ЗАЩИТА ДАННЫХ В СИСТЕМАХ МОНИТОРИНГА БЕЗОПАСНОСТИ КРУПНОМАСШТАБНЫХ ОБЪЕКТОВ

Полтавцева М.А., Калинин М.О.
Санкт – Петербургский политехнический университет Петра Великого
poltavtseva@ibks.spbstu.ru

Аннотация: В работе рассматриваются особенности систем управления данными при мониторинге безопасности крупномасштабных объектов. Выделены особенности угроз и возможностей нарушителя. На основе принципов построения защищенных систем управления большими данными авторами предложены решения по концептуальному описанию данных и операций системы мониторинга, обеспечению технологической и архитектурной полноты защиты. Проведена классификация узлов – обработчиков в соответствии с принципом минимизации доверия. Предложена новая архитектура типового звена управления данными системы мониторинга безопасности в защищенном исполнении.

Ключевые слова: Большие данные, информационная безопасность, мониторинг безопасности крупномасштабных объектов.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-03102

Введение

Современные тенденции в области цифрового управления и производства приводят к широкому применению информационных систем для автоматизированного мониторинга, в том числе – мониторинга крупномасштабных объектов промышленного характера. Характерные черты таких систем, такие как: распределенность, взаимодействие через публичные сети (включая Интернет), связь с реальными физическими объектами и процессами, делают их привлекательными для нарушителя.

В последнее время происходит все большее число инцидентов безопасности, связанных с крупномасштабными промышленными и инфраструктурными системами: нефтепереработкой, водоочисткой, электросетями, системами управления умного города и транспортными системами. Такая ситуация порождает необходимость не только мониторинга событий безопасности в крупномасштабных системах, но и защиты самой системы обеспечения устойчивого функционирования от злоумышленника.

1 Защищенный мониторинг безопасности крупномасштабных объектов

Сегодня мониторинг безопасности используется в различных отраслях и связан с решением целого ряда задач: оценки физических объектов [1,2], защите систем «умного города» [3] и транспортных систем [4], энергетике [5]. Он является динамически развивающейся областью

исследований, особенно в киберфизической области, в отношении крупномасштабных систем. Это связано как с развитием систем защиты информации, так и с все большей компьютеризацией и комплексностью систем управления [6]. Мониторинг безопасности в киберфизических системах, использующих цифровое управление физическими объектами и процессами, рассматривается в работах Флинка [7], Кнаппа [8], Даса и Канта [9], Зегжды[10], Саенко[11]. В работе [7] обосновывается необходимость сочетания цифровой и физической защиты киберфизических систем, выделяются требования к безопасности и конфиденциальности данных. В свою очередь Кнапп [8], как и работа [12], рассматривает промышленный мониторинг сравнительно с известными системами мониторинга крупномасштабных сетей. В отечественных исследованиях [10, 11, 13] оцениваются перспективы и предлагаются решения по построению систем крупномасштабного мониторинга безопасности.

Эффективность задач мониторинга безопасности сегодня зависит от обработки больших объемов данных [2,3,10,11], корректность и конфиденциальность которых достаточно важны [14]. От корректности и скорости обработки этой информации зависит качество защиты крупномасштабного объекта [15]. Требование конфиденциальности обусловлено тем, что для оценки защищенности используются важные данные реальных систем, попадание которых к злоумышленнику также может нанести существенный вред [16]. Однако, системы управления Большими данными на сегодняшний день имеют ряд проблем с защитой информации [17, 18], связанных с технологическим развитием самих решений [19] и изменением в модели угроз [20]. Это отмечается целым рядом исследователей [21-24]. Таким образом, задача защиты информации в этом классе систем является сейчас высоко актуальной. Настоящая работа описывает новый подход и соответствующие практические решения для построения защищенных систем управления Большими данными в информационных системах мониторинга безопасности крупномасштабных объектов.

2 Подход к обеспечению безопасности систем управления данными мониторинга

2.1 Угрозы для системы управления данными при мониторинге безопасности

Новые угрозы в системах управления большими данными связаны со сложным жизненным циклом фрагментов обрабатываемой информации и снижением степени доверия у узлам - обработчикам. Системы мониторинга безопасности крупномасштабных объектов имеют иерархическую структуру, для секционирования и своевременного реагирования на угрозы с одной стороны, и комплексной оценки состояния системы – с другой. Это позволяет классифицировать их как гетерогенные по составу инструментов географические системы.

В таких системах дополнительные угрозы связаны с несколькими аспектами (рис. 1):

1. Передачей данных по сетям связи;
2. Сложностью обеспечения доверия всем компонентам обработки информации;
3. Сложностью защиты и широкими возможностями логического вывода со стороны внутреннего нарушителя.

Последствия таких угроз также могут быть существенными. Целью нарушителя может быть дискредитация и нарушения в системе работы мониторинга безопасности, что открывает возможности для прочих нарушений. Возможно получение злоумышленником данных об объекте, его организации (географической и структурной), системе защиты. И, наконец, существует возможность получения доступа к управляющим данным, связанным с принятием решения по функционированию физического объекта. Если система мониторинга безопасности совмещена с системой общего мониторинга (как правило, используется общая архитектура данных), это возможность, в конечном итоге, влиять на функционирование объекта в обход систем защиты.

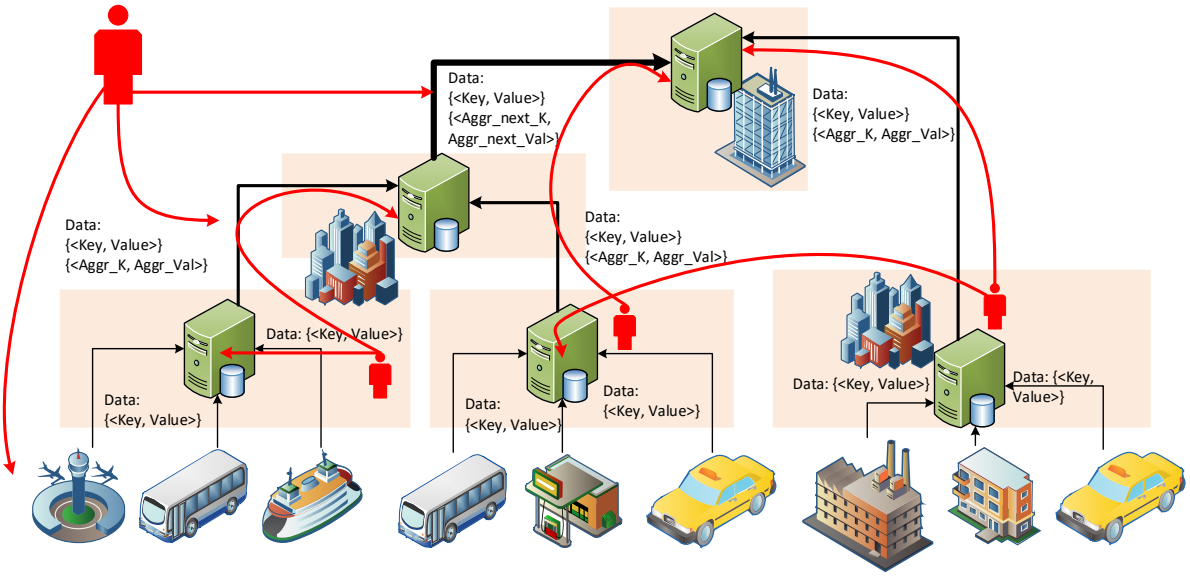

Рис. 1. Угрозы в иерархической системе мониторинга безопасности

Следовательно, основными угрозами для систем мониторинга безопасности крупномасштабных объектов становятся:

1. Нарушение конфиденциальности данных объекта защиты, в том числе, путем логического вывода [25];
2. Нарушение конфиденциальности данных об объекте защиты, включая режимы его функционирования, структурные особенности и т.д.
3. Нарушение целостности данных и работоспособности (доступности) системы мониторинга объекта защиты, и, как следствие, снижение защищенности объекта.
4. Нарушение корректности функционирования объекта защиты путем нарушения целостности и подмены данных мониторинга (в том числе, мониторинга безопасности).
5. Получение нарушителем доступа и возможности воздействия на другие компоненты программно-аппаратного комплекса путем эксплуатации уязвимостей инструментов управления данными.

В качестве основных путей реализации этих угроз можно выделить новые аспекты, связанные с распределенной иерархической природой системы управления данными:

1. Использование внутренним нарушителем доступа к периферийным узлам обработки и передачи данных, включая физическое искажение данных, получение доступа и модификация данных при их передаче между различными программными компонентами обработки и управления на всех уровнях системы.
2. Использование внутренним нарушителем недостатков согласования политик доступа отдельных инструментов в рамках системы управления Большими данными.
3. Использование внешним нарушителем уязвимостей компонентов обработки и хранения данных, связанных общей коммуникационной средой на всех уровнях системы.

Из-за сложной иерархической структуры в системах мониторинга крупномасштабных объектов увеличивается вероятность реализации угрозы внутренним нарушителем, усложняются традиционные меры защиты. Важно сказать, что нарушитель, имея доступ к периферийным компонентам крупномасштабного объекта, через инфраструктуру обработки и передачи данных может оказывать влияние на всю систему в целом.

2.2 Подход к обеспечению безопасности

Исходы из вышеизложенного, можно классифицировать систему управления Большими данными при мониторинге безопасности крупномасштабных объектов как систему с не доверенными обработчиками, описываемую моделью [26]. Для обеспечения безопасности таких систем необходимо применение комплексного подхода. Основными задачами безопасности при построении системы управления данными становятся:

1. Отслеживание взаимосвязей и соблюдение политики доступа к данным на протяжении всего жизненного цикла обработки информации;

2. Защита данных на протяжении всего жизненного цикла при передаче, хранении и обработке с учетом низкой степени доверия к узлам – обработчикам.

Большинство современных решений по защите Больших данных [27,18] не предлагает комплексного решения проблемы, за исключением согласованных подходов на основе одного программного стэка и частных облаков. Географическая распределенность и использование различных инструментов для управления данными в системе мониторинга крупномасштабных объектов делает невозможным использование предложенных решений. Для систем этого класса в работе [29] предложен консистентный подход к обеспечению защищенности, основанный на принципах консистентности описания данных и процессов, полноты защиты и минимизации доверия. В данной работе рассматривается построение защищенных систем мониторинга безопасности в соответствии с этими принципами.

3 Консистентное представление данных и процессов мониторинга безопасности

3.1 Представление данных мониторинга безопасности в агрегатной модели

Согласно работам [30-34], данные мониторинга в различных областях представляют собой наборы временных рядов параметров, использующихся для дальнейшего анализа. Таким образом, с точки зрения системы хранения важным представляется два набора данных. Во-первых, набор фактических данных вида <Paremeter, {Timestamp, Value}>, где Parameter –фиксируемое значение, {Timestamp, Value} – набор значений, где каждому значению сопоставлено время его формирования. Во-вторых, это справочники метаданных:

1. Справочник параметров;
2. Справочник временных рядов.

Это два связанных набора метаданных. Первый справочник определяет фиксируемый набор параметров системы, второй – для каждого параметра определяет характеристики значений временного ряда. В промышленной системе с гетерогенными источниками данных этот набор данных расширяется дополнительными метаданными (см. например [35]). Для унификации представления данных и операций по их обработке в системе безопасности, сформируем схему данных в концептуальной агрегатной модели [29] (рис.2).

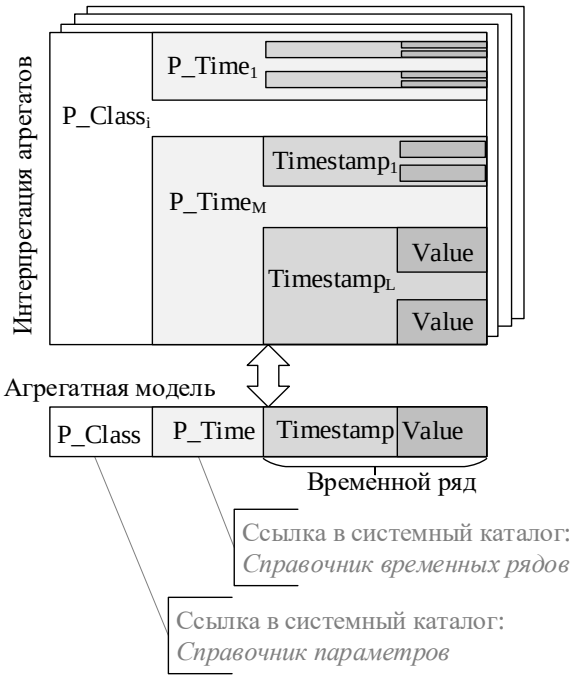

Рис. 2. Агрегатное представление данных мониторинга

В качестве базового агрегата предлагается использовать пару <Key, Value> где в качестве ключа выступает кортеж <P_Class, P_Time, Timestamp>, где P_Class - параметр, P_Time – идентификатор временного ряда, Timestamp – временная метка значения, а значение агрегата представляет собой <Value> временного ряда. В этом случае базовый составной агрегат вида *<<P_Class, P_Time, Timestamp>, <Value>>* раскладывается на вложенные агрегаты вида: *<P_Class, <P_Time, <Timestamp, Value>>*. Составной ключ базового агрегата уникально идентифицирует его

в пределах системы, однако на практике используется система вложенности, так как, не смотря на то, что метка Timestamp не уникальна в пределах системы, набор ключей вышележащих агрегатов в сочетании с меткой Timestamp определяет уникальное значение. Этот подход соответствует функции порождения ключа по умолчанию $F_{key}^{default}(A^F)$ [36]. При необходимости могут быть добавлены уровни вложенности, связанные с иерархической агрегацией географически распределенной системы: идентификатор источника данных или другие мета - параметры.

3.2 Процессы обработки данных при мониторинге безопасности

Операции над данными в системе мониторинга предлагается разделить на две группы. Первая группа – это операции оперативного управления информацией, включая ее запись, выборку и пересылку. Основными ключами выборки данных являются:

1. Параметры;
2. Временные ряды, отражающие различную степень агрегации данных.

Вторая группа – операции аналитической обработки, которые можно разделить на:

1. Операции формирования временного ряда большей размерности.
2. Сложные вычислительные операции над компонентами ряда.

С точки зрения агрегатной модели эти действия представляет следующий набор операций:

$Create(P\_Class,\{\})$ - ввод нового параметра в систему.

$Create(P\_Time,\{\})$ и $Include(<P\_Class,\{\}>,<P\_Time,\{\}>)$ - отражает создание временного ряда соответствующего параметра;

$Create(Timestamp,Value)$ и $Include(<P\_Class \cdot P\_Time,\{\}>,<Timestamp,Value>)$ - создание агрегата, отражающее факт записи значения в систему управления данными. В данном случае операция конкатенации ключей $P\_Class \cdot P\_Time$ отражает принадлежность временного ряда к конкретному параметру.

Выборка данных по ключу осуществляется модельной операцией $a = Select(Key, A^{\cup})$.

Перестроение временных рядов, как и проведение аналитических операций выражается в агрегатной модели через функцию порождения новых агрегатов вида $a^F = CreateF(Key, F(A^F)), A^F \subseteq A$, где A – множество агрегатов в системе, a^F – порождаемый агрегат, а A^F – множество агрегатов, участвующих в порождении нового значения. Тогда $F(A^F)$ – функция, выполняемая над множеством агрегатов A^F.

3.3 Управление доступом

Так как доступ различных участников (поставщиков данных, аналитиков) к системе мониторинга регламентируется характером требуемых (поставлямых) им данных или подключения, разграничение доступа предлагается регламентировать на основе ABAC [37]. В этом случае основными атрибутами, определяющими права доступа, будут:

1. Параметр;
2. Время поступления данных;
3. Точка (географическое положение или узел) поступления данных;
4. Источник данных.

При необходимости могут использоваться дополнительные атрибуты. Все эти характеристики получаются в момент поступления кортежа автоматически. Использование идентификатора источника позволяет дополнительно проводить его верификацию. Для участников процесса сбора и обработки данных можно выделить несколько ролей в отношении системы мониторинга:

1. Источник данных. Это узел, не запрашивающий, а являющийся поставщиком данных определенного типа и характера в систему.
2. Аналитик или потребитель данных. Это узел, применяющий данные и строящий к ним аналитические запросы. По сути, он обладает правом выполнения над данными функций множества F_A.
3. Обработчик данных. Это программный компонент (или пользователь) осуществляющий над данными операции обработки и загружающий результаты своих действий в систему.

Права доступа пользователя и, следовательно, для конечного пользователя также определяются в терминах кортежа *<Parameter, Time_in, Incoming_node/Source>* При этом временная характеристика Time_in задается диапазоном, внося в ABAC элементы интеллектуализации [38]. Источник данных обладает единственным правом на запись информации в систему, то есть вызов

функций: $Include(< P\_Class \cdot P\_Time, \{\} >, Create(< Timestamp, Value >))$ строго в указанном формате с учетом атрибутов соединения.

В свою очередь, потребитель данных несмотря на то, что получает на выходе итоговый кортеж, имеет потенциальный доступ ко всей информации, которая использовалась при его порождении. На сегодняшний день уязвимостям логического вывода подвержены практически все хранилища информации, а для агрегирующих статистических баз данных эта проблема существует достаточно давно [39]. Таким образом, политика безопасности должна распространяются на все агрегаты, участвовавшие в порождении доступных для пользователя (человека или программного компонента) данных. Для достижения этого свойства права доступа конечного потребителя определяются кортежем <*Parameter, Time_in, Incoming_node/Source*> над входными агрегатами. Пава доступа к производным агрегатам определяются на основании входящих в них исходных.

Обезличивание данных (фактически, создание новых данных на основе исходных) уничтожающее любою связь между исходной и порожденной информацией, и формирующие новые «исходные» кортежи, должно подчиняться следующим правилам:

1. Производиться на доверенном узле.
2. Учитывать при порождении данных требования k-анонимности и другие технологии защиты статистической информации [40-42].

Указанные решения позволяют обеспечить выполнение политики безопасности на всем протяжении обработки данных и снизить вероятность эксплуатации уязвимости логического вывода.

4 Полнота защиты и минимизация доверия

4.1 Обеспечение технологической и архитектурной полноты защиты данных

Обеспечение полноты защиты связано с последовательным построением системы защиты «снизу вверх» и полнотой отображения структур логического уровня обработки данных на концептуальный уровень проверки безопасности [29]. При обработке данных мониторинга безопасности используются несколько типов хранилищ данных [11, 30-34]:

1. Хранилища данных в памяти для оперативного хранения обрабатываемых пакетов при препроцессинге и анализе данных;
2. Долговременные хранилища на диске сырых данных;
3. Долговременные хранилища да диске исторических данных анализа.

Первые два типа хранилищ относятся к системам с низкой структуризацией данных, ориентированным на быструю выборку и запись информации. К ним относятся системы управления базами данных на основе моделей Ключ – значение и Семейство столбцов. Между агрегатной моделью данных и этими логическими представлениями существует по крайней мере один метод однозначного отображения [36], гарантирующий технологическую полноту защиты.

Множество аналитических операций по порождению новых временных рядов и агрегированных значений в системе мониторинга описывается как $F_A = \{f \mid f \in F\}$. При этом $F_A = F_{agr} \cup F_{analitics}$, где F_{agr} – это простые агрегирующие функции (сумма, количество, среднее), а $F_{analytics}$ – более сложные аналитические решения. В то же время компонентами хранения (СУБД) в памяти и на диске выполняются простые операции вставки, удаления, изменения и выборки данных, множество которых определим как F_{dops}. Все функции обработки данных можно определить как совокупность $F = F_A \cup F_{dops}$, гарантируя полноту отображения с точки зрения процессов обработки.

Нижем уровнем системы управления Большими данными, согласно архитектуре ANSI/SPARC, является сетевая инфраструктура и физическое хранение данных в СУБД [26]. Не останавливаясь на сетевой безопасности, безопасности операционных систем, оборудования и т.д., которым посвящено много специализированных работ, рассмотрим физическую защиту данных путем шифрования. Требованиями к системе шифрования являются: безопасность, высокая скорость операций с данными (что означает выполнение операций над данными без расшифрования), небольшое увеличение объема данных. Современными подходами к шифрованию в этой области являются:

1. Полностью гомоморфное шифрование (FHE - Fully Homomorphic Encryption)
2. Линейное разделение секрета (LSS - Linear Secret Sharing)
3. Garbled Circuits (GB)

Сегодня характеристиками, пригодными для промышленного применения обладают алгоритмы гомоморфного шифрования, относящиеся к категории OPE (Order – Preserving Encryption). Они обеспечивают шифрование с сохранением порядка и позволяют выполнять над зашифрованными данными операции сравнения. Анализ OPE – схем показывает наибольшую потенциальную эффективность R-OPE [43] шифрования, предложенного Шатиловым. Использование этой схемы позволяет выполнять над зашифрованными данными операции сравнения на равенство и сравнения порядка, достаточные для простых NoSQL СУБД в системе управления Большими данными.

4.2 Минимизация доверия и архитектура системы мониторинга

Принцип минимизации доверия в системе управления большими данными [29] определяет классификацию узлов системы на доверенных и не доверенные для распределения между ними операций. Иерархическая организация системы мониторинга определяет схему взаимодействия географически распределенных компонент, представленную на рисунке 3.

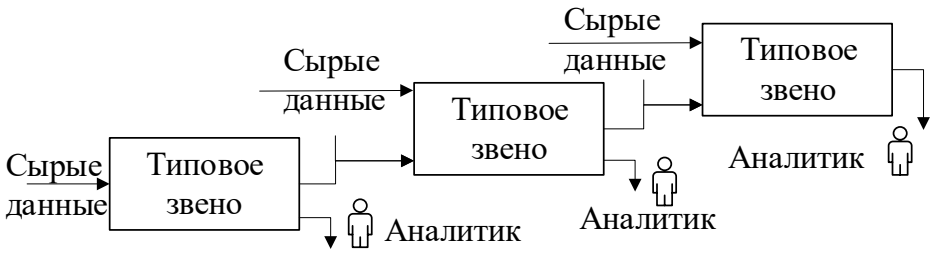

Рис. 3. Иерархическое взаимодействие распределенных подсистем управления данными

Типовое звено обработки осуществляет сбор и предварительную обработку исходных данных своего уровня, хранение данных, анализ собранных данных совместно с анализом данных поступивших с нижележащих слоев мониторинга. Схема типового звена мониторинга приведена на рисунке 4.

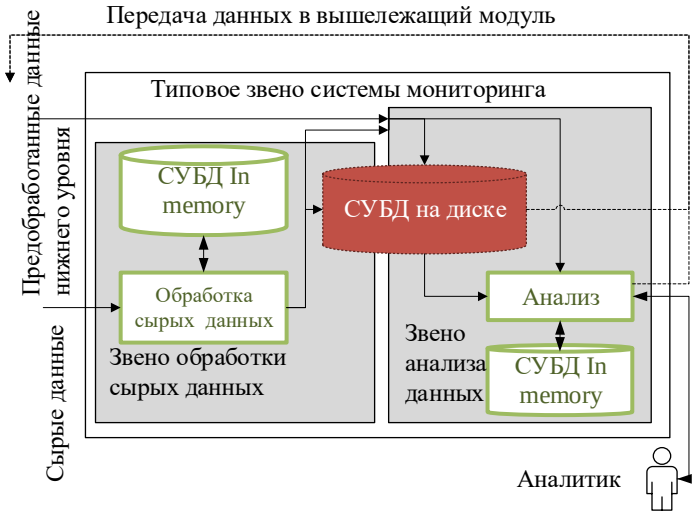

Рис.4 Типовое звено системы управления данными распределенного мониторинга

Для классификации узлов типового звена по принципу секретности используется аналогичная классификация операций над данными и отображение их на узлы - исполнители. Предложенная Шатиловым К.А. схема шифрования OPE позволяет выполнять операции сравнения на равенство и на порядок, позволяя выполнять F_{dops} в защищенном исполнении, при условии исключения аналитических операций из технологических операций Map-Reduce, с выносом их на узлы анализа. Для выполнения операций NoSQL СУБД типа ключ – значение и семейство столбцов, как и базовых операций Map_reduce, достаточно иметь возможность сравнения данных на точное совпадение и на

равенство. Аналитические функции множества F_A требуют намного большей функциональности, которая на сегодня не реализуется системами шифрования с должной эффективностью. Таким образом, операции категории FA должны выполняться на доверенном узле.

Таким образом, формируется итоговая архитектура типового звена системы управления Большими данными, представленная на рисунке 5.

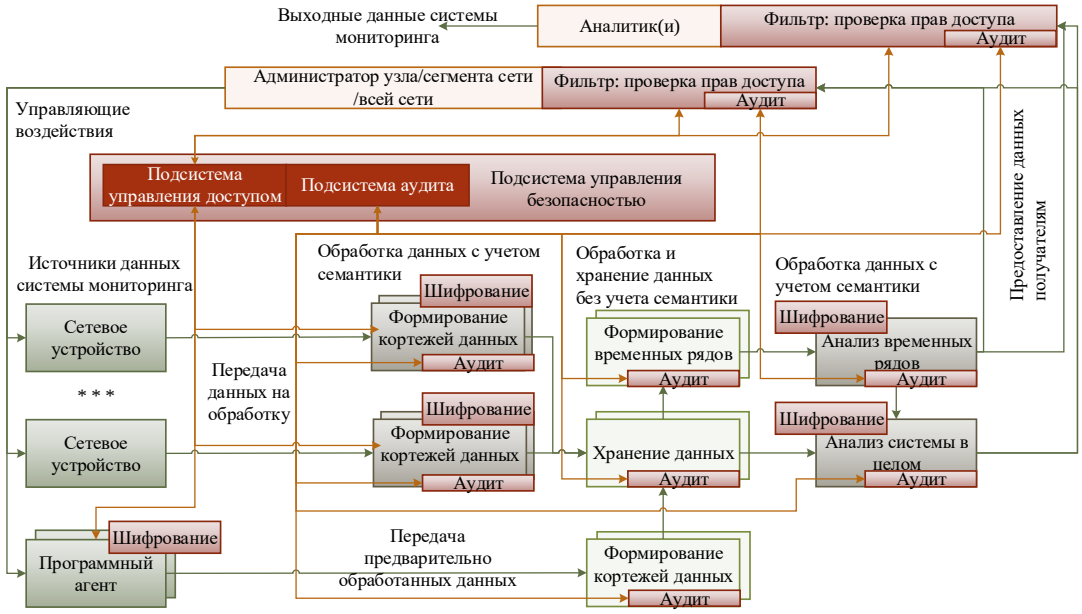

Рис. 5. Архитектура типового звена системы управления Большими данными

Модули, связанные с доверенной обработкой данных снабжены фреймворками шифрования, осуществляющими дешифровка и шифрование данных. Они должны располагаться на доверенных узлах системы. Узлы, выполняющие хранение, выборку и фильтрацию данных (обработку данных без учета семантики) могут выполнять свои функции над зашифрованными данными в не доверенном режиме.

Заключение

В качестве основных особенностей, с точки зрения обработки данных в защищенном режиме, в системах мониторинга крупномасштабных объектов можно выделить иерархическую, географически распределенную организацию и сложный жизненный цикл данных. Это приводит к повышению вероятности реализации угроз, связанных с компрометацией одного из узлов – обработчиков и эксплуатацией уязвимостей логического вывода. Результатом реализации этих угроз может стать возможность для злоумышленника не только получение данных о физическом процессе и режиме функционирования объектов, но и дискредитация системы защиты, возможность влияния на целевую систему.

Построение защищенной системы управления большими данными для систем мониторинга безопасности крупномасштабных объектов является сложной актуальной задачей. Применение принципов построения защищенных систем управления данными, таких как принцип единства представления данных и процессов, принцип технологической и архитектурной полноты и принцип минимизации доверия позволяют комплексно подойти к этому вопросу, определив основные концептуальные структуры, подходы к построению разграничения доступа на их основе, разделение узлов и операций между ними.

Предложенная авторами схема разделения узлов является технологически зависимой, так как ориентирована на современную систему шифрования OPE. С одной стороны, этот подход требует пересмотра распределения задач по узлам при применении менее гибкого к операциям над данными шифрования (например, AES). Однако, при развитии шифровальных методов распределение функций обработки информации между узлами может быть пересмотрено в сторону расширения числа операций, выполняемых на не доверенных узлах. Таким образом, технологическая зависимость или технологическая гибкость в данном случае является скорее преимуществом архитектуры, позволяющим адаптировать ее для различных систем по мере развития шифровальных средств.

Предложенная авторами архитектура типового звена мониторинга разработана с учетом современных методов защиты информации, управления данными и специфики систем мониторинга безопасности.

Литература

1. *Scardapane S., Scarpiniti M., Bucciarelli M., Colone F., Mansueto M. V., Parisi R.,* Microphone array based classification for security monitoring in unstructured environments // AEU - International Journal of Electronics and Communications. Vol. 69. 2015, Is. 11. – P. 1715-1723 DOI: 10.1016/j.aeue.2015.08.007.
2. *Mohapatra S.K., Sahoo P.K., Wu S-L.* Big data analytic architecture for intruder detection in heterogeneous wireless sensor networks // Journal of Network and Computer Applications. Vol. 66. 2016, - P 236-249 DOI: 10.1016/j.jnca.2016.03.004.
3. *Lim C., Kim K-J., Maglio P.P.* Smart cities with big data: Reference models, challenges, and considerations // Cities. Vol. 82. 2018, - P. 86-99 DOI: 10.1016/j.cities.2018.04.011.
4. *Zhao X., Wang N., Han R., Xie B., Yu Y., Li M., Ou J.* Urban infrastructure safety system based on mobile crowdsensing // International Journal of Disaster Risk Reduction. Vol. 27. 2018, - P. 427-438 DOI: 10.1016/j.ijdrr.2017.11.004.
5. *De La Torre Parra G., Rad P., Choo K-K. R.,* Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities // Journal of Network and Computer Applications. Vol. 135. 2019, - P. 32-46 DOI: 10.1016/j.jnca.2019.02.022.
6. *Rouf Y., Shtern M., Fokaefs M., Litoiu M.* A hierarchical architecture for distributed security control of large scale systems // ICSE-C '17 Proceedings of the 39th International Conference on Software Engineering Companion, Argentina, Buenos Aires, 20-28 May 2017, p.118-120
7. *Fink G.A., Edgar T.W., Rice T.R., MacDonald D.G., Crawford C.E.* Chapter 9 - Security and Privacy in Cyber-Physical Systems // Editor(s): Houbing Song, Danda B. Rawat, Sabina Jeschke, Christian Brecher, In Intelligent Data-Centric Systems. Cyber-Physical Systems. - Academic Press. 2017, - P. 129-141, DOI: 10.1016/B978-0-12-803801-7.00009-2.
8. *Knapp E. D., Langill J.T.* Chapter 12 - Security Monitoring of Industrial Control Systems // Editor(s): Eric D. Knapp, Joel Thomas Langill, Industrial Network Security (Second Edition). - Syngress. 2015, - P. 351-386 DOI:0.1016/B978-0-12-420114-9.00012-5
9. *Das S.K., Kant K., Zhang N.* Handbook on Securing Cyber-Physical Critical Infrastructure. - Morgan Kaufmann. 2012, DOI: 10.1016/C2011-0-04434-4.
10. *Pavlenko E., Zegzhda D.* Sustainability of cyber-physical systems in the context of targeted destructive influences // Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS. 2018, - P. 830-834 DOI: 10.1109/ICPHYS.2018.8390814
11. *Kotenko I., Saenko I., Branitskiy A.* Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018, Vol.6. 10 p. DOI: 10.1109/ACCESS.2018.2881998
12. *Chapman C.* Chapter 9 - Live traffic analytics using “Security Onion” // Editor(s): Chris Chapman, Network Performance and Security. – Syngress. 2016, - P. 259-294 DOI: 10.1016/B978-0-12-803584-9.00009-3.
13. *Lavrova D., Poltavtseva M., Shtyrkina, A.* Security analysis of cyber-physical systems network infrastructure // Proceedings - 2018 IEEE Industrial Cyber-Physical Systems, ICPS. 2018, - P. 818-823 DOI: 10.1109/ICPHYS.2018.8390812
14. *Habeeb R.A.A., Nasaruddin F., Gani A., Hashem I. A. T., Ahmed E., Imran M.* Real-time big data processing for anomaly detection: A Survey // International Journal of Information Management. Vol. 45. 2019, - P. 289-307 DOI: 10.1016/j.ijinfomgt.2018.08.006.
15. *Wang M., Yang S., Wu B.* Hierarchical Representation Learning based spatio-temporal data redundancy reduction // Neurocomputing. Vol. 173. Part 2. 2016, - P. 298-305, DOI: 10.1016/j.neucom.2015.02.099
16. *Ullah F., Babar M.A* Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review // Journal of Systems and Software. Vol. 151. 2019, - P. 81-118 DOI: 10.1016/j.jss.2019.01.051.
17. *Полтавцева М.А.* Проблемы обеспечения информационной безопасности в системах управления Большими данными // ВСПУ РАН, Москва, 17-20 июня 2019. - 5с.
18. *Akeel F. Y.* Secure data integration systems // Thesis for the degree of Doctor of Philosophy, 2017. https://eprints.soton.ac.uk/415716/1/Final_thesis.pdf

19. *Poltavtseva M. A.* Evolution of Data Management Systems and Their Security // 2019 International Conference on Engineering Technologies and Computer Science (EnT). – Moscow. Russia. 2019, P. 25-29 DOI: 10.1109/EnT.2019.00010
20. *Полтавцева М.А., Зегжда Д.П., Калинин М.О.* Модель угроз безопасности систем управления Большими данными // Проблемы информационной безопасности. Компьютерные системы. № 2. 2019. с. 16-28
21. *Alshboul Y., Wang Y., Nepali R. K.* Big Data LifeCycle:Threats and Security Model. // Proceedings of the 21st Americas Conference on Information Systems (AMCIS 2015). 2015, - P. 1 – 7
22. *Mehmood A., Natgunanathan I., Xiang Y., Hua G., Guo S.* Protection of Big Data Privacy // IEEE Access Vol. 4. 2016, - P.1821 – 1834 DOI: 10.1109/ACCESS.2016.2558446
23. *Perera C., Ranjan R., Wang L., Khan S.U., Zomaya A.Y.* Big data privacy in the internet of things era // IT Professional. Vol. 17. Is. 3. 2015, - P. 32–39
24. *Семенов Н.А., Полтавцев А.А.* Организация безопасности архитектур данных на базе облачных систем // Проблемы информационной безопасности. Компьютерные системы. № 4. 2018, - С. 33-43
25. *Delugach H.S., Hinke T.H.* AERIE: Database inference modeling and detection using conceptual graphs. // Pfeiffer H.D., Nagle T.E. (eds) Conceptual Structures: Theory and Implementation. Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence). - Springer, Berlin, Heidelberg. Vol 754. 1993, – P. 206-215.
26. *Полтавцева М.А.* Моделирование систем управления большими данными в информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. № 1. 2019б - С. 69-78
27. *Blanco C., García-Saiz D., Peral J., Maté A., Oliver A., Fernández-Medina E.* How the Conceptual Modelling Improves the Security on Document Databases. // Conceptual Modeling. ER 2018. Lecture Notes in Computer Science. - Springer, Cham. Vol 11157. 2018, - P.497-504 DOI: 10.1007/978-3-030-00847-5_36
28. *Ashwin K.T.K., Hong L., Johnson P.T., Xiaofeh H.* Content Sensitivity Based Access Control framework for Hadoop // Digital Communications and Networks Vol. 3, Is. 4. 2017, - P. 213-225 DOI: 10.1016/j.dcan.2017.07.007
29. *Полтавцева М.А.* Консистентный подход к построению защищенных систем обработки и хранения больших данных // Проблемы информационной безопасности. Компьютерные системы. № 2. 2019, - С. 29-44
30. *Han S., Gong T., Nixon M., Rotvold E., Lam K., Ramamritham K.* RT-DAP: A Real-Time Data Analytics Platform for Large-Scale Industrial Process Monitoring and Control // 2018 IEEE International Conference on Industrial Internet (ICII). - Seattle, WA. 2018, - P. 59-68. DOI: 10.1109/ICII.2018.00015
31. *Lavrova D.S.* An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. Vol. 50. Is 8. 2016, - P. 673-681 DOI: 10.3103/S0146411616080125
32. *Smith R., Middlebrook R., Turner R., Huggins R., Vardy S., Warne M.* Large-scale pesticide monitoring across Great Barrier Reef catchments – Paddock to Reef Integrated Monitoring, Modelling and Reporting Program // Marine Pollution Bulletin. Vol. 65. Is. 4–9. 2012, - P. 117-127, DOI: 10.1016/j.marpolbul.2011.08.010
33. *Adiba N., Li Y., Gupta A.* US20110153603A1 Time series storage for large-scale monitoring system // https://patents.google.com/patent/US20110153603A1/en
34. *Kroll S. A., Horwitz R.J., Keller D. H., Sweeney B.W., Jackson J.K., Perez L.B.* Large-scale protection and restoration programs aimed at protecting stream ecosystem integrity: the role of science-based goal-setting, monitoring, and data management // Freshwater Science. Vol 38. No. 1. 2019, - P. 23-39 DOI: 10.1086/701756
35. *Печенкин А.И., Полтавцева М.А., Лаврова Д.С.* An approach to data normalization in the internet of things for security analysis // Программные продукты и системы. 2016. № 2. - С. 83-88.
36. *Poltavtseva M.A.* Conceptual data modeling using aggregates to ensure large-scale distributed systems data security // https://www.researchgate.net/publication/333566799_Conceptual_data_modeling_using_aggregates_to_ensure_large-_scale_distributed_systems_data_security
37. *Jutla D. N., Bodorik P.* PAUSE: A privacy architecture for heterogeneous big data environments // 2015 IEEE International Conference on Big Data (Big Data). - Santa Clara, CA, USA. 2015, - P. 1919-1928 DOI: 10.1109/BigData.2015.7363969

38. *Haourani L.E., Elkalam A.A., Ouahman A.A.* Knowledge Based Access Control a model for security and privacy in the Big Data // Proceedings of the 3rd International Conference on Smart City Applications (SCA '18). - ACM, New York, USA. 2018, - P. 1-8 DOI: 10.1145/3286606.3286793
39. *Yang Y.J., Li Y.J., Deng R.H.* New paradigm of inference control with trusted computing // Data and Applications Security Xxi, Proceedings. Vol. 4602. 2007, -P. 243-258.
40. *Samarati P., Sweeney L.* Generalizing data to provide anonymity when disclosing information // Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems, Seattle, Washington, USA. – ACM. 1998, P. 188.
41. *Ciriani V., d. Vimercati S.D.C., Foresti S., Samarati P.* k -Anonymous Data Mining: A Survey // Privacy-Preserving Data Mining. Vol. 34. 2008, - P. 105-136.
42. *Popeea T., Constantinescu A., Gheorghe L., Tapus N.* Inference Detection and Database Security for a Business Environment // Intelligent Networking and Collaborative Systems (INCoS). 2012, - P. 612-617.
43. *Shatilov, K., Boiko, V., Krendelev, S., Anisutina, D., Sumaneev, A.* Solution for secure private data storage in a cloud // Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. 2014. – P. 885- 889