Smart Policing for a Smart World Opportunities, Challenges and Way Forward

Muhammad Mudassar Yamin*[1], Andrii Shalaginov†[1], and Basel Katt‡[1]

[1]Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik

October 2019

Abstract

Our world is getting evolved to smart world day by day. This smart world is being developed to make people life easier through the data generated by the smart devices. Data is the fuel that powers the smart world evolution, however, making things smart have its consequences. Smart devices are inherently vulnerable to cyber attacks, that's why we are observing an increase in crimes related to cyber space comparing to physical space. To address these crimes, police of the future need to evolve as well and data will be at the center stage of this evolution. In this contribution we are proposing a data centric policing proposal for smart cities. We analyzed current and developing technologies and the opportunities they offered for smart policing for a smart world.

Key words– Smart Cities, Police, IOT, Crime, Machine Learning

1 Introduction

Due to the density of data acquisition devices such as trivial environmental sensors or more complex video cameras, the future *Smart City* serves as a Panopticon of potential surveillance. This acts as a deterrent to discourage criminal activity since data may easily be acquired to facilitate an investigation against the individual in the future. With an assumption that a number of heterogeneous devices and sensors are owned by or have agreements with law enforcement, future Software Defined Networks (SDN) and Virtual Network Functions (VNF)

*Corresponding Author: muhammad.m.yamin@ntnu.no

†andrii.shalaginov@ntnu.no

‡basel.katt@ntnu.no

may be able to overcome such data heterogeneity. The data that have been acquired may be stored in a cloud to facilitate spikes in user demand. Machine Learning as a Service can be used to deliver processing for prediction of future actions based on the historical data, anomaly detection, activity classification, human behaviour recognition, or object recognition [8].

Generally, the function of the police is the responsibility for the well-being of its citizens. Technology is expected to become more reliable when it comes to providing automated reasoning and security, but we cannot rule out the fact that humans are the weakest links in modern Information and Communication Technologies (ICT) societies. With the evolution of a digitally-dense future cities, the importance of the systems used and the reliance of humans on those systems will increase manifold times. To curb the number of incidents, the new-age police will have a challenge to keep the people informed, have the computational capacity to process all collected data from sensors/autonomous systems and adapt to the new opportunity model [25] provided by smart cities (directly competing with the adversaries). Worryingly, critical infrastructure can be influenced by either party. If these challenges are met, it will enable future police in investigations (current and retrospectively) and frame smart responses to the forthcoming crime.

Police organizations worldwide are looking to leverage emerging technologies to fight against physical and cyber crimes. Such crimes are more prevalent than ever before due to the Internet of Things (IoT) and the development of smart cities with corresponding digitally-dense infrastructure. Mark Goodman, a man who has had a career in law enforcement, a futurist for the FBI, and senior advisor to Interpol stated that "*More connections to more devices mean more vulnerabilities*" [20]. And the increasing dangers are clear: in 2017 IoT attacks increased by 600%, and in a study 70% of businesses believe their security risk increased significantly. As it stands today, more than 4,000 ransomware attacks occur each day, and statistically grow more than 350% every year. These vulnerabilities affecting smart cities are not new, but now, their consequences can be far more severe due to the cyber-physical nature of smart cities. Now, hackers do not only pose a threat to data, but to human lives as well. So, there can be anticipated new technological challenges that people and police in Smart Cities of future will face in addition to societal challenges already solved through "Big Data for Social Good" initiatives [42].

Even with the change in the *modus operandi* of the Police in smart cities resulting in Smart Police; the functions of the Law Enforcement Agency (LEA) remain somewhat the same i.e. – *To ensure Public order, Public safety, Crime prevention, Detection and Investigation.* The infrastructure, that the new age technology will bring-forth, will potentially change the dynamics of Policing. A whole new Opportunity structure will come to surface. Both the LEAs as well as the adversaries will be presented with new means to safeguard or to attack the systems in use. All the challenges and opportunities will revolve around a very central aspect – real-world non-synthetic *Data* and its corresponding utilization in Intelligent Decision-Support Systems (IDSS) [21]. While there is a high likelihood of discovering new vulnerabilities in smart cities hardware ans software, this creates new opportunities to both the criminals and the law enforcement agencies. It is our belief, that LEA must and can take a more proactive approach to preventing, detecting, and investigating crime in both the cyber and physical realms in future smart cities. Anticipated challenges and corresponding opportunities are given below:

Challenges

1. Due to huge amount of data that needs to be collected through a large number of autonomous systems and sensors, the obscurity and complexity may create a novel attack vector.

2. Who will own this data? - who is the data custodian, processor, access control models on information (processed day). The "chain of custody" during criminal investigation needs to be maintained.

3. The integrity of the data can be compromised during capture storage attributed to Public functions.

4. With a large volume of data to be processed, huge computational capabilities will be required resulting in latency with, often critical, decisions.

5. Data processing and police notification of reasoning now becomes a challenge.

6. Historically, when crime in a city reduces, it increases on the outskirts. Since the technology is deployed in the main city with dense population, law enforcement will have to be done in conventional ways to ensure public order outside center.

7. With a wide range of ad-hoc systems and a need to respect privacy of the citizens, the information sharing can pose a significant obstacle on regional, national and international levels.

Opportunities

1. Over the course of history, the role of the Police has predominantly been *reactive.* However, if the data can be provided to the LEAs in time, they can be *proactive* in preventing the crime.

2. Autonomous and semi-autonomous vehicles, unmanned aerial vehicles (UAV)s and robots will make law enforcement not only more efficient, but safe for the police officers, delegating life-threatening tasks to machines.

3. Application of Computational Intelligence provides ways to outsource time consuming manual tasks to automated models, allowing police officers to prioritize other decisive tasks.

4. The data acquisition sources can be shared by various agencies, based on their body function, to use it to their advantage. (*For example:* if an adversary is planning an attack on an asset of national relevance and the

contextual data is captured; it can be sent to the national agencies to prevent the act from happening in the first place like big weapon consignment captured on surveillance, a drug deal etc.)

5. The role of the community and so-called "crowd-sourcing" cannot be ruled out in crime prevention and investigation [11]. Platforms like social media, apps for smart phones and citizen awareness campaigns can be a key to an aware and well informed society.

6. With strong control measures in place, the criminals will be discouraged to do a crime in the first place due to high price / high efforts.

In this contribution the researchers present the winning idea[1] of INTERPOL Thinkathon 2018 challenge in which we proposed a semi-autonomous crime detection, prevention, and investigation system [39]. That can assist law enforcement agents by processing the data acquired from heterogeneous sensors, and disseminate and render relevant information to the law enforcement agencies or even make autonomous decisions in the appropriate circumstances. To be concise, our solution is essentially to apply a city-wide Intelligent Intrusion Detection-like system as an integral component to our modern age Smart Cities. To tie the ideas together, we illustrated some example scenarios depicting some potential outcomes of our proposed solution. The *first* scenario exhibits a physical crime that leaves digital traces. The *second* scenario stages a cyber-physical crime, that demonstrates how smart appliances and internet enabled technology may be abused. The *third* scenario is an example of a crime occurring purely in cyberspace, to round off the cyber-physical relationships.

This paper is organized as follows, the researchers start with discussing Smart City technologies and their applications in the Section 2. Afterwards, we focus on data, wherein we consider issues pertaining to the acquisition of data, its handling, and processing. This also includes potential methods of analysis to be performed on the processed data presented in the Section 3. The synthesis of these ideas drives our attention to the newly spawned opportunity model in the context of smart city policing, where we discuss relevant challenges and opportunities with the help of three crime scenarios in the Section 4. After that we share future technologies that can make this fantasy a reality in the Section 5 and conclude the paper with the Section 6.

2 State of the Art: Data as a key component of Smart Cities' infrastructure

Future Smart Cities will ensemble large network of ubiquitous heterogeneous devices scattered across physically-distributed locations. This will lead to many technological opportunities such as increase mobility, fine-tuned geographical

[1] The idea has been originally prepared and presented by the team from the Norwegian University of Science Technology during the competition at the Interpol in October, 2018: https://twitter.com/INTERPOL_GCI/status/1039803723071905793

location detection and improved situational awareness aiding police investigators to tackle crimes with aid of data analytics.

2.1 Data Sources

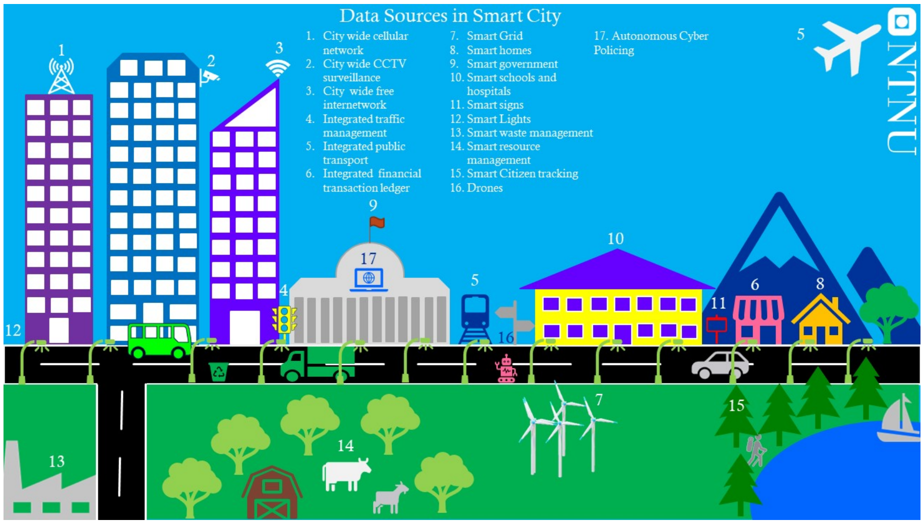
Data Sources in Smart City
1. City wide cellular network
2. City wide CCTV surveillance
3. City wide free internetwork
4. Integrated traffic management
5. Integrated public transport
6. Integrated financial transaction ledger
7. Smart Grid
8. Smart homes
9. Smart government
10. Smart schools and hospitals
11. Smart signs
12. Smart Lights
13. Smart waste management
14. Smart resource management
15. Smart Citizen tracking
16. Drones
17. Autonomous Cyber Policing
NTNU
1
2
3
4
5
9
17
5
10
11
6
8
12
16
7
15
13
14

Figure 1: Data Sources in Smart Cities

Smart City infrastructure intrinsically implies distributed network of sensors and resource-constrained end-point devices that can be used to acquire data and model cyber situational awareness [6, 2]. There can be mentioned several general categories of data sources found in the literature with respect to their usage motivation [26, 7]:

1. Specialized public services such as access Radio-frequency identification (RFID) tags, stationary Closed-circuit television (CCTV) cameras [40, 41], cameras on movable objects (like cards, bikes, police officers);

2. Personal information flow such as bank statements, shopping transactions, call data, Global Positioning System (GPS) data (car, on foot, bicycle, public transportation), health sensors;

3. Environmental sensors such as waste and garbage, air pollution level, traffic congestion, parking, noise level, humidity, temperature, etc.

Large fraction of such data can be considered as publicly-available, however, some contain sensitive and Personal Data as defined by recent General Data Protection Regulation (GDPR) implementation [18]. The publicly accessible data sources which can be used in smart city policing is represented in figure 1.

2.2 Data Handling/Storage

Cheap deployment of technologies and high bandwidth networks will boost presence of versatile devices in every aspect of every day's life. As result, small pieces of data samples collected at regular intervals across all end-points, once put together, will form a considerable flow of information that cannot be handled by small-scale data storage solutions [14, 33]. This will enable every aspect of Big Data paradigm: *Variety, Variability, Volume, Velocity and Value. Volume* and *Velocity* are successfully handled by hardware and software solutions for large data storage and high-speed network connections. These are so-called "Data Lakes" capable of handling enormous loads with guaranteed performance, integrity and availability. At the same time, *Variability* and *Variety* of data become a real challenge when it comes to extracting the *Value* from the collected data for the Smart Police of future. Therefore, it is important to look for an advanced method capable of handling such challenges and bringing down the amount of manual labor required by police officers.

2.3 Data Acquisition

The data from aforementioned low-level components travel through middleware, including corresponding IoT hubs and services across Public Internet and Smart Grid into the data storage centers, either locally in the Smart City or globally [17]. Energy-efficient multi-agent systems ensure reliable communications in resource-constrained environment with nearly real-time performance as well as guaranteed freshness of collected data. The main challenges related to acquisition of the data is related to (i) communication protocols, (ii) data formats, levels of granularity and metadata, (iii) interaction model (subscription, regular, etc) and intervals, (iv) abstraction and representation level for the management and decision makers (e.g., video stream of pool of identified objects) [38] . However, once tackled, the data acquisition will provide unlimited opportunities for versatile data analytic needed in context of safety and security in Smart Cities of future. Finally, there will be a possibility to harmonize previous historical data from different storage engines, including paper based reports.

2.4 Data Processing

Since the amount of data generated by various components of Smart Cities is growing dramatically every year, mankind faces problems related to the fact that data are so complex, sparse and different. Existing data processing methods will not be able to handle it in near future. Therefore, one of the focus areas should be on data fusion, cleansing, correlation and processing to advance threat intelligence and information processing by Law Enforcement Agencies [24, 16]. In addition to this, such focus will enable development of new methods and simulation of possible criminal scenarios based on the available historical information. Further on, information rendering is important aspect of future policing focusing on information sharing between LEAs and future reporting not only internally, yet also externally to public.

2.5 Decision Support / Privacy Aware Analytics

State-of-the-Art analytics tools used in modern Crime Investigation are based on the keyword search and manual content exploration, while recent developments also added approximate pattern matching and so-called e-Discovery that helps and simplifies manual work of forensics investigations. Undoubtedly, this offers flexibility and speed in crime investigations, yet will not meet growing demand in advanced data analytic and decision support systems. Therefore, Big Data problems need a different approach to tackle large-scale data seized or correlated for a criminal case. As result, there is a strong need to apply Computational Intelligence methods capable of fast training and timely data processing [32]. This will enable future police in Smart Cities to effectively detect of new attacks, discover new adversarial trends and predict any future malicious patterns from the available historical data. Finally, intelligent data handling will result in building and providing timely response to ongoing crimes and best possible assistance in investigation of committed crimes.

Another aspect that became increasingly demanded in modern cyber-based society is protection of personal and sensitive personal information. Intelligent applications used for decision support will be able to handle Personal Data through application of homographic encryption methods that allows usage of computational methods over encrypted data and text [29]. However, this is an important issue that future police will face due to the fact that personal data protection regulations differs regionally and culturally. Notwithstanding, police main function will be to maintain public order, enforce the law, prevent any illegal crime activities before they happen and ensure reliable and timely crime investigation. Therefore, it is important to understand that colossal and agile data collection in Smart Cities will contribute to safer and secure environment despite multiple social and technical challenges affiliated with automated data processing and decision support in legal framework as it exist now.

3 Proposed Approach to Facilitate Smart Policing

Access to information before and after the crime plays a pivotal role in crime prevention, response and investigation. The researchers analyzed major crime incidents and identified that information sharing between multiple police levels is not ideal [22]. This is due to the fact that multiple entities with in the police may have access to information which according to them may not be relevant or confidential to other entities within the police. *Our proposed solution works by collecting information from multiple sources and creating a big picture of the environment.* In such way, it will be possible to identify relevant information and share it with relevant police entities for appropriate response It is expected that traditional criminals with increased surveillance in the smart city will be hesitant to commit a crime within city vicinity [27]. Traditional criminals will most likely focus on city suburbs where surveillance capabilities of police will be limited to city centers [12]. However, due to the transformation of city to a smart city by digital devices, provides an opportunity to cyber criminals to commit crime within the city center, Due to the inherent anonymity provided by cyberspace and crypto currencies it would be very difficult for the police to catch cyber criminals. Our proposed solution considers the smart city a big Intrusion Detection and Prevention System. The researchers used the NIST cyber security functions when considering the applications of proposed system on smart cities [30]. NIST cyber security framwork is presented in Figure 2.

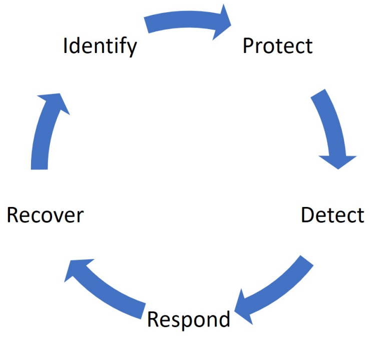

Figure 2: NIST Cyber Security Functions

In the system, first activity profiling of citizens will be performed. The activity profiling will be based upon human out of the loop autonomous technologies to preserve citizens privacy. Data will be collected from multiple sensors present within the smart city. Through the activity profiling a baseline of normal citizen behavior will be created. The baseline will be used to Identify and Protect citizens based upon historical criminal activity. Warnings will be issued for citizens performing activities in crime infested areas and police presences will be marked in crime infested areas to protect citizens by deterring criminals in performing malicious activity. Outliers from the baseline will be detected, and alerts will be generated based upon suspicious activity without human in the loop. Outlier and alert information will be passed on to human investigators for decision making and setting next line of actions. The system will suggest the next line of actions with possible outcomes in order to facilitate human decision maker to respond to a threat in an effective manner. The System is designed to deploy swarm of autonomous vehicles on land, air, sea and cyber space to perform intelligence surveillance and recon sense operations to respond and recover crime evidence and when the need arises to protect human life can also engage criminal with human assisted decision making. The system will provide unprecedented situational awareness to the police officers of the future. Which will enable the police officers to make smart decision based upon evolving threats. This will reduce the number of man hours required by police officer to do their jobs. A schematic diagram presenting working of proposed system can be seen in the Figure 3.

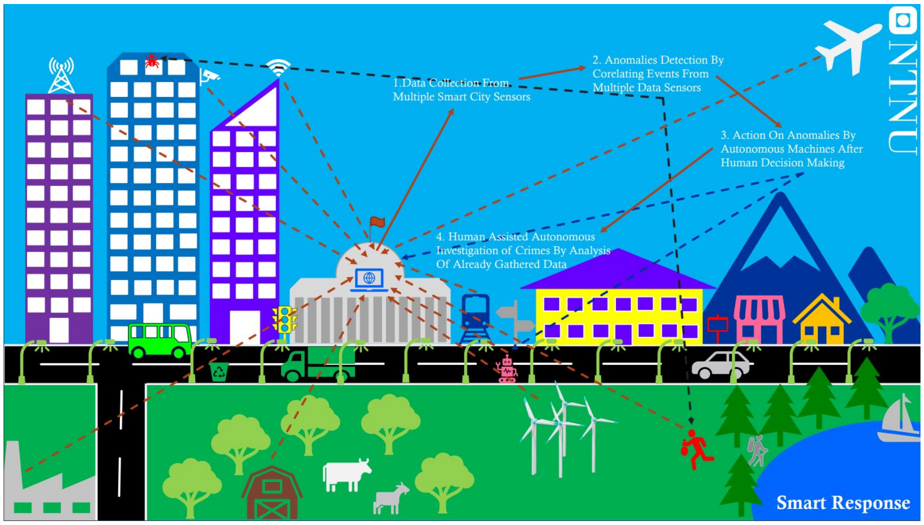
1.Data Collection From
Multiple Smart City Sensors
2. Anomalies Detection By
Corelating Events From
Multiple Data Sensors
3. Action On Anomalies By
Autonomous Machines After
Human Decision Making
4. Human Assisted Autonomous
Investigation of Crimes By Analysis
Of Already Gathered Data
NTNU
Smart Response

Figure 3: Concept for Future Smart City Policing

3.1 Smart Policing: Anticipated Methods

Following intelligent methods can be used to facilitate automated reasoning and proactive approach in Smart Police of future.

3.1.1 Human Out of The Loop Activity profiling

A lot of data will be generated by the sensors and devices present within the smart cities, and making sense of that data for crime prevention, responses and investigation will be challenge. Moreover, Data ownership, Data Sovereignty and citizen privacy related issues need to be addressed. Analyzing the smart city generated data by humans is difficult and privacy alarming, therefor research need to be carried out in privacy preserving technologies on citizen data. Human out of the loop technologies, can assist in analyzing citizen data while preserving citizen privacy. These technologies are autonomous systems that operate independently without human interference. Their decision making is based upon predefined rule set up by humans [35]. The rule set can be applied on a general set off data for identification of benign and malicious activities. For this identification of behavior benign and malicious citizen activity profiling is required. Activity profiling is the process of establishing individual citizen profile based upon a set of behavior metrics of citizen activities within the smart city.

The behavior metrics includes multiple parameters like travel history, transaction details, internet activity and other parameters data which can be collected from the sensors and devices present in the smart city. The activity profiling will then be utilized to generalize the citizens activity and establishing a baseline for normal citizen activity. The baseline of citizen activity profile will then be used to identify anomalies in citizens behavior for a proactive approach of crime prevention and response. In case the was not detected by the system the activity profile can be utilized for the investigation of crime and for fine tuning the system for similar future crimes.

3.1.2 Information and Computational Intelligence Model Fusion

Data fusion is the process of aggregating data from multiple data sources in order to produce more comprehensive and accurate information compare to an individual data source [10]. As multiple sensors are available in the smart city their functionality is increased by fusing data from multiple sensors it in commonly preferred as sensor fusion. For crime prevention, response and investigation data fusion will play a pivotal role in smart cities, as it will provide high level situational awareness to the autonomous system for analyzing information and supporting decision making in an evolving threat landscape.

3.1.3 Baseline Comparison

Behavior metrices of each and every citizen in the city can be compared with baseline of normal citizen activity developed during the activity profiling. The baseline comparison method will quantify the differences of normal and abnormal citizen activity created over a specific period of time which will then help to identify person of interest from a large population data set of citizens activity profiles. This can be achieved through state-of-the-art outlier detection algorithms. Other mean of information gathering like autonomous vehicles then can be deployed for citizen specific information gathering which can be used in proactive investigation of not normal behavioral activity.

3.1.4 Outlier detection

Outlier value are extreme deviations from the data under observation which are considered as anomalies in the data. There are two types of outlier univariate and multivariate. Univariate outliers are identified by single feature in data distribution values while multivariate outliers are identified by multiple features in data distribution values. In a smart city data will be generated from multiple data sources so outliers can be detected with multivariate outlier detection algorithms. However, it is very hard to identify outlier on large amount of multi-dimensional data set therefore new and efficient methods will be required to for the detection of anomalies. Advances in machine learning algorithms can assist in solving this problem.

3.1.5 Anomaly detection with Machine Learning

Machine Learning (ML) is a data analysis method which automates the process of analytic model development. Machine learning is a part of artificial intelligence in which systems are developed that can learn from data to identify patterns in data for making decision with minimal and no human interaction. Two main approaches of machine learning are developed to learn from data these are supervised and unsupervised learning algorithms. In supervised learning algorithms the input data is labeled and is trained over a set of training data with input and desired output. In unsupervised machine learning algorithms set of data which only contains inputs is given to the algorithm. The algorithms learn from data that has not been labeled or categorized which then identifies a structure and pattern in the data, like grouping or clustering of data points. Unsupervised learning algorithms identifies similarities in the data points and classify data by presence and absence of those similarities. In case of anomaly detection in citizen behavior both type machine learning algorithm can play their role. Particular threshold of specified several behavioral matrices of a citizen can be set for the identification of anomalies in a supervised manner and data classification. Unsupervised learning algorithms can identify anomalies without specifying a behavioral matrices however it consider the data which classification is in majority percentage as normal. A semi supervised machine learning approach can assist in analyzing large amount of data with minimum human interferences. Despite the advantage the machine learning algorithms offers in data classification and decision-making process a black box, explain ability of that decision-making process will going to be a big challenges criminal proceeding [36]. Theory of argumentation can assist to solve this problem.

3.1.6 Explanation of Decision Based upon Arguments

Theory of argumentation [4] focused on reaching conclusion based upon sound arguments. As the machine learning algorithms will provide a lot of data classification methods their effective usage in crime investigation prevention and response will require sound reasoning and it very difficult to achieve because law of the land is different at different places to argue on those reasons. Specific rule set need to define which are according to the law of the land for making argument based upon data classification for criminal jurisdiction in an autonomous manner.AI that can identify admissible evidence from set of given data will assist in reducing the time requirements for persecution. The technologies that are need to developed for this purpose are need to be transparent [9]. The inherent black box processing nature of machine learning algorithms is therefore not suitable for this purpose [28]. Hence it is expected that theory of argumentation can play key role in developing such technologies

3.1.7 Cyber Threat Intelligence and Threat Level Assessment

After identification of anomalies in citizen behavior the system needs to assign a threat level for a better response to the anomaly. The threat level assignment needs to consider multiple factors like the time period in which the anomaly becomes dangerous to other citizens, risks which the anomaly pose, the resources required to investigate the anomaly etc. This will help in better resource utilization on by assigning resources on immediate threats of crime. Every city has different threshold value of threat for different crimes, so the threat level assignment system is need to be developed according to specific city requirements. Sharing of that intelligence information in an autonomous manner will also play a key role [45] as there will be massive amount of information generated by the devices present in the smart city.

3.2 Modern Experimental Technologies and Collaborations

Vision of the future LEA needs in Smart Cities has been addressed by corresponding development of novel technologies and human interaction approaches

3.2.1 Police drones

Police drones can play a vital role in future smart cities crime prevention, investigation and response. They offer quite a lot of benefits compare to human police officers. First, they remove human officers out of the danger zone, second the drones are not affected by emotional break down and racial stereotypes and finally they are dispensable. More ever police drones are arguably more efficient in executing similar tasks assigned to a human police officer. This makes them viable in law enforcement and crime investigation in future smart cities, however, these drones only operate in physical world for cyber world radical new technologies will be required for law enforcement and crime investigation.

3.2.2 Cyber Police bots

As digital infrastructure is being rapidly expanding in the smart cities, security of this digital infrastructure will be a big challenge. Traditional police force seems ill equipped considering recent major cyber incidents. Technologies that enable police to petrol cyber world for the identification, detection and prevention of cyber incident need to be developed. Due to the massive digital footprint of smart cities it is humanly not possible for securing each and every device from the new vulnerabilities which are discovered every day. Autonomous technologies that can petrol the cyber space and identify and prevent potential vulnerabilities exploitation will enhance police capabilities in tackling cybercrimes.

3.2.3 Public Private Partnership

Bruce Schneier once said *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.* We can design and build sophisticated technologies but if it is not human centric then the technology will create more problems then solutions.

Methods to incentives information sharing between public and LEA are under development [3]. This will help to improve the performance of predictive police [37] mechanism which are powered by advance machine learning algorithms [43].

3.2.4 Smart Cities Standards

Multitude of work is going on developing smart cities standards, the govern technical, process/management and strategic/leadership aspects of smart cities. For technical aspects PAS 212 is developed for automatic resource discovery of IOT Devices. In term of process/management ISO/TS 37151, ISO 37100, ISO/IEC 30182 and ISO 37156 are developed. They provide key performance indicators, vocabulary,data concept and exchange models respectively. In term of strategic/leadership ISO 37101 is developed for the overall management of the smart city and its infrastructure. in order to measure he maturity level of smart cities infrastructure 37153:2017 [5] is developed. ISO 37153:2017 govern the infrastructure standards and used to measure the maturity level of smart cities infrastructure.

3.3 Challenges and Drawbacks

While implementation of such system is within the technical grasp of modern technologies some challenges still needs to be tackled with. Citizen privacy will be the biggest challenge in the implementation of such system as the system is working on collecting and processing citizen data its security need to be ensured with privacy preserving technologies like multi-party computation [19]. Data tampering for the data sources will create false anomaly condition with in the system which will cause false alert, so integrity of the data produced at the sensors must need to be ensured methods like template protection [23] can be useful to tackle this problem. More ever with increased data fusion from multiple data sensors data dimensions will increase which will make it very difficult in data processing for anomaly detection with current existing computational methods. Machine learning bias will also be a challenge for training the algorithms in a more neutral manner.

4 Use-case Scenarios in Smart Cities: modus operandi and police response

To support the ideas of future policing, there have been suggested the following scenarios that comprehend general categories of crimes found in both digital and physical realms.

4.1 Physical Crime Scenario for 'Detection' aspect

Before omnipresence of the Internet, all of the crimes were committed in a physical domain with all the traces left by perpetrators and victims.

Storyline. The city centers will contains most of the audio /visual data collection sensors so criminals will be hesitant in conducting crime in city centers. In a hypothetical scenario a individual is doing hiking in city suburb and provide an easy opportunity for a criminals. The criminal snatched the smartphone and additional items from the robber and ran away.

Infrastructure. Unknown to criminal the hiking trail was equipped with International Mobile Subscriber Identity (IMSI) catchers and based upon the previous activities of the hiker on the hiking trail an alert is generated that something is not right and an individual was identified moving with a different two different IMSI. The police officer can dispatch a drone for further investigation and tackling the criminal which is autonomously identified by his own subscriber identity number.

4.2 Cyber-Physical Crime Scenario for 'Prevention' aspect

With growing inclusiveness of ICT technologies, crimes a re moving towards involvement of new technologies and previously unseen attack vectors.

Storyline. The crime opportunity structure in smart cities will be changed digital devices will be prone to vulnerabilities and cyber criminals will take the advantage of Those vulnerabilities. In a hypothetical scenario cyber criminals plans to launch a cyber physical ransomware attack on smart locks, to lock the citizens and demand ransomware.

Infrastructure. Autonomous cyber policing bots detected communication on dark net about a particular smart lock vulnerability the information is then correlated with scans from public exploit scanning utilities which indicated working and work in progress of the vulnerability weaponization of smart locks. The information is then pass on to smart lock OEM (Orignal Equipment Manufacturer) to quickly launch an update to allow smart lock users unlock the lock with another backup key.

4.3 Cyber Crime Scenario for 'Investigation' aspect

Future perpetrators will find more elaborate and sophisticated ways of attacking system and breaching privacy of individuals as well as harming security on a state level.

Storyline In a hypothetical scenario cyber criminal performs a bank heist this time it was not detected or prevented.

Infrastructure. Data collection from both physical and cyber sensors is utilized for the identification of cyber criminals. Forensic investigation of attack chain will be done that how attackers penetrated the bank firewalls, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) through security logs then the data is correlated with ISP traffic history for the identification of command and controls channel of attackers.

5 Way Forward for Smart Cities Research

Considering aforementioned challenges and demands of the policing in future Smart Cities, there can be seen following measures to increase both awareness and readiness of general public and specialized response forces.

5.1 Cyber Ranges

Cyber Ranges are platforms that are designed to emulate the network infrastructure of an organization. The emulated network infrastructure can be then used for testing, training, education and experimentation purposes. Cyber ranges provide the capability to develop a digital twin of smart city in which the digital infrastructure of smart city can be tested and experimented with. As stated earlier in the crime opportunity structure the focus of the crimes is shifting towards cyber domain, so this capability can be utilized to proactively develop and test new crime scenarios ranging from cyber to cyber physical domain. This will help the future smart city police to develop strategies to counter crimes before they happen.

Cyber ranges can be good for cyber security exercises and experimentation [46, 44] however to be utilized in an effective manner for the betterment of society, they also need to incorporate the societal view [47]. Integration of societal and technical prospective in cyber range will provide the opportunity to deal with the human aspect associated with the cyber domain in a time of crisis [31]. This will enable the future police to better train in complex scenarios and tackle crime by incorporating the human prospective as well. This results in better and well prepared police force of the future that can handle crime in a proactive manner not in a reactive manner.

5.2 Digital Forensics Readiness and Incident Response

Another important approach that needs to be integrated in policies and future technology deployment organization- and cities-wise is forensics readiness. This is a concept that represents a model where devices are properly configured to retain evidences and data for possible cyber crime investigation on the basis of ”need-to-know” principle. Rowlingson in 2014 [34] defined ten measures and activities that are required to ensure so-called Network Forensics Readiness. Those include aspects such as data handling, legal compliance, policy development and employees training. Future Smart Cities will enable huge data traffic that will not be possible to keep in ”Data Lakes” for a long time. Therefore, proper Digital Forensics-friendly data collection and processing nodes need to designed to ensure timely investigation of the incidents without any impact on the human-oriented services of Smart Cities. Moreover, measures that will be implemented should aim not only at so-called ”extremistan” events and crimes (high-impact low-likelihood), yet also at more frequent events with lower impact to be able to provide adequate response to crimes [15, 1].

The next important aspect is Incident Response, which will require corresponding knowledge of the previous crime historical information with corresponding action plans, involving individuals, organizations and cities. Current State of the Art include integration of such regular and ad-hoc teams as Special Weapons and Tactics (SWAT), Community Emergency Response Team (CERT) and Hazardous Materials Management (HAZMAT). While, those have been introduced since 1960 and proved efficiency, Smart Cities put new demands towards cross-departments and cross-response teams collaboration [13]. This requires rethinking of the traditional physical crimes model towards more advanced cyber-oriented components of the city that might be affected. Omnipresent Situational Awareness and Threats (Physical and Cyber) Intelligence will give new insights in addition to conventional digital forensics readiness in place.

6 Conclusion

Preventative measures and reactive measures for fighting crime are blending. The cyber and physical world are increasingly blending as well. Development of such system will present opportunity to enable future police officers to use data to prevent/investigate crime. This will keep LEA ahead compare to the adversaries in new crime opportunity structure. As indicated in opportunity structure model and enabling factors such as the availability of relevant information and technology that will enable future smart police to work **proactivaly**.

As Bejamin Franklin once stated *”Security without liberty is called prison”*, security by consensus [25] should be followed when such technology is developed. Else it will give immense power to people controlling such technologies. These technologies can solve allot of problems that we are facing today in term of physical and digital crime, however developing such technologies may have unintended consequences in wrong hands.

7 Acknowledgment

The authors are grateful for the support by the Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology (NTNU). The researchers would like to acknowledge the NTNU team participation in the Interpol Thinkathon 2018 competition: Danny Lopez Murillo, Kyle Porter and Ivan Talwar, who equally contributed in development of the winning idea. The researchers would also like to thank the valuable feedback from our coaches Basel Katt, Jens-Petter Sandvik, Katrin Frank and Stewart James Kolwaski, without which this work would not be possible.

References

[1] Nurul Hidayah Ab Rahman, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, 3(1):50–59, 2016.

[2] Mohammad Abu-Matar and John Davies. Data driven reference architecture for smart city ecosystems. In *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 1–7. IEEE, 2017.

[3] Vivek Agrawal. Information security risk management practices: Community-based knowledge sharing. 2018.

[4] Robert Alexy. A theory of legal argumentation: The theory of rational discourse as theory of legal justification. 2009.

[5] L Anthopoulos and G Giannakidis. Policy making in smart cities: Standardizing city's energy efficiency with task-based modelling. *Journal of ICT Standardization*, 4(2):111–146, 2016.

[6] Željko Bačić, Tomislav Jogun, and Ivan Majić. Integrated sensor systems for smart cities. *Tehnički vjesnik*, 25(1):277–284, 2018.

[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*, volume 292, 2011.

[8] Philip Boucher. How artificial intelligence works. `http://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-how-artificial-intelligence-works.pdf`.

[9] Joanna Bryson and Alan Winfield. Standardizing ethical design for artificial intelligence and autonomous systems. *Computer*, 50(5):116–119, 2017.

[10] Federico Castanedo. A review of data fusion techniques. *The Scientific World Journal*, 2013, 2013.

[11] Irena Pletikosa Cvijikj, Cristina Kadar, Bogdan Ivan, and Yiea-Funk Te. Towards a crowdsourcing approach for crime prevention. In *Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers*, pages 1367–1372. ACM, 2015.

[12] Irvin Dawid. As cities become safer crime decamps for the suburbs.

[13] Marios-Panagiotis Efthymiopoulos. Cyber-security in smart cities: the case of dubai. *Journal of Innovation and Entrepreneurship*, 5(1):11, 2016.

[14] William D. Eggers, Bill, Rana Sen, Rana, Deloitte, Center for Government Insights, and Deloitte Consulting LLP. Building the smart city with data, digital, and design — deloitte us, Jan 2018.

[15] Mohamed Elyas, Atif Ahmad, Sean B Maynard, and Andrew Lonie. Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, 52:70–89, 2015.

[16] EY. Smart policing for smart cities. `http://www.governancenow.com/files/FICCIReport-SMARTPolicingforSmartCities.pdf`, 2015.

[17] Aditya Gaur, Bryan Scotney, Gerard Parr, and Sally McClean. Smart city architecture and its applications based on iot. *Procedia computer science*, 52:1089–1094, 2015.

[18] GDPREU. Gdpr - personal data. `https://gdpr-info.eu/issues/personal-data/`.

[19] Oded Goldreich. Secure multi-party computation. *Manuscript. Preliminary version*, 78, 1998.

[20] Marc Goodman. *Future crimes: Everything is connected, everyone is vulnerable and what we can do about it*. Anchor, 2015.

[21] Hans W Gottinger and H-P Weimann. Intelligent decision support systems. In *Methodology, Implementation and Applications of Decision Support Systems*, pages 1–27. Springer, 1991.

[22] John S Hollywood and Zev Winkelman. *Improving Information-Sharing Across Law Enforcement: Why Can't We Know?* National Criminal Justice Reference Service, 2015.

[23] EJC Kelkboom, Xuebing Zhou, J Breebaart, Raymond NJ Veldhuis, and C Busch. Multi-algorithm fusion with template protection. In *2009 IEEE 3rd international conference on biometrics: Theory, applications, and systems*, pages 1–8. IEEE, 2009.

[24] Andrej Kovacevic. Police are using big data to predict future crime rates, Nov 2018.

[25] Stewart Kowalski. The sbc model as a conceptual framework for reporting it crimes. In *Proceedings of the IFIP TC9/WG9. 6 Working Conference on Security and Control of Information Technology in Society on board M/S Illich and ashore*, pages 207–226. North-Holland Publishing Co., 1993.

[26] Chiehyeon Lim, Kwang-Jae Kim, and Paul P Maglio. Smart cities with big data: Reference models, challenges, and considerations. *Cities*, 82:86–99, 2018.

[27] Cameron McWhirter and Gary Fields. Crime migrates to suburbs, Dec 2012.

[28] Donald Michie, David J Spiegelhalter, CC Taylor, et al. Machine learning. *Neural and Statistical Classification*, 13, 1994.

[29] Michele Minelli. *Fully Homomorphic Encryption for Machine Learning*. PhD thesis, PSL University, 2018.

[30] NIST. Cybersecurity framework. `https://www.nist.gov/cyberframework`.

[31] Grethe Østby, Muhammad Mudassar Yamin, and Bilal Al Sabbagh. siems in crisis management: detection, escalation and presentation–a work in progress. In *5th interdisciPlinary cyber research conference 2019*, page 38, 2019.

[32] PredPol. Machine learning and policing. `http://blog.predpol.com/machine-learning-and-policing`.

[33] Carmen Rotuna, Carmen Elena Cîrnu, Dragos Smada, and Alexandru Gheorghiță. Smart city applications built on big data technologies and secure iot. *Ecoforum Journal*, 6(3), 2017.

[34] Robert Rowlingson. A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3):1–28, 2004.

[35] Bobak Shahriari, Kevin Swersky, Ziyu Wang, Ryan P Adams, and Nando De Freitas. Taking the human out of the loop: A review of bayesian optimization. *Proceedings of the IEEE*, 104(1):148–175, 2016.

[36] Andrii Shalaginov. *Advancing Neuro-Fuzzy Algorithm for Automated Classification in Largescale Forensic and Cybercrime Investigations: Adaptive Machine Learning for Big Data Forensic*. PhD thesis, Norwegian University of Science and Technology, 2018.

[37] Aaron Shapiro. Reform predictive policing. *Nature News*, 541(7638):458, 2017.

[38] Uthayasankar Sivarajah, Muhammad Mustafa Kamal, Zahir Irani, and Vishanth Weerakkody. Critical analysis of big data challenges and analytical methods. *Journal of Business Research*, 70:263–286, 2017.

[39] Torkjell Jonsson Trædal. Norsk forskning på framtidens politi til topps i interpol, Oct 2018.

[40] Mohib Ullah and Faouzi Alaya Cheikh. A directed sparse graphical model for multi-target tracking. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 1816–1823, 2018.

[41] Mohib Ullah, Faouzi Alaya Cheikh, and Ali Shariq Imran. Hog based real-time multi-target tracking in bayesian framework. In *2016 13th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 416–422. IEEE, 2016.

[42] UNICEF. Big data for social good. `http://unicefstories.org/tag/big-data-for-social-good/`.

[43] Tong Wang, Cynthia Rudin, Daniel Wagner, and Rich Sevieri. Learning to detect patterns of crime. In *Joint European conference on machine learning and knowledge discovery in databases*, pages 515–530. Springer, 2013.

[44] Muhammad Mudassar Yamin and Basel Katt. Inefficiencies in cyber-security exercises life-cycle: A position paper. In *AAAI Fall Symposium: ALEC*, pages 41–43, 2018.

[45] Muhammad Mudassar Yamin and Basel Katt. A survey of automated information exchange mechanisms among certs. In *CERC*, pages 311–322, 2019.

[46] Muhammad Mudassar Yamin, Basel Katt, Espen Torseth, Vasileios Gkioulos, and Stewart James Kowalski. Make it and break it: An iot smart home testbed case study. In *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, page 26. ACM, 2018.

[47] Muhammmd Mudassar Yamin, Basel Katt, and Mazaher Kianpour. Cyber weapons storage mechanisms. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pages 354–367. Springer, 2019.