Analysis of the Security and Privacy Risks and Challenges in Smart Cities' Traffic Light System

Belal Asad*, Neetesh Saxena[†] and Vasilis Katos*

*Department of Computing & Informatics, Bournemouth University, Poole, United Kingdom

[†]School of Computer Science & Informatics, Cardiff University, Cardiff, United Kingdom

Email: {s5119592, vkatos}@bournemouth.ac.uk, nsaxena@ieee.org

Keywords. IoT, Security, Smart Cities, Smart traffic lights, Privacy.

Abstract

Currently, the IoT network is the fastest growing network in the world that brings the smart cities revolution. The increase in the smart cities development poses several security and privacy risks. With the acceleration of times, we can now hastily observe the lack of privacy in our life. The major security and privacy issues occur because of either non-consideration of its security and privacy aspects or having inappropriate controls in place. Many of these issues could be resolved by applying advanced IoT-enabled solutions. This paper presents security and privacy risks and challenges against issues within traffic lights system, which is a complex and critical smart cities system. The paper also addresses a proposed secure and privacy-aware system for future traffic light system.

1 Introduction

The Internet of Things (IoT) is a growing platform that foresees the interconnection of billions to trillions of devices around us. This improvement of the IoT encouraged the technical world to move further to the intelligence world which so-called smart cities. The smart city is an improved urban incorporate Information and Communication Technology (ICT) and different types of IoT. The main objective of building smart cities is to magnify the personal satisfaction by employing new ideas in real-life. A smart city is a future, where it focuses on using and exploiting both tangible and intangible assets (e.g., transport infrastructures and human capital) [1]. Smart transportation system is one of the main components of a smart city. The smart transportation system is designed to improve the safety and efficiency of the traditional road. Improving traffic management and increase the productivity of the urban require more information and knowledge in different aspects. Traffic lights are one part of the intelligent transportation system, as it contains many different subsystems to avoid the traffic congestion and negative impacts on people [2]. Nowadays, systems for controlling the traffic can be found in several European Union (EU) countries. In some cases, different types of artificial intelligence techniques have been deployed [2]. In 2010, BMW and Siemens proposed a system of networked traffic lights that can communicate with nearby cars [3]. Furthermore, the smart traffic light system requires to collect real-life data and use it among the intelligent transportation networks to make correct decisions. The smart traffic light system is based on IoT and ICT technologies, but this system has several security and privacy issues [3].

Rest of the paper is organized as follows. Section 2 addresses the smart traffic light system's security and privacy risks and challenges. Section 3 discusses existing solutions, protocols and cryptographic algorithms against these security risks. Section 4 illustrates privacy-enhancing technologies against the smart traffic light systems privacy risks and critically appraise these technologies. Section 5 proposes and describes a scalable security and privacy system solution for the smart traffic light system and Section 6 concludes this work.

2 Security and Privacy Risks and Challenges

As the smart traffic light system is based on IoT and ICT technologies and both of them based on the internet, there are security and privacy risks concerns present. By looking at the current traffic light systems, there are several smart traffic management systems, which are either CCTV camera-based systems or IoT devices-based systems [4]. Figure 1 shows the information flow of the current smart traffic light system.

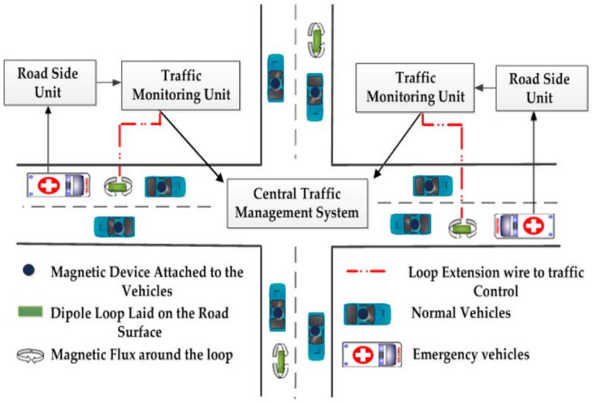

Road Side Unit
Traffic Monitoring Unit
Traffic Monitoring Unit
Road Side Unit
Central Traffic Management System
● Magnetic Device Attached to the Vehicles
Dipole Loop Laid on the Road Surface
Magnetic Flux around the loop
Loop Extension wire to traffic Control
Normal Vehicles
Emergency vehicles

Fig. 1. Smart traffic management system [4].

Furthermore, Figure 2 demonstrates the whole process of the traffic signal system that helps to understand the possibilities of attacks that may occur in any layer and the related privacy issues. This section focuses on the security and the privacy risks and vulnerabilities in currently existing systems. The IoT architecture in Figure 3 shows that ICT technology is a part of the IoT scheme [5]. Figure 3 addresses the different levels of the IoT architecture used in the smart traffic lights. Consequently, each level has several issues [5].

2.1 Machine-to-Machine (M2M) Device Domain

This layer consists of simple nodes lacking power and memory [5]. Applying the same encryption algorithms or frequency hopping communications that are used in the traditional network is not feasible [6]. The security issues in this level are related to the used technologies, such as Radio-Frequency Identification (RFID), Wireless Sensor Network (WSN), and Global Positioning System (GPS).

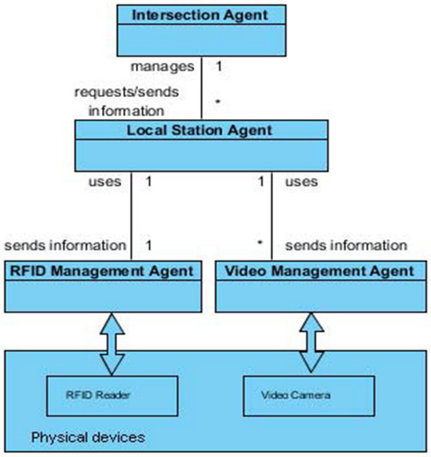


Fig. 2. Traffic light system architecture [4].

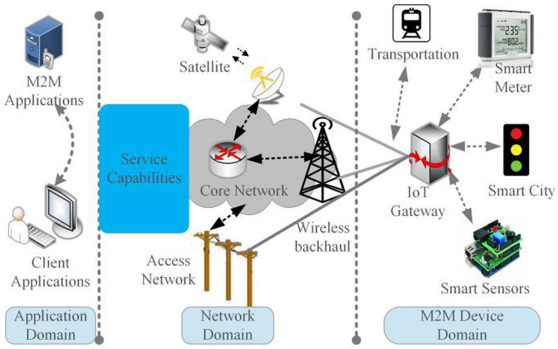


Fig. 3. High-level IoT architecture [5].

1. Denial of Service (DoS) attacks (on RFID): DoS attack is one of the most used cyber-attack methods in the network security [7]. The IoT network from the smart traffic light makes an environment for this kind of attack, as the network has low power and storage and it is dealing with a significant changeable amount of data at the same time [7]. This type of attack generally focuses on the weakest part of the network like a sensor node [7]. Furthermore, the European Telecommunications Standards Institute (ETSI) has been directed by the EU to include an RF (Radio Frequency) band in use for ITS (Intelligent Traffic Systems) [7]. All the previous drawbacks with the frequency band are known and available, which makes the intelligent traffic light a fertile environment for Distributed DoS (DDoS) attacks [7]. The available solutions for this variability are summarized as follows:

- Building a strong access control and policies.
- Checking and testing the network.

2. Security issues of RFID technology: RFID is a contactless technology that automatically identifies the targeted tag signal [8]. The RFID technology is widely used in ITS that discloses security issues discussed as below:

a) Conflict collision: A large number of nodes in the smart traffic light system may let the RFID reader to read from multiple tags simultaneously. Consequently, the system will get incorrect data [9]. The available solutions to this problem are summarized as follows:

- Applying scope-based anti-collision algorithm [9].
- Applying the time-based algorithm [9].

The first solution needs extra time to calculate the working scope between the readers that requires a supplemental central control area [9].

b) Uniform coding: The traffic management system deals with different types of vehicles from several countries and standards. Currently, there is no international uniformed encoding standard for RFID tag [11]. This issue could occur a system error when a foreign vehicle enters the network [11]. To avoid any error in the system, there should be a uniformed encoding combining the Unique Identification Number (UID) that is supported by Japan Electronic Product Code (EPC) format which is supported by Europe [10].

Table 1. Privacy threats and challenges

No.	privacy threat	detailed information
1.	Localization and tracking:	The threat of Localization and Tracking means people's location may be recorded by the devices or smartphone, which means the attackers can deduce some sensitive information from their locations or trajectory [20]. For example, The ANPR system are used to help deter, detect and disrupt criminality at a force, regional, local and national level [16]. The car's plate and identification can be used to track the driver and know about his behavior instead of providing safety and tracking suspicious situations [14]. This issue can be solved by reducing the (ANPR) Automatic number plate recognition terms and let this system recognize and read the plate number according to specific attributes [14].
2.	Lifecycle transitions:	When people are using the service provided by IoT, the sensors may collect their private information, transmit it to the cloud for storage or further analysis and return the result. In this way, the data transmitted between different phases may divulge sensitive information. One of the methods to reduce this threat is to devise a mechanism to detect different phases of data processing and provide applicable solutions to protect the sensitive data [20].
3.	Storied Data Volumes:	The security cameras on the traffic lights recording and collecting different attributes about people without a specific reason [13]. This information is stored according to the local policies; on the ITS network this information may leak for different reasons [14].
4.	Linkage:	Different systems may share various data from individuals with each other and provide additional services for them [14]. However, this may disclose unexpected results that the individuals do not want to share. To mitigate this threat, informed consent from individuals should be given [20]. Besides, access control with privacy policies describing the permission, use, collection across the systems and data anonymization techniques can be useful [20].
5.	red light speed camera and Identification:	The squeamish capturing sensors may let the camera capture a vehicle without doing an actual felony [14]. Since IoT devices will collect a myriad of sensitive information for the individuals, it is possible for the malicious attackers or unwanted third parties to use this data and link the identifier to a certain person [20]. There are several ways to prevent this kind of attack, such as anonymization techniques, identity management and local processing [20]. The privacy issue here can be solved by applying the GDPR policy and requirements [14].

2.2 Network Domain and Application Domain

This layer contains the wireless and wired networks to transfer the collected data to the application domain [11]. The ITS wireless network is divided into two different types: Wi-Fi-based and Ad hoc-based [11]. The Wi-Fi-based part connects the network to the Internet that includes risks the network for an attack like an injection attack [12]. Injection attack affects the system decision where original data may replace with malicious data [12]. The Ad-hoc part is to connect the nodes of the system to each other [12]. The IoT nodes are easy to access and remove from the network that allows the attackers to capture a node and access to critical resources and information [12]. The ideas currently resolved the issues are as follows:

- Applying the access control and network encryption on the Wi-Fi part [11].
- On the Ad-hoc side using different types of Authorization & authentication between nodes [12].

The goal of such a system is to resolve transportation issues [20]. The ITS uses a large number of sensors to collect and analyze data continuously to improve a specific area [20]. The connected heterogeneous devices may exchange a large number of sensitive information through the World Wide Web using different wireless means, which drive us to several privacy threats and challenges [20]. Table 1 shows privacy threats and related system challenges.

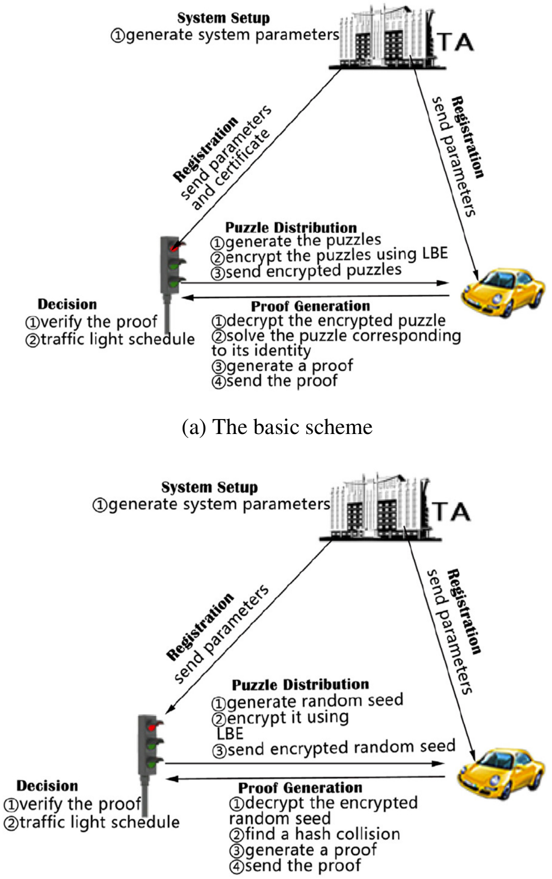
3 Analysis: Algorithms and Protocols

This section analyses the existing cryptographic algorithms and protocols that are used to provide a secure system and defeats the security risks. In 2018, Liu et al. [17] proposed two schemes working as one system using Fog computing based on Location-Based Encryption (LBE) and cryptographic puzzle to secure the intelligent traffic light control [17]. The traffic light in this system needs to verify one puzzle for each vehicle in a time slot [17]. They proposed another improved scheme to reduce the computation and communication overhead of the traffic light in which the traffic signal only needs to perform lightweight operations. Furthermore, it needs to broadcast only a single puzzle [17]. Figure 4 presents the basic ideas of the improved scheme and the basic one.

The proposed system is a new approach, which requires further studies, time, and applies the scheme on the realistic ITS to figure out the efficiency and effectiveness of the system. The system has been confirmed by virtual experiments [17]. The results of the virtual experiments highlighted the efficiency of this system in terms of time only. The system still needs to be applied and examined to see if it can defeat the security risks. [17]. The following list is the most commonly used security algorithms in traffic light based on IoT technology [15]: RSA – Rivest–Shamir-Adleman Algorithm, AES – Advanced Encryption Standard Algorithm:, and DES – Algorithm: Data Encryption Standard. Table 2 shows the main advantages, specifications and drawbacks of the above algorithms. Table 3 illustrates and explains that the RSA algorithm is not suitable for ITS based on IoT technology.

Table 2. Analysis of various factors [18 - 19]

Factors	AES	DES	RSA
Developed	2000	1977	1978
Key Size	128, 192, 256 bits	56 bits	> 1024 bits
Block Size	128 bits	64 bits	Minimum 512 bits
Ciphering & deciphering key	Same	Same	Different
Scalability	Not Scalable	It is scalable algorithm due to varying the key size and Block size.	Not Scalable
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption	Faster	Moderate	Slower
Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Excellent Secured	Not Secure Enough	Least Secure
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Stimulation Speed	Faster	Faster	Faster
Trojan Horse	Not proved	No	No
Hardware & Software Implementation	Faster	Better in hardware than in software	Not Efficient
Ciphering & Deciphering Algorithm	Different	Different	Same



(a) The basic scheme

(b) The improved scheme

Fig. 4. (a) The basic scheme and (b) improved scheme.

Table 3. Analysis of various factors [18]

S.NO	*Algor*	*Pack Size (KB)*	*Encrypt Time (Sec)*	*Decrypt Time (Sec)*	*Buff Size*
1	DES	153	3.0	1	157
	AES		1.6	1.1	152
	RSA		7.3	4.9	222
2	DES	118	3.2	1.2	121
	AES		1.7	1.2	110
	RSA		10.0	5.0	188
3	DES	196	2.0	1.4	201
	AES		1.7	1.24	200
	RSA		8.5	5.9	257
4	DES	868	4.0	1.8	888
	AES		2.0	1.2	889
	RSA		8.2	5.1	934
5	**DES**	312	3.0	1.6	319
	AES		1.8	1.3	300
	RSA		7.8	5.1	416

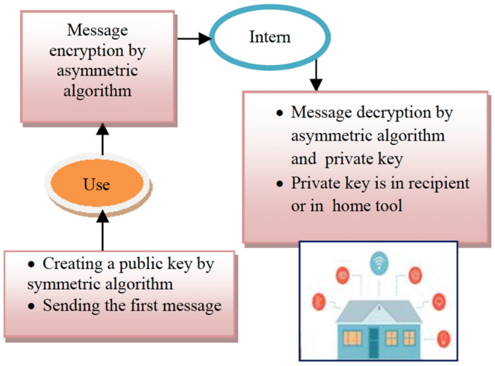

Message encryption by asymmetric algorithm
Intern
• Message decryption by asymmetric algorithm and private key
• Private key is in recipient or in home tool
Use
• Creating a public key by symmetric algorithm
• Sending the first message

Fig. 5. HAN encryption algorithm usage in IoT [15].

Algorithm	*HAN*	*AES*	*RSA*
Period of time for implementing the whole algorithm per second	0.321081	2.718182	2.350752

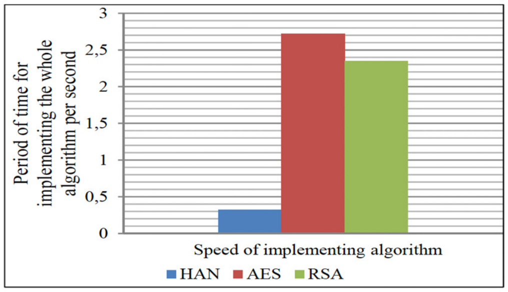


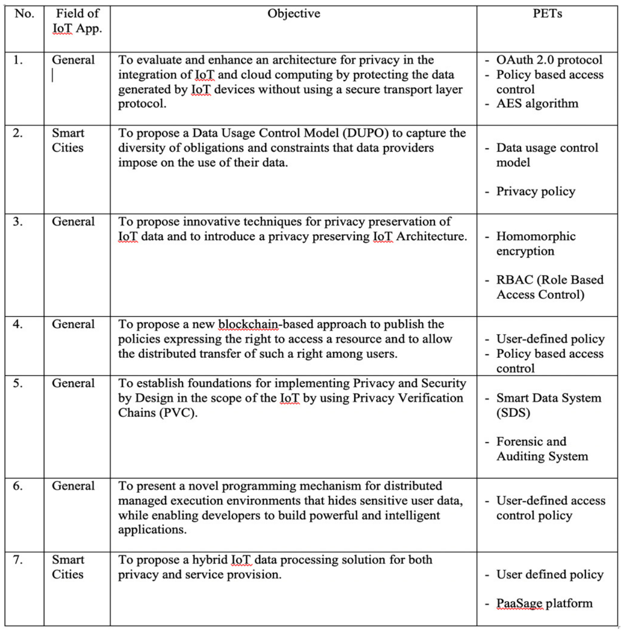
Fig. 6. Total speed of HAN algorithm [15].

HAN – Algorithm: This algorithm is considered as a hybrid encryption algorithm that combining of AES symmetric encryption algorithm and NTRU asymmetric encryption algorithm for IoT improvement [15]. HAN algorithm builds keys fast and it also improves the internet security during the algorithm implementation [15]. Figure 5 shows the algorithm implementation steps in IoT. The HAN algorithm is safe due to multinomial usage in decryption, encryption, and digital signature to receive the correct message [15]. This algorithm has more advantages than its drawbacks. Figure 6 illustrates the total speed of the HAN algorithm in comparison with AES and RSA algorithms. By comparing the results above we can see that the HAN algorithm is the best scheme to use in the ITS. The HAN algorithm is still a new scheme, which requires further experiments and examinations.

4 Privacy Enhancing Technologies

The Privacy Enhancing Technologies (PETs) in IoT is classified by Shi-Cho Cha et al. [20] into three research domains as follows: 1) Control over data, 2) Enforcement, and 3) Anonymization or Pseudonymization [20]. These research domains are further divided into seven aspects [20]. This section addresses and illustrates the domains in terms of smart traffic light systems. Figure 7 shows the main relation between seven domains of PETs in IoT [20].

Table 4. Existing studies and enhancing technologies under the "Personal Data Protection" domain [20 – 21- 22]



No.	Field of IoT App.	Objective	PETs
1.	General	To evaluate and enhance an architecture for privacy in the integration of IoT and cloud computing by protecting the data generated by IoT devices without using a secure transport layer protocol.	- OAuth 2.0 protocol - Policy based access control - AES algorithm
2.	Smart Cities	To propose a Data Usage Control Model (DUPO) to capture the diversity of obligations and constraints that data providers impose on the use of their data.	- Data usage control model - Privacy policy
3.	General	To propose innovative techniques for privacy preservation of IoT data and to introduce a privacy preserving IoT Architecture.	- Homomorphic encryption - RBAC (Role Based Access Control)
4.	General	To propose a new blockchain-based approach to publish the policies expressing the right to access a resource and to allow the distributed transfer of such a right among users.	- User-defined policy - Policy based access control
5.	General	To establish foundations for implementing Privacy and Security by Design in the scope of the IoT by using Privacy Verification Chains (PVC).	- Smart Data System (SDS) - Forensic and Auditing System
6.	General	To present a novel programming mechanism for distributed managed execution environments that hides sensitive user data, while enabling developers to build powerful and intelligent applications.	- User-defined access control policy
7.	Smart Cities	To propose a hybrid IoT data processing solution for both privacy and service provision.	- User defined policy - PaaSage platform

The largest domain of these seven areas is the Personal Data Protection [20]. Most of the privacy-enhancing technologies in this area not only aim to conserve the critical data but the PETs also aim to raise awareness to the users on how their sensitive data is processed [21]. Table 4 shows the existing studies and enhancing technologies under the "Personal Data Protection" domain. The Holistic Privacy-Preservation domain directs and provides a solution that combines anonymization techniques, separate awareness of sensitive data, and secure data access to terminate the likability between the person and the data [23]. Some of the exists enhancing technologies in this category are as follows:

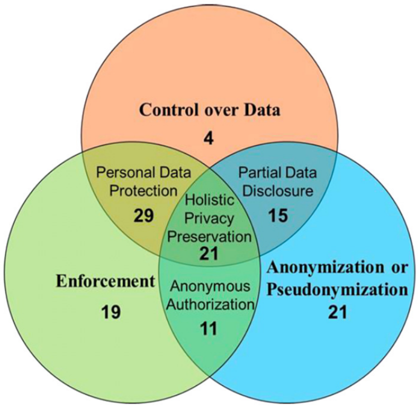


Fig. 7. Coverage of Each Categorization of PETs.

4.1 Personal data managers and Adaptive inference discovery service

Applying these two techniques to build a general structure and overseeing the issue from claiming security from the unwanted revelation about particular information.

4.2 Attribute-based cryptography and Anonymous credential systems

In 2007, Li et al. [24] proposed a framework based on these two techniques to enable a secure and privacy-aware data likability on the Internet of Things [20]. Table 5 and Table 6 show some of the existing technologies which are related to the smart traffic light and ITS in general. As this section illustrates the majority of the enhancing technologies currently available, this is considered as a critical area as people want to keep their private information away from anyone else. Moreover, with a large number of the available techniques this area still needs improvement [23].

Table 5. Existing studies and enhancing technologies under the "Anonymization or Pseudonymization" domain [20 – 25]

No.	Field of IoT App.	Objective	PETs
1.	General	To propose a new approach to cloud-based machine learning ML services that can reduce the privacy concern.	- Neural networks partial data processing
2.	General	To propose a conditional privacy-preserving authentication with access likability (CPAL) for a roaming service, which provides universal secure roaming service and multilevel privacy preservation	- Group signature - Hybrid Linear Combination Encryption

Table 6. Existing studies and enhancing technologies under the "Partial Data Disclosure" domain [20 – 25]

No.	Field of IoT App.	Objective	PETs
1.	Smart Cities	To propose a privacy management scheme for the user to estimate the risk of sharing private data like Identification data.	- k-anonymity - Privacy quantification
2.	Smart Cities	To propose a tool called 'Sensitivity Inspector' that detects sensitivity in smart transportation data and inculcates privacy awareness among smart city users.	- Sensitivity Inspector

5 Proposed Secure Privacy-aware System

From the previous sections, the traditional world is converting itself into a smart world [17]. The countries around the modern world compete in building ideal smart cities. As motioned in the Introduction section, the most important part of the smart city is the intelligent transportation systems and the core of these systems is the smart traffic light system [4]. Going through the security and privacy risks and their solutions, we can observe that the existing solutions are not good enough for the smart cities traffic system and very much need to be improved. This section presents a proposed secure and privacy-aware system for future traffic light systems. Figure 8 explains a standard architecture for the proposed system. First of all, to avoid the majority of privacy issues related to cameras, in the proposed system the smart traffic light is without any cameras. The whole system works with the use of IoT sensors which connect to a smart plate. The car's smart plate contains an RFID tag and this tag will hold all the details of the vehicle's owner. The information inside this tag is updated whenever the person enters the car. The traffic light system detects the car's plate tag when it is close enough. The system uses a combination of AES and NTRU algorithms.

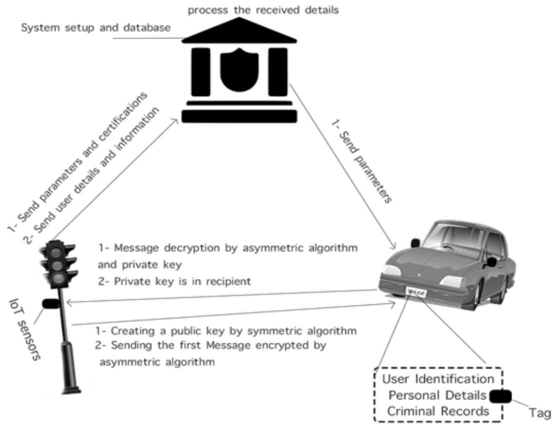

process the received details
System setup and database
1- Send parameters and certifications
2- Send user details and information
1- Send parameters
1- Message decryption by asymmetric algorithm
and private key
2- Private key is in recipient
IoT sensors
1- Creating a public key by symmetric algorithm
2- Sending the first Message encrypted by
asymmetric algorithm
User Identification
Personal Details
Criminal Records
Tag

Fig. 8. Standard architecture for the proposed system.

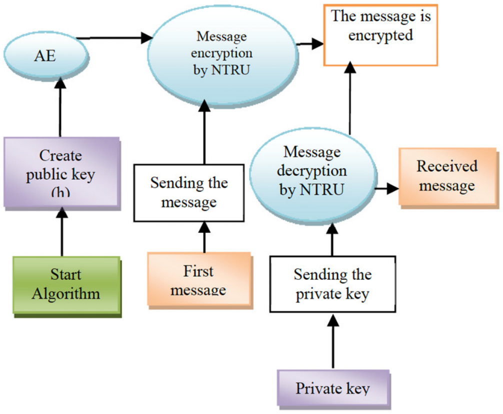


Fig. 9. HAN encryption algorithm steps sending public key [15].

We choose this security algorithm for the proposed system according to the results in Figure 6. The security process works as shown in Figure 8 by using the HAN algorithm. Figure 9 shows the HAN encryption algorithm steps sending the public key. We considered each traffic signal block as a home so each block can communicate with the police station. The system here is scalable as it does not hold any information and that gives us extra storage. The system sends details from the car's plate to the police station to do the online checking. The RFID tag can also be used instead of the red light camera or the speed camera. In this system, we avoid two of the leading privacy issues by replacing the cameras by sensors and processing the data online instead of tracking and holding the information. The third party in this system is the police station as the police station will be responsible for configuring the signals and to build the smart plates. Consequently, the police station will have the keys to prove the connection between the traffic light system and the vehicle. Third party is a trusted party like a police station.

6 Conclusion

As the IoT is growing rapidly, it helps to create a smart traffic signal to be implemented in real life to reduce traffic congestion. This paper focuses on the security and privacy challenges and risks in the smart traffic light that needs to be addressed. We have also analyzed the currently used algorithms and techniques in the traffic light system. With shortcomings and limitations of the existing techniques and algorithms, we discussed a proposed scheme which utilizes the combination of the best algorithms and enhancing privacy technologies. The proposed system is connected to the police satiation as a third party to give more privacy on the sensitive information.

References

[1] D. Popescul and L. Radu, "Data security in smart cities: challenges and solutions", *Informatica Economica*, 20, pp. 29-38, (2016).

[2] C. E. Turcu, V. Găitan, and C. Turcu, "An internet of things-based distributed intelligent system with self-optimization for controlling traffic-light intersections", *Stefancel Mare University of Suceava smart cities conference*, pp. 1-5, (2012).

[3] M. Richard, Networked traffic lights could save time, fuel, and lives, TreeHugger, (2019). [Online]. Available: https://www.treehugger.com/cars/networked-traffic-lights-could-save-time-fuel-and-lives.html.

[4] P. Rizwan, R. Babu, and K. Suresh, "Real-time smart traffic management system for smart cities by using internet of things and big data", *International Conference on Emerging Technological Trends*, 2016, 1-6.

[5] A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications", *IEEE Communications Magazine*, 53(9), pp. 48-54, (2015).

[6] H. Suo, J. W. Hui, C. Zoua, and J. Liua, "Security in the internet of things: a review", *International Conference on Computer Science & Electronics Engineering*, pp. 1-6, (2012).

[7] L. Liang, K. Zheng, Q. Sheng, and X. Huang, "A denial of service attack method for an IoT system", *International Conference on Information Technology in Medicine and Education*, pp. 360-364, (2016).

[8] I. Woungang, S. Dhurandher, and A. Awad, "Security and privacy in internet of things and cloud computing systems", *Security and Privacy*, 1(3), pp. 1-2, (2018).

[9] B. Lv, J. Pan, Q. Ma, and Z. Xiao, "Research progress and application of RFID anti-collision algorithm", *International Conference on Telecommunication Engineering*, pp. 124-128, (2008).

[10] L. Liu, A. Hui, and S. Lai, "ALOHA-based anti-collision Algorithms used in the RFID system", *IEEE Inter. Conf. on Networking and Mobile Computing*, pp. 1-4, (2006).

[11] V. Q. Jing, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges", *International Conference on Telecommunication Engineering*, pp. 1-6, (2010).

[12] C. Li and C. L. Chen, "A multi-stage control method applied in the fight against phishing attacks", *26th Computer Security Scholarly Communication Across the Country*, 145, (2011).

[13] U. Chinanu, "Architectural layers of internet of things: analysis of security threats and their countermeasures", *Scientific Review*, 4(10), pp. 80-89, (2018).

[14] EUGDPR – Information Portal. Eugdpr.org, (2019). [Online]. Available: https://eugdpr.org/.

[15] A. Safi, "Improving the security of internet of things using encryption algorithms", *Intern. Journal of Computer and Information Engineering*, 11(5), pp. 558-561, (2017).

[16] Automatic Number Plate Recognition. Police.uk, (2019). [Online]. Available: https://www.police.uk/information-and-advice/automatic-number-plate-recognition/.

[17] J. Liu, "Secure intelligent traffic light control using fog computing", *Future Generation Computer Systems*, 78, pp. 817-824, (2018).

[18] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution technique", *International Journal of Science and Research*, 2(4), pp. 170-174, (2013).

[19] A. Berzati, J.-G. Dumas, and L. Goubin, "Fault attacks in RSA public key", *RSA Conference on Topics in Cryptologyages*, 9(5), pp. 414-428, (2009).

[20] S. Cha, T. Hsu, Y. Xiang, and K. Yeh, "Privacy enhancing technologies in the internet of things: perspectives and challenges", *IEEE Internet of Things Journal*, 21(9), pp. 1-28, (2018).

[21] K. Passia, Information Technology — Security Techniques — Privacy Framework. ISO.org, (2011). [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en.

[22] P. Ashley, S. Hada, G. Karjoth, C. Powers, and M. Schunter, Enterprise Privacy Authorization Language (EPAL-1.2). W3.org, 2019. [Online]. Available: https://www.w3.org/Submission/2003/SUBM-EPAL-20031110/.

[23] A. M. Elmisery, S. Rho, and D. Botvich, "A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things", *IEEE Access*, 4, pp. 8418-8441, (2016).

[24] N. Li, T. Li, and S. Venkatasubramania, "t-closeness: privacy beyond k-anonymity and diversity", *IEEE 23rd International Conference on Data Engineering (ICDE)*, pp. 106-115, (2007).

[25] F. Knirsch, G. Eibl, and D. Engel, "Multi-resolution privacy-enhancing technologies for smart metering", *EURASIP Journal on Information Security*, 6, pp. 1-13, (2017).