approve the block then the transaction is confirmed and added to the chain. After that, the fee is transferred from entity A to authority B's account.

B. Security Framework

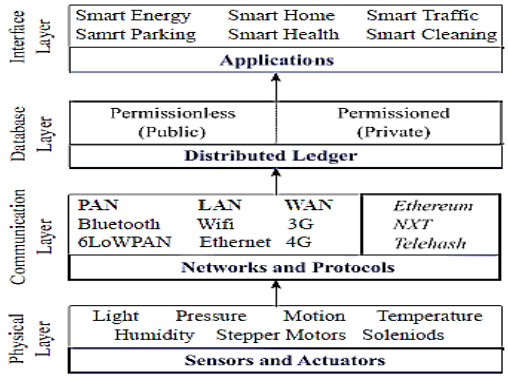

Figure 1: Smart city security framework

1) Physical Layer: As shown in Fig. 1, smart city devices are equipped with sensors and actuators which collect and forward data to the upper layer protocols. Some of these devices such as Nest thermostat and Acer Fitbit are vulnerable to security attacks due to lax encryption and access control mechanisms [10]. Further, there is no single standard for smart devices so that the data generated by them can beshared and integrated to provide cross- functionality. Vendors require an agreed-upon implementation and communication standards to overcome these problems in smart devices.

2) Communication Layer: In this layer, smart city networks use different communication mechanisms such as Bluetooth, 6LoWPAN, WiFi, Ethernet, 3G, and 4G to exchange information among different systems. The block chain protocols need to be integrated with this layer to provide security and privacy of transmitted data. For example, the transaction records can be converted into blocks using telehash which can be broadcast in the network. Protocols like BitTorrent can be used for peer to peer communication whereas Ethereum can provide smart contract functionalities. However, integration of existing communication protocols with block chain is a major challenge since the requirements vary from application to application. A potential solution can be implementing multiple block chains with the help of a blockchain access layer to provide application specific functionalities.

3) Database Layer: In block chain, distributed ledger is a type of decentralized database that stores records one after another. Each record in the ledger includes a time stamp and a unique cryptographic signature. The complete transaction history of the ledger is verifiable and auditable by any legitimate user. There are two different types of distributed ledger in practice: i) permission less and ii) permissioned. The key benefits of permission less ledger are that it is censorship resistant and transparent. However, the public ledger has to maintain complex shared records and it consumes more time to reach the consensus compared to the private ledger. Further, public ledgers may also be subjected to anonymous attacks. Therefore, it is recommended to use private ledgers to ensure scalability, performance, and security for realtime applications like traffic systems in a smart city.

4) Interface Layer: This layer contains numerous smart applications which collaborate with each other to make effective decisions. For example, a smart phone application can provide location information to the smart home system so that it turns on the air conditioner 5 minutes prior to reach at home. However, the applications should be integrated carefully since vulnerabilities in one application may give intruders access to other dependent processes.

VI. CONCLUSION

For the smart cites in India mostly used IoT Based application for automation but it is needed security so in this paper we proposes a blockchain based security framework to enable secure data communication in a smart city. The main advantage of using blockchain is that it is resilient against many threats. Further, it provides a number of unique features such as improved reliability, better fault tolerance capability, faster and efficient operation, and scalability. Thus, integration of blockchain technology with devices in a smart city will create a common platform where all devices would be able to communicate securely in a distributed environment. The future works will aim to design a system level model in order to investigate the interoperability and scalability of different platforms used in a smart city.

REFERENCE

[1]. United Nations, World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352), Dept. of Economic and Social Affairs, ISBN: 978-92-1-151517-6, pp. 1–32, 2014.
[2]D. Makrushin and V. Dashchenko, Fooling the 'Smart City', Technical Report, Kaspersky Lab, pp. 1–22, Sep. 2016.
[3] Prof. Rahul R. Papalkar International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518 on " Preserve Identity across distributed Server using Federated Identity Management System"
[4] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks," in Foundations of Security Analysis and Design V, ser. Lecture Notes in Computer Science, A. Aldini, G. Barthe, and R. Gorrieri, Eds. Springer Berlin / Heidelberg, vol. 5705, pp. 289–338.
[5] A. Bartoli, H. J., M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid m2m networks," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, oct. 2010, pp. 333 –338.
[6] OWASP Foundation, OWASP Top 10-2013: The the Most Critical Web Application Security Risks, 2013.
[7] W. R. Claycomb and A. Nicoll, Insider Threats to Cloud Computing: Directions for New Research Challenges, in 36th Annual Computer Soft. and Appl. Conf., pp. 387–394, 2012.
[8] HMGovernment, Government cloud strategy, pp. 1–24, 2011.
[9] K. Christidis and M. Devetsikiotis, Blockchains and Smart Contracts for the IoTs, IEEE Access, Special section on the plethora of Research in IoT, pp. 2292–2303, 2016.
[10] M. Selinger, Test: Fitness wristbands reveal data, Test AVTEST GmbH, Klewitzstr, Germany, pp. 1–7, Jun. 2015.
[11] (2009) Smart grid cyber security strategy and requirements. [Online]. Available: www.nist.gov
[12] A. Bartoli, H. J., M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure lossless aggregation for smart grid m2m networks," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, oct. 2010, pp. 333 –338.